Специальная публикация NIST

NIST SP 800-160v1r1

Создание доверенных безопасных систем

Ron Ross
Mark Winstead
Michael McEvilley

Эта публикация доступна бесплатно по адресу:
Https://doi.org/10.6028/NIST.SP.800-160v1r1

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Специальная публикация NIST

NIST SP 800-160v1r1

Создание доверенных безопасных систем

Ron Ross
Отдел компьютерной безопасности
Лаборатория информационных технологий

Mark Winstead
Michael McEvilley
Корпорация MITRE

Эта публикация доступна бесплатно по адресу:
Https://doi.org/10.6028/NIST.SP.800-160v1r1

Ноябрь 2022

Министерство торговли США
Gina M. Raimondo, секретарь

Национальный институт стандартов и технологий
Laurie E. Locascio, директор NIST и заместитель министра торговли по стандартам и технологиям

Для адекватного описания экспериментальных процедур или концепций в настоящем документе могут быть указаны некоторые коммерческие организации, оборудование или материалы. Такое упоминание не означает рекомендации или одобрения со стороны Национального института стандартов и технологий (NIST), а также не означает, что данные организации, материалы или оборудование обязательно являются лучшими из имеющихся для данной цели.

В данной публикации могут содержаться ссылки на другие издания, разрабатываемые NIST в соответствии с возложенными на него уставными обязанностями. Информация, содержащаяся в данной публикации, включая концепции и методологии, может использоваться федеральными агентствами еще до завершения работы над сопутствующими публикациями. Таким образом, до завершения работы над каждой публикацией текущие требования, рекомендации и процедуры, если они существуют, остаются в силе. В целях планирования и перехода на новые стандарты федеральные агентства могут пожелать внимательно следить за разработкой этих новых публикаций NIST.

Организациям рекомендуется ознакомиться со всеми проектами публикаций в период публичных комментариев и направить свои замечания в NIST. Многие публикации NIST по кибербезопасности, кроме указанных выше, доступны по адресу https://csrc.nist.gov/publications.

Полномочия

Данная публикация была разработана NIST в соответствии с уставными обязанностями, возложенными на него в соответствии с Федеральным законом о модернизации информационной безопасности (FISMA) от 2014 г., 44 U.S.C. § 3551 и далее, Публичный закон (P.L.) 113-283. NIST отвечает за разработку стандартов и руководств по информационной безопасности, включая минимальные требования к федеральным информационным системам, однако такие стандарты и руководства не должны применяться к системам национальной безопасности без прямого одобрения соответствующих федеральных должностных лиц, осуществляющих политические полномочия в отношении таких систем. Данное руководство соответствует требованиям Циркуляра A-130 Управления по управлению и бюджету (OMB).

Ничто в данной публикации не должно восприниматься как противоречащее стандартам и руководствам, которые в соответствии с законом министр торговли сделал обязательными для федеральных агентств. Настоящее руководство также не должно рассматриваться как изменяющее или заменяющее существующие полномочия министра торговли, директора OMB или любого другого федерального должностного лица. Данная публикация может использоваться неправительственными организациями на добровольной основе и не является объектом авторского права в США. Однако NIST будет признателен за указание авторства.

Правила технической серии NIST

Copyright, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

История публикации

Утверждено редакционным советом NIST 2022-11-08
Заменяет NIST SP 800-160 Vol. 1 (Nov. 2016; обновлено 2018-03-21) https://doi.org/10.6028/NIST.SP.800-160v1

Как цитировать эту публикацию Технической серии NIST:

Ross R, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (Национальный институт стандартов и технологий, Гайтерсбург, MD), Специальная публикация (SP) NIST SP 800-160v1r1. https://doi.org/10.6028/NIST.SP.800-160v1r1

iDs ORCID автора
Рон Росс: 0000-0002-1099-9757

Контакты

security-engineering@nist.gov
Национальный институт стандартов и технологий
Отдел компьютерной безопасности, Лаборатория информационных технологий
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Все замечания подлежат опубликованию в соответствии с Законом о свободе информации (FOIA).

Аннотация

В данной публикации описывается основа для разработки принципов, концепций, мероприятий и задач по созданию доверенных безопасных систем. Такие принципы, концепции, мероприятия и задачи могут эффективно применяться в рамках усилий по созданию систем для формирования единого подхода к обеспечению безопасности любой системы, независимо от ее назначения, типа, масштаба, размера, сложности или стадии жизненного цикла. Целью данной публикации является развитие инженерии систем в области разработки доверенных систем в условиях противоборства (в общем случае - *инженерия безопасности систем*), а также создание основы для разработки образовательных и учебных программ, профессиональных сертификатов и других критериев оценки.

Ключевые слова

доверие; инженерные разработки; инженерные специальности; инженерия эксплуатации; внедрение; информационная безопасность; политика информационной безопасности; инспекция; интеграция; тестирование проникновения; потребности защиты; анализ требований; устойчивость; пересмотр; оценка рисков; управление рисками; обработка рисков; архитектура безопасности; проектирование безопасности; требования безопасности; спецификации; заинтересованные стороны; система систем; компонент системы; элемент системы; жизненный цикл системы; системы; создание систем (инженерия систем); создание (инженерия) безопасности систем; доверенность; подтверждение соответствия; проверка

Отчеты по технологиям компьютерных систем

Лаборатория информационных технологий (ITL) Национального института стандартов и технологий (NIST) содействует развитию экономики и общественного благосостояния США, обеспечивая техническое руководство инфраструктурой измерений и стандартов страны. ITL разрабатывает тесты, методы испытаний, справочные данные, примеры реализации концепций и технические анализы для содействия развитию и продуктивному использованию информационных технологий. В обязанности ITL входит разработка управленческих, административных, технических и физических стандартов и рекомендаций по экономически эффективной защите и обеспечению приватности информации, не связанной с национальной безопасностью, в федеральных информационных системах. Специальные публикации серии 800 информируют об исследованиях, рекомендациях и информационно-разъяснительной работе ITL в области безопасности информационных систем, а также о его совместной деятельности с промышленными, правительственными и научными организациями.

Уведомление о раскрытии патентной информации

УВЕДОМЛЕНИЕ: ITL обратилась к владельцам патентов, использование которых может потребоваться для выполнения указаний или требований данной публикации, с просьбой сообщить ITL о таких патентах. Однако владельцы патентов не обязаны отвечать на запросы ITL, и ITL не проводила патентный поиск, чтобы определить, какие патенты, если таковые имеются, могут быть применимы к данной публикации.

На дату публикации и после обращения ITL к компаниям с просьбой указать патентные формулы, использование которых может потребоваться для выполнения указаний или требований данной публикации, таких патентных формул не было указано.

ITL не утверждает и не подразумевает, что при использовании данной публикации не требуются лицензии во избежание нарушения патентных прав.

Отказ от ответственности

Настоящая публикация должна использоваться в качестве дополнения к **международному стандарту ISO/IEC/IEEE 15288** и другим поддерживающим его международным стандартам. Организациям, использующим данную публикацию, рекомендуется ознакомиться с соответствующими международными стандартами, чтобы понять контекст материалов, приведенных в приложениях G-K. Материалы из ISO/IEC/IEEE 15288, на которые даны ссылки в данной публикации, использованы с разрешения Института инженеров по электротехнике и электронике. Это указано следующим образом:

Перепечатано с разрешения IEEE, Copyright IEEE 2015, Все права защищены.

Перепечатанный материал был обновлен для отражения любых изменений в международном стандарте.

Список таблиц

Список иллюстраций

Предисловие

12 мая 2021 г. президент подписал указ "О повышении уровня кибербезопасности страны" [1]. В указе говорилось следующее:

> «Соединенные Штаты сталкиваются с постоянными и все более изощренными вредоносными кибер акциями, угрожающими безопасности и неприкосновенности частной жизни американского народа, государственного и частного секторов. Федеральное правительство должно совершенствовать свои усилия по выявлению, сдерживанию, защите, обнаружению и реагированию на эти действия и субъекты.»

Далее в Указе описывается целостный характер проблем кибербезопасности, стоящих перед страной, в которой вычислительные технологии встроены во все типы систем - от вычислительных систем общего назначения, обеспечивающих работу предприятий, до киберфизических систем, управляющих работой электростанций и обеспечивающих американское население электроэнергией. Федеральное правительство должно задействовать весь объем своих полномочий и ресурсов для защиты и обеспечения безопасности своих компьютерных систем, независимо от того, являются ли эти системы облачными, локальными или гибридными. В сферу защиты и безопасности должны входить как системы, обрабатывающие данные (т.е. информационные технологии [ИТ]), так и системы, запускающие механизмы, обеспечивающие нашу безопасность (т.е. операционные технологии [ОТ]).

В ответ на указ необходимо:

- Определить активы заинтересованных сторон и потребности в защите;
- Обеспечить защиту, соизмеримую со значимостью потери активов и коррелирующую с возможностями угроз и противника;
- Разработать сценарии и осуществить моделирование сложности систем для обеспечения строгой основы для рассмотрения, управления и устранения неопределенности, связанной с этой сложностью;
- Принять инженерный подход, основанный на принципах доверенного безопасного проектирования, и применять эти принципы на протяжении всего жизненного цикла систем.

Создание доверенных и безопасных систем не может происходить в вакууме, где есть отдельные элементы программного обеспечения, аппаратных средств, информационных технологий и человеческого фактора (например, разработчики, операторы, пользователи, злоумышленники). Скорее, для этого требуется междисциплинарный подход к защите, определение всех активов, где может произойти потеря, и понимание неблагоприятных факторов, включая то, как противники атакуют и компрометируют системы. Таким образом, в данной публикации рассматриваются инженерные действия, необходимые для разработки защищенных и живучих систем, включая компоненты, входящие в их состав, и сервисы, зависящие от этих систем. Цель состоит в том, чтобы рассматривать вопросы безопасности с точки зрения требований заинтересованных сторон и потребностей в защите, а также использовать установленные инженерные процессы для обеспечения того, чтобы эти требования и потребности удовлетворялись с надлежащей точностью и строгостью на протяжении всего жизненного цикла системы.

Создание доверенных и безопасных систем - это серьезная задача, требующая значительных инвестиций в требования, архитектуру и проектирование систем, компонентов, приложений и сетей. Доверенная система предоставляет убедительные доказательства того, что она соответствует предъявляемым к ней требованиям и обеспечивает защиту и эксплуатационные качества, необходимые заинтересованным сторонам. Внедрение дисциплинированного, структурированного и основанного на

стандартах набора действий и задач по инженерии безопасности систем является важной отправной точкой и принудительной функцией для инициирования необходимых изменений.

"Обеспечение удовлетворительных мер безопасности в компьютерной системе само по себе является проблемой проектирования системы. Для обеспечения комплексной безопасности требуется сочетание аппаратных средств, программного обеспечения, средств связи, физических, кадровых и административно-процессуальных мер безопасности. В частности, одних только программных средств защиты недостаточно."

"Меры безопасности для компьютерных систем" (The Ware Report), Целевая группа по компьютерной безопасности Совета по оборонной науке Rand Corporation, февраль 1970 г.

"Для доверия к предназначению необходимы системы, которые ведут себя предсказуемо и соразмерно".

General Michael Hayden
Бывший директор Агентства национальной безопасности (NSA) и Центрального разведывательного управления (ЦРУ), Сиракузский университет, октябрь 2009 года

"В прошлом считалось, что для подтверждения защищённости системы, достаточно обеспечить доверие в том, что процесс выявления опасностей является максимально полным и что каждая выявленная опасность имеет одну или несколько связанных с ней мер безопасности. Хотя исторически такой подход достаточно эффективно использовался для обеспечения контроля известных рисков, становится все более очевидным, что по мере усложнения систем и увеличения стоимости их проектирования, создания и эксплуатации требуется переход к более целостному подходу."

Национальное управление по аэронавтике и исследованию космического пространства (NASA) Руководство по безопасности систем, Предисловие, том 1, ноябрь 2011 г.

"Весь этот экономический бум в области кибербезопасности представляется в значительной степени следствием плохой инженерии."

Carl Landwehr
Сообщения Ассоциации вычислительной техники (ACM), февраль 2015 г.

"Кибербезопасность требует не только действий правительства. Защита нашей страны от злоумышленников требует от федерального правительства партнерства с частным сектором. Частный сектор должен адаптироваться к постоянно меняющейся среде угроз, обеспечивать создание и безопасную эксплуатацию своих продуктов, а также сотрудничать с федеральным правительством для создания более безопасного киберпространства... Постепенные улучшения не обеспечат нам необходимой безопасности; вместо этого федеральное правительство должно пойти на смелые изменения и значительные инвестиции, чтобы защитить жизненно важные институты, которые лежат в основе американского образа жизни."

Правительственный указ (EO) о повышении кибербезопасности страны, май 2021 г.

"Инженерия безопасности [систем] должна стать основой инженерии систем, а не просто специальной дисциплиной. Концепции безопасности должны быть основополагающими в инженерном образовании, а знания в области безопасности должны быть основополагающими в командах разработчиков. Основы безопасности должны быть четко поняты заинтересованными сторонами и эффективно оценены таким образом, чтобы учесть широкие цели с функциями и результатами безопасности."

Безопасность в будущем проектирования систем (FuSE), дорожная карта основополагающих концепций, Международный симпозиум INCOSE, июль 2021 г.

Признательность

Авторы с благодарностью признают и высоко оценивают значительный вклад отдельных лиц и организаций государственного и частного секторов, конструктивные замечания которых повысили общее качество, тщательность и полезность данной публикации. В частности, мы хотим поблагодарить Jeff Brewer, Ken Cureton, Jordan Denmark, Rick Dove, Holly Dunlap, Jim Foti, Michael Hankins, Daryl Hild, M. Lee, Tom Llanso, Jimmie McEver, Perri Nejib, Cory Ocker, Daniel Patrick Pereira, Victoria Pillitteri, Greg Ritter, Thom Schoeffling, Theresa Soloway, Nick Stegman, Gary Stoneburner, Gregory Touhill, Isabel Van Wyk, Adam Williams, Drew Wilson, Carol Woody, William Young, and Michael Zisa. Авторы также хотели бы выразить признательность членам Международного совета по проектированию систем (INCOSE), в том числе членам рабочих групп "Проектирование системной безопасности" и "Устойчивые системы", за многочисленные обсуждения содержания данного документа. Наконец, авторы выражают благодарность студентам, участвовавшим в учебных курсах INCOSE и MITRE Systems Security Engineering, чьи замечания и ценные идеи помогли направить и обосновать многие из предложенных в данной публикации изменений.

Исторический вклад

Авторы с благодарностью выражают признательность Джанет Кэрриер Орен, одному из первоначальных авторов Специальной публикации NIST 800-160, том 1. Авторы также хотели бы выразить признательность следующим организациям и частным лицам за их исторический вклад в подготовку данной публикации:

Организации: Агентство национальной безопасности; Военно-морская аспирантура; Управление закупок, технологий и логистики Министерства обороны; Управление науки и технологий Министерства национальной безопасности, отдел кибербезопасности; Международный совет по проетированию систем; ВВС США; Технологический институт ВВС; Northrop Grumman Corporation; The MITRE Corporation; The Boeing Company; Lockheed Martin Corporation.

Личности: Beth Abramowitz, Max Allway, Kristen Baldwin, Dawn Beyer, Debora Bodeau, Paul Clark, Keesha Crosby, Judith Dahmann, Kelley Dempsey, Holly Dunlap, Jennifer Fabius, Daniel Faigin, Jeanne Firey, Robin Gandhi, Rich Graubart, Kevin Greene, Richard Hale, Daryl Hild, Kesha Hill, Danny Holtzman, Cynthia Irvine, Brett Johnson, Ken Kepchar, Stephen Khou, Alvi Lim, Logan Mailloux, Dennis Mangsen, Doug Maughn, Rosalie McQuaid, Joseph Merkling, John Miller, Thuy Nguyen, Perri Nejib, Lisa Nordman, Dorian Pappas, Paul Popick, Roger Schell, Thom Schoeffling, Matthew Scholl, Peter Sell, Gary Stoneburner, Glenda Turner, Edward Yakabovicz, and William Young.

И наконец, авторы с уважением отмечают основополагающую работу в области компьютерной безопасности, начатую в 1960-х годах. Видение, понимание и самоотверженные усилия первых пионеров в области компьютерной безопасности послужили философской и технической основой для принципов, концепций, методов и практических приемов обеспечения безопасности, используемых в данной публикации для решения критически важной проблемы создания доверенных безопасных систем.

ВЗГЛЯД НА БЕЗОПАСНОСТЬ С ПРАВИЛЬНОЙ ТОЧКИ ЗРЕНИЯ

"В течение первых нескольких десятилетий в кибербезопасности, как растущей дисциплины, доминировала разработка продуктов для решения некоторых аспектов проблемы. Системы становятся все более сложными и взаимосвязанными, создавая еще больше возможностей для атак, что, в свою очередь, создает еще больше возможностей для создания защитных продуктов, которые принесут некоторую ценность в обнаружение или предотвращение того или иного аспекта атак. В конечном счете, это превращается в игру в "крота", в которой из одной из множества нор появляется симулированный крот, и задача состоит в том, чтобы уничтожить крота до того, как он вернется в свою нору. Кроты представляют собой новые атаки, а дыры - огромное количество потенциальных уязвимостей, как известных, так и еще не обнаруженных.

В основе инженерии, как дисциплины, лежит наука. Иногда инженерия опережает науку, как, например, при строительстве мостов, когда основы материаловедения были недостаточно хорошо изучены. Было построено много мостов, многие из них рухнули, некоторые остались, а конструкции тех, что остались, были скопированы. В конечном итоге, чтобы инженерия продвинулась дальше, наука должна догнать инженерию. Наука, лежащая в основе инженерии кибербезопасности [и в целом безопасности], сложна и трудна. С другой стороны, сейчас нет времени, чтобы начать работу, потому что она актуальна и важна для будущего...."

-- O. Sami Saydjari
Инженерия доверенных систем, McGraw-Hill, август 2018 г.

ЗНАЧЕНИЕ НАУКИ И ИНЖЕНЕРИИ

Пересекая мост, мы вполне обоснованно ожидаем, что он не рухнет и мы доедем в пункт назначения без происшествий. При строительстве мостов основное внимание уделяется равновесию, статическим и динамическим нагрузкам, вибрациям и резонансу. Физика в сочетании с принципами и концепциями гражданского строительства позволяет получить продукт, который мы считаем надежным, что дает нам уверенность в том, что мост пригоден для использования по назначению.

Для разработчиков систем также существуют фундаментальные принципы и концепции, которые можно найти в математике, информатике, компьютерной и электротехнике, инженерии систем и программной инженерии, которые при правильном использовании обеспечивают необходимый уровень доверия. Доверенные безопасные системы достигаются путем значительных и существенных инвестиций в укрепление базовых систем и компонентов систем с помощью междисциплинарных усилий в области инженерии систем, руководствуясь четко определенными требованиями безопасности, безопасными архитектурами и проектами. Такие усилия уже давно доказали, что они позволяют находить разумные инженерные решения сложных и трудных проблем безопасности систем. Только в этих условиях можно создать системы, которые будут обладать достаточной безопасностью и уровнем доверенности, достаточным для целей, для которых они были созданы

"Ученые изучают мир таким, какой он есть, инженеры создают мир, которого никогда не было."

Theodore von Kármán
Лауреат Национальной медали за науку 1962 г.

КРИТИЧЕСКОЕ ПОВЕДЕНИЕ СИСТЕМ В БУДУЩЕМ

"Чтобы обеспечить поведение системы, проектант систем должен определить группу подсистем и то, как именно эти подсистемы должны взаимодействовать друг с другом. Именно подсистемы и их взаимодействия формируют поведение на уровне системы. Многие из нас считают, что автомобиль, который может проходить повороты под углом 60 градусов на скорости 200 миль в час, обладает ценным поведением системы. А можем ли мы с такой же уверенностью отнести безопасность, приватность, доверие и доступность к поведению системы? Это поведение требует такого же тщательного проектирования и анализа на уровне системы для достижения оптимальных решений, таких как показатели поведения системы, о котором я говорил выше. И в этом есть очевидная необходимость - инвесторы хотят, чтобы система сохраняла их данные в тайне, была защищённой, доверенной, чтобы их меры не были скомпрометированы киберугрозой, и была высоко доступной.

Если мы, проектанты системы, готовы признать эти модели поведения как модели поведения системы, то мы несем ответственность за их реализацию как часть нашей работы. Если же мы предпочитаем рассматривать эти модели поведения как атрибуты частей нашей системы, но не системы в целом, то, скорее всего, мы будем считать это работой для "проектантов-специалистов". Я обратился к прошлому поведению нашего сообщества проектантов систем. Я обнаружил примеры того, как проектанты систем ставили перед нашими коллегами-"проектантами-специалистами" такие задачи в процессе распределения требований. Думаю, мы ошиблись. Наши "специальные" коллеги, скорее всего, примут эти выделенные требования и сосредоточатся на создании защищённых, приватных, доверенных и доступных частей системы, а не на обеспечении защищённого, приватного, доверенного и доступного поведения системы. Это правда, что вы можете построить более защищённую систему, создавая защищённые части. Однако вы не можете построить действительно защищённую систему, не имея защищённых частей, взаимодействующих друг с другом защищённым способом. То же самое можно сказать и для других вариантов поведения системы (приватного, доверенного, доступного и т. д.) ".

-- **John A. Thomas**
Президент INCOSE
INCOSE Insight, июль 2013 года.

1. Введение

Современные системы[1] являются сложными по своей природе. Рост размера, числа и типов компонентов и технологий[2], составляющих эти системы, а также системных зависимостей приводит к различным последствиям - от неудобств до катастрофических потерь из-за неблагоприятных условий[3] в среде применения. Управление сложностью доверенных безопасных систем требует достижения соответствующего уровня уверенности в целесообразности, правильности концепции, философии и проекте системы для получения только запланированного поведения и результатов. Это закладывает основу для удовлетворения потребностей заинтересованных сторон в защите и обеспечении безопасности с достаточной уверенностью в том, что система функционирует только так, как предполагалось, подвергаясь различным неблагоприятным воздействиям, и реалистично связывает эти ожидания с ограничениями и неопределенностью. Невозможность решения проблем сложности и безопасности приведет к тому, что нация будет подвержена потенциально серьезным, тяжелым или катастрофическим последствиям.

Термин "*безопасность*" используется в данной публикации для обозначения независимости от условий, которые могут привести к потере активов с неприемлемыми последствиями.[4] Заинтересованные стороны должны определить сферу безопасности с точки зрения активов, к которым применяется безопасность, и последствий, по которым оценивается безопасность.[5] *Инженерия систем* обеспечивает основу для последовательного и структурированного подхода к созданию доверенных безопасных систем. Как субдисциплина инженерии систем, *инженерия безопасности систем* рассматривает вопросы, связанные с обеспечением безопасности и направленные на достижение безопасных результатов. Усилия по обеспечению безопасности осуществляются на соответствующем уровне точности и строгости, необходимом для достижения целей достижения *доверенности* и доверия.

> Питер Нойман описал в [2] понятие доверенности следующим образом:
> "Под доверенностью мы подразумеваем простое доверие к выполнению любых критических требований, которые могут потребоваться для конкретного компонента, подсистемы, системы, сети, приложения, миссии, предприятия или других сущностей. Требования к доверенности обычно включают (например) такие характеристики, как безопасность, надежность, результативность и живучесть в условиях широкого спектра потенциальных неблагоприятных факторов. Показатели доверенности являются значимыми лишь в той мере, в какой a) требования являются достаточно полными и четко определенными и b) могут быть точно оценены. "

---

[1] *Система* - это совокупность частей или элементов, обладающих таким поведением или значимостью, которые не свойственны отдельным компонентам [3]. К элементам, составляющим систему, относятся аппаратные средства, программное обеспечение, данные, люди, процессы, процедуры, объекты, материалы и сущности естественного происхождения [4].

[2] Термин "*технология*" в данной публикации используется в самом широком контексте и включает в себя вычислительные, коммуникационные и информационные технологии, а также любые механические, гидравлические, пневматические или структурные компоненты систем, содержащих или использующих такие технологии. Такой взгляд на технологию обеспечивает более широкое признание цифровой, вычислительной и электронной машинной основы современных сложных систем и растущую важность гарантированной доверенности этой основы для обеспечения функциональных возможностей системы и взаимодействия с ее физическими элементами - машинами и людьми.

[3] Термин "*неблагоприятные условия*" относится к тем условиям, которые могут привести к потере активов (например, угрозы, атаки, уязвимости, опасности, сбои и воздействия).

[4] Формулировка, используемая в данном определении безопасности, является намеренной. Ross Anderson отметил в [5], что "теперь, когда всё приобретает возможности подключения, невозможно обеспечить защищённость без безопасности, и эти экосистемы появляются". Исходя из этого наблюдения, определение безопасности было выбрано для достижения соответствия с преобладающим определением защищённости.

[5] Адаптирован с [6].

Инженерия безопасности систем предоставляет дополнительные возможности, которые расширяют концепцию доверенности и позволяют создавать доверенные безопасные системы. Доверенность - это не только очевидное соответствие набору требований. Требования также должны быть полными, непротиворечивыми и корректными. С точки зрения безопасности, доверенная система отвечает набору четко определенных требований, включая требования безопасности. С помощью свидетельств и экспертных оценок доверенные безопасные системы могут ограничивать и предотвращать воздействие современных неблагоприятных факторов. Такие угрозы могут иметь как злонамеренную, так и не злонамеренную форму и исходить из различных источников, включая физические и электронные. Неблагоприятные факторы могут включать в себя атаки со стороны решительных и умелых противников, человеческие ошибки бездействия и неверных действий, аварии и инциденты, неисправности и отказы компонентов, злоупотребления и неправильное использование, а также природные и антропогенные катастрофы.

> "Безопасность встроена в системы. Вместо двух проектных групп, разрабатывающих две системы, одна из которых предназначена для защиты другой, инженерия систем определяет и проектирует единую систему с безопасностью, встроенной в систему и ее компоненты ".
> - Цель обеспечения безопасности в будущем инженерии систем [7]

1.1. Назначение и применимость

Эта публикация предназначена для:

- Обеспечения основы для создания дисциплины по инженерии безопасности систем как части инженерии систем с точки зрения ее принципов, концепций, действий и задач;
- Формирования единого подхода к обеспечению безопасности любой системы, независимо от ее назначения, типа, масштаба, размера, сложности и стадии жизненного цикла;
- Демонстрации того, как выбранные принципы, концепции, действия и задачи безопасности систем могут быть эффективно применены в работах по инженерии систем;
- Продвижения инженерии безопасности систем как дисциплины, которая может быть применена и изучена;
- Основы разработки образовательных и учебных программ, включая индивидуальные сертификации и другие критерии профессиональной оценки.

Соображения, изложенные в данной публикации, применимы ко всем федеральным системам, кроме тех, которые отнесены к системам национальной безопасности в соответствии с секцией 3542 раздела 44 U.S.C.[6] Эти соображения получили широкое развитие с технической точки зрения и с точки зрения технического управления, с тем чтобы дополнить аналогичные соображения для систем национальной безопасности, и могут использоваться для таких систем с одобрения федеральных должностных лиц, которые осуществляют политические полномочия в отношении таких систем. Правительствам штатов, местных общин и племен, а также сущностям частного сектора рекомендуется рассмотреть возможность использования материалов, содержащихся в настоящей публикации, в соответствующих случаях.

[6] Повышение доверенности систем является важной задачей, требующей значительных инвестиций в требования, архитектуру, проектирование и разработку систем, компонентов систем, приложений и сетей. Политика в [8] требует от федеральных ведомств внедрения принципов, концепций, методов и процессов жизненного цикла системной безопасности, изложенных в данной публикации, для всех дорогостоящих активов.

Утверждение о применимости не означает ограничения технического и управленческого применения этих соображений. То есть принципы, концепции и методы инженерии безопасности, описанные в данной публикации, являются частью подхода к проектированию доверенной безопасности, описанного в Приложении D, и могут применяться в любом из следующих случаев:

- **Разработка новой возможности или системы**
  Работы инженерии включают в себя такие виды действий, как поиск концепции, предварительные или прикладные исследования для уточнения концепции и/или целесообразности применения технологий, используемых в новой системе, а также оценку альтернативных решений. Эти работы начинаются на этапах разработки концепции и жизненного цикла системы.

- **Изменение существующей возможности или системы**
  - *Реактивные модификации систем, находящихся в эксплуатации:* Работы инженерии, проводимые в ответ на неблагоприятные обстоятельства, которые снижают или не позволяют системе достичь проектных целей. Эти работы могут проводиться на этапах производства, использования или поддержки жизненного цикла системы и могут осуществляться как одновременно с повседневной эксплуатацией системы, так и независимо от нее.
  - *Плановые модернизации систем, находящихся в эксплуатации, с продолжением поддержки повседневной деятельность:* Плановая модернизация системы может расширять возможности существующей системы, предоставлять новые возможности или представлять собой технологическое обновление существующих возможностей. Эти работы проводятся на этапах производства, использования или поддержки жизненного цикла системы.
  - *Плановые обновления систем, находящихся в эксплуатации, которые приводят к появлению новых систем:* Работы инженерии выполняются как при разработке новой системы с жизненным циклом, отличным от жизненного цикла системы, находящейся в эксплуатации. Модернизация выполняется в среде разработки, независимой от системы, находящейся в эксплуатации.

- **Развитие существующих возможностей или систем**
  Работы инженерии включают перенос или адаптацию системы или ее реализации из одной среды эксплуатации или набора условий эксплуатации в другую среду эксплуатации или набор условий эксплуатации.[7]

- **Вывод из эксплуатации существующей возможности или системы**
  Работы инженерии по выводу из эксплуатации системных функций, сервисов, элементов или всей системы, которые могут включать в себя передачу системных функций и сервисов в другую систему. Эти работы проводятся на стадии вывода из эксплуатации жизненного цикла системы и могут осуществляться в процессе поддержания текущей эксплуатации.

- **Разработка специализированной, специфичной для конкретной области, или специального назначения возможности или системы**
  - *Специализированная система безопасности, или система, предназначенная для обеспечения безопасности:* В результате работ инженерии создается система, которая удовлетворяет потребности, связанные с обеспечением безопасности, или выполняет задачи, связанные с обеспечением безопасности, и представляет собой отдельную систему, которая может осуществлять мониторинг других систем или взаимодействовать с ними. К таким системам могут

[7] В настоящее время растет потребность в повторном использовании или использовании успешных результатов внедрения систем в средах эксплуатации, отличающихся от тех, в которых они были изначально спроектированы и разработаны. Такое повторное использование или повторная реализация систем в других средах эксплуатации является более эффективным и дает потенциальные преимущества в обеспечении максимальной совместимости между различными системами. Следует отметить, что повторное использование может нарушить предположения, использованные для определения доверенности системы или ее компонента.

относиться системы наблюдения, физической защиты, мониторинга, а также системы предоставления услуг безопасности.

- *Высоконадежная специализированная система:* В результате работ инженерии создается система, удовлетворяющая потребности в управлении автотранспортом в реальном времени, промышленными и коммунальными процессами, вооружением, атомными электростанциями и другими специальными задачами. Такие системы могут включать в себя несколько рабочих состояний или режимов с различными формами ручного, полуручного, автоматического или автономного режимов. Такие системы обладают высокими детерминированными свойствами, строгими временными ограничениями, функциональными блокировками и тяжелыми или катастрофическими последствиями отказов.

- **Разработка системы систем**
  Работы инженерии выполняются над набором составляющих систем, каждая из которых имеет своих заинтересованных лиц, основное назначение и запланированное развитие. Объединение составляющих систем в систему систем, как отмечено в [9], позволяет получить возможности, которые в противном случае было бы трудно или нецелесообразно реализовать. Эти усилия могут быть предприняты в рамках различных систем - от относительно неформальной, незапланированной концепции системы систем и ее эволюции, возникающей со временем благодаря добровольному участию, до более формального исполнения, причем наиболее формальной является концепция системы систем, которая направляется, структурируется, планируется и достигается посредством централизованных проектных усилий. Любое результирующее эмерджентное поведение часто создает возможности и дополнительные проблемы для разработки системной безопасности.

1.2. Целевая аудитория

Эта публикация предназначена для разработчиков систем, разработчиков безопасности и других специалистов. Термин "разработчик безопасности систем" используется для обозначения разработчиков систем и специалистов по безопасности, которые применяют концепции и принципы и выполняют действия и задачи, описанные в данной публикации.[8] Эта публикация может также использоваться специалистами, выполняющими другие действия или задачи жизненного цикла системы, включая:

- Лиц, ответственных за управление безопасностью, управление рисками и надзор;
- Лиц, ответственных за проверку, подтверждение соответствия, тестирование, оценку, аудит, анализ, инспекцию и мониторинг безопасности;
- Лиц, ответственных за закупки, бюджетирование и управление проектами;
- Лиц, ответственных за эксплуатацию, техническое обслуживание, обеспечение, логистику и поддержку;
- Поставщиков продуктов, систем и услуг, связанных с технологиями;
- Преподавателей учебных заведений, предлагающих программы по проектированию систем, проектированию компьютеров, информатике, проектированию программного обеспечения и компьютерной безопасности.

[8] Действия и задачи по разработке безопасности систем могут применяться к механизму, компоненту, элементу системы, системе, системе систем, процессам или организациям. Независимо от размера или сложности сущности, для создания доверенных систем, удовлетворяющих потребностям и интересам заинтересованных сторон в области защиты, необходима междисциплинарная команда системных разработчиков. Эти процессы должны быть адаптированы для повышения эффективности.

1.3. Как использовать эту публикацию

Данная публикация предназначена для использования в качестве справочного и образовательного ресурса для разработчиков систем, специалистов инженерных специальностей, архитекторов, проектировщиков и всех лиц, участвующих в разработке доверенных безопасных систем и компонентов систем. Предполагалось, что он должен быть гибким в применении для удовлетворения разнообразных потребностей организаций. Не предполагается, что все технические материалы, приведенные в данной публикации, будут использоваться в рамках разработки систем. Напротив, концепции и принципы проектирования доверенной безопасности, приведенные в приложениях D-F, а также процессы жизненного цикла систем и связанные с безопасностью действия и задачи, приведенные в приложениях G-K, могут применяться организациями выборочно, полагаясь на опыт и знания проектных команд, которые определят, что является правильным для их целей. Применение содержания этой публикации позволяет достичь результатов в области безопасности, соответствующих взглядам инженерии систем на процессы жизненного цикла систем.

Процессы жизненного цикла системы, описанные в данной публикации, позволяют использовать преимущества любой методологии разработки систем или программного обеспечения. Эти процессы в равной степени применимы к водопадному, спиральному, DevOps, гибкому и другим подходам. Процессы могут применяться рекурсивно, итеративно, одновременно, последовательно или параллельно и к любой системе независимо от ее размера, сложности, назначения, области, среды эксплуатации или особого характера. Полный объем применения материалов данной публикации определяется потребностями заинтересованных сторон в необходимых возможностях, потребностями в защите и проблемами, при этом особое внимание уделяется соображениям стоимости, сроков и результативности.

1.4. Организация данной публикации

Остальная часть этой публикации организована следующим образом:

- В главе 2 представлен обзор инженерии систем и основных концепций, связанных с доверенными безопасными системами. Сюда входят фундаментальные понятия, которые касаются структуры и типов систем, основ инженерии систем, а также концепций доверия и доверенности систем и компонентов систем.
- Глава 3 описывает основные концепции безопасности систем и подход к созданию доверенных безопасных систем. Сюда входят понятия безопасности и безопасности систем, природа и характер систем, понятия активов и потери активов, рассуждения о потере активов, определение потребностей в защите, точки зрения на безопасность систем, демонстрация безопасности систем и введение в проектирование безопасности систем.
- Глава 4 содержит основы инженерии безопасности систем, которые включают контекст проблемы, контекст решения и контекст доверенности.

В следующих разделах представлена дополнительная информация для поддержки создания доверенных безопасных систем:

- Ссылки
- Приложение A: Глоссарий
- Приложение B: Акронимы
- Приложение C: Политика и требования в области безопасности

- Приложение D: Проектирование доверенной безопасности
- Приложение E: Принципы проектирования доверенной безопасности
- Приложение F: Доверенность и доверие
- Приложение G: Обзор процессов жизненного цикла систем
- Приложение H: Технические процессы
- Приложение I: Процессы технического управления
- Приложение J: Организационные процессы реализации проектов
- Приложение K: Процессы согласования
- Приложение L: Журнал регистрации изменений

ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ РЕШЕНИЯ

Эффективность любой проектной дисциплины требует сначала глубокого понимания проблемы и рассмотрения всех возможных решений, прежде чем приступать к решению выявленной проблемы. Для достижения максимальной эффективности в разработке безопасности систем, требования к защите от потери активов должны определяться деятельностью, предназначением и всеми другими заинтересованными сторонами. Требования безопасности определяются и управляются как четко определенный набор требований к разработке и не могут рассматриваться независимо или постфактум.

В контексте разработки системной безопасности термин "*защита*" имеет широкую область и в первую очередь ориентирован на понятие активов и потерю активов, приводящие к неприемлемым последствиям. Возможности защиты, предоставляемые системой, выходят за рамки предотвращения и направлены на контроль событий, условий и последствий, которые представляют собой потерю активов. Это достигается в виде конкретных возможностей и ограничений на архитектуру, проектирование, функционирование, реализацию, создание, выбор технологий, методов и инструментов системы и должно быть "заложено" как часть процесса жизненного цикла системы.

Понимание потребностей заинтересованных сторон защите активов (включая активы, которыми они владеют, и активы, которыми они не владеют, но должны защищать) и выражение этих потребностей посредством набора четко определенных требований безопасности - это инвестиции в предназначение организации и успех деятельности в современную эпоху глобальной торговли, мощных вычислительных систем и сетевого взаимодействия.

2. Обзор инженерии систем

В этой главе представлены концепции систем, инженерии систем, доверия и доверенности, которые обеспечивают основу для создания доверенных безопасных систем.

2.1. Понятия систем

Многие понятия систем важны для обоснования создания доверенных безопасных систем. К ним относятся: что такое система, структура системы, категории систем и концепция системы систем.

2.1.1. Системы и структура систем

Система[9] это совокупность частей или элементов, которые вместе демонстрируют такое поведение или значение, которое не свойственно отдельным компонентам. Свойства системы (т.е. атрибуты, качества или характеристики) определяются частями или элементами системы и их индивидуальными свойствами, а также отношениями и взаимодействиями между частями или элементами, системой и ее средой [3]. Создаваемая система разрабатывается или адаптируется для взаимодействия с предполагаемой оперативной средой для достижения одной или нескольких намеченных целей при соблюдении соответствующих ограничений [3]. На Рис.1 показана базовая структура системы, включая ее составные элементы.[10] [11]

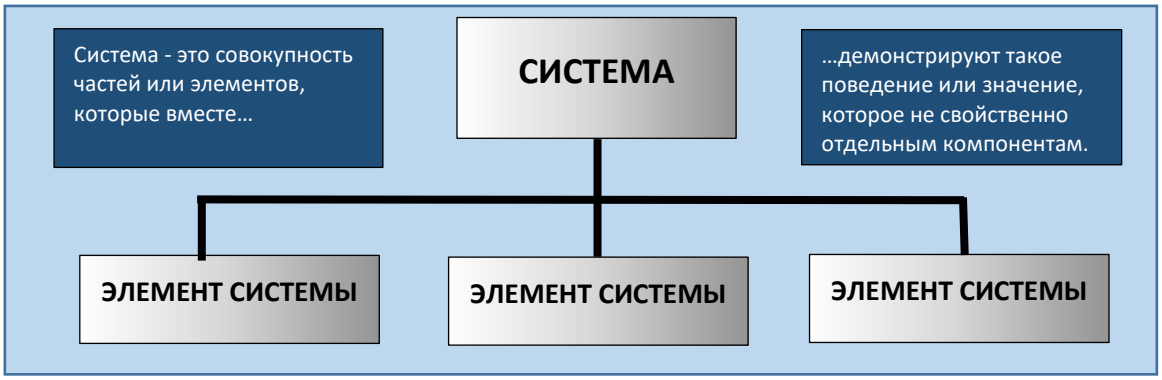

Рисунок 1. Взаимосвязь между основной системой и элементами системы

Назначение системы заключается в предоставлении одной или нескольких возможностей. Эти возможности могут прямо или косвенно взаимодействовать, управлять или мониторить физические, механические, гидравлические или пневматические устройства, другие системы или возможности, а также могут обеспечивать возможность создания, доступа, манипулирования, передачи, хранения или обмена ресурсами, такими как данные и информация.

[9] Примерами систем являются информационные системы, системы связи, финансовые системы, производственные системы, транспортные системы, логистические системы, медицинские системы, системы вооружения, механические системы, космические системы, промышленные системы управления (ПСУ), оптические системы или электрические системы. Системы могут быть физическими или концептуальными, использовать информационные технологии (IT) или операционные технологии (OT), включать людей, быть киберфизическими и использовать Интернет вещей (IoT) или другие технологии.

[10] Элементом системы может быть дискретный компонент, продукт, сервис, подсистема, система, организация, человек, инфраструктура или предприятие. Элементы системы реализуются аппаратным, программным и микропрограммным обеспечением, выполняющим операции с информацией или данными; физическими структурами, устройствами и компонентами в среде функционирования; а также людьми, процессами и процедурами для эксплуатации, обеспечения и поддержки этих элементов.

[11] Системы с небольшим количеством активных функций или без них (например, физическая инфраструктура) также могут обладать гарантированной доверенностью. Например, в системе межгосударственных автомагистралей используются барьеры безопасности, такие как "стены Джерси" (элемент системы), которые способствуют повышению доверенности транспортной системы.

Рис.2 представляет собой общую иерархическую модель для представления системы. Не все системы, такие как сети, имеют иерархическую сущность. Не иерархические системы имеют модели, которые могут более точно отражать взаимосвязи их составляющих элементов. Системный элемент сам по себе может считаться системой (т.е. состоять из других системных элементов). Реализация системы интереса включает рекурсивное разрешение ее структуры до положения, где могут быть реализованы понятные и управляемые элементы системы (т.е. разработаны, куплены или повторно использованы) и последующую интеграцию этих элементов в систему.

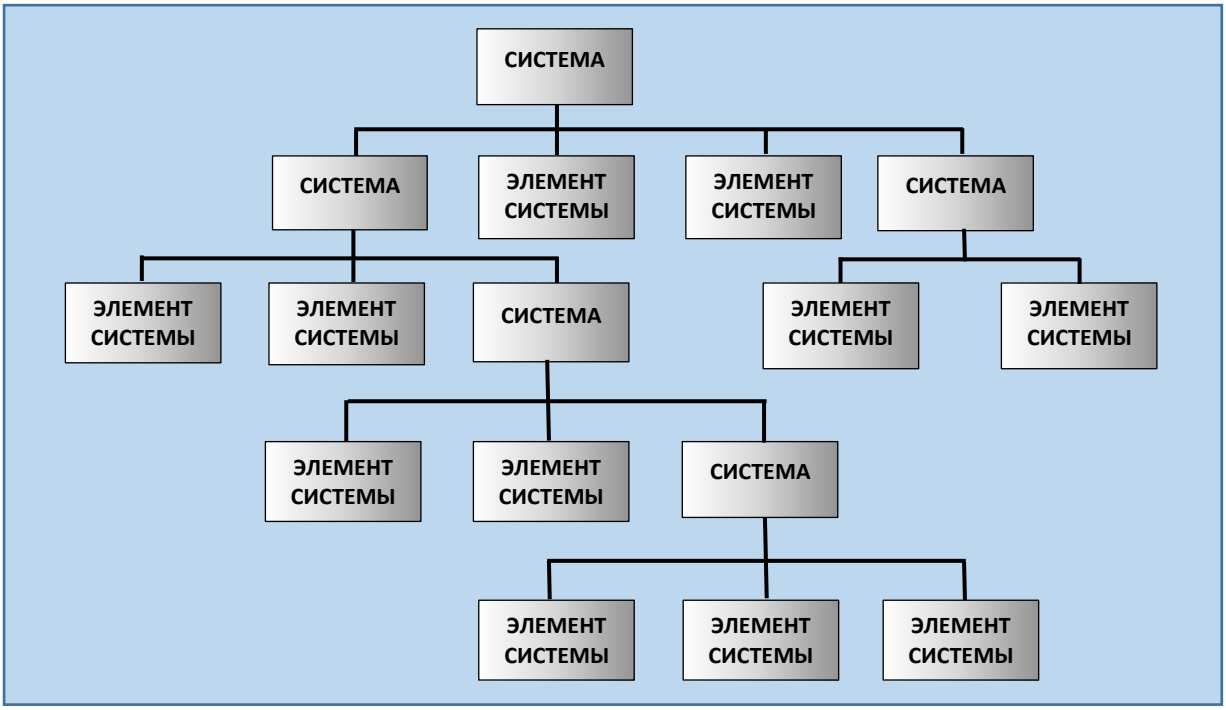

Рис. 2. Модель системы и ее элементов

Система систем - это система, взаимодействующие элементы которой сами являются системами. Она предоставляет уникальные возможности, которые не могут обеспечить входящие в нее системы самостоятельно. Система систем может включать межсистемную инфраструктуру, средства и процессы, необходимые для интеграции или взаимодействия составляющих ее систем [10].

2.1.2. Взаимодействие, обеспечение и взаимодействие систем

Взаимосвязанные системы - это системы, которые взаимодействуют с интересующей нас системой. Интерфейсные системы имеют интерфейс для обмена данными, энергией или другими ресурсами с интересующей нас системой. Взаимосвязанная система обменивается ресурсами с интересующей нас системой на одной или нескольких стадиях жизненного цикла системы, например, система, которая взаимодействует в целях сопровождения, или система, используемая для разработки интересующей нас системы. Отношения с взаимосвязанными системами могут быть либо двунаправленными, либо однонаправленными. Взаимосвязанные системы имеют две специфические подгруппы: обеспечивающие системы и взаимодействующие системы.

- *Обеспечивающие системы* предоставляют основные сервисы, необходимые для создания и поддержания интересующей нас системы. Примеры обеспечивающих систем включают среды разработки программного обеспечения, производственные системы, системы обучения и системы технического обслуживания.

- *Взаимодействующие системы* взаимодействуют с интересующей нас системой с целью совместного выполнения функции.

Рис.3 иллюстрирует взаимосвязь между интересующей нас системой и ее взаимосвязанными системами как в операционной, так и в нерабочей (внешней) среде.

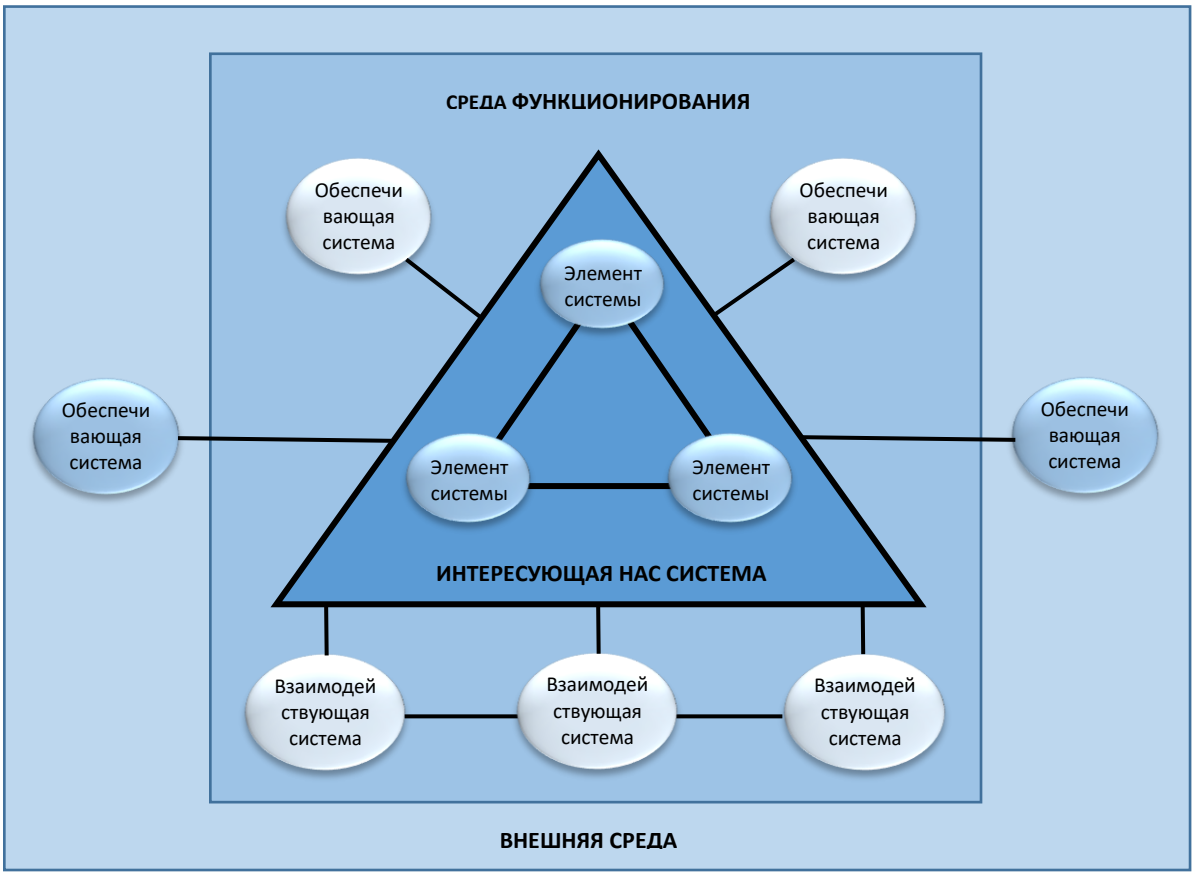

Рис. 3. Интересующая нас система и взаимодействующие системы

2.2. Основы инженерии систем

Инженерия систем[12] - это трансдисциплинарный и интегративный подход к обеспечению успешной реализации, использования и вывода из эксплуатации разработанных систем. Он использует системные принципы и концепции, а также научные, технологические и управленческие методы для создания таких систем [12]. Инженерия систем является системно-целостной по своей природе, при которой вклад различных инженерных и специальных дисциплин оценивается и балансируется для создания целостного потенциала системы. Инженерия систем применяет системологию и системное мышление[13] для удовлетворения часто противоречивых потребностей и приоритетов заинтересованных сторон в рамках ограничений по стоимости, срокам, результативности и эффективности. Цель состоит в ограничении неопределенности и тем самым управлении рисками. Инженерия систем ориентирована

[12] Как отмечается в [11], трансдисциплинарные подходы выходят "за рамки дисциплин по поиску и использованию связей для решения сложных проблем. Трансдисциплинарное мышление поощряет мыслить в терминах новых отношений между традиционно различными дисциплинами и фокусироваться на новых концепциях, которые могут возникнуть из такого мышления".

[13] Системология - междисциплинарная область, изучающая сложные системы в природе, обществе и науке. Она направлен на разработку междисциплинарных основ, которые применимы в различных областях, таких как социальные науки, инженерия, биология и медицина. Системное мышление - это дисциплина изучающая целостности, взаимосвязи и закономерности [13].

на результат и использует проектные процессы для реализации системы, эффективно управляя сложностью и выступая в качестве основного интегрирующего механизма для технической, управленческой и вспомогательной деятельности, связанной с проектированием. Наконец, инженерия систем ориентирована на данные и аналитику, чтобы гарантировать, что все решения и заключения принимались на основе данных, полученных в результате анализа, проведенного с соответствующим уровнем достоверности и строгости.

Работы по созданию систем являются сложными, специфичными для системы и зависят от контекста[14], что требует тесной координации между *проектной командой* и заинтересованными сторонами на всех стадиях жизненного цикла[15] системы. Хотя инженерия систем обычно рассматривается с точки зрения её роли в процессе разработки в рамках приобретения потенциала, усилия и обязанности по инженерии систем не заканчиваются после завершения разработки системы и передачи в среду эксплуатации для повседневного использования. Заинтересованные стороны, ответственные за использование, поддержку и вывод системы из эксплуатации, постоянно предоставляют данные проектной команде. Эти данные отражают опыт, проблемы и вопросы, связанные с эксплуатацией, поддержкой и обеспечением функционирования системы. Заинтересованные стороны также консультируют проектную команду по вопросам усовершенствования и улучшения системы. Кроме того, объектовые инженеры обеспечивают на местах инженерную поддержку организаций, занимающихся эксплуатацией, обслуживанием и обеспечением систем на протяжении всего жизненного цикла.

Существует множество дополнительных источников, в которых более подробно рассматриваются вопросы инженерии систем.[16] Подобные обсуждения выходят за рамки данной публикации.

2.3. Доверие и доверенность

Понятия *доверия и доверенности* являются основополагающими для создания доверенных безопасных систем, при принятии решений о предоставлении доверия, а также при определении степени доверия на основе продемонстрированной доверенности. Доверие - это вера в то, что сущность отвечает определенным ожиданиям и на нее можно положиться. Термины "*вера*" и "*можно*" предполагают, что доверие может быть предоставлено сущности независимо от того, является ли сущность заслуживающей доверия или нет. Заслуживающая доверия сущность - это сущность, для которой существует достаточное количество свидетельств, подтверждающих её заявленную доверенность. Таким образом, доверенность - это продемонстрированная способность и, следовательно, достоинство сущности, которой доверяют, оправдывать ожидания, в том числе оправдывать ожидания в условиях неблагоприятной ситуации. Поскольку доверенность является чем-то продемонстрированным, она основывается на свидетельствах, подтверждающих утверждение или суждение о том, что сущность заслуживает доверия [2] [20] [21].

Поскольку доверие не обязательно основано на суждении о доверенности, при принятии решения о доверии сущности следует учитывать значимость (т.е. последствия, результаты и воздействия) ожиданий, того, что ожидания не оправдаются из-за неисполнения обязательств, будь то

[14] Международный совет по инженерии систем (INCOSE) отмечает в [14], что "инженерия систем в применении специфична для потребностей заинтересованных сторон, пространства решения, результирующего системного решения (решений) и контекста на протяжении всего жизненного цикла системы" и "системная инженерия влияет и подвержена влиянию внутренних и внешних ресурсных, политических, экономических, социальных, технологических, экологических и правовых факторов".
[15] Номенклатура стадий жизненного цикла системы варьируется, но обычно включает анализ концепции; анализ решений; технологическое созревание; проектирование и разработку системы; проектирование и разработку производства; производство и развертывание; обучение, эксплуатацию и поддержку; а также списание и утилизацию.
[16] INCOSE предлагает руководство по инженерии систем [15] и Книгу знаний по инженерии систем [13] в качестве общих ресурсов. Национальное управление по аэронавигации и исследованию космического пространства (НАСА) также предлагает материалы по инженерии систем в том виде, в котором они применяются в сообществе NASA. Среди публикаций - "Руководство по инженерии систем NASA" [17] и два тома расширенного руководства по инженерии систем [18] [19].

некомпетентность, недостатки или неудачи. Доверие, предоставленное без установления требуемой доверенности, является существенным фактором риска. Концепции доверия и доверенности рассматриваются в Приложении F.

ИНЖЕНЕРИЯ ДЛЯ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ

В январе 2022 года INCOSE опубликовала документ «Видение инженерии систем». [16]. Он призван вдохновлять, направлять и информировать о стратегическом направлении развития мирового сообщества системной инженерии. Основным элементом, определяющих будущее состояние инженерии систем, является повышение уверенности в системах для улучшения практики создания доверенных систем.

Как отмечалось в [7], ключевая проблема, которую необходимо решить для реализации концепции «Видение 2035», заключается в том, что "системная безопасность перешла от традиционного акцента на доверии к большему акценту на риск". Необходимо доказать уровень безопасности системы с помощью доказательной базы доверия.

3. Концепции безопасности систем

В этой главе описываются аспекты, необходимые для создания систем с точки зрения безопасности. Подход к созданию систем с точки зрения безопасности требует понимания концепции безопасности (раздел 3.1), концепции адекватно безопасной системы (раздел 3.2) и характеристик систем (раздел 3.3). Он также требует понимания концепции активов (раздел 3.4), концепций потерь и контроля за потерями (раздел 3.5), как обосновывать потерю активов (раздел 3.6) и определения потребности в защите (раздел 3.7). При удовлетворении этих потребностей рассматриваются конкретные точки зрения (раздел 3.8) и способы демонстрации безопасности, включая адекватность (раздел 3.9). Поддисциплина инженерии систем, охватывающая эти вопросы, называется инженерия безопасности систем (раздел 3.10).

3.1. Концепция безопасности

Система, свободная от тех условий, которые могут привести к потере активов с неприемлемыми последствиями, должна обеспечивать предполагаемое поведение и результаты, а также избегать любого непреднамеренного поведения и результатов, которые представляют собой потери. Термин "*предполагаемое*" отражается в двух случаях, оба из которых должны быть удовлетворены:

- *Предположение пользователя:* Поведение и результаты системы, ожидаемые пользователем;
- *Предположение проекта:* Поведение и результаты системы, которые должны быть достигнуты в результате проектирования.

Система, которая предоставляет возможности в соответствии с замыслом проекта, но не соответствующая замыслу пользователя, представляет собой потерю. Например, потеря управления транспортным средством может быть результатом отказа функции управления рулевым управлением транспортного средства (т.е. несоответствия замыслу проекта) или в результате атаки, лишающей водителя возможности управления (т.е. несоответствия замыслу пользователя).

Основной целью безопасности является обеспечение того, чтобы имели место только предполагаемое поведение и результаты как системы, так и внутри системы.[17] Все потребности и интересы в области безопасности вытекают из этой цели, которая основывается на концепции *разрешения* того, что допускается и не допускается.[18] Таким образом, основной целью мер безопасности является обеспечение ограничений в виде правил для разрешенного и запрещенного поведения и результатов. Этой целью управления - и основополагающим принципом доверенного безопасного проекта - является *опосредованный доступ*. Если доступ не опосредован (т.е. не контролируется посредством наложения ограничений) в соответствии с набором не противоречащих друг другу правил, то нет оснований утверждать, что безопасность достигнута.

Правила опосредованного доступа определяются набором политик безопасности[19], которые отражают или вытекают из законов, директив, нормативных документов, концепций жизненного цикла,[20] требований или других конкретно сформулированных целей заинтересованных сторон. Политика безопасности включает область управления, которая устанавливает границы, в пределах которых

[17] Предполагаемое поведение включает в себя взаимодействие. К соответствующим взаимодействиям относятся взаимодействия «человек-машина» и «машина-машина». Взаимодействие «человек-машина» преобразуются в взаимодействие «машина-машина», в результате чего элемент машины действует от имени человека.
[18] Злоумышленник стремится к несанкционированному поведению или результату. Злоумышленники пытаются выполнить то, на что у них нет полномочий, даже если такое поведение или результат разрешены для других сущностей.
[19] Политика безопасности - это набор правил, регулирующих поведение системы и элементов системы, связанное с безопасностью (Приложение C).
[20] Концепции жизненного цикла включают эксплуатацию, обеспечение, развитие, поддержку, обучение, запуск и завершение.

применяется политика. Правила политики безопасности определяются в терминах субъектов (активные сущности), объектов (пассивные сущности) и операций, которые субъект может выполнять или требовать от объекта.[21] Эти правила регулируют поведение и результаты «субъект-объект» и «субъект-субъект». Каждое правило политики безопасности должно быть точным, последовательным, совместимым и полным в отношении целей заинтересованных сторон для определенной области управления.[22] Несогласованность, несовместимость, неточность или неполнота правил политики безопасности приводят к пробелам в защите. Не менее важно, чтобы возможности системы по защите безопасности были согласованы с ожиданиями политики и могли их реализовать.

Привилегии[23] определяют набор разрешенного и запрещенного поведения и результатов, предоставленных субъекту. Привилегии являются основой для принятия решений об опосредованном доступе. Ограничительная практика применения политик безопасности по умолчанию заключается в том, что механизм реализации разрешает только то, что явно разрешено политикой, и запрещает все остальное. Для того чтобы система считалась доверено безопасной, необходимо иметь достаточную уверенность в том, что система способна обеспечить выполнение политики безопасности на постоянной основе в течение всего времени действия политики (Приложение F).

3.2. Понятие адекватной безопасности системы

Адекватная безопасность - это понятие, позволяющее делать осмысленные суждения об идеалистической сущности целей безопасности. Определение безопасности выражает идеал, который включает в себя три важнейшие характеристики безопасной системы:

- Она позволяет реализовать требуемые возможности системы, несмотря на преднамеренные и непреднамеренные неблагоприятные факторы;
- Она накладывает ограничения, обеспечивающие, что при удовлетворении первой характеристики реализуются только желаемые поведение и результаты, связанные с требуемыми возможностями системы;
- Она обеспечивает соблюдение ограничений, основанных на наборе правил, чтобы гарантировать, что при удовлетворении второй характеристики могут происходить только авторизованные взаимодействия и операции «человек-машина» и «машина-машина».

Эти характеристики должны быть достигнуты в той степени, в какой это практически возможно, что приводит к разрыву между идеальной безопасной системой и теми показателями безопасности, которые система может надежно достичь.[24] Суждение о том, что система адекватно безопасна[25] требует доказательного определения того, что показатели безопасности оптимизированы с учетом всех других целей и ограничений. Область условий, относящихся к безопасности, и приемлемый уровень безопасности определяются в зависимости от потребностей заинтересованных сторон. Для обеспечения адекватной безопасности система должна:

- Соответствует минимально допустимым уровням[26] безопасности, определяемым опытом, анализом или комбинацией обоих;
- Является настолько безопасной, насколько это практически возможно (ASARP).

---

[21] Активные сущности проявляют поведение (например, выполняемый процесс), а пассивные сущности - нет (например, данные, файл).
[22] На самом высоком уровне доверия политики безопасности формально специфицируются и проверяются.
[23] Привилегии также называются разрешениями или правами.
[24] Поскольку безопасность системы асимметрична - то есть можно наблюдать, что она безопасна, но ни какое наблюдение не позволяет объявить произвольную систему безопасной [22], - идеал не может быть достигнут без некоторой неопределенности.
[25] Концепция адекватной безопасности является адаптацией концепции адекватной безопасности от [23].
[26] Ниже таких уровней система считается небезопасной.

Безопасная, насколько это практически возможно, означает, что повышение уровня безопасности потребует непропорционального ухудшения достижения других целей по стоимости, срокам или результативности системы, нарушит системные ограничения или потребует неприемлемых решений, например, неприемлемого изменения способа выполнения операций.

Адекватно защищенная система не обязательно исключает все условия, которые могут привести или приводят к нежелательным последствиям. Минимально допустимые уровни показателей безопасности и интерпретации понятия "*безопасна настолько, насколько это практически возможно*" не могут быть неизменными на протяжении всего срока службы системы. Информация, собранная в процессе эксплуатации системы, и извлеченные уроки могут послужить руководством и основой для изменений, повышающих планку допустимости и реализуемости.

Поэтому понятие адекватной безопасности является по своей сути контекстно-зависимым и субъективным по своей природе. Оно основано на утверждениях и ожиданиях относительно целей безопасности системы и определении того, насколько эти цели были достигнуты. Рисунок 4 иллюстрирует компромиссы между безопасностью системы и стоимостью, сроками и техническими показателями системы.

Рис. 4. Безопасность и стоимость системы /Сроки/Технические показатели

Оценка адекватной безопасности системы требует понимания состояний системы. Все системы работают в определенном наборе состояний и переходят из одного в другое. Эти состояния и переходы могут соответствовать или определяться характеристиками системы, такими как способ функционирования (например, запуск, работа, холостой ход, восстановление), способ использования (например, эксплуатация, обучение, обслуживание, мирное время, военное время), а также условиями окружающей среды (например, находится система под огнем или нет, температурные диапазоны). Существуют характеристики безопасности, которые определяют, является ли каждое состояние или переход безопасным, небезопасным или неопределенным (т.е. неизвестно, безопасным или

небезопасным). Адекватная безопасность зависит от умения различать безопасные, небезопасные и неопределенные состояния и поддерживать работу системы в безопасных состояниях, применяя принципы *«Защищённый отказ»* и *«Защищённое восстановление».*

Состояния системы могут быть безопасными (т.е. какие состояния желательны и допустимы) и небезопасными (т.е. какие состояния нежелательны и недопустимы). В идеале безопасная система - это система, которая начинает выполнение в безопасном состоянии и не переходит в небезопасное состояние. То есть каждый переход из одного состояния в другое приводит к тому же или другому безопасному состоянию. Каждый переход из одного состояния в другое также должен быть безопасным. На рис. 5 показано подмножество идеализированных переходов из одного безопасного состояния системы в другое.

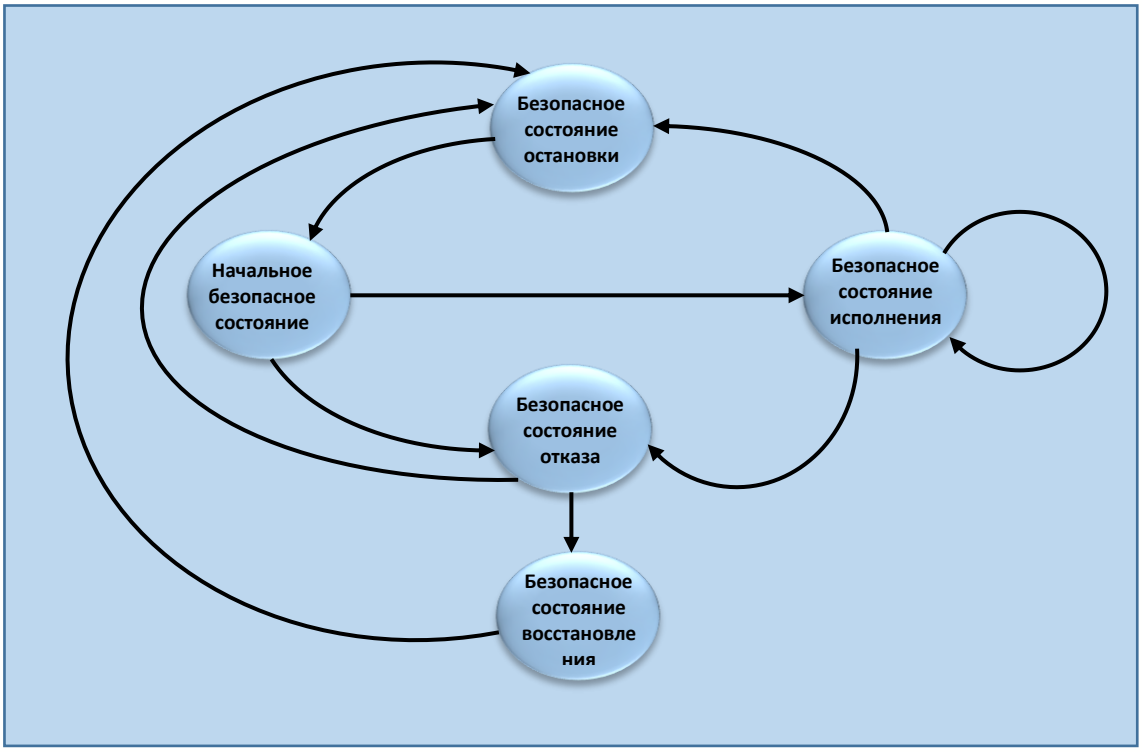

Рис. 5. Идеализированные условные переходы системы из одного безопасного состояния в другое

Защищённый отказ требует возможности (1) обнаружить, что система находится в небезопасном состоянии, и (2) обнаружить переход, который переведет систему в небезопасное состояние для целей реагирования, чтобы избежать порождения нового отказа. Защищённый отказ требует ответных и корректирующих действий, включая (при необходимости) переход в безопасное состояние остановки с защищенным восстановлением для продолжения работы в восстановленном, реконфигурированном или альтернативном безопасном режиме работы. Другие цели заинтересованных сторон могут потребовать продолжения функционирования в не полностью безопасном состоянии и должны быть отражены, при необходимости, в таких аспектах, как политика и требования (раздел C.3).

Защищённое восстановление требует способности предпринимать реактивные, ответные или корректирующие действия для безопасного перехода из небезопасного состояния в безопасное состояние (или менее небезопасное состояние). Безопасное состояние, достигнутое после завершения действий защищённого восстановления, включает в себя такие действия, которые ограничивают или предотвращают любой дальнейший переход в другое состояние, а также действия, которые представляют собой тип ухудшенной возможности, режима или функционирования.

3.3. Характеристики систем

Характеристики систем, их взаимосвязи с другими системами и роли в системе систем - все это влияет на безопасность и определение адекватной безопасности и надежности системы. К таким характеристикам систем можно отнести:

- Тип, функции и основное назначение системы;
- Технологические, механические, физические характеристики и характеристики персонала системы;
- Состояния и режимы работы системы;
- Критичность или важность системы;
- Последствия неспособности системы соответствовать ожиданиям, правильно функционировать, производить только запланированные действия и результаты, а также обеспечивать собственную защиту (т.е. самозащиту)[27];
- Концепция системы для обеспечения возможностей;
- Подход к приобретению системы;
- Подход к административному и оперативному управлению;
- Ценность, чувствительность и критичность активов, доверенных системе и используемых ею;
- Интерфейсы системы и системы, взаимодействующие через эти интерфейсы;
- Роль в качестве составной системы в одной или нескольких системах.

3.4. Понятие активов

Актив - это элемент, имеющий ценность. Существует множество различных видов активов. В целом активы подразделяются на материальные и нематериальные. К материальным активам относятся физические объекты, такие как аппаратное обеспечение, вычислительные платформы, другие технологические компоненты и люди. Нематериальные активы включают людей, микропрограммное обеспечение, программное обеспечение, возможности, функции, услуги, торговые марки, интеллектуальную собственность, данные, авторские права, патенты, имидж или репутацию[28]. Внутри категорий активов активы могут быть дополнительно идентифицированы и описаны в терминах общих классов активов, как показано в табл. 1.

Таблица 1. Общие классы активов

КЛАСС АКТИВОВ	ОПИСАНИЕ	КРИТЕРИИ ЗАЩИТЫ ОТ ПОТЕРЬ
МАТЕРИАЛЬНЫЕ РЕСУРСЫ И ИНФРАСТРУКТУРА	К этому классу активов относятся материальные ценности (например, здания, сооружения, оборудование) и физические ресурсы (например, вода, топливо). Он также включает основные физические и организационные структуры и объекты (т.е. инфраструктуру), необходимые для осуществления какой-либо деятельности или функционирования предприятия или общества.[29] Инфраструктура может состоять из активов других классов.	*Материальные ресурсы* защищены от потерь, если они не украдены, не повреждены и не уничтожены, а также способны функционировать или использоваться по назначению, по мере необходимости и когда это необходимо. *Инфраструктура* защищена от потерь, если она соответствует ожиданиям по производительности, предоставляя только разрешенные и запланированные

[27] В той мере, в какой это возможно, самозащита является необходимой возможностью, позволяющей системе обеспечивать требуемые возможности заинтересованных сторон и одновременно защищать их активы от потерь и последствий потерь.
[28] Люди - это, пожалуй, самый важный и ценный из всех нематериальных активов. Защита и безопасность в явном виде учитывают человеческие ресурсы.
[29] Адаптировано из определений *инфраструктуры* в Merriam Webster и Oxford.

КЛАСС АКТИВОВ	ОПИСАНИЕ	КРИТЕРИИ ЗАЩИТЫ ОТ ПОТЕРЬ
	Например, Национальная система воздушного пространства (NAS) может рассматриваться как инфраструктура, которая сама является системой и содержит другие элементы, являющиеся формами систем и инфраструктур, такие как система управления воздушным движением, навигационные средства, метеорологические средства, аэропорты и воздушные суда, которые маневрируют в пределах NAS.	возможности и производя только разрешенные и запланированные результаты.
ВОЗМОЖНОСТИ СИСТЕМЫ	Этот класс активов представляет собой набор возможностей или сервисов, предоставляемых системой. Как правило, возможности системы определяются (1) характером системы (например, развлекательная, автомобильная, медицинская, финансовая, промышленная или рекреационная) и (2) использованием системы для достижения целей предназначения или деятельности.	*Возможности системы* защищены от потери, если система удовлетворяет ожиданиям по производительности, предоставляя только разрешенные и предусмотренные возможности и производя только разрешенные и предусмотренные результаты.
ЛЮДСКИЕ РЕСУРСЫ	К этому классу активов относится персонал, который является частью системы и прямо или косвенно вовлечен в ее работу или испытывает на себе ее влияние. Последствия потерь, связанных с системой, могут существенно изменить значимость этого класса активов (например, воздействие на персонал в результате отказа системы наведения в самолете существенно отличается от воздействия на персонал в результате взлома системы, компрометирующей информацию об индивидуальных кредитных картах).	*Людские ресурсы* защищены от потерь, если они не получают травм, не болеют и не погибают.
ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ[30]	К этому классу активов относятся коммерческие секреты, рецепты, технологии[31] и другие объекты, обеспечивающие преимущество перед конкурентами. Преимущество зависит от конкретной области и может называться конкурентным, технологическим или боевым преимуществом.	*Интеллектуальная собственность* защищена от потери, если она не украдена, не испорчена, не уничтожена, не скопирована, не подменена несанкционированным образом и не подвергнута реинжинирингу несанкционированным образом.
ДАННЫЕ И ИНФОРМАЦИЯ	К этому классу активов относятся все типы данных и информации (совокупности данных), а также все кодировки и представления данных и информации (например, цифровые, оптические, аудио- и визуальные). Существуют общие классы чувствительности данных и информации, которые не подпадают под перечисленные выше категории, такие как классифицированная информация, контролируемая неклассифицированная информация (CUI) и неклассифицированные данные и информация.	*Данные и информация* защищены от потери в результате несанкционированного изменения, утечки, проникновения и уничтожения.
ПРОИЗВОДНЫЕ НЕМАТЕРИАЛЬНЫЕ АКТИВЫ	Этот класс активов состоит из производных, нематериальных активов, таких как имидж, репутация и доверие. Эти активы определяются, оцениваются и подвергаются позитивному и негативному влиянию - как успешному, так и неэффективному - в результате обеспечения адекватной защиты активов других классов.	Защита *нематериальных активов* от потерь осуществляется путем обеспечения адекватной защиты активов других классов.

Активы могут также рассматриваться как отдельные объекты или как совокупность или группа объектов,

[30] Термин "*интеллектуальная собственность*" определяется как результат творческого мыслительного процесса человека, имеющий определенную интеллектуальную или информационную ценность [24]. Примерами могут служить дизайн микрокомпьютеров и компьютерные программы.

[31] Термин "*технология*" определяется как применение научных знаний, инструментов, методов, мастерства, систем или способов организации для решения проблемы или достижения цели [25].

охватывающая типы или классы активов (например, данные о персонале, функции управления огнем, возможности датчиков окружающей среды). В данной публикации используется термин "*актив, представляющий интерес*", чтобы подчеркнуть и установить границы объема рассуждений для конкретного актива, типа актива или класса активов. Оценка актива является ключевым фактором при принятии решений об инвестициях в защиту актива (раздел 3.6). В тех случаях, когда актив связан с несколькими заинтересованными сторонами, могут существовать различные, противоречивые, конкурирующие или конфликтующие мнения об оценке, которые необходимо разрешить.

3.5. Понятия потерь и контроля потерь

Потеря - это изъятие или уничтожение актива или невозможность сохранить или продолжить иметь актив в желаемом состоянии или форме.[32] Потеря обычно возникает в результате неблагоприятного события или условия, которые приводят к неприемлемым последствиям, результатам или воздействиям. Конкретная потеря определяется и оценивается независимо от причинно-следственных событий и условий, необходимых для его возникновения (т.е. инициирующего события, например, ошибки бездействия, или события эксплуатации, например, атаки). Примеры результирующих неблагоприятных событий или условий и их результатов, воздействий или последствий включают:

- *Неблагоприятное событие или условие:* Данные похищены или случайно опубликованы на общедоступном сайте и теперь находятся не только в распоряжении владельца или уполномоченных им лиц.
- *Последствие, воздействие или результат:* Потеря доли рынка и конкурентных преимуществ объясняется тем, что в утерянных или похищенных данных содержатся подробные инструкции по методу точной обработки, которыми не располагает ни одна другая компания.
- *Неблагоприятное событие или условие:* У автомобиля спускает колесо, которое больше не выдерживает вес автомобиля.
- *Последствие, воздействие или результат:* Человек не может управлять автомобилем и нуждается в альтернативном транспорте, чтобы добраться до работы, магазина или поехать в отпуск.
- *Неблагоприятное событие или условие:* Потеряна или поставлена под сомнение уверенность в правильности работы интересующей системы.
- *Последствие, воздействие или результат:* Доверие к системе и ее результатам утрачено, независимо от того, оправдана потеря доверия или нет.

Хотя состояние или событие потери является негативным по отношению к предполагаемой норме, эффект от потери может быть либо нейтральным/незначительным, либо негативным/косвенным. Например, спущенное колесо на автомобиле, который используется только для поездок по бездорожью, является нейтральным/незначительным, если такие поездки не планируются или не рассматриваются.

Потери могут возникнуть вследствие одной или комбинации преднамеренных или непреднамеренных причин, событий и условий. Они могут включать в себя санкционированное или несанкционированное использование системы; преднамеренные действия по нарушению или подрыву; сбои, ошибки и отказы в работе людей и машин; действия людей по неправильному использованию и злоупотреблениям; а также возникновение побочного продукта, побочные эффекты и особенности взаимодействия. Эти потери могут быть несущественными для целей предназначения или деятельности, которые поддерживает система. Цели могут быть достигнуты, несмотря на то, что немедленные или возможные потери влияют на другие цели заинтересованных сторон.

[32] Адаптировано из определения *потери*, данного в Merriam Webster.

Потенциальная возможность возникновения потерь предполагает необходимость разработки целей контроля потерь, которые служат основой для суждений об эффективном решении задач по предотвращению и ограничению потерь. Сюда входят возникающие неблагоприятные события и условия, а также их последствия. Цели контроля потерь также служат основой для получения свидетельств уверенности в том, что спроектированная, построенная, используемая и эксплуатируемая система будет адекватно защищать от потерь при реализации ее проектного замысла. Цели контроля потерь отражают идеал сохранения характеристик активов (т.е. состояния, условий, формы, полезности) в той мере, в какой это практически возможно, несмотря на возможность изменения этих характеристик. Цели допускают неопределенность в виде ограничений на возможные действия (т.е. не всех потерь можно избежать) и ограничений на эффективность действий (т.е. все, что делается, имеет свои границы эффективности и набор потенциальных видов отказа).

В силу неопределенности невозможно гарантировать, что потери в той или иной форме не произойдут. Необходимо уделять особое внимание защите от последствий потерь, включая каскадные или волнообразные события (т.е. непосредственный эффект потерь вызывает дополнительные непредвиденные или нежелательные последствия или приводит к возникновению дополнительных потерь). Таким образом, целостная защита от потерь и непредвиденных или нежелательных последствий потерь учитывает весь спектр возможных потерь, включая типы потерь и последствия потерь, связанные с каждым классом активов. Это важно, учитывая, что все формы неблагоприятных факторов невозможно предугадать. Поэтому при защите от потерь целесообразно ориентироваться на контролируемое следствие, а не на причину.

Цели контроля потерь, приведенные в табл. 2, касаются возможностей контроля потенциальных потерь и их последствий с учетом пределов определенности, выполнимости и практичности. В совокупности цели контроля потерь включают в себя проблемы, связанные с безопасностью, живучестью, защищённостью и устойчивостью системы. Следует отметить, что удовлетворение целей контроля потерь может потребовать компромиссов. Предотвращение или ограничение потери одного актива может происходить за счет недопущения или ограничения потери другого актива, а также за счет компромиссов с другими целями (например, затратами и календарным планом).

Таблица 2. Цели контроля потерь

ЦЕЛЬ КОНТРОЛЯ ПОТЕРЬ	ОБСУЖДЕНИЕ
ПРЕДОТВРАЩЕНИЕ ПОТЕРЬ *(Предотвращение возникновения потерь)*	• Это тот случай, когда потерь можно полностью избежать. То есть, несмотря на наличие неблагоприятных условий: – Система продолжает обеспечивать только предполагаемое поведение и производит только предполагаемые результаты – Желаемые свойства системы и используемые ею активы сохраняются. – Активы продолжают существовать. • Предотвращение потерь может быть достигнуто любой комбинацией: – Предотвращение или устранение события или событий, вызывающих потерю – Предотвращение или устранение условия или условий, допускающих потерю – Устранение негативных последствий, несмотря на события или условия • Такие термины, как "*избежать*", "*продолжать*", "*задержать*", "*отклонить*", "*устранить*", "*усилить*", "*предотвратить*", "*перенаправить*", "*удалить*", "*выдержать*" и "*противостоять*", обычно используются для характеристики подходов к достижению этой цели, при которых потери не происходят, несмотря на воздействие на систему неблагоприятных факторов. • Термин "*выдержать*" относится к цели обеспечения отказоустойчивости, при которой неблагоприятные факторы в виде сбоев, ошибок и отказов становятся несущественными, не изменяют и не препятствуют реализации разрешенного и предполагаемого поведения и результатов системы (т.е. сбои, ошибки и отказы являются допустимыми).

ЦЕЛЬ КОНТРОЛЯ ПОТЕРЬ	ОБСУЖДЕНИЕ
ОГРАНИЧЕНИЕ ПОТЕРЬ *(Ограничение размера потерь)*	• Это касается случаев, когда потери могут возникнуть или возникли, а их размер должен быть ограничен. • Размер потерь может быть ограничен любой комбинацией следующих факторов: – Ограничение развития (например, миграция, распространение, разброс, колебания, домино или каскадные эффекты) – Ограничение продолжительности (например, миллисекунды, минуты, часы, дни) – Ограничение значимости (например, снижение полезности, выполнение функций, предоставление услуг или возможностей) – Ограничение величины (например, биты или байты данных/информации) • Принятие решения об ограничении масштабов потерь может потребовать определения приоритетов приемлемых потерь среди множества потерь, при этом цель ограничения потерь одного актива требует согласия с потерей какого-либо другого актива. • Крайним случаем ограничения потерь является недопущение уничтожения актива. • Такие термины, как "*выдержать*", "*противостоять*", "*удалить*", "*продолжать*", "*ограничить*", "остановить" и "перезапустить", относятся к этой категории в том случае, если потеря произошла, а система может или способна ограничить ее последствия. • Восстановление потерь и отсрочка потерь - два способа ограничения потерь: – Восстановление потерь: Действия, предпринимаемые системой или разрешённые системой для восстановления (или обеспечения возможности восстановления) части или всей ее способности функционировать (т.е. действовать, взаимодействовать, производить результаты) и восстановления активов, используемых системой (например, повторная визуализация, перезагрузка или воссоздание данных и информации, включая программное обеспечение в системе). Восстановление актива, полное или частичное, может ограничить развитие, продолжительность, значимость или величины потерь. – Отсрочка потери: Событие потери откладывается до тех пор, пока не уменьшится негативный эффект или когда отсрочка позволяет более эффективно реагировать или быстрее восстанавливаться. • Предполагается, что системные и внешние условия могут привести к потерям, но принимаются меры для ограничения последствий. • Для характеристики подходов к достижению этой цели обычно используются такие термины, как локализация, восстановление, реставрация, реконфигурация, перезапуск.

3.6. Рассмотрение потерь активов

Как показано на фиг.6, элементы структурированного подхода к рассмотрению потерь активов включают в себя (1) контекст потерь, (2) уверенность в устранении потерь, (3) значимость потерь, (4) устранение потерь и (5) причину потерь. Эти элементы обеспечивают основу защиты активов для определения целей защиты системы, оптимизации возможностей защиты системы и оценки общей пригодности и эффективности реализованных средств защиты.[33] Эти элементы также сгруппированы в две цели для облегчения рассмотрения представляющего интерес актива:

- **Цель 1:** Определение потребностей в защите актива
  - *Контекст потерь*: Область и критерии, ограничивающие рассмотрения потери актива;
  - *Значимость потерь*: Эффект от потери актива (или последствия), основанный на определении его ценности;[34]
  - *Уверенность в устранении потерь:* Уверенность, которая должны быть достигнута на основе аргументов, основанных на свидетельствах об эффективности того, что предпринимается для устранения потенциальных и фактических потерь.

[33] Применение подхода рассмотрения активов, одинаково способствует рассмотрению активов в терминах предназначения (т.е. рассмотрения активов, определяемого предназначением), организации (т.е. рассмотрения активов, определяемого организацией) и предприятия (т.е. рассмотрения активов, определяемого предприятием).

[34] Оценка ценности определяется заинтересованными сторонами. Факторы, которые могут учитывать заинтересованные стороны, включают различные затраты, связанные с активом, и последствия потери. Последствия потери могут быть краткосрочными (например, завершение деловой операции) или долгосрочными (например, длительная потеря работоспособности в ожидании замены актива).

- **Цель 2:** Удовлетворение потребностей в защите актива
  - *Причина потери:* События, условия или обстоятельства, которые описывают то, что произошло ранее и что может произойти в будущем, которые представляют собой потенциал для возникновения потери;
  - *Устранение потери:* Различные действия, предпринимаемые для осуществления контроля над потерями, насколько это практически возможно. Цели контроля заключаются в предотвращении потерь и ограничении их масштабов и продолжительности. Ограничение потерь включает восстановление после потерь в той степени, в какой это практически возможно.

Рис. 6. Рассмотрение защиты активов

Актив, представляющий интерес - это класс активов, тип активов или отдельный актив, который рассматривается. Обоснование потерь основывается на интересующем активе. Отделение интересующего актива от всех остальных активов обеспечивает ясность в интерпретации потерь для интересующего актива и в соответствующих суждениях о пригодности и эффективности применяемых средств защиты. Сосредоточение внимания на конкретном классе, типе или дискретном элементе активов также позволяет точно отслеживать требования, которые поддерживают анализ, необходимый для определения влияния изменения требований к защите.

Контекст потери устанавливает границу, область и сроки для рассмотрения, анализа, оценки и выводов об активе, представляющем интерес. Контекст потерь также служит основой для соотношения и отслеживания зависимостей и взаимодействий между активами и группирования активов для защиты. Контекст временных рамок потерь особенно важен, поскольку актив, представляющий интерес, имеет

жизненный цикл,[35] который отличается от системы, представляющей интерес.[36] Например, актив, представляющий интерес, может быть создан, сконфигурирован или модифицирован вне области управления системы, представляющей интерес, но при этом находится в области работ по проектированию. Актив, представляющий интерес, попадающий в область управления системы, представляющей интерес, может иметь различные потребности в защите, связанные с состоянием или режимом работы системы (например, защита рабочего режима системы может отличаться от защиты учебного режима системы). Кроме того, активы жизненного цикла системы (раздел 3.8) могут существовать только в рамках системы разработки или производства и связанных с ними вспомогательных сред. Последствия потерь для этих активов могут переходить в потери, связанные с системой, представляющей интерес. Поэтому контекст потерь включает в себя жизненный цикл актива, состояние и режим работы системы, а также другие временные периоды или характеристики, в течение которых потери рассматриваются.

ВРЕМЕННЫЕ РАМКИ ПОТЕРЬ – ПРИМЕР

Финансовый портфель (т.е. актив или набор активов) с конкретными инвестиционными целями и соображениями приемлемости рисков может быть создан финансовым консультантом для клиента, профинансирован клиентом и впоследствии управляться с помощью нескольких систем одной или нескольких институциональных инвестиционных компаний на протяжении всего жизненного цикла портфеля. Каждый актив, представляющий интерес в рамках портфеля, может иметь различные потребности в защите в разное время в зависимости от типа актива, рыночных условий, юрисдикции регулятора, позиции по риску и других факторов управления активами, которые накладываются на систему.

Значимость потерь - это негативный эффект (последствия) на актив, представляющий интерес, или результирующий негативный эффект связанный с активом. Значимость потерь лучше всего описывается как опыт, которого следует избегать, что оправдывает инвестиции для защиты от возникновения потерь и минимизации масштабов негативных последствий в случае их возникновения. Значимость потерь определяется и оценивается как суждение, основанное на эффектах. То есть она определяется без учета того, как и почему возникает потеря, вероятности её возникновения, а также намерений или отсутствия намерений, связанных с потерей.[37]

Значимость потерь позволяет ответить на следующие вопросы:

- Каковы последствия, результаты и проблемы, которые возникают в результате потери интересующего актива?
- Какова серьезность этих последствий, результатов и проблем?

[35] Срок службы актива может отличаться от срока службы системы. Активы могут существовать до появления системы и сохраняться после вывода системы из эксплуатации. Значение потери актива может иметь последствия, не зависящие от системы, ее функций, целей деятельности и предназначения.

[36] Жизненный цикл актива совпадает с жизненным циклом системы, когда активом, представляющим интерес, является система, представляющая интерес. Жизненный цикл актива может быть таким же или короче, чем жизненный цикл системы, для тех активов, которые созданы системой, представляющей интерес и требуются только во время работы системы, представляющей интерес.

[37] Определение значимости потерь не является определением риска.

Значимость потерь требует ясности в том, что означает потеря для актива, представляющего интерес. Примеры терминов, используемых для описания потери активов, включают: способность, доступность, точность, доверие, преимущество (технологическое, конкурентное, боевое), возможность, контроль, корректность, существование, инвестиции, владение, результативность, владение, точность, качество, удовлетворенность и время.

ЗНАЧЕНИЕ ПОТЕРЬ - ПРИМЕР

Значимость потерь, связанных со спущенной шиной, определяется и оценивается без учета того, как и почему спустилась шина (например, прокол, производственный дефект, удар о бордюр или другой предмет), а также без учета злого умысла (например, порез шины, ослабление штока клапана). Независимо от того, как и почему спустило колесо, значение потерь остается неизменным (например, потеря управления при движении автомобиля, невозможность управлять автомобилем при его остановке, потеря времени на замену или ремонт шины для приведения автомобиля в рабочее состояние). Значимость потерь из-за спущенного колеса заключается в невозможности управлять транспортным средством, а результатом неблагоприятного воздействия может стать столкновение с каким-либо другим объектом (т.е. авария). Негативные последствия нарушения рулевого управления (потеря контроля) носят конкретный характер, в то время как негативные последствия аварии носят общий характер (многие другие обстоятельства могут привести к аварии без потери способности управлять автомобилем).

Уверенность в устранении потерь обеспечивает наличие совокупности объективных свидетельств, подтверждающих эффективность, достаточность и пригодность защитных мер для удовлетворения потребностей в защите активов. Уверенность в устранении потерь носит кумулятивный характер. Она начинается с определения проблем, связанных с потерями интересующего актива, и постоянно возрастает по мере лучшего понимания и решения этих проблем в контексте потерь, значимости потерь, причин потерь и способов их устранения. База свидетельств, обеспечивающая уверенность, формируется в результате деятельности по верификации и подтверждению соответствия, осуществляемой на протяжении всего жизненного цикла активов и системы, включая разработку и анализ требований. Ключевым информационным элементом этих мероприятий является обеспечение того, чтобы их результаты способствовали достижению требуемой уверенности.

Причиной потери[38] является отдельное событие или сочетание событий, условий и обстоятельств, которые приводят к той или иной форме потери актива. Причины потери актива составляют континуум событий и условий, который включает: намеренные, неумышленные, случайные, непредвиденные, неправильное употребление, злоупотребления, ошибки, дефекты, неисправности, слабости и отказы [26]. Этот континуум охватывает все человеческие, машинные, физические и естественные факторы потерь. К рассмотрениям причин потерь применимы следующие соображения:

- Отдельные события и условия, которые сами по себе могут привести к потере;
- Комбинации, последовательности и совокупные события и условия;

[38] Для описания причин потери активов используется множество терминов. Некоторые из этих терминов специфичны для определённого сообщества интересов или области специализации, в то время как другие охватывают все сообщества и специализации. Существуют также случаи, когда один и тот же термин может использоваться по-разному в разных сообществах и областях специализации (например, термин "угроза" имеет различную интерпретацию в разных сообществах, например, физическая безопасность, кибербезопасность, торговля, правоохранительные органы, промышленность, военные боевые действия и военная разведка). В качестве синонимов причины потери активов используются такие термины, как: атака, нарушение, компрометация, опасность, несчастье, угроза, нарушение и уязвимость.

- События и условия, которые желательны, предполагаемы и даже запланированы, но приводят к непредвиденным, непредусмотренным и непредсказуемым результатам;
- Каскадные и волнообразные события и условия.

Наконец, причины потери активов отвечают на следующие вопросы:

- Как могут произойти потери?
- Как в прошлом происходили потери?

Однако определение того, как может произойти потеря, не требует задавать или отвечать на вопрос: «Что может произойти или возможно?»[39]

Устранение потерь осуществляется с помощью защитных мер, обеспечивающих соблюдение ограничений, гарантирующих, что в системе будут происходить только разрешенные и предполагаемые действия и результаты. К ним относятся:

- Защитные меры, которые обеспечивает *машинная часть* системы (т.е. архитектура и конструкция системы, использование инженерных элементов и устройств в рамках архитектуры и конструкции);
- Защитные меры, обеспечиваемые *человеком* в системе (т.е. персонал, практика, процедуры, использование инструментов для поддержки человека как элемента системы, а также роль человека в проектировании и создании машинной части системы);
- Защитные меры, обеспечиваемые *физической средой* (например, контролируемые зоны доступа, точки доступа к объекту, физический мониторинг, контроль окружающей среды, пожаротушение)

Терминология, используемая для описания средств и методов, включает: механизмы, конфигурации, меры, защитные меры, контрмеры, возможности, методы, блокировки, практика, процедуры, процессы и запреты. Они могут применяться в соответствии с регулирующими политиками, нормативными документами, законами, практикой, стандартами и технологиями.

ЗАЩИТА НА ОСНОВЕ АКТИВОВ - ПРОЕКТИРОВАНИЕ ДЛЯ УСПЕХА

Не зацикливайтесь на том, что вероятно произойдёт. Вместо этого сосредоточьтесь на том, что может произойти, и будьте готовы. Именно это означает техника обеспечения безопасности путем принятия стратегии упреждения и реагирования (раздел D.2) в форме концепции безопасного функционирования, учитывающей весь спектр потерь активов и связанных с ними последствий. Это означает упреждающее планирование и проектирование для предотвращения потери актива, которую вы не готовы принять, чтобы иметь возможность минимизировать последствия, если такая потеря произойдет, и быть в состоянии своевременно отреагировать на потерю, когда это произойдет.

[39] Этот момент отличает анализ того, что может произойти, от оценки риска, определяющей вероятность больше нуля и меньше единицы того, что неблагоприятное событие произойдет.

3.7. Определение потребностей в защите

Заинтересованные стороны должны достигать их цели предназначения или деятельности безопасным способом, обеспечивающим сохранность активов и ограничивающим масштабы их потери. Защита активов должна быть постоянной, что позволит заинтересованным сторонам реалистично рассчитывать на постоянный успех в плане способности их систем поддерживать и достигать их целей.

Масштаб и ожидания в отношении защиты активов имеют основополагающее значение для достижения цели проектирования доверенной безопасной системы. Потребности в защите обычно соотносятся с серьезностью последствий, связанных с потерей актива. Потребности в защите определяются на основе всех потребностей, интересов, приоритетов и ограничений, связанных с защитой и сохранением активов заинтересованных сторон и системы. Существует три позиции на потребности в защите: (1) позиция *заинтересованных сторон*, (2) позиция *системы* и (3) позиция *соглашений*. На рис. 7 показаны основные исходные данные, используемые для определения потребностей в защите, и результаты, получаемые в результате определения этих потребностей.

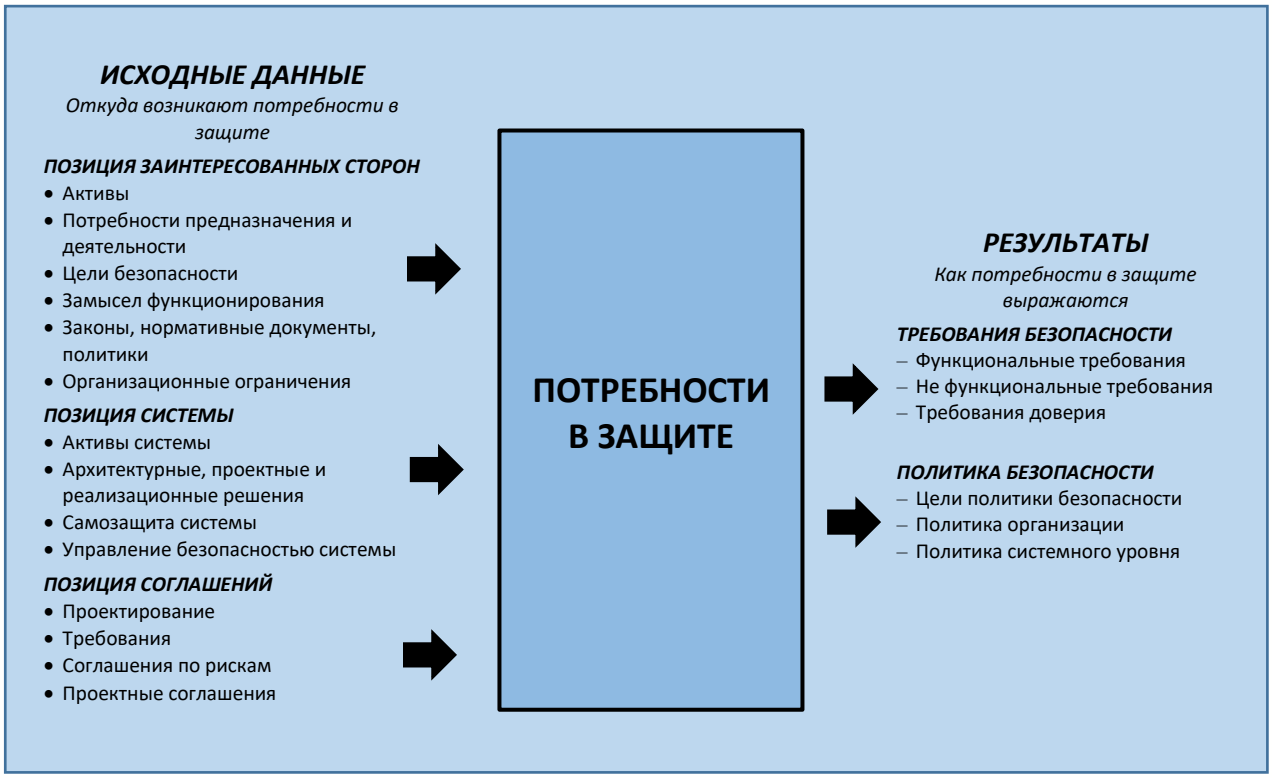

Рис. 7. Определение потребностей в защите

Назначение установления потребностей в защите заключается в решении вопроса о том, какие активы следует защищать, и определении приоритетности такой защиты. Это может быть достигнуто без учета причины или условия, от которых необходимо защитить. Как показано на рис. 8, потребность в защите определяется на основе взаимосвязи между интересующим активом, контекстом потерь, типом потерь и последствиями потерь. Такой подход позволяет определить потребность в защите, которая после подтверждения заинтересованными сторонами всех интересующих их активов служит основой для разработки целей и требований безопасности.[40]

[40] Требования представляют собой формальное и четкое выражение потребностей, интересов, приоритетов и ограничений, которые должны быть удовлетворены для функционирования, эксплуатации и поддержки системы. Каждое требование

Рис. 8. Взаимосвязь между активами, потерями и последствиями

Подводя итог, можно сказать, что на определение потребностей в защите влияют следующие соображения:

- Активы имеют различные классы и типы.
- Активы связаны с заинтересованными сторонами и системой.
  - Некоторые активы связаны с заинтересованными сторонами (т.е. активы заинтересованных сторон) и имеют назначения, использование и существование, которые не зависят от проектируемой системы;
  - Некоторые активы связаны с системой, зависят от характеристик проекта и поведения системы и обычно неизвестны заинтересованным сторонам.
- Интерпретация потерь имеет двойственный характер.
  - Влияние на интересующий актив;
  - Влияние на тех, кто оценивает интересующий актив.
- Интерпретация потерь зависит от времени и состояния.
  - Охватывает континуум внутри и между типами и классами активов;
  - Может изменяться в течение жизненного цикла актива и в зависимости от состояния, в котором актив существует или используется.
- Суждения об активах носят субъективный характер.
  - Оценка стоимости активов

сопровождается методами проверки для подтверждения того, что требование удовлетворено. Требования должны быть точными, однозначными, всеобъемлющими, поддающимися оценке и выполнимыми.

- Последствия потерь активов
- Пригодность, эффективность и надежность защиты активов

Точка зрения заинтересованных сторон основана на активах, принадлежащих заинтересованным сторонам. Поэтому, эти заинтересованные стороны определяют потребности в защите. Точка зрения системы основана на активах, необходимых для функционирования системы. Эти активы определяются системными проектами решениями, а также критичностью и приоритетностью[41] актива в обеспечении или поддержке функций системы. Заинтересованные стороны, как правило, не знают о существовании системных активов и не могут принимать решения о необходимости защиты системных активов. Защита системных активов является элементом проекта доверенной безопасной системы.

Потребности в защите постоянно пересматриваются и корректируются по мере возникновения отклонений, изменений и соглашений в течение всего жизненного цикла системы. К ним относятся созревание концепций проектирования и жизненного цикла системы, более глубокое понимание среды эксплуатации (например, более глубокое понимание неблагоприятных факторов) и изменения в понимании последствий потери активов. Пересмотр потребностей в защите является необходимой частью итеративной сущности проектирования систем. Проектирование безопасности системы необходимо для обеспечения полноты понимания проблемного пространства, изучения всех возможных решений и создания доверенной безопасной системы.

3.8. Позиции рассмотрения безопасности системы

Три основополагающие позиции рассмотрения безопасности системы включают *функцию системы*, *функцию безопасности* и *активы жизненного цикла*. Эти позиции рассмотрения определяют соображения, которые используются в качестве соображений доверенного безопасного проекта для любого типа системы, предполагаемого использования и последствий отказа системы.

Каждая система создается для удовлетворения потребностей заинтересованных сторон. Эти потребности образуют функцию системы - назначение или роль системы, выполняемую совокупностью предоставляемых ею возможностей в сочетании с ее предполагаемым использованием. Функция системы является доминирующей точкой зрения и определяет контекст для функции безопасности и связанных с ней активов жизненного цикла системы.

Потребности заинтересованных сторон в возможностях включают в себя потребности в возможностях защиты Потребности в защите соответствуют концепции потребностей заинтересованных сторон в возможностях и составляют функцию безопасности системы – совокупность целей или роли системы для безопасного удовлетворения потребностей заинтересованных сторон в возможностях. Функция безопасности предусматривает введение ограничений, обусловленных безопасностью, как часть общего проекта системы. Цель ограничений - избегать, уменьшать и допускать слабые места, дефекты, слабости и недостатки системы, которые могут представлять собой уязвимости, которые могут быть использованы или спровоцированы. Эти уязвимости могут содержаться в структуре или поведении системы и могут противодействовать, препятствовать или минимизировать способность системы эффективно удовлетворять своему замыслу и обеспечивать требуемые возможности. Таким образом, ограничения также позволяют синтезировать функцию безопасности в рамках функции системы бесконфликтным способом.

Функция безопасности системы имеет как пассивные, так и активные аспекты:

- Пассивные аспекты функции безопасности не проявляют поведения (т.е. не являются функциональ-

[41] Критичность и приоритет, основанные на оценке активов, обычно используются при принятии решений о потребностях в защите. Актив с более высокой критичностью и приоритетом будет иметь преимущество при обеспечении защиты, если существуют ограничения, требующие выбора между общими потребностями в защите.

ными по своей природе). Они включают в себя архитектуру системы и элементы проекта. Пассивные аспекты являются частью структуры системы и, следовательно, воплощаются в архитектуре системы. Например, функциональная архитектура может сегментировать функции системы (включая функции безопасности) на различные подсистемы, уменьшая возможность интерференции между функциями, а также ограничивая распространение ошибочного поведения. Пассивные аспекты по своей сути снижают восприимчивость системы к воздействиям, опасностям и уязвимостям, тем самым ограничивая, а то и вовсе устраняя, возможность возникновения сценариев потерь. Использование пассивных аспектов, как правило, обеспечивает большую уверенность в защитных возможностях системы.

- Активные аспекты функции безопасности проявляют поведение (т.е. являются функциональными по своей природе). Они включают в себя спроектированные функции и устройства, называемые мерами, контрмерами, возможностями, препятствиями, механизмами, блокировками, защитными мерами или сервисами. Активные аспекты используются или распределяются в рамках архитектуры системы, имеют определенный проект, а также возможности и ограничения, которые влияют на их пригодность и эффективность в зависимости от назначения.
- Пассивные и активные аспекты функции безопасности учитываются в соглашениях, как обсуждается в разделе D.4.4. Активные аспекты могут также потребовать дополнительного оборудования или нагрузить существующее оборудование, что повышает требования к размерам, весу и мощности (SWaP) и делает активные аспекты проблемой для систем с ограничениями SWaP (например, спутников).

Активы жизненного цикла связаны с системой, но не проектируются и не поставляются вместе с системой. Их связь с системой означает, что они могут быть непосредственной причиной потери или каналом/средством, через который могут возникнуть потери. Активы жизненного цикла имеют несколько типов:

- Системы, взаимодействующие с системой, представляющей интерес, включая концептуальные системы;
- Интеллектуальная собственность в различных формах, включая запатентованные алгоритмы, технологии и технологические решения;
- Данные и информация, связанные с системой;
- Возможности и системы по разработке, производству, изготовлению и сбыту, применяемые для использования, эксплуатации и поддержания системы в рабочем состоянии.[42]

3.9. Демонстрация безопасности системы

Демонстрация надлежащей безопасности системы (раздел 3.2), позволяет заинтересованным сторонам убедиться в том, что их цели, потребности, интересы и связанные с ними ограничения были учтены. Такая демонстрация должна рассматривать систему как эмерджентное целое[43], состоящее из:

- Необходимых возможностей, которые она предоставляет;
- Возможностей защиты;

---

[42] Примерами могут служить средства и комплексы разработки программного и аппаратного обеспечения; среды и средства моделирования и имитации; устройства, компоненты и комплексы технического обслуживания и диагностики; тренажеры и генераторы сценариев испытаний; системы обучения. Хотя эти средства не обязательно входят в сферу проектирования представляющей интерес системы, поведение и результаты работы этих систем имеют последствия для безопасности, которые должны быть учтены при разработке представляющей интерес системы. Поведение и результаты, которые необходимо учитывать, включают в себя те, которые могут прямо или косвенно включать, сопрягать, взаимодействовать и совместно функционировать с представляющей интерес системой.

[43] [43] *Свойство эмерджентности* - это свойство, проявляемое сущностями, которое имеет смысл только при отнесении его к целому, а не к какому-либо отдельному составляющему элементу [27]. К эмерджентным свойствам систем относятся ее возможности, защищенность, безопасность, надежность, устойчивость, живучесть, гибкость, ремонтопригодность и доступность. Более подробно эмерджентность рассматривается в Приложении D.

- Пределов определённости.[44]

В частности, пределы определенности применяются к требованиям и принятию потенциальных ошибок, несоответствий или пробелов в полноте и охвате этих требований. Поэтому требования и соответствующие методы проверки и подтверждения соответствия, хотя и являются необходимым аспектом демонстрации адекватной безопасности, недостаточны для того, чтобы считать систему адекватно безопасной. Предоставляемый уровень уверенности должен быть соразмерен с рассматриваемыми последствиями потери активов. База свидетельства для демонстрации уверенности должна регистрироваться, отслеживаться, поддерживаться и развиваться по мере возникновения изменений, имеющих отношение к демонстрации адекватной безопасности на протяжении всего жизненного цикла системы. Кроме того, база свидетельств должна быть значимой для профильных экспертов с учётом субъективных, конкурирующих и часто противоречащих друг другу потребностей и убеждений заинтересованных сторон.

Демонстрация этой обоснованной уверенности или доверия достигается на основе базы свидетельств, обеспечиваемой системным анализом и другими действиями по подготовке свидетельств.[45] База свидетельств используется в рамках подхода к структурированному рассмотрению, как это показано в примерах по доверию (раздел 4.3). При этом рассматриваются потребности и возможности системы, количественные и качественные факторы, влияющие на систему, а также то, каким образом эти возможности и факторы создают базу свидетельств, на основе которой проводится дальнейший анализ в контексте безопасности системы. В свою очередь, эти анализы подкрепляют обоснованные и аргументированные выводы, которые служат основой для достижения консенсуса между заинтересованными сторонами в отношении адекватной безопасности системы (Приложение F).

> Ни одна система не может обеспечить **абсолютную безопасность** в силу ограниченности человеческих возможностей, неопределенности, существующей в жизненном цикле каждой системы, а также ограничений по стоимости, срокам, эксплуатационным качествам, осуществимости и практичности. Поэтому, для **достижения адекватной** безопасности оптимизируются компромиссы между противоречивыми, конкурирующими и конфликтующими потребностями и ограничениями, что отражает решение, принимаемое заинтересованными сторонами.

3.10. Инженерия безопасности систем

Как субдисциплина инженерии систем, инженерия безопасности систем - это междисциплинарный и интегративный подход к обеспечению успешной реализации, использования и вывода из эксплуатации созданных доверенных безопасных систем. В инженерии безопасности систем используются принципы и концепции систем, безопасности и другие, а также научные, технологические и управленческие методы. Инженерия безопасности систем обеспечивает применение этих принципов, концепций, методов и практик в течение жизненного цикла системы для достижения целей заинтересованных сторон по обеспечению доверенности и защите активов, несмотря на неблагоприятные факторы. Она также помогает уменьшить и контролировать причины и условия, которые могут привести к уязвимости и, как следствие, уменьшает влияние, которое могут оказать на систему неблагоприятные факторы.

[44] Отдельная функция или механизм могут быть проверены и подтверждены на корректность в соответствии с атрибутами качества и результативности. Эти результаты помогают определить степень безопасности системы, но сами по себе недостаточны.

[45] Хотя свидетельства, полученные в результате демонстрации соответствия набору ожиданий или критериев, могут подтвердить суждения об адекватной безопасности, сами по себе такие свидетельства не являются основанием для утверждения об адекватной безопасности.

Инженерия безопасности систем пересекается с другими субдисциплинами и использует множество специальностей для выполнения мероприятий и задач по обеспечению безопасности систем. Эти специальности включают компьютерную безопасность; безопасность связи; безопасность передачи данных; безопасность электронных излучений; защита от несанкционированного доступа; физическая безопасность; доверие к информации, программному, аппаратному обеспечению и цепочкам поставок; а также технологические специальности, такие как биометрия и криптография.

Инженерия безопасности систем также использует вклад других вспомогательных инженерных дисциплин и специальностей для анализа и управления сложностью, взаимосвязанностью, динамичностью и восприимчивостью, связанными с технологиями на основе аппаратного, программного и микропрограммного обеспечения.[46] Это включает разработку, производство, обработку и распространение технологий на протяжении всего жизненного цикла системы.[47]

На рис. 9 показаны взаимосвязи между инженерией систем, инженерией безопасности систем, обеспечением безопасности и другими специальными проектными областями.

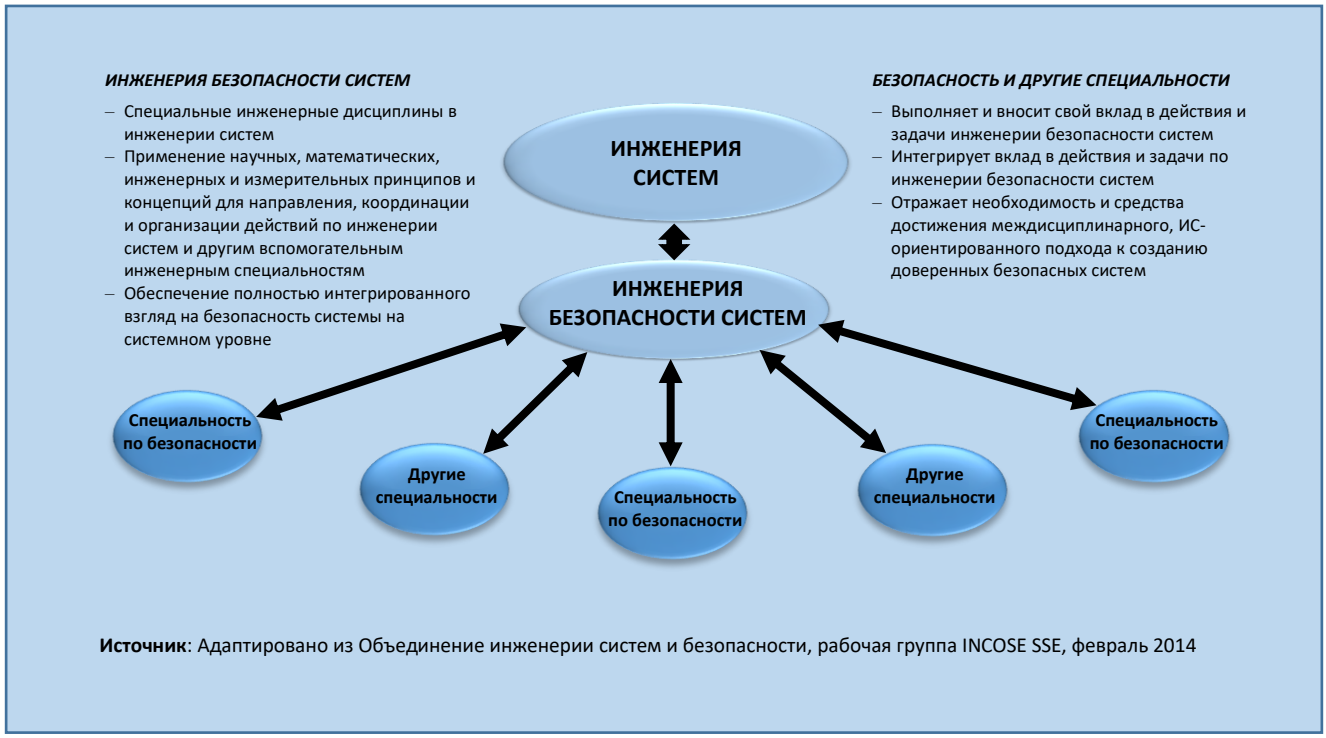

Рис. 9. Инженерия систем и другие специальные инженерные дисциплины

В рамках междисциплинарных усилий инженерии систем, направленных на создание доверенной безопасной системы, при инженерии безопасности систем осуществляется:

- Работа с заинтересованными сторонами для обеспечения определения целей безопасности, потребностей и интересов защиты, потребностей в доверии, требований безопасности (включая показатели эффективности [ПЭ] и показатели результативности [ПР]) и соответствующих методов

[46] К вспомогательным инженерным дисциплинам и специальностям относятся инженерия надежности, доступности и ремонтопригодности (НДР), инженерия программного обеспечения, инженерия отказоустойчивости и инженерия человеческих факторов (эргономика).

[47] Это включает оценку потенциальных недостатков в доверии к цепочкам поставок, когда третьи стороны и повторное использование учитываются при планировании системы и ее реализации.

подтверждения соответствия;

- Определение требований[48] к безопасности системы и соответствующих методов проверки;
- Разработка взглядов и точек зрения на архитектуру и проект системы исходя из безопасности;
- Выявление и оценка восприимчивости и уязвимости к опасностям и неблагоприятным факторам на протяжении всего жизненного цикла;
- Разработка упреждающих и реактивных функций, включенных в сбалансированную стратегию контроля потерь активов и связанных с ними последствий потерь;
- Предоставление соображений по безопасности для обоснования усилий по созданию систем с целью сокращения ошибок, недостатков и слабых мест, которые могут представлять собой уязвимость безопасности;
- Проведение анализа безопасности системы и интерпретация результатов других системных анализов в поддержку принятия решений по проектным соглашениям и управлению рисками;
- Определение, количественное выражение и оценка затрат и выгод от использования средств, функций и соображений безопасности для обоснования оценок альтернативных решений, проектных компромиссов и решений по обработке рисков;[49]
- Демонстрация с помощью доказательной аргументации, что требования безопасности и доверенности системы были удовлетворены до требуемого уровня доверия;
- Привлечение специалистов по безопасности и других специальностей для рассмотрения всех возможных решений.

БЕЗОПАСНОСТЬ - ЭМЕРДЖЕНТНОЕ СВОЙСТВО ПРОЦЕССА РАЗРАБОТКИ

Система разрабатывается для достижения возможностей, определяемых предназначением и потребностями деятельности заинтересованных сторон. Безопасность является эмерджентным свойством системы, которое достигается благодаря принципиальному процессу разработки, отражающему потребности и интересы заинтересованных сторон в области защиты. Разработанные возможности безопасности вносят вклад в общие возможности системы, удовлетворяющие потребности предназначения и деятельности заинтересованных сторон. Ни одна система не может обеспечить абсолютную безопасность из-за пределов человеческой уверенности, неопределенности, существующей в жизненном цикле каждой системы, и ограничений по стоимости, срокам, результативности, осуществимости и практичности. Поэтому для обеспечения адекватной безопасности необходимо постоянно находить компромиссы между противоречивыми, конкурирующими и конфликтующими потребностями и ограничениями.

[48] Важно понимать контекст, в котором термин "требования к безопасности системы" используется в данной публикации. Например, из-за сложности безопасности систем существует несколько типов и целей требований к безопасности систем (раздел 3.8 и Приложение C).

[49] Термин "обработка риска" используется в [4] и определяется в [28].

4. Основы инженерии безопасности систем

Основы инженерии безопасности систем [29] представляют собой концептуальное видение ключевых контекстов, в которых осуществляется деятельность по инженерии безопасности систем. Они определяют, ограничивают и фокусируют работы и задачи на достижении целей безопасности заинтересованных сторон и представляют согласованное, хорошо сформированное, основанное на фактических данных обоснование для поддержки суждений о достижении целей.[50] Основы не зависят от типа системы и модели процесса проектирования или приобретения. Их следует трактовать не как последовательность потоков или этапов, а как набор взаимодействующих контекстов, каждый из которых имеет свои собственные системы сдержек и противовесов. Основы инженерии безопасности систем акцентируют внимание на интегрированном, целостном подходе к безопасности на всех этапах жизненного цикла системы и применяются для достижения основных целей каждой стадии жизненного цикла.

Основы определяют три контекста для выполнения работ и задач: (1) контекст проблемы, (2) контекст решения, (3) и контекст доверенности. Эти три контекста способствуют обеспечению того, чтобы в основе разработки лежало достаточно полное понимание проблемы. Это понимание стимулирует усилия по поиску решения и поддерживается набором действий по разработке и реализации решения. Оно также демонстрирует состоятельность решения в обеспечении адекватной безопасности в условиях конкурирующих и зачастую противоречащих друг другу ограничений.

Несмотря на то, что основы представляются как последовательное выполнение в трех контекстах, предполагается, что они должны реализовываться итеративным и рекурсивным способом в замкнутом цикле. Такой подход облегчает уточнение описания проблемы, предлагаемого решения и целей доверенности по мере того, как проект развивается от концепции к реализованному решению. Обратная связь с замкнутым циклом облегчает взаимодействие между тремя контекстами основ и необходимым анализом безопасности системы для непрерывного выявления и устранения отклонений, которые возникают в проектных работах. Цикл обратной связи также помогает достичь непрерывного совершенствования процессов в системе, включая рассмотрение результатов одной фазы жизненного цикла (т.е. решений по фазе) в качестве входных данных для следующей фазы (т.е. проблемы для следующей фазы).

Три контекста основ имеют общую фундаментальную базу анализа безопасности систем, включая системный анализ с интерпретацией результатов анализа с точки зрения безопасности (раздел H.6). Анализ безопасности системы позволяет получать данные для поддержки разработки и принятия решений заинтересованными сторонами.[51] Такие анализы дифференцируются для применения в контексте проблемы, решения и доверенности и используют различные концепции, принципы, технологии, средства, методы, процессы, практики и инструменты. Анализ безопасности системы:

- Предоставляет соответствующие данные и технические интерпретации системных проблем с точки зрения безопасности системы;
- Дифференцирован в своем применении в соответствии с областью и целями применения в рамках инженерии безопасности систем;

[50] Адаптирован из [6].

[51] Разработка и принятие решений заинтересованными сторонами включает архитектуру, доверие, поведение, стоимость, критичность, проект, эффективность, эмерджентность, подверженность воздействию, соответствия назначению, концепции жизненного цикла, устойчивость к проникновению, результативность (включая результативность системы безопасности), потребности в защите, цели безопасности, приватность, требования, устойчивость, риск, стойкость функций, угрозы, соглашения, неопределенность, уязвимость, проверку и подтверждение соответствия.

- Выполняется с уровнем точности, строгости и формальности для получения данных с уровнем достоверности, который соответствует доверию, требуемому заинтересованными сторонами и проектной группой (Приложение F).

Рис. 10 иллюстрирует основы инженерии безопасности систем и её ключевые компоненты.

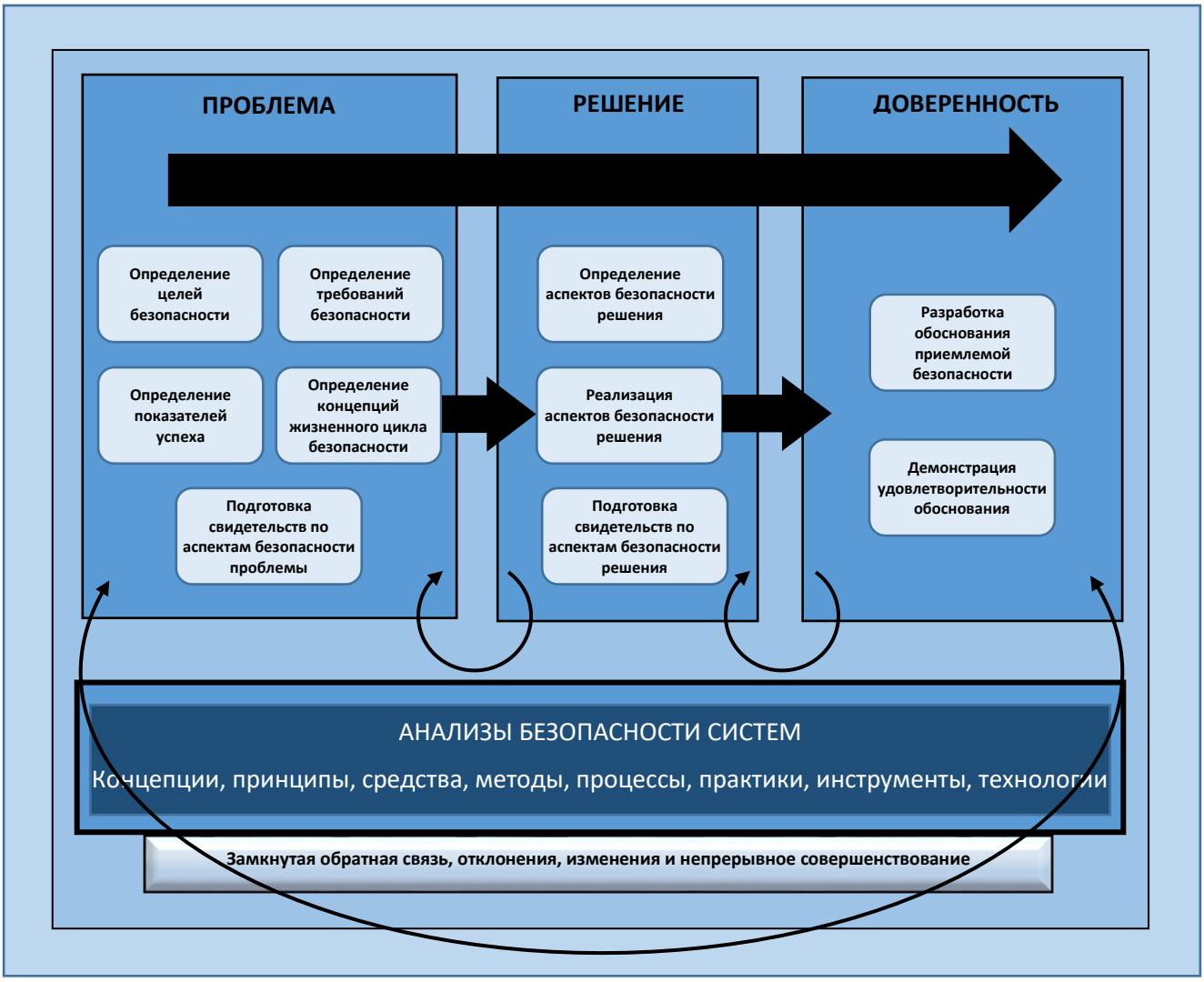

Рис. 10. Основы инженерии безопасности систем

4.1. Контекст проблемы

Контекст проблемы определяет основу для создания адекватно безопасной системы. Основное внимание в нем уделяется опасениям заинтересованных сторон по поводу неприемлемых потерь с учетом их предназначения, операционных возможностей, а также потребностей и интересов в результативности, а также всех связанных с этим ограничений по стоимости, срокам, результативности и рискам. Контекст проблемы позволяет проектной группе сосредоточиться на получении как можно более полного представления о проблеме заинтересованных сторон, изучить все возможные варианты класса решений и выбрать вариант или варианты класса решений, которые будут реализованы. Контекст проблемы включает в себя:

- Определение целей безопасности;

- Определение требований безопасности;
- Определение показателей успеха;
- Определение концепций безопасности жизненного цикла.[52]

Цели безопасности являются основополагающими, устанавливающими и определяют то, что означает адекватная безопасность с точки зрения защиты от потери активов и значимости такой потери. Цели безопасности имеют соответствующие показатели успеха. Эти показатели успеха представляют собой конкретные и поддающиеся измерению критерии в отношении показателей результативности деятельности и интересов заинтересованных сторон. Показатели успеха включают в себя как стойкость защиты, так и уровень доверия в спроектированных возможностях защиты. Эти меры влияют на разработку требований безопасности и утверждений о доверии.

Потребности в защите определяются на основе целей безопасности, концепций жизненного цикла и интересов заинтересованных сторон. Потребности в защите впоследствии преобразуются в требования безопасности заинтересованных сторон и связанные с ними ограничения, а также меры, необходимые для подтверждения выполнения всех требований. Четко определенное и подтверждённое заинтересованными сторонами определение и контекст проблемы обеспечивают основу для всей инженерии систем и инженерии безопасности систем, а также поддерживающей деятельности.

Контекст проблемы может быть интерпретирован в рамках фазы жизненного цикла как основанный на решениях более ранних стадий жизненного цикла, тем самым обеспечивая более точное описание проблемы и связанных с ней ограничений. Например, требования заинтересованных сторон могут быть *решением* на ранней фазе жизненного цикла, которое затем ограничивает деятельность, осуществляемую на более поздних стадиях жизненного цикла.

4.2. Контекст решения

Контекст решения устанавливает аспекты безопасности и ограничения для архитектуры и проекта системы, которые (1) удовлетворяют требованиям и целям контекста проблемы, (2) реализуют проект системы и (3) дают достаточные свидетельства, чтобы продемонстрировать, что требования и цели контекста проблемы были удовлетворены.[53] Контекст решения основан на сбалансированной упреждающей и реактивной стратегии[54] защиты безопасности системы, которая осуществляет контроль за событиями, условиями, потерей активов и значимостью потерь в той степени, в какой это возможно, практически осуществимо и приемлемо для заинтересованных сторон. Контекст решения включает:

- Определение аспектов безопасности решения;
- Реализация аспектов безопасности решения;

---

[52] Термин *«концепция безопасности жизненного цикла»* относится к процессам и действиям, связанным с системой на протяжении всего жизненного цикла (от разработки концепции до вывода из эксплуатации) с учетом конкретных соображений безопасности. Она является расширением концепции эксплуатации и включает процессы и работы, связанные с разработкой, прототипированием, оценкой альтернативных решений, обучением, логистикой, поддержкой, обеспечением, развитием, модернизацией, ремонтом и утилизацией. Каждая концепция жизненного цикла имеет одно или несколько соображений и ограничений безопасности, которые должны быть полностью интегрированы в жизненный цикл, чтобы обеспечить достижение целей безопасности системы. Концепции безопасности жизненного цикла включают в себя концепции, применяемые при получении и управлении программами. Концепции безопасности жизненного цикла могут влиять на такие факторы, как запросы на информацию, запросы на предложение, описания работ, выбор источников, среды разработки и тестирования, операционные среды, цепочки поставок, вспомогательные инфраструктуры, дистрибуция, логистика, поддержка, обучение, разрешения и фоновые проверки.

[53] Ограничения безопасности преобразуются и включаются в требования к проектированию системы с помощью тегов метаданных для определения значимости безопасности

[54] Стратегия защиты безопасности системы соответствует общей концепции безопасного функционирования. Концепция безопасного функционирования, определенная в контексте проблемы, представляет собой стратегию упреждающей и реактивной возможности защиты на протяжении всего жизненного цикла системы (Раздел D.2). Цель этой стратегии состоит в том, чтобы обеспечить свободу от конкретных опасений, связанных с потерями активов и их последствиями.

- Подготовка свидетельств для аспектов безопасности решения.

Аспекты безопасности решения включают в себя разработку стратегии защиты системы; выделенные, декомпозированные и выведенные требования безопасности; представления архитектуры безопасности; проект безопасности; аспекты безопасности, возможности и ограничения в процедурах жизненного цикла системы; и меры по проверке показателей безопасности. Аспекты безопасности решения реализуются при реализации проекта системы в соответствии с архитектурой системы и при удовлетворении требованиям безопасности. Свидетельства, связанные с аспектами безопасности решения, получаются с точностью и строгостью, зависящими от уровня доверия[55], определяемого целями безопасности. Свидетельства доверия получаются стандартными методами проверки проектирования систем (такими, как анализ, демонстрация, инспекция, тестирование и оценка) и дополнительными методами подтверждения соответствия, применяемыми в соответствии с требованиями заинтересованных сторон. Применение контекста решения может интерпретироваться как предоставление части решения, ограничивающей следующую итерацию контекста проблемы.

4.3. Контекст доверенности

Контекст доверенности - это контекст принятия решений, который обеспечивает основанную на свидетельствах демонстрацию - посредством аргументации - того, что представляющая интерес система считается заслуживающей доверия (или нет) на основе набора утверждений, вытекающих из целей безопасности. Этот контекст состоит из:

- Разработки и поддержания обоснования доверия;
- Демонстрации того, что обоснование доверия удовлетворительно.

Контекст доверенности основан на понятии обоснования доверия. Обоснование доверия - это хорошо определенный и структурированный набор аргументов и совокупность свидетельств, показывающих, что система удовлетворяет конкретным утверждениям.[56] Обоснование доверия представляет собой аргументированные, проверяемые артефакты, которые подтверждают заявление о том, что утверждение верхнего уровня или набор утверждений удовлетворены, включая систематизированную аргументацию и лежащие в её основе свидетельства и явные предположения, которые поддерживают утверждения [30]. Утверждения могут строиться из подутверждений. Для данной стадии жизненного цикла системы результат может в достаточной степени удовлетворять подутверждению или набору подутверждений, таких как подутверждение, что требования заинтересованных сторон являются достаточно всеобъемлющими, чтобы поддержать утверждение о том, что реализованная система является адекватно безопасной.

Обоснования доверия используются для демонстрации того, что система обладает каким-либо сложным эмерджентным свойством, таким как, защищенность, безопасность, устойчивость, надежность или живучесть. Эффективное обоснование доверия к безопасности содержит основополагающие утверждения по безопасности, вытекающие из целей обеспечения, достоверные и релевантные свидетельства, подтверждающие эти утверждения, и веские аргументы, которые связывают различные свидетельства с поддерживаемыми утверждениями по безопасности. В результате получается убедительное заявление о том, что адекватная безопасность была достигнута и обусловлена потребностями и ожиданиями заинтересованных сторон.

Обоснования доверия обычно включают в себя вспомогательную информацию, такую как предположения, ограничения и умозаключения, которые влияют на процесс аргументации. В рамках

[55] Доверие - это мера уверенности, связанная с данным требованием. По мере повышения уровня доверия увеличивается и объем, глубина и строгость, связанные с проводимыми методами и анализами (Приложение F).
[56] Институт программной инженерии, Университет Карнеги-Меллон.

разработки обоснования доверия предметный экспертный анализ определяет, что все требования безопасности подтверждаются свидетельствами и аргументами, связывающими свидетельства с утверждениями. Обоснования доверия должны поддерживаться в соответствии с отклонениями на протяжении всего процесса разработки.

Конкретная форма обоснования доверия и уровень строгости и формальности в получении требуемого свидетельства - это факторы пространства соглашений. Они включают целевой (т.е. желаемый) уровень доверия, характер последствий, для которых требуется доверие, а также размер и сложность измерений, которые влияют на определение доверенности. Обоснование доверия является проектной конструкцией и должно регулироваться для обеспечения того, чтобы затраченные усилия оправдывались потребностью свидетельства в определении доверенности. Утверждения о доверии являются ключевым фактором доверенности и разрабатываются на основе целей безопасности и связанных с ними показателей успеха независимо от реализации системы и подтверждающих свидетельств. Доверенность и доверие рассматриваются далее в приложении F.

ОСНОВЫ ИНЖЕНЕРИИ БЕЗОПАСНОСТИ СИСТЕМ - ПОЧЕМУ ЭТО ВАЖНО

Установление контекстов проблемы, решения и доверенности в качестве ключевых компонентов основ инженерии безопасности систем помогает обеспечить, что безопасность системы основана на достижении достаточно полного понимания проблемы, определяемого набором целей безопасности заинтересованных сторон, соображений безопасности, потребностей в защите и требований безопасности. Это понимание имеет важное значение для разработки эффективных решений в области безопасности, т.е. системы, которая является достаточно доверенной и адекватно безопасной для защиты активов заинтересованных сторон с точки зрения потерь и связанных с ними последствий.

Ссылки

[1] Executive Order 14028 (2021), Improving the Nation's Cybersecurity. (The White House, Washington, DC), May 12, 2021. https://www.federalregister.gov/d/2021-10460

[2] Neumann P (2004) Principled Assuredy Trusterly Composable Architectures, CDRL A001 Final Report, SRI International, Menlo Park, CA. http://www.csl.sri.com/users/neumann/chats4.pdf

[3] Sillitto H, Martin J, McKinney D, Griego R, Dori D, Krob D, Godfrey P, Arnold E, Jackson L (2019) INCOSE-TP-2020-002-06, Systems Engineering and System Definitions. https://www.incose.org/docs/default-source/default-document-library/incose-se-definitions-tp 2020 002 06.pdf? sfvrsn=b1049bc6_0

[4] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2015) ISO/IEC/IEEE 15288:2015 – Systems and software engineering – Systems life cycle processes.https://www.iso.org/standard/63711.html

[5] Anderson R (2020) Security Engineering: A Guide to Building Dependable Distributed Systems (Wiley) 3rd Ed.

[6] National Aeronautics and Space Administration (2011) System Safety Handbook Volume 1: System Safety Framework and Concepts for Implementation, NASA/SP-2010-580, Ver. 1.0.https://ntrs.nasa.gov/api/citations/20120003291/downloads/20120003291.pdf

[7] Dove R, Willett K, McDermott T, Dunlap H, MacNamara DP, Ocker C (2021) Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundational Concepts. INCOSE International Symposium. https://doi.org/10.1002/j.2334-5837.2021.00832.x

[8] Office of Management and Budget (2018) Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M-19-03, December 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

[9] Maier M (1998) Architecting Principles for Systems-of-Systems. The Aerospace Corporation. https://onlinelibrary.wiley.com/doi/abs/10.1002 / % 28SICI%291520 - 6858%281998%291%3A4%3C267%3A%3AAID-SYS3%3E3.0. CO%3B2-D

[10] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2019) ISO/IEC/IEEE 21841:2019 – Systems and software engineering – Taxonomy of systems of systems.

https://www.iso.org/standard/71957.html

[11] Madni AM (2017) Transdisciplinary Systems Engineering: Exploiting Convergence in a Hyper-Connected World. Springer International Publishing. https://link.springer.com/book/10.1007/978-3-319-62184-5

[12] International Council On Systems Engineering (2022) What Is Systems Engineering? https://www.incose.org/systems-engineering

[13] BKCASE Editorial Board (2019) The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.0, ed Cloutier RJ (The Trustees of the Stevens Institute of Technology, Hoboken, NJ). https://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge__(SEBoK)

[14] International Council On Systems Engineering (2022) Systems Engineering Principles. https://www.incose.org/products-and-publications/se-principles –

[15] International Council on Systems Engineering (2015) System Engineering Handbook – A Guide for System Engineering Life Cycle Processes and Activities, INCOSE TP-2003-002-04. https://www.incose.org/products-and-publications/se-handbook

[16] International Council on Systems Engineering (2022) Systems Engineering Vision 2035. https://www.incose.org/about-systems-engineering/se-vision-2035

[17] National Aeronautics and Space Administration (2017) Systems Engineering Handbook, NASA SP-2016-6105, Rev 2. https://www.nasa.gov/sites/default/files/atoms/files/nasa_systems_engineering_handbook_0. PDF

[18] National Aeronautics and Space Administration (2016) Expanded Guidance for NASA Systems Engineering. Vol. 1: Systems Engineering Practices. https://ntrs.nasa.gov/citations/20170007238

[19] National Aeronautics and Space Administration (2016) Expanded Guidance for NASA Systems Engineering. Vol. 2: Crosscutting Topics, Special Topics, and Appendices https://ntrs.nasa.gov/citations/20170007239

[20] Schroeder MD, Clark DD, and Saltzer JH (1977) The Multics Kernel Design Project. Proceedings of Sixth ACM Symposium on Operating Systems Principles. https://web.mit.edu/Saltzer/www/publications/rfc/csr-rfc-140.pdf

[21] Levin T, Irvine C, Benzel T, Bhaskara G, Clark P, and Nguyen T (2007) Design Principles and Guidelines for Security, Technical Report NPS-CS-07-014. Naval Postgraduate School. https://nps.edu/web/c3o/technical-reports

[22] Herley C (2016) Unfalsifiability of Security Claims. Microsoft Research, Proceedings of the National Academy of Sciences. https://doi.org/10.1073/pnas.1517797113

[23] National Aeronautics and Space Administration (2014) System Safety Handbook Vol. 2: System Safety Concepts, Guidelines, and Implementation Examples, NASA/SP-2014-612, Ver. 1.0. https://ntrs.nasa.gov/api/citations/20150015500/downloads/20150015500.pdf

[24] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2017) ISO/IEC/IEEE 24765:2017 – Systems and software engineering – Vocabulary. https://www.iso.org/standard/71952.html

[25] International Organization for Standardization (2013) ISO 16290:2013 – Space systems – Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment. https://www.iso.org/standard/56064.html

[26] Avizienis A, Laprie J, Randell B, and Landwehr C (2004) Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1.

[27] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2019) ISO/IEC/IEEE 21840:2019 – Systems and software engineering – Guidelines for the utilization of ISO/IEC/IEEE 15288 in the context of system of systems (SoS). https://www.iso.org/standard/71956.html

[28] International Organization for Standardization (2009) ISO Guide 73:2009 – Risk management – Vocabulary. https://www.iso.org/standard/44651.html

[29] McEvilley M (2015) Towards a Notional Framework for Systems Security Engineering. NDIA 18th Annual Systems Engineering Conference.

[30] International Organization for Standardization/International Electrotechnical Commission (2011) ISO/IEC 15026-2:2011 – Systems and software engineering – Systems and software assurance – Part 2: Assurance case.
https://www.iso.org/standard/80625.html

[31] International Organization for Standardization /International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2018) ISO/IEC/IEEE 29148:2018, Systems and software engineering – Life cycle processes – Requirements engineering.
https://www.iso.org/standard/72089.html

[32] International Council on Systems Engineering (2022) Guide to Writing Requirements, Rev. 3.1.
https://connect.incose.org/pages/store.aspx

[33] Young W, Leveson NG (2014) An Integrated Approach to Safety and Security based on Systems Theory. Communications of the ACM. Volume 57, Issue 2, 2014, pp. 31-35.
https://dl.acm.org/doi/10.1145/2556938

[34] Department of Defense Standard Practice (2012) MIL-STD-882E System Safety.

[35] Uchenick GM, Vanfleet WM (2005) Multiple Independent Levels of Safety and Security: High Assurance Architecture for MSLS/MLS. IEEE Military Communications Conference, pp. 610-614 Vol. 1.

[36] Leveson NG (2011) Engineering a Safer World – Systems Thinking Applied to Safety, Chapter 14, MIT Press, ISBN 978-0-262-01662-9.
https://direct.mit.edu/books/book/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied

[37] Anderson J (1972) Computer Security Technology Planning Study, Technical Report ESD-TR-73- 51. Air Force Electronic Systems Division, Hanscom AFB.
https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72a.pdf

[38] Department of Defense (DoD) Standard (1985) 5200.28-STD Trusted Computer System Evaluation Criteria.
https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf

[39] Hild D, McEvilley M, Winstead M (2021) Principles for Trustworthy Design of Cyber-Physical Systems. MITRE Technical Report, MTR210263.
https://figshare.com/articles/preprint/Design_Principles_for_Cyber_Physical_Systems_pdf/1 5175605

[40] Saleh JH, Marais KB, and Favaro FM (2014) System safety principles: A multidisciplinary engineering perspective. Journal of Loss Prevention in the Process Industries, Vol. 29.

[41] Sheard S, Konrad M, Weinstock C, and Nichols W (2018) A Complexity Measure for System Safety Assurance. INCOSE International Symposium, Adelaide Australia.
https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2017.00373.x

[42] Neumann P (2000) Practical Architectures for Survivable Systems and Networks. Technical Report, Final Report, Phase Two, Project 1688, SRI International, Menlo Park, California.
http://www.csl.sri.com/neumann/survivability.html

[43] Smith RE (2012) A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles. IEEE Security & Privacy, Vol. 10, No. 6, November/December 2012.

[44] [44] Saltzer JH, Kaashoek MF (2009) Principles of Computer System Design. Morgan Kaufmann Publishers, Burlington, MA.

[45] [45] Moller N, Hansson SO (2008) Principles of Engineering Safety: Risk and Uncertainty Reduction. Reliability Engineering & System Safety, Vol. 93, No. 6, June 2008.

[46] Saltzer JH, Schroeder MD (1975) The Protection of Information in Computer Systems. Proceedings of the IEEE Vol. 63, No. 9, September 1975.
https://www.cs.virginia.edu / ~ evans/cs551/saltzer

[47] Jackson S, Ferris T (2013) Resilience Principles for Engineered Systems. Systems Engineering, Vol. 16, No. 2, July 2013.
https://onlinelibrary.wiley.com/doi/abs/10.1002/sys.21228

[48] Simovici DA, Djeraba C (2008) Partially Ordered Sets. Mathematical Tools for Data Mining: Set Theory, Partial Orders, Combinatorics, Springer.

[49] Adcock R, Jackson S, Singer J, Hybertson D (2020) Principles of Systems Thinking. Stevens Institute of Technology.
https://www.sebokwiki.org/wiki/Principles_of_Systems_Thinking

[50] Schroeder MD (1972) Cooperation of mutually suspicious subsystems in a computer utility. Ph.D. dissertation, M.I.T., Cambridge, MA.
https://web.mit.edu / ~ saltzer/www/publications/TRs+TMs/Multics/TR-104.pdf

[51] Department of Defense (2007) MIL-HDBK-454B, General Guidelines for Electronic Equipment.
https://www.dla.mil/Portals/104/documents/landAndMaritime/v/va/pSMC/documents/IM_MIL_HDBK_454B_151030.pdf

[52] National Security Agency (2002) Technical Report: Information Assurance Technical Framework (IATF), Release 3.1.
https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA606355.xhtml

[53] Ross R, Pillitteri V, Graubart R, Bodeau D, and McQuaid R (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-160 Volume 2, Revision 1.
https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

[54] Lampson BW (1973) A Note on the Confinement Problem. Communications of the ACM 16, 10, pp. 613-615, October 1973.
https://dl.acm.org/doi/10.1145/362375.362389

[55] Popek G (1974) The Principle of Kernel Design. NCC, AFIPS Cong. Proc., Vol. 43.

[56] Benjamin A, et al. (2014) Developing Probabilistic Safety Performance Margins for Unknown and Underappreciated Risks," PSAM-12 International Conf. on Probabilistic Safety and Management, June 2014.

[57] Pagani LP (2004) On the Quantification of Safety Margins. PhD Dissertation, Massachusetts Institute of Technology.

[58] Neumann P (2017) Fundamental Trustworthiness Principles. SRI International, Menlo Park CA.

[59] Bryant WD, Ball RE (2020) Developing the Fundamentals of Aircraft Cyber Combat Survivability: Part 2. Joint Aircraft Survivability Program Office, Aircraft Survivability Journal, Spring 2020.

[60] Ball RE (2003) Основы анализа и проекта боевой живучести летательных аппаратов. 2-й Выпуск. Образовательная серия AIAA.
https://arc.aiaa.org/doi/book/10.2514/4.862519

[61] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2019) ISO/IEC/IEEE 15026-1:2019, Systems and software engineering – Systems and software assurance – Part 1: Concepts and vocabulary.
https://www.iso.org/standard/73567.html

[62] Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, Defense Science Board (2017) Task Force on Cyber Supply Chain.
https://dsb.cto.mil/reports/2010s/DSBCyberSupplyChainExecutiveSummary-Distribution_A.pdf

[63] Saydjari OS (2018) Engineering Trustworthy Systems: Get Cybersecurity Design Right the First Time, McGraw-Hill.
https://books.apple.com/us/book/engineering-trustworthy-systems-get-cybersecurity-design/id1413527360

[64] Rinehart DJ, Knight JC, and Rowanhill J (2017) Understanding What it Means for Assurance Cases to Work. NASA/CR–2017-219582.
https://catalog.libraries.psu.edu/catalog/20766348

[65] Goal Structuring Notation Community Standard, Version 2 (2018) The Assurance Case Working Group.
https://scsc.uk/r141B:1? t=1

[66] National Aeronautics and Space Administration (2019) AdvoCATE: Assurance Case Automation Toolset. https://ti.arc.nasa.gov/tech/rse/research/advocate

[67] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[68] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020.
https://doi.org/10.6028/NIST.SP.800-53r5

[69] Snyder D, Powers JD, Bodine-Baron E, Fox B, Kendrick L, Powell MH (2015) Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles. Rand Corporation.
https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf

[70] Department of Defense Instruction 5200.39 (2020) Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E).
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520039p.pdf

[71] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2011) ISO/IEC/IEEE 42010 – Systems and Software Engineering – Architecture description.
https://www.iso.org/standard/50508.html

[72] International Organization for Standardization (2020) ISO 19014:2020 – Earth-moving machinery – Functional safety – Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system.
https://www.iso.org/standard/70718.html

[73] International Organization for Standardization (1989) ISO 7498-2:1989 – Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. https://www.iso.org/standard/14256.html

[74] Institute of Electrical and Electronics Engineers (2012) Std. 828-2012 – IEEE Standard for Configuration Management in Systems and Software Engineering, IEEE Computer Society. https://standards.ieee.org/standard/828-2012.html

[75] International Organization for Standardization (1998) ISO 14258:1998 – Industrial automation systems – Concepts and rules for enterprise models.
https://www.iso.org/standard/24020.html

[76] International Organization for Standardization (2011) ISO 27026:2011 – Space systems – Programme management – Breakdown of project management structures.
https://www.iso.org/standard/43961.html

[77] American National Standards Institute/American Institute of Aeronautics and Astronautics (2018) G-043B-2018, Guide to The Preparation of Operational Concept Documents.
https://webstore.ansi.org/Standards/AIAA/ANSIAIAA043B2018 –

[78] International Organization for Standardization (2015) ISO 9000:2015 – Quality management systems – Fundamentals and vocabulary.
https://www.iso.org/standard/45481.html

[79] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2017) ISO/IEC/IEEE 15939:2017 – Systems and software engineering – Measurement process.
https://www.iso.org/standard/71197.html

[80] International Organization for Standardization/International Electrotechnical Commission (2009) ISO/IEC 10746-2:2009 – Information technology – Open distributed processing –Reference model: Foundations – Part 2. https://www.iso.org/standard/55723.html

[81] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2021) ISO/IEC/IEEE DIS 24748-6 – Systems and Software Engineering – Life Cycle Management – Part 6: Systems and Software Integration.
https://www.iso.org/standard/81563.html

[82] E-Government Act [incl. FISMA] (P.L. 107-347), December 2002.
https://www.govinfo.gov/app/details/PLAW-107publ347

[83] International Organization for Standardization (2012) ISO 13008:2012 – Information and documentation – Digital records conversion and migration process.
https://www.iso.org/standard/52326.html

[84] International Organization for Standardization/Technical Report (2001) ISO/TR 18307:2001 – Health informatics – Interoperability and compatibility in messaging and communication standards – Key characteristics. https://www.iso.org/standard/33396.html

[85] International Organization for Standardization/International Electrotechnical Commission (2020) ISO/IEC 19989-3:2020(en) – Information security – Criteria and methodology for security evaluation of biometric systems – Part 3, Presentation attack detection.
https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:19989:-3:ed-1:v1:en

[86] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2017) ISO/IEC/IEEE 12207:2017 – Systems and software engineering

– Software life cycle processes.
https://www.iso.org/standard/63712.html

[87] International Organization for Standardization (2019) ISO 17757:2019 – Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety. https://www.iso.org/standard/76126.html

[88] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2019) ISO/IEC/IEEE 21839:2019 – Systems and software engineering – System of systems (SoS) considerations in life cycle stages of a system. https://www.iso.org/standard/71955.html

[89] Committee on National Security Systems (2022) Instruction No. 4009, Committee on National Security Systems (CNSS) Glossary.
https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[90] International Organization for Standardization/International Electrotechnical Commission (2016) ISO/IEC TR 29110-1:2016, Systems and software engineering – Lifecycle profiles for Very Small Entities (VSEs) – Part 1: Overview.
https://www.iso.org/standard/62711.html

[91] International Organization for Standardization/International Electrotechnical Commission (2011) ISO/IEC 25010:2011 – Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models.
https://www.iso.org/standard/35733.html

[92] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2021) ISO/IEC/IEEE 24774:2021 – Systems and software engineering – Life cycle management – Specification for process description. https://www.iso.org/standard/78981.html

[93] International Organization for Standardization/Society of Automotive Engineers (2021) ISO/SAE 21434:2021 – Road vehicles – Cybersecurity engineering.
https://www.iso.org/standard/70918.html

[94] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2018) ISO/IEC/IEEE 24748-2:2018 – Systems and software engineering – Life cycle management – Part 2: Guidelines for the application of ISO/IEC/IEEE 15288 (System life cycle processes).
https://www.iso.org/standard/70816.html

[95] Institute of Electrical and Electronics Engineers (2014) IEEE Std 15288.1TM-2014 –Standard for Application of Systems Engineering on Defense Programs, IEEE Computer Society. https://ieeexplore.ieee.org/stamp/stamp.jsp? arnumber=7105318

[96] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2018) ISO/IEC/IEEE 24748-1:2018 – Systems and software engineering – Life cycle management – Part 1: Guidelines for life cycle management. https://www.iso.org/standard/72896.html

[97] International Council on Systems Engineering (2022) Needs, Requirements, Verification, Validation Lifecycle Manual. https://connect.incose.org/pages/store.aspx

[98] International Organization for Standardization/International Electrotechnical Commission (2015) ISO/IEC 15026-3:2015 – Systems and software engineering – Systems and software assurance – Part 3: System integrity levels. https://www.iso.org/standard/64842.html

[99] International Organization for Standardization/International Electrotechnical Commission (2021) ISO/IEC 15026-4:2021 – Systems and software engineering – Systems and software assurance – Part 4: Assurance in the life cycle. https://www.iso.org/standard/74396.html

[100] International Organization for Standardization/International Electrotechnical Commission (2008) ISO/IEC 21827:2008 – Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®).
https://www.iso.org/standard/44716.html

[101] International Organization for Standardization/Technical Specification (2010) ISO/TS 18152:2010 – Ergonomics of human-system interaction – Specification for the process assessment of human-system issues. https://www.iso.org/standard/56174.html

[102] International Organization for Standardization/International Electrotechnical Commission (2010) ISO/IEC TR 25060:2010 – Systems and software engineering – Systems and software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability: General framework for usability-related information.
https://www.iso.org/standard/35786.html

[103] International Organization for Standardization/International Electrotechnical Commission (2014) ISO/IEC 25063:2014 – Systems and software engineering – Systems and software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability: Context of use description.
https://www.iso.org/standard/35789.html

[104] International Organization for Standardization (2010) ISO 9241-210:2010 – Ergonomics of human-system interaction – Part 210: Human-centered design for interactive systems.
https://www.iso.org/standard/52075.html

[105] International Organization for Standardization/International Electrotechnical Commission (2019) ISO/IEC 25030:2019 – Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Quality Requirements.
https://www.iso.org/standard/72116.html

[106] International Organization for Standardization/International Electrotechnical Commission (2009) ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
https://www.iso.org/standard/72891.html

[107] International Organization for Standardization/International Electrotechnical Commission (2008) ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.
https://www.iso.org/standard/72892.html

[108] International Organization for Standardization/International Electrotechnical Commission (2008) ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.
https://www.iso.org/standard/46413.html

[109] International Organization for Standardization/International Electrotechnical Commission (2011) ISO/IEC 27034-1:2011 – Information technology – Security techniques – Application security – Part 1: Overview and concepts.
https://www.iso.org/standard/44378.html

[110] International Council on Systems Engineering (2010) Systems Engineering Measurement Primer – INCOSE TP-2010-005-02. https: https://www.incose.org/docs/default-

source/ProductsPublications/systems-engineering-measurement-primer---december-2010.pdf

[111] International Organization for Standardization/International Electrotechnical Commission (2021) ISO/IEC 27036-1:2021 – Cybersecurity – Supplier relationships – Part 1: Overview and concepts. https://www.iso.org/standard/82905.html

[112] International Organization for Standardization/International Electrotechnical Commission (2022) ISO/IEC 27036-2:2022 – Cybersecurity – Supplier relationships – Part 2: Requirements. https://www.iso.org/standard/82060.html

[113] International Organization for Standardization/International Electrotechnical Commission (2013) ISO/IEC 27036-3:2013 – Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security. https://www.iso.org/standard/59688.html

[114] International Organization for Standardization/International Electrotechnical Commission (2015) ISO/IEC 16350:2015 – Information technology – Systems and software engineering – Application management. https://www.iso.org/standard/57922.html

[115] International Organization for Standardization/International Electrotechnical Commission (2006) ISO/IEC 14764:2006 – Software Engineering – Software Life Cycle Processes – Maintenance. https://www.iso.org/standard/39064.html

[116] International Organization for Standardization (2018) ISO 10004:2018 – Quality management – Customer satisfaction – Guidelines for monitoring and managing. https://www.iso.org/standard/71582.html

[117] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2019) ISO/IEC/IEEE 42020:2019 – Software, systems and enterprise – Architecture processes. https://www.iso.org/standard/68982.html

[118] Institute of Electrical and Electronics Engineers (2018) Std. P1012, IEEE Standard for System, Software, and Hardware Verification and Validation, IEEE Computer Society. https://standards.ieee.org/ieee/1012/7324

[119] International Organization for Standardization/International Electrotechnical Commission (2013) ISO/IEC 29119-1:2013 – Software Testing: Concepts and Definitions. https://www.iso.org/standard/45142.html

[120] International Organization for Standardization/International Electrotechnical Commission (2021) ISO/IEC 29119-2:2021 – Software and systems engineering – Software testing – Part 2: Test processes. https://www.iso.org/standard/79428.html

[121] International Organization for Standardization/International Electrotechnical Commission (2021) ISO/IEC 29119-3:2021 – Software and systems engineering – Software testing – Part 3: Test documentation. https://www.iso.org/standard/79429.html

[122] International Organization for Standardization/International Electrotechnical Commission (2021) ISO/IEC 29119-4:2021 – Software and systems engineering – Software testing –Part 4: Test techniques. https://www.iso.org/standard/60245.html

[123] Roedler G, Jones C (2005) Technical Measurement, International Council on Systems Engineering, INCOSE TP-2003-020-01. https://www.incose.org/docs/default-source/ProductsPublications/technical-measurement-guide---dec2005.pdf? sfvrsn=4&sfvrsn=4

[124] International Organization for Standardization/International Electrotechnical Commission (2021) ISO/IEC 16085:2021 –Systems and software engineering–Life cycle processes –Risk management. https://www.iso.org/standard/74371.html

[125] International Organization for Standardization(2018)ISO 31000:2018 –Risk management– Guidelines. https://www.iso.org/standard/65694.html

[126] International Organization for Standardization (2017) ISO 10007:2017 –Quality management systems – Guidelines for configuration management.
https://www.iso.org/standard/70400.html

[127] Electronic Industries Alliance (2019) EIA 649C, Configuration Management Standard. https://www.sae.org/standards/content/eia649c

[128] [128]International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2019) ISO/IEC/IEEE 15289:2019 –Systems and software engineering – Content of life-cycle information items(documentation). https://www.iso.org/standard/74909.html

[129] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers(2015)ISO/IEC/IEEE 26531:2015 – Systems and software engineering – Content management for product life-cycle, user and service management documentation.
https://www.iso.org/standard/43090.html

[130] International Organization for Standardization (2015) ISO 9001:2015 – Quality management systems – Requirements. https://www.iso.org/standard/62085.html

[131] Institute of Electrical and Electronics Engineers (2014) IEEE Std. 730-2014 – IEEE Standard for Software Quality Assurance Processes.
https://standards.ieee.org/ieee/730/5284

[132] Department of Defense (2020) DoD Directive 8140.01 – Cyberspace Workforce Management.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.PDF?ver=si7QmZONMCW2tStUt4ws3Q%3D%3D

[133] Petersen R, Santos D, SmithMC, WetzelKA,Witte G(2020) Workforce Frameworkfor Cybersecurity (NICE Framework). (NationalInstitute of Standards and Technology,Gaithersburg, MD), NIST SP 800-181 Revision 1.
https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

[134] International Organization for Standardization/International Electrotechnical Commission(2015) ISO/IEC 33002:2015 – Information technology –Process assessment –Requirements for performing process assessment.
https://www.iso.org/standard/54176.html

[135] Stember, M (1991) Advancing thesocialsciences through theinterdisciplinary enterpriseTheSocialScience Journal, 28:1, 1-14.

Приложение A. Акронимы

ACM
Ассоциация вычислительной техники

AIAA
Американский институт аэронавтики и астронавтики

ANSI
Американский национальный институт стандартов

ASARP
Безопасно настолько, насколько это целесообразно и практически возможно

CD
Кросс-доменные решения

CNSS
Комитет по системам национальной безопасности

COTS
Коммерческий коробочный продукт

CUI
Контролируемая неклассифицированная информация

DoD
Министерство обороны

EIA
Альянс компаний электронной промышленности

EO
Правительственное распоряжение

FISMA
Федеральный закон о модернизации информационной безопасности

FOIA
Закон о свободе информации

FuSE
Будущее системного проектирования

GSN
Нотация структурирования целей

IEC
Международная электротехническая комиссия

IEEE
Институт инженеров электротехники и электроники

INCOSE
Международный совет по системному проектированию

ISO
Международная организация по стандартизации

ИТ
Информационная технология

ITL
Лаборатория информационных технологий

MOE
Показатели эффективности

MOP
Показатели результативности

НАСА
Национальное управление по аэронавтике и исследованию космического пространства

NICE
Национальная инициатива по просвещению в области кибербезопасности

NIST
Национальный институт стандартов и технологий

NDIA
Национальная оборонно-промышленная ассоциация

OMB
Министерство управления и бюджета

OT
Операционная технология

SEBoK
Свод знаний по системному проектированию

SecDOP
Порядок приоритетности проектирования системы безопасности

SoS
Система систем

SP
Специальная публикация

SSE
Проектирование системы безопасности

SWaP
Размер, вес и энергия

USC
Кодекс Соединенных Штатов

Приложение B. Глоссарий

abstraction, абстракция
Представление объекта, которое фокусируется на информации, имеющей отношение к конкретной цели, и игнорирует остальную информацию. [24]

acquirer, покупатель
Заинтересованная сторона, которая приобретает или закупает продукт или услугу у поставщика.

acquisition, приобретение
Процесс получения системы, продукта или сервиса. [4]

activity, действие
Набор согласованных задач процесса. [4]

adequate security (systems), адекватно безопасная (система)
Соответствует минимально допустимым уровням безопасности, определенным анализом, опытом или сочетанием того и другого, и является настолько безопасной, насколько это практически возможно (т.е. постепенное повышение уровня безопасности потребует недопустимого или непропорционального ухудшения достижения других целей системы, например, результативности системы, или нарушит системные ограничения).

adverse consequence, негативное последствие
Нежелательное последствие, связанное с потерей. [61]

adversity, неблагоприятные условия
Условия, которые могут привести к потере активов (например, угрозы, атаки, уязвимости, опасности, сбои и воздействия).

agreement, соглашение
Взаимное признание условий, на которых осуществляются рабочие отношения (например, меморандум о соглашении или контракт). [4]

anomaly, аномалия
Состояние, отклоняющееся от ожиданий, основанных на спецификациях требований, проектной документации, пользовательских документах или стандартах, а также на чьем-либо восприятии или опыте. [24]

anti-tamper, защита от вмешательства
Работы по проектированию систем, направленные на предотвращение или задержку использования критически важной программной информации в оборонных системах США во внутренних и экспортных конфигурациях, препятствующие разработке контрмер, непреднамеренной передаче технологий или изменению системы из-за реверсивной техники. [70]

См. вмешательство.

architecture, архитектура
Фундаментальные концепции или свойства, относящиеся к системе в ее окружении, воплощенные в ее элементах, взаимосвязях и принципах ее проектирования и эволюции. [71]

См. архитектура безопасности.

architecture (system), архитектура (системы)
Фундаментальные концепции или свойства системы в ее окружении, воплощенные в ее элементах, взаимосвязях, а также в принципах ее проектирования и эволюции. [71]

architecture description, описание архитектуры
Рабочий продукт, используемый для выражения архитектуры. [71]

architecture framework, основа архитектуры
Конвенции, принципы и практика для описания архитектур, установленные в конкретной области применения и/или сообществе заинтересованных сторон. [71]

architecture view, представление архитектуры
Рабочий продукт, выражающий архитектуру системы с точки зрения конкретных системных потребностей. [71]

architecture viewpoint, рассмотрение архитектуры
Рабочий продукт, устанавливающий соглашения для построения, интеграции и использования представлений архитектуры для формирования конкретных системных интересов. [71]

artifact, образец
Рабочие продукты, которые создаются и используются в ходе проекта для фиксации и передачи информации (например, модели, исходный код). [72]

aspect, аспект
Части, особенности и характеристики, используемые для описания, рассмотрения, интерпретации или оценки чего-либо.

asset, актив
Все, что имеет ценность для человека или организации. [24]

Примечание 1: Активы имеют взаимосвязанные характеристики, которые включают ценность, критичность и степень, в которой на них полагаются для достижения предназначения и целей деятельности организации. Исходя из этих характеристик, в решениях, используемых организацией, должны быть предусмотрены соответствующие средства защиты.

Примечание 2: Актив может быть материальным (например, физический объект, такой как аппаратное обеспечение, программное обеспечение, микропрограмма, вычислительная платформа, сетевое устройство или другие технологические компоненты) или нематериальным (например, информация, данные, товарный знак, авторское право, патент, интеллектуальная собственность, имидж или репутация).

assurance, доверие
Основания для обоснованной уверенности в том, что заявленное было или будет достигнуто. [61]

Примечание 1: Доверие, как правило, предоставляется относительно набора конкретных утверждений. Область и направленность таких утверждений могут различаться (например, утверждения безопасности, утверждения защищённости), и сами утверждения могут быть взаимосвязаны.

Примечание 2: Доверие достигается с помощью технологий и методов, которые дают достоверные свидетельства для обоснования утверждений.

assurance case, пример доверия
Аргументированный, проверяемый образец, созданный в поддержку утверждения о том, что его высокоуровневое утверждение (или набор утверждений) удовлетворено, включая систематизированную аргументацию и лежащие в его основе свидетельства и явные предположения, которые поддерживают утверждение(я). [61]

assurance evidence, свидетельство доверия
Информация, на основании которой обосновываются решения относительно доверия, доверенности и риска решения.

Примечание: Подтверждающие свидетельства относятся только к согласованному набору утверждений. С точки зрения безопасности основное внимание уделяется свидетельствам доверия для утверждений, касающихся безопасности, в то время как другие инженерные дисциплины могут иметь свою собственную направленность (например, защищенность).

availability, доступность
Свойство быть доступным и пригодным для использования по требованию авторизованной сущности. [73]

baseline, базовый
Формально утвержденная версия элемента конфигурации, независимо от носителя информации, формально назначенная и зафиксированная в конкретное время в течение жизненного цикла элемента конфигурации. [74]

Примечание: Процесс проектирования создает множество образцов, которые поддерживаются в качестве базовых в течение всего процесса проектирования и после его завершения. Процессы управления конфигурацией при проектировании управляют базовыми образцами. В качестве примеров можно привести базовые требования заинтересованных сторон, базовые требования к системе, базовые архитектуры/конструкции и базовые конфигурации.

behavior, поведение
Способ, которым сущность функционирует, такой как действие, реакция или взаимодействие.

Как элемент системы, система или система систем действует, реагирует и взаимодействует. [75]

body of evidence, набор свидетельств
Совокупность свидетельств, используемых для обоснования доверия, доверенности и риска, связанных с системой.

breakdown structure, структура разбиения (элементов)
Основа для эффективного управления некоторыми аспектами действий для программы или проекта. [76]

Примечание: Примеры включают структуру разбиения работ, декомпозицию определенной области проекта на постепенно более низкие уровни, состоящие из элементов работ, и структуру разбиения продукта (т.е. декомпозицию продукта на его компоненты).

claim, утверждение
Истинно-ложное описание ограничений на значения однозначно определенного свойства, называемого свойством утверждения; и ограничения в отношении неопределенности значений свойства, подпадающего под эти ограничения, в течение срока действия утверждения в заявленных условиях. [61]

complex system, сложная система
Система, в которой существуют нетривиальные связи между причиной и следствием: каждое следствие может быть обусловлено несколькими причинами; каждая причина может способствовать нескольким следствиям; причины и следствия могут быть связаны в виде контуров обратной связи, как положительной, так и отрицательной; и причинно-следственные цепи являются циклическими и сильно запутанными, а не линейными и разделяемыми. [3]

component, компонент

См. *Элемент системы.*

concept of operations, концепция действий
Вербальное и графическое описание в общих чертах предположений или намерений организации в отношении действий или серии действий в отношении новых, измененных или существующих систем организации. [77]

Примечание 1: Концепция действий часто воплощается в долгосрочных стратегических планах и ежегодных планах деятельности. В последнем случае концепция действий в плане охватывает ряд взаимосвязанных действий, которые должны проводиться одновременно или последовательно для достижения цели деятельности организации.

Примечание 2: Концепция действий обеспечивает основу для ограничения области деятельности, возможностей системы, интерфейсов и среды деятельности.

concept of secure function, концепция безопасного функционирования
Стратегия достижения безопасного функционирования системы, которая воплощает в себе возможности упреждающей и реактивной защиты системы.

Примечание 1: Эта стратегия направлена на предотвращение, минимизацию или обнаружение событий и условий, которые могут привести к потере актива и вытекающим из этого неблагоприятным последствиям; предотвращение, минимизацию или выявление потери активов или неблагоприятных последствий для активов; непрерывное обеспечение возможностей системы на приемлемом уровне, несмотря на воздействие угроз или неопределенности; и устранение неблагоприятных последствий для активов в целях восстановления полных возможностей системы или восстановление возможностей системы до некоторого приемлемого уровня.

Примечание 2: Концепция безопасного функционирования адаптирована из исторических и других концепций безопасных системы, таких как философия защиты, теория проектирования и эксплуатации и теория соответствия.

concern, интерес
Вопрос, представляющий интерес или важность для заинтересованной стороны. [71]

concern (system), интерес (системный)
Интерес в системе, относящейся к одной или нескольким заинтересованным сторонам. [71]

configuration item, элемент конфигурации
Элемент или объединение аппаратных средств, программного обеспечения или обоих компонентов, подлежащих управлению конфигурацией, и обрабатываемых как единая сущность в процессе управления конфигурацией. [4]

consequence, последствие
Эффект (изменение или не изменение), обычно связанный с событием или условием, или с системой и обычно допускаемый, облегчаемый, вызываемый, предотвращаемый, изменяемый или вносимый событием, условием или системой. [61]

constraints, ограничения
Ограничение на систему, её проект, её реализацию или процесс, используемый для разработки или модификации системы.

Ограничение, ограничивающее проектное решение, реализацию или исполнение системы. [31]

> *Примечание:* Ограничение - это фактор, который накладывается на решение силой или принуждением и может ограничивать или изменять проект.

control, управление
Целенаправленные действия над или в рамках процесса для достижения конкретных целей.

Механизм, с помощью которого осуществляется действие.

criticality, критичность
Степень влияния, которое требование, модуль, ошибка, сбой, отказ или другой элемент оказывают на разработку или функционирование системы.

customer, владелец
Организация или лицо, получающее продукт. [78]

cyber-physical system, киберфизическая система
Система, интегрирующая вычисления с физическими процессами, поведение которой определяется как вычислительными (цифровыми и другими формами), так и физическими частями системы. [27]

data, данные
Представление фактов, концепций или инструкций способом, подходящим для передачи, интерпретации или обработки людьми или автоматическими средствами.

Набор значений, назначенных базовым показателям, производным показателям и/или индикаторам. [79]

derived requirement, производное требование
Требование, выведенное или вытекающее из сбора и организации требований для конкретной конфигурации и решения системы. [31]

> *Примечание 1.* Следующее требование более высокого уровня называется *родительским* требованием, а производное требование от родительского называется *дочерним* требованием.

> *Примечание 2:* Производное требование, как правило, определяется при выявлении требований заинтересованных сторон, анализе требований, сравнительных оценках или подтверждении соответствия.

design, проектирование, проект
Процесс определения архитектуры, элементов системы, интерфейсов и других характеристик системы или элемента системы. [24]

Результат процесса, согласующийся с выбранной архитектурой, элементами системы, интерфейсами и другими характеристиками системы или элемента системы. [4]

> *Примечание 1:* Информация, включая спецификацию элементов системы и их взаимосвязей, которая является достаточно полной для поддержки совместимой реализации архитектуры.

> *Примечание 2:* Проект предоставляет подробную физическую структуру, поведение, временные взаимосвязи и другие атрибуты элементов системы на уровне реализации.

design characteristics, характеристики проекта
Атрибуты или отличительные особенности проекта, относящиеся к измеримому описанию продукта или сервиса. [24]

design margin, проектный резерв
Резерв, выделенный при проектировании на основе оценок неопределенности и неизвестных величин. Этот запас часто расходуется по мере развития проекта. [17]

domain, домен
Набор элементов, данных, ресурсов и функций, которые имеют общие черты в комбинациях (1) поддерживаемых ролей, (2) правил, регулирующих их использование, и (3) потребностей в защите. [24]

> *Примечание:* Домены безопасности могут отражать одно или любую комбинацию из следующего: различия в возможностях, функционале или сервисах; потоки данных и потоки управления, связанные с различиями в возможностях, функционале или сервисах; конфиденциальность данных и информации; безопасность данных и информации; или административные, управленческие, операционные или ведомственные полномочия. Домены безопасности, определенные в контексте одного или нескольких из этих элементов, отражают ориентированное на защиту разделение системы, которое приводит к отношениям, основанным на соображениях доверия.

emergence, эмержентность
Поведение и результаты, вытекающие из того, как отдельные элементы системы формируют систему в целом.

> *Примечание:* Поведение и результаты работы системы не являются результатом работы отдельных элементов системы, из которых она состоит. Скорее, эмерджентное поведение и результаты системы, или свойства, являются результатом композиции множества элементов системы.

enabling system, вспомогательная система
Система, которая поддерживает интересующую нас систему на этапах ее жизненного цикла, но не обязательно вносит непосредственный вклад в ее функционирование во время эксплуатации. [4]

engineered system, разработанная система
Система, спроектированная или адаптированная для взаимодействия с предполагаемой операционной средой для достижения одной или нескольких намеченных целей при соблюдении применимых ограничений. [3]

engineering team, команда разработчиков
Сотрудники команды разработчиков системы, отвечающие за безопасность, разработчики безопасности системы, которые являются частью команды разработчиков системы, или их комбинация.

environment, среда
Контекст, определяющий установки и обстоятельства всех воздействий на систему. [71]

error, ошибка
Разница между требуемой и фактической результативностью или поведением системы или элемента системы.

event, событие
Возникновение или изменение определенного набора обстоятельств. [28]

evidence, свидетельство
Основания для веры или неверия; данные, на которых основываются доказательства или устанавливается истина или ложь.

> *Примечание 1:* Свидетельства могут быть объективными или субъективными. Свидетельства получаются с помощью измерений, результатов анализов, опыта и наблюдения за поведением во времени.

> *Примечание 2:* С точки зрения безопасности основное внимание уделяется достоверным свидетельствам, используемым для получения доверия, подтверждения доверенности *и* оценки риска.

facility, возможность
Физические средства или оборудование для облегчения выполнения действий (например, здания, документы, инструменты). [4]

flaw, недостаток
Несовершенство или дефект.

generalized reference monitor concept, концепция обобщенного диспетчера доступа
Абстрактная модель необходимых и достаточных свойств, которые должны быть достигнуты любым механизмом, который обеспечивает соблюдение ограничений. [36] [37]

incident, инцидент
Аномальное или неожиданное событие, набор событий, состояние или ситуация в любое время в течение жизненного цикла проекта, продукта, сервиса или системы. [4]

information, информация
Знания, которыми можно обмениваться между пользователями, о вещах, фактах, концепциях и так далее, в предметной области. [80]

Примечание: Хотя информация обязательно имеет форму представления для того, чтобы ее можно было передать, именно интерпретация этого представления (смысл) имеет значение. Форма представления может считаться данными.

information item, информационный элемент
Отдельно идентифицируемая совокупность информации, которая производится, хранится и предоставляется для использования человеком. [81]

information system, информационная система
Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, обмена, распространения или утилизации информации. [82]

См. *систем*а.

interface, интерфейс
Везде, где два или более логических, физических или обоих элементов системы или элементов программной системы встречаются и действуют друг на друга или взаимодействуют друг с другом. [4]

interoperating system, взаимодействующая система
Система, которая обменивается информацией с интересующей нас системой и использует информацию, которой обменялись. [4]

integrity, целостность
Свойство полноты и неизменности. [83]

life cycle, жизненный цикл
Эволюция системы, продукта, услуги, проекта или другой созданной человеком сущности от замысла до вывода из эксплуатации. [4]

life cycle model, модель жизненного цикла
Структура процессов и действий, связанных с жизненным циклом, которые могут быть организованы в виде этапов, которая также служит общим ориентиром для взаимодействия и понимания. [4]

lifecycle security concepts, понятия безопасности жизненного цикла
Процессы, методы и процедуры, связанные с системой на протяжении всего ее жизненного цикла и обеспечивающие особый контекст для интерпретации безопасности системы. Концепции безопасности жизненного цикла применяются во время управления программой, разработки, проектирования, приобретения, производства, изготовления, выпуска, эксплуатации, поддержания, обучения и списания.

likelihood, вероятность
Шанс на то, что что-то произойдет. [28]

margin, запас
Резервная сумма, мера или степень, допускаемая или предоставляемая на случай непредвиденных обстоятельств или особых ситуаций. Допуски, создаваемые для учета неопределенности и рисков. [39]

См. *проектный запас* и *эксплуатационный запас.*

mechanism, механизм
Процесс или система, используемые для получения определенного результата.

Фундаментальные процессы, связанные с действием, реакцией или другим природным явлением или ответственные за них.

Естественный или установленный процесс, с помощью которого происходит или достигается что-либо.

Примечание 1: Как правило, средство достижения цели.

Примечание 2: Механизм может быть технологическим или нетехнологическим (например, аппарат, устройство, инструмент, процедура, процесс, система, операция, способ, технология, средство или среда).

См. *механизм безопасности*.

module, модуль
Программная единица, который является дискретной и идентифицируемой в отношении компиляции, объединения с другими единицами и загрузки.

Дискретный и идентифицируемый элемент с четко определенным интерфейсом и четко определенной целью или ролью, действие которого описывается как отношения между входами, выходами и сохраненным состоянием. [24]

monitoring, мониторинг
Постоянная проверка, контроль, критическое наблюдение или определение состояния с целью выявления изменений по сравнению с требуемым или ожидаемым уровнем результативности. [28]

operational concept, концепция применения
Вербальное и графическое изложение предположений или намерений организации в отношении действия или серии действий конкретной системы или связанного набора конкретных новых, существующих или модифицированных систем. [77]

Примечание: Концепция применения призвана дать общую картину действий с использованием одной или нескольких конкретных систем или набора связанных систем в среде деятельности организации с точки зрения пользователей и операторов.

См. *концепция действий.*

operational environment, среда применения (эксплуатации)
Контекст, определяющий условия и обстоятельства всех влияний на поставляемую систему.

Примечание: Среды применения (эксплуатации) включают физические (например, наземные, воздушные, морские, космические) и киберпространственные контексты.

operational margin, эксплуатационный запас
Запас, который явно предназначен для обеспечения пространства между наихудшим нормальным рабочим состоянием и точкой, в которой происходит сбой (вытекает из физического проектного запаса). [3] [6]

operator, оператор
Физическое лицо или организация, выполняющие действия с системой. [4]

Примечание 1: Роль оператора и роль пользователя могут принадлежать, одновременно или последовательно, одному и тому же лицу или организации.

Примечание 2: Отдельный оператор в сочетании со знаниями, квалификациями и процедурами может рассматриваться как элемент системы.

Примечание 3: Оператор может выполнять действия в применяемой системе, или вне применяемой системы, в зависимости от того, находятся ли инструкции по применению в пределах границ системы или вне их.

organization, организация
Группа людей и средств с определённым распределением обязанностей, полномочий и отношений. [4] [78].

Примечание: Выделенная часть организации (даже небольшая, как отдельное лицо) или выделенная группа организаций могут рассматриваться как организация, если у них есть обязанности, полномочия и отношения. Совокупность лиц, организованная с определенным с целью - например, клуб, профсоюз, корпорация или общество - является организацией.

outcome, результат
Результат выполнения (или невыполнения) функции или процесса(ов). [84]

party, сторона
Организация, заключающая соглашение. [4]

penetration testing, тестирование проникновения
Тестирование, используемое в анализе уязвимостей для оценки уязвимости, с целью выявления уязвимостей системы на основе информации о системе, собранной в ходе соответствующих работ по оценке. [85]

problem, проблема
Трудность, неопределенность или иным образом реализованное и нежелательное событие, набор событий, условие или ситуация, которые требуют расследования и корректирующих действий. [4]

process, процесс
Набор взаимосвязанных или взаимодействующих работ, которые используют входные данные для достижения желаемого результата. [78]

process purpose, назначение процесса
Высокоуровневая цель выполнения процесса и вероятные результаты эффективной реализации процесса. [4]

Примечание: Цель внедрения процесса - обеспечить выгоду для заинтересованных сторон.

process outcome, результат процесса
Наблюдаемый результат успешного достижения назначения процесса. [86]

product, продукт
Результат процесса. [78]

Примечание: Существует четыре общие категории продуктов: оборудование (например, механическая часть двигателя); программное обеспечение (например, компьютерная программа); сервисы (например, транспортировка); и обработанные материалы (например, смазочный материал). Оборудование и обработанные материалы, как правило, являются материальными продуктами, в то время как программное обеспечение или сервисы, как правило, являются нематериальными.

project, проект
Усилия с определенными начальными и конечными критериями, направленные на создание продукта или сервиса в соответствии с указанными ресурсами и требованиями. [4]

Примечание: Проект иногда рассматривается как уникальный процесс, включающий координируемые и контролируемые действия и состоящий из работ технического управления и технических процессов, определенных в настоящем документе.

protection needs, потребности защиты
Неформальное изложение или выражение требований безопасности заинтересованных сторон, направленных на защиту информации, систем и сервисов, связанных с функциями предназначения и деятельности, на протяжении всего жизненного цикла системы.

Примечание: Выяснение требований и анализ безопасности преобразуют потребности защиты в формализованное изложение требований безопасности заинтересованных сторон, управление которыми осуществляется в рамках утвержденного базового набора требований заинтересованных сторон.

qualification, квалификация
Процесс демонстрации способности сущности выполнять определенные требования. [86]

quality assurance, доверие к качеству
Часть управления качеством направлена на обеспечение уверенности в том, что требования к качеству будут выполнены. [78]

quality characteristic, характеристика качества
Неотъемлемая характеристика продукта, процесса или системы, связанная с требованием. [78]

Примечание: Критические характеристики качества обычно включают характеристики, связанные со здоровьем, безопасностью, защищенностью, доверием, надежностью, доступностью и поддерживаемостью.

quality management, управление качеством
Скоординированная деятельность по руководству и контролю организации в отношении качества.[78]

reference monitor concept, концепция диспетчера доступа
Абстрактная модель необходимых и достаточных свойств, которые должны быть достигнуты любым механизмом, выполняющим функцию посредничества управления доступом. [21] [37]

reference validation mechanism, механизм подтверждения доступа
Реализация концепции диспетчера доступа, которая проверяет каждый доступ к ресурсам на соответствие списку разрешенных санкционированных прав доступа. [37]

requirement, требование
Формулировка, которая отражает или выражает потребность и связанные с ней ограничения и условия. [31]
Условие или возможность, которые должны быть выполнены или которыми должна обладать система или элемент системы для удовлетворения соглашения, стандарта, спецификации или других формально установленных документов. [131]

requirements engineering, разработка требований
Междисциплинарная функция, которая обеспечивает посредничество между доменами приобретателя и поставщика для установления и поддержания требований, которые должны выполняться системой, программным обеспечением или сервисом, представляющими интерес. [31]

Примечание: Разработка требований касается обнаружения, выявления, разработки, анализа, подтверждения, утверждения, управления, сообщения и документирования требований.

resource, ресурс
Актив, используемый или расходуемый во время выполнения процесса. [4]

Примечание 1: Включает различные сущности, такие как финансирование, персонал, средства, капитальное оборудование, инструменты и коммунальные сервисы, такие как энергетическая, водная, топливная и коммуникационная инфраструктуры.

Примечание 2: Ресурсы включают то, что может быть повторно использовано, возобновлено или израсходовано.

retirement, вывод из эксплуатации
Прекращение активной поддержки со стороны организации эксплуатации и технического обслуживания, частичная или полная замена на новую систему или установка модернизированной системы. [4]

risk, риск
Влияние неопределенности на цели. [28]

Примечание 1: Эффект - это отклонение от ожидаемого, положительное или отрицательное. Положительный эффект также известен как возможность.

Примечание 2: Цели могут иметь различные аспекты (например, финансовые цели, цели в области здравоохранения и безопасности, экологические цели) и могут применяться на различных уровнях (например, стратегическом, общеорганизационном, проектном, продуктовом и процессном).

Примечание 3: Риск часто характеризуется ссылкой на потенциальные события и последствия или их комбинацию.

Примечание 4: Риск часто выражается в виде сочетания последствий события (включая изменения обстоятельств) и связанной с этим вероятности возникновения.

Примечание 5: Неопределенность - это состояние, даже частичное, недостатка информации, связанной с пониманием или знанием события, его последствий или вероятности.

risk analysis, анализ риска
Процесс понимания природы риска и определения уровня риска. [28]

risk assessment, оценивание рисков
Общий процесс выявления рисков, анализа рисков и оценки рисков. [28]

risk criteria, критерии риска
Условия, по которым оценивается значимость риска. [28]

risk evaluation, оценка риска
Процесс сравнения результатов анализа риска с критериями риска для определения того, является ли риск и/или его величина приемлемыми или допустимыми. [28]

risk identification, идентификация рисков
Процесс выявления, распознавания и описания рисков. [28]

risk management, управление рисками
Скоординированная деятельность организации по руководству и контролю в отношении рисков. [28]

risk tolerance, допустимый риск
Готовность организации или заинтересованной стороны взять на себя риск после обработки риска для достижения своих целей. [28]

Примечание: На допустимый риск могут влиять правовые или нормативные требования.

risk treatment, обработка риска
Процесс изменения риска. [28]

safety, защищённость
Ожидание того, что система при определенных условиях не придёт к состоянию, в котором жизнь, здоровье, имущество или окружающая среда человека находятся под угрозой. [86]

security, безопасность
Независимость от тех условий, которые могут привести к потере активов с неприемлемыми последствиями.

security architecture, архитектура безопасности
Набор физических и логических представлений (т.е. взглядов) об архитектуре системы, относящихся к безопасности, которые передают информацию о том, как система разделена на домены безопасности, и использует элементы, относящиеся к безопасности, для применения политик безопасности внутри и между доменов безопасности на основе того, как данные и информация должны быть защищены.

Примечание: Архитектура безопасности отражает домены безопасности, размещение элементов, имеющих отношение к безопасности, в доменах безопасности, взаимосвязи и доверенные отношения между элементами, имеющими отношение к безопасности, а также поведение и взаимодействие между элементами, имеющими отношение к безопасности. Архитектура безопасности, как и архитектура системы, может быть выражена на различных уровнях абстракции и с различными масштабами.

security design order of precedence, порядок приоритетности проектирования системы безопасности
Подход к проектированию, позволяющий свести к минимуму потенциал потерь при проектировании и использовать архитектурные особенности для создания структуры для реализации спроектированных элементов и устройств безопасности.

security domain, домен безопасности
Набор активов и ресурсов, на которые распространяется общая политика безопасности. [85]

Примечание: Домен безопасности определяется правилами (политикой) для пользователей, процессов, систем и сервисов, которые применяются к действиям внутри домена и к действиям с аналогичными сущностями в других доменах.

security function, функция безопасности
Возможность, предоставляемая системой или элементом системы. Возможность может быть выражена в общем виде как концепция или точно указана в требованиях.

security mechanism, механизм безопасности
Устройство или метод для достижения цели, имеющей отношение к безопасности.

security policy, политика безопасности
Набор правил, регулирующих все аспекты поведения системы и элементов системы, относящихся к безопасности.

Примечание 1: Элементы системы включают в себя технологии, оборудование и человеческие элементы.

Примечание 2: Правила могут быть изложены на высоких уровнях абстракции (например, политика организации, определяющая приемлемое поведение сотрудников при выполнении ими функций

предназначения и деятельности) или на низких уровнях абстракции (например, политика операционной системы, определяющая допустимое поведение выполняемых процессов и использование ресурсов этими процессами).

security relevance, значимые для безопасности
Функции или ограничения, на которые прямо или косвенно полагаются для удовлетворения потребностей в защите.

Примечание: Термин *«значимость для безопасности»* используется для дифференциации роли системных функций, которые в отдельности или в сочетании демонстрируют поведение, дают результат или обеспечивают возможность санкционированного и предполагаемого поведения или результатов системы.

security requirement, требование безопасности
Требование, имеющее отношение к безопасности.

security risk, риск безопасности
Влияние неопределенности на цели, связанные с потерей активов и соответствующими последствиями. [28]

Примечание: [28] определяет риск как влияние неопределенности на цели. Кроме того, риск может быть положительным или отрицательным.

security service, сервис безопасности
Возможность или функция безопасности, предоставляемая сущностью.

security specification, спецификация безопасности
Требования к части системы, имеющей отношение к безопасности.

Примечание: Спецификация безопасности может быть предоставлена в виде отдельного документа или может быть включена в более широкую спецификацию.

self-protection, самозащита
Защита, предоставляемая сущностью для обеспечения своего правильного поведения и функционирования, несмотря на неблагоприятные условия.

Примечание: Хотя сущность в идеале должна быть в состоянии обеспечить всю необходимую самозащиту, на практике сущности ограничены в той мере, в какой они могут обеспечить свою собственную защиту без зависимости от одной или нескольких других сущностей.

service, сервис
Выполнение деятельности, работы или обязанностей. [4]

Примечание 1: Сервис является самодостаточным, целостным, дискретным и может состоять из других сервисов.

Примечание 2: Сервис, как правило, является нематериальным продуктом.

situational awareness, понимание ситуации
Восприятие элементов в системе и/или среде и осознание их значения, которое может включать в себя прогнозирование будущего состояния воспринимаемых элементов и неопределенности, связанной с этим состоянием. [87]

specification, спецификация
Элемент информации, определяющий полным, точным, проверяемым образом требования, проект, поведение или другие ожидаемые характеристики системы, сервиса или процесса. [128]

См. *спецификация безопасности.*

stage, стадия
Период в жизненном цикле сущности, который относится к состоянию её описания или реализации. [4]

Примечание 1: В настоящем документе стадии относятся к основным вехам прогресса и достижений сущности на протяжении всего её жизненного цикла.

Примечание 2: Стадии часто перекрываются.

stakeholder, заинтересованная сторона
Физическое лицо или организация, имеющие право, долю, притязание или интерес в системе или в обладании её характеристиками, соответствующими их потребностям и ожиданиям. [4]

stakeholder (system), заинтересованная сторона (в системе)
Физическое лицо, команда, организация или их группы, имеющие интерес к системе. [71]

strength of function, стойкость функции
Критерий, выражающий минимальные усилия, необходимые для того, чтобы преодолеть заданное поведение безопасности реализованной функции безопасности путем прямой атаки на лежащие в ее основе механизмы безопасности.

Примечание 1: Стойкость функции имеет предпосылку, которая предполагает, что основные механизмы безопасности реализованы правильно. Концепция стойкости функции может в равной степени применяться к сервисам или другой абстракции, основанной на возможностях, обеспечиваемых механизмами безопасности.

Примечание 2: Термин *"robustness, устойчивость"* сочетает в себе понятия доверия к правильной реализации со стойкостью функции для обеспечения более точной детализации при определении доверенности системы.

susceptibility, восприимчивость
Невозможность избежать неприятностей.

supplier, поставщик
Организация или физическое лицо, которое заключает договор с приобретателем на поставку продукта или сервиса. [4]

Примечание 1: Другими терминами, обычно используемыми для поставщика, являются подрядчик, производитель, продавец или вендор.

Примечание 2: Приобретатель и поставщик иногда являются частью одной и той же организации.

system, система
Совокупность частей или элементов, которые вместе демонстрируют поведение или значение, не свойственные отдельным компонентам. Системы могут быть физическими или концептуальными, или сочетать в себе и то, и другое. [3] [4]

Примечание 1: Система иногда рассматривается как продукт или как сервисы, которые она предоставляет.

Примечание 2: На практике толкование её значения часто уточняется с помощью ассоциативного существительного (например, авиационная система). Альтернативно, слово "система" заменяется просто контекстно-зависимым синонимом (например, летательный аппарат), хотя это потенциально может затушевать перспективу принципов системы.

Примечание 3: Полная система включает в себя все связанное с ней оборудование, средства, материалы, компьютерные программы, сервисы, микропрограммы, техническую документацию и персонал, необходимые для эксплуатации и поддержки в той степени, в какой это необходимо для самодостаточного использования в намеченной среде.

system element, элемент системы
Член набора элементов, составляющих систему. [4]

Примечание: Элемент системы - это дискретная часть системы, которая может быть реализована в соответствии с заданными требованиями.

system of interest, интересующая нас система
Система, жизненный цикл которой рассматривается. [4]

system of systems, система систем
Интересующая нас система, системными элементами которой сами являются системами; обычно они представляют собой крупномасштабные междисциплинарные проблемы с несколькими гетерогенными распределенными системами. [15]
Набор систем или элементов системы, которые взаимодействуют для обеспечения уникальных возможностей, которые ни одна из составляющих систем не может реализовать самостоятельно. [88]

system context , контекст системы
Конкретные элементы системы, границы, взаимосвязи, взаимодействия и рабочая среда, определяющие систему.

system life cycle, жизненный цикл системы
Период, который начинается, когда система задумана и заканчивается, когда система больше не доступна для использования. [24]
См. *стадии жизненного цикла*.

system security requirement, требования безопасности системы
Требования к системе, имеющие отношение к безопасности. Требования безопасности системы определяют возможности защиты, обеспечиваемые системой, характеристики результативности и поведения, проявляемые системой, а также свидетельства, используемые для определения того, что требования безопасности системы выполнены.

Примечание 1: Ввиду сложности безопасности системы, требования безопасности системы имеют несколько типов и назначений, в том числе (1) структурные требования безопасности, которые выражают пассивные аспекты возможностей защиты, обеспечиваемые архитектурой системы и (2) функциональные требования безопасности, которые выражают активные аспекты возможностей защиты, обеспечиваемые сконструированными элементами и устройствами (например, механизмы безопасности, запреты, меры безопасности, меры защиты, блокировки и контрмеры).

Примечание 2: Каждое требование безопасности системы выражается таким образом, чтобы сделать возможной его проверку с помощью анализа, наблюдения, тестирования, инспекции, измерения или других определенных и достижимых средств.

systems engineering, инженерия систем
Трансдисциплинарный и интегративный подход, позволяющий успешно реализовывать, использовать и выводить из эксплуатации сконструированные системы, используя системные принципы и концепции, а также научные, технологические и управленческие методы. [3]
Междисциплинарный подход, определяющий общие технические и управленческие усилия, необходимые для преобразования набора потребностей, ожиданий и ограничений заинтересованных сторон в решение и поддержки этого решения на протяжении всего срока его службы. [24]

systems security engineer, инженер по безопасности систем
Специалист, специализирующийся в области безопасности систем, независимо от его формальной должности. Кроме того, термин *"инженер по безопасности систем"* относится к нескольким лицам, которые работают в одной команде или сотрудничающих группах.

systems security engineering, инженерия безопасности систем
Трансдисциплинарный и интегративный подход для обеспечения успешной безопасной реализации, использования и вывода из эксплуатации разработанных систем с использованием системных, безопасности и других принципов и концепций, а также научных, технологических и управленческих методов. Инженерия безопасности систем - это раздел инженерии систем.

tampering, вмешательство
Преднамеренное, несанкционированное действие, приводящее к изменению системы, компонентов систем, их предполагаемого поведения или данных. [89]

task, задача
Требуемые, рекомендуемые или допустимые действия, направленные на содействие достижению одного или нескольких результатов процесса. [4]

threat, угроза
Потенциальная причина неприемлемой потери активов и нежелательные последствия или воздействия такой потери.

Примечание: Конкретные причины потери активов могут быть вызваны различными условиями и событиями, связанными с неблагоприятными обстоятельствами, обычно называемыми сбоями, опасностями или угрозами. Независимо от использованного конкретного термина основу потери актива составляет все формы намеренных, неумышленных, случайных, непредвиденных действий, неправильного употребления, злоупотребления, ошибок, слабостей, дефектов, неисправностей, и/или событий отказов и связанных с ними условий.

traceability, прослеживаемость
Различимая связь между двумя или более логическими сущностями, такими как требования, элементы системы, проверки или задачи. [90]

traceability matrix, матрица прослеживаемости
Матрица, фиксирующая взаимосвязь между двумя или более продуктами процесса разработки (например, матрица, фиксирующая взаимосвязь между требованиями и проектом данного программного компонента). [24]

trade-off, компромисс
Принятие решений, выбираемых из различных требований и альтернативных решений на основе чистой выгоды для заинтересованных сторон. [4]

trade-off analysis, анализ компромисса
Определение эффекта уменьшения одного или нескольких ключевых факторов и одновременного увеличения одного или нескольких других ключевых факторов в решении, разработке или реализации проекта.

transdisciplinary, трансдисциплинарный
Создание единой интеллектуальной структуры, выходящей за рамки дисциплинарных аспектов. [135]

trust, доверие
Уверенность в то, что сущность отвечает определенным ожиданиям и, поэтому, на неё можно положиться. [39]

> *Примечание:* Термин *"доверие"* подразумевает, что доверие может быть предоставлено сущности независимо от того, является ли она доверенной или нет.

trust relationship, доверенные отношения
Согласованные отношения между двумя или более элементами системы, которые регулируется критериями безопасного взаимодействия, поведения и результатов в отношении защиты активов.

> *Примечание:* Это относится к доверенным отношениям между элементами системы, реализованными аппаратным, микропрограммным и программным обеспечением.

trustworthiness, доверенность
Свойство обеспечивать доверие при выполнения любых критических требований, которые могут потребоваться для конкретного компонента, подсистемы, системы, сети, приложения, предназначения, предприятия или других сущностей. [2]

> *Примечание: С* точки зрения безопасности доверенная система отвечает конкретным требованиям безопасности в дополнение к удовлетворению другим критически важным требованиям.

trustworthy, доверенный
Степень, в которой поведение компонента явно соответствует установленным требованиям.

user, пользователь
Лицо или группа лиц, взаимодействующие с системой или получающие выгоды от системы в процессе ее использования. [91]

> *Примечание:* Роль пользователя и роль оператора иногда возлагается, одновременно или последовательно, на одно и тому же лицо или организацию.

validation, подтверждение соответствия
Подтверждение, посредством предоставления объективных свидетельств того, что требования в отношении конкретного предполагаемого использования или применения были выполнены. [78]

> *Примечание:* Система способна выполнять намеченное использование, цели и задачи (т.е. удовлетворять требованиям заинтересованных сторон) в намеченной среде эксплуатации. Создана правильная система.

verification, верификация
Подтверждение, посредством предоставления объективных свидетельств того, что установленные требований выполнены. [78]

> *Примечание:* Верификация - это набор действий, по сравнению системы или элемента системы с требуемыми характеристиками. Это включает в себя, но не ограничивается, заданными требованиями, описанием проекта и самой системой. Система создана правильно.

view, представление
Представление всей системы с точки зрения соответствующего набора интересов. [92]

> *Примечание:* Представление может охватывать всю исследуемую систему или только ее часть.

viewpoint, точка зрения
Спецификация соглашений для построения и использования представления. [92]

vulnerability, уязвимость
Слабость, которая может быть использована или спровоцирована, чтобы вызвать неблагоприятный эффект.

Неспособность противостоять неблагоприятным факторам.

> *Примечание:* Уязвимость может существовать в любом месте на протяжении всего жизненного цикла системы, например, в CONOPS, процедурах, процессах, требованиях, проекте, реализации, использовании и поддержке системы.

weakness, слабость
Дефект или характеристика, которые могут привести к нежелательному поведению. [93]

> *Примечание:* Примеры включают отсутствующее требование или спецификацию; архитектурный или проектный недостаток; недостаток реализации, включая дефекты аппаратных средств или программного обеспечения; или использование устаревшей или недопустимой функции, включая устаревшие криптографические алгоритмы.

Приложение C. Политика и требования безопасности

В настоящем приложении рассматриваются соображения[57], касающиеся политики и требований безопасности в поддержку приложений D, E и H. Охватываемые темы включают правила и область управления для политики безопасности (раздел C.1), требования безопасности заинтересованных сторон и системы (раздел C.2), а также взаимосвязь между требованиями безопасности, политикой и механизмами (раздел C.3).

C.1. Политика безопасности

Политика безопасности - это набор правил (раздел C.1.1), который регулирует поведение и результаты в пределах определенной области управления (раздел C.1.2). Политика, как правило, включает в себя набор политик, отражающих потребности и ожидания, установленные органом с конкретной областью и назначением (раздел C.1.2). Правила политики имеют иерархию, начиная с целей верхнего уровня политики безопасности, которые уточняются и распределяются между политиками безопасности организации, которые, в свою очередь, уточняются и распределяются между политиками безопасности системы.

C.1.1. Правила

Правила политики безопасности излагаются в терминах авторизованных отношений, в которых участвуют субъекты (т.е. активные сущности) и объекты (т.е. пассивные сущности). Правила регулируют операции, которые субъект может выполнять или применять над другими субъектами (т.е. операции "субъект-субъект"), и операции, которые субъект может выполнять или применять над объектами (т.е. операции "субъект-объект"). Правила должны быть точными, последовательными, совместимыми и полными в отношении целей безопасности заинтересованных сторон в пределах определенной области управления. Неточные, несогласованные, несовместимые или неполные наборы правил приводят к нежелательному поведению и результатам.

C.1.2. Область управления

Политики безопасности отражают и основывается на законах, директивах, нормативных документах, концепциях жизненного цикла[58], требованиях или целях заинтересованных сторон. Каждая политика включает область управления, которая устанавливает границы, в пределах которых применяется политика. Типичная область применения включает в себя:

- **Цели политики безопасности (Защиты):** Набор целей, отражающий предпочтительное состояние или то, что должно быть достигнуто. Эти цели включают активы, подлежащие защите, заявления о намерении защищать активы в рамках конкретной сферы ответственности заинтересованных сторон и область защиты. Цели политики безопасности являются основой для разработки всех остальных форм политики безопасности.
- **Политика безопасности организации:** Набор правил[59], регулирующих достижение организацией своих целей. Правила предоставляют людям разумную возможность определить, нарушают ли их действия политику безопасности или соответствуют ей. Политика безопасности организации определяет поведение людей при выполнении ими своего предназначения и бизнес-функций и используется для разработки процессов и процедур.

[57] В этом приложении политика рассматривается таким образом, что она предшествует проектированию. Однако политику может потребоваться изменить, чтобы привести ее в соответствие с возможностями системы, поставляемой "как есть".
[58] Концепции жизненного цикла включают эксплуатацию, поддержание, развитие, поддержку, обучение, ввод в эксплуатацию и вывод из эксплуатации.
[59] Правила могут быть отражены в законах и практиках.

- **Политика безопасности системы**: - Политика, определяющая возможности системы по обеспечению безопасности. Это набор ограничений и свойств, определяющих, как система обеспечивает выполнение политики безопасности организации или способствует ее выполнению.
- **Политика безопасности персонала:** политика, определяющая ожидания в отношение персонала.[60] Она включает в себя поведение персонала, использующего или поддерживающего систему.

Политика безопасности проходит через итерационный процесс уточнения, в ходе которого абстрактная формулировка политики безопасности декомпозируется на более конкретные формулировки политики безопасности. Уточнение происходит параллельно с распределением и декомпозицией требований. На рисунке 11 показано распределение политики безопасности по организации.

Рис. 11. Распределение обязанностей по политике безопасности

C.2. Требования безопасности

Требование - это заявление, которое переводит или выражает конкретную потребность и связанные с ней ограничения и условия.[61] Требования безопасности отражают или выражают потребности в защите (раздел 3.7), и связанные с ней ограничения и условия. Ограничения также отражают интересы по поводу функций системы, архитектуры системы и проекта для обеспечения того, чтобы они были определены таким образом, чтобы избежать и уменьшить уязвимости, дефекты, недостатки и слабые места (раздел 3.8) и соответствовать потребностям активных функций безопасности.

Требования могут быть классифицированы как (1) *требования заинтересованных сторон*, которые учитывают необходимость удовлетворения в независимом от проекта способе и (2) *требования к*

[60] Эти ожидания часто охватывают действия персонала, которые могут подвергнуть их негативному внешнему влиянию (например, использование социальных сетей).
[61] Общие требования и процессы определения описаны в таких источниках, как [31] и [32].

системе, которые выражают конкретные решение, которое будет поставляться (проектно-зависимый способ). На рис. 12 показаны два типа требований и их связь с проверкой и подтверждением соответствия системы.

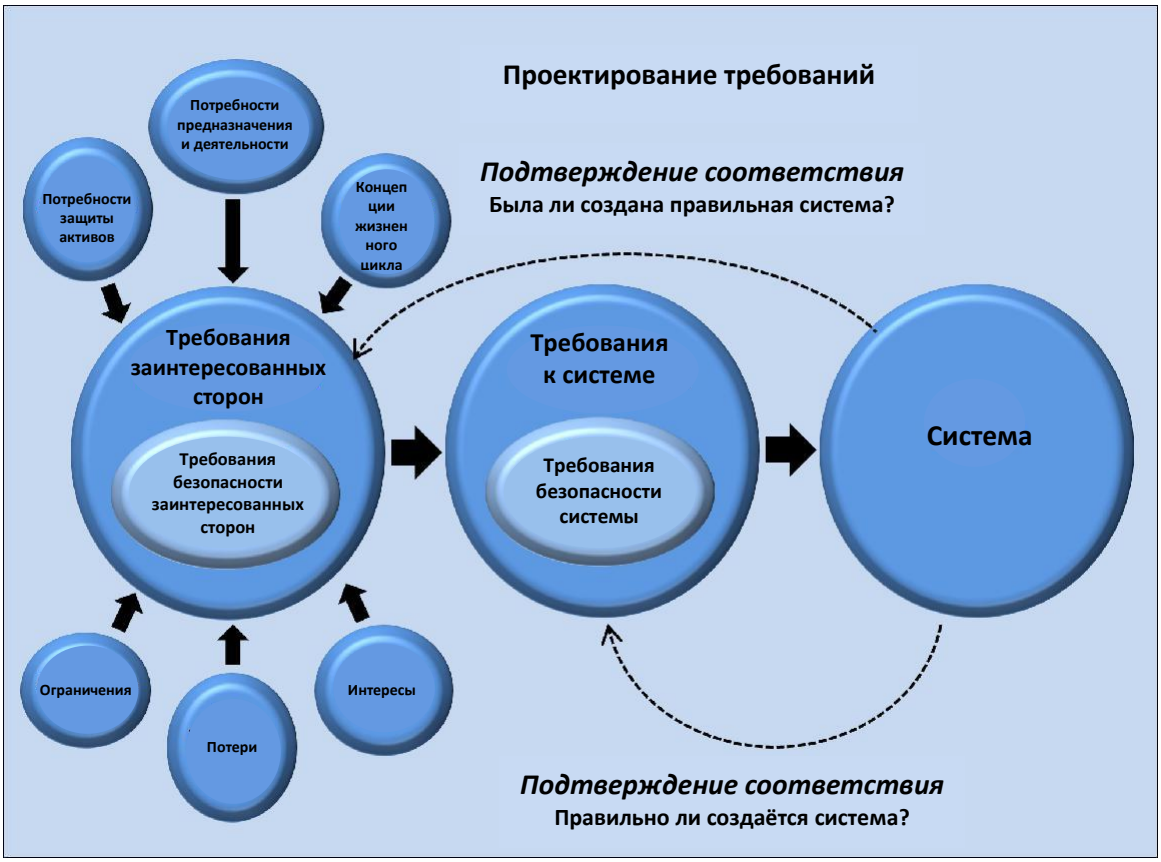

Рис. 12. Требования заинтересованных сторон к системе

Требования безопасности и связанные с безопасностью ограничения и условия в отношении других требований определяются различными элементами, такими как те, которые изображены на рисунке 13.

C.2.1. Требования безопасности заинтересованных сторон

Требования безопасности заинтересованных сторон - это требования заинтересованных сторон, имеющие отношение к безопасности. Эти требования определяют:

- Защиту, необходимую для предназначения или деятельности, данных, информации, процессов, функций, персонала и активов системы.
- Роли, обязанности и связанные с безопасностью действия лиц, выполняющих и поддерживающих процессы предназначения или деятельности.
- Взаимодействие между элементами решения, имеющими отношение к безопасности.
- Доверие, которое должно быть получено в решении по безопасности.

Соображения безопасности систем в рамках действий и задач, описанных в приложениях H, I, J и K, обеспечивают перспективу безопасности, чтобы гарантировать, что требования безопасности заинтересованных сторон были включены в требования заинтересованных сторон, и что требования безопасности заинтересованных сторон соответствуют всем другим требованиям заинтересованных сторон.

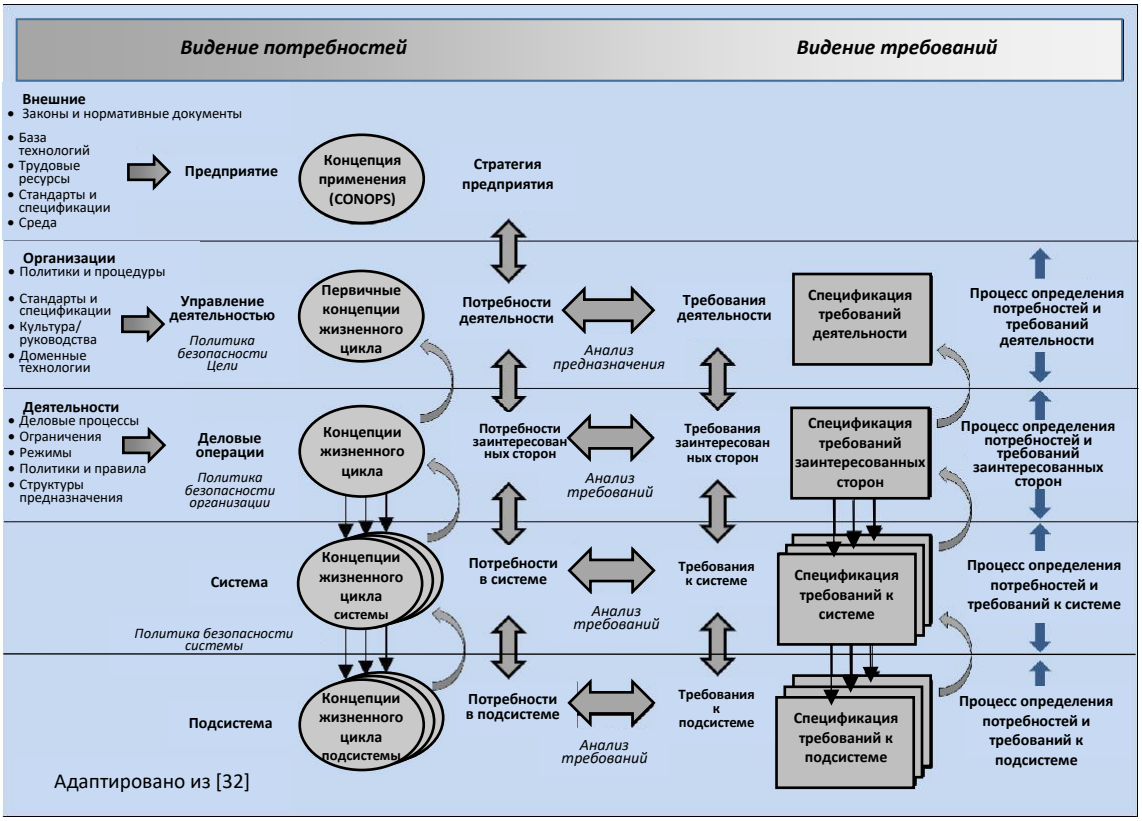

Рис. 13. Сущности, влияющие на разработку требований безопасности

C.2.2. Требования к безопасности систем

Требования к системе определяют техническое представление системы или решения, удовлетворяющее указанным потребностям заинтересованных сторон. Требования к системе представляют собой преобразование установленных требований заинтересованных сторон. Требования к системе определяют, что система или решение должны делать для удовлетворения требованиям заинтересованных сторон. Требования к безопасности системы - это требования к системе, имеющие отношение к безопасности. Эти требования определяют:

- Возможности защиты, предоставляемые решением по безопасности.
- Характеристики результативности и поведения, демонстрируемые решением по безопасности.
- Процессы, процедуры и технологии обеспечения доверия.
- Ограничения, накладываемые на систему, и процессы, методы и инструменты, используемые для реализации системы.

- Свидетельства, необходимые для определения того, что требования безопасности системы выполнены.[62]

Из-за сложности безопасности системы требования к безопасности системы имеют несколько типов и назначений, в том числе (1) структурные требования безопасности, которые выражают пассивные аспекты возможностей защиты, обеспечиваемые главным образом архитектурой системы и (2) функциональные требования безопасности, которые выражают активные аспекты возможностей защиты, обеспечиваемые инженерными функциями и устройствами (например, механизмы безопасности, меры обеспечения, меры безопасности, блокировки, переопределения и контрмеры). Декомпозиция требований безопасности выполняется как часть декомпозиции требований к системе и согласуется с различными уровнями иерархической абстракции и формами требований к системе.

СОСТОЯНИЕ СИСТЕМЫ, ПОЛИТИКА И ТРЕБОВАНИЯ

Системы работают в безопасных, небезопасных и неопределенных состояниях (раздел 3.2). Политика безопасности системы и требования к системе учитывают эти состояния и переходы между состояниями, включая те, которые отражают принципы проектирования *«Защищённый отказ»* и *«Защищённое восстановление»*. Например, требования отражают необходимость: (1) обнаруживать небезопасные состояния системы; (2) обнаруживать переход, который приведет к небезопасному состоянию; (3) осуществить переход в безопасное состояние остановки; (4) осуществить восстановление в восстановленный, реконфигурированный или альтернативный безопасный режим работы; и, при необходимости, (5) продолжать работать в небезопасном или неопределенном состоянии, когда другие потребности преобладают над потребностями в защите.

C.3. Определение требований, политик и механизмов

Термины *требования*, *политика* и *механизмы* часто используются в абстрактном смысле, позволяющем рассматривать их как синонимы. Однако, когда эти термины используются в контексте инженерии доверенных безопасных систем, они отличаются по своему значению и важности для определения, реализации, использования и поддержания систем.

Политика безопасности определяет поведение, необходимое для достижения безопасного состояния, в то время как механизм безопасности является средством для достижения необходимого поведения. Различие между политикой безопасности и механизмом безопасности распространяется и на различие между требованиями безопасности и политикой безопасности. Требования безопасности определяют атрибуты возможностей, поведения и качества, которые демонстрируют и которыми обладают механизмы безопасности, а также ограничения для каждого из них. Политика безопасности определяет поведение механизмов безопасности в контексте применения и ограничения на их поведение. С точки зрения системы человек является элементом системы и может служить механизмом безопасности. Поэтому ожидается, что человек будет вести себя в соответствии с соответствующей политикой безопасности и требованиями безопасности.

Требования, политики и механизмы имеют важную взаимосвязь. Требования безопасности системы определяют возможности и поведение, которые может предоставить механизм безопасности. Политика безопасности определяет аспекты, которые механизм должен обеспечивать для достижения целей

[62] Каждое требование к безопасности системы, как и любое другое требование к системе, формулируется таким образом, чтобы сделать возможной проверку с помощью инспекции, анализа, демонстрации, тестирования или других определенных и достижимых средств [31].

организации. Это означает, что безопасность системы не может быть достигнута, если требования безопасности не полностью определяют минимальные возможности, необходимые для реализации политики безопасности. Это также означает, что удовлетворение требований само по себе не приводит к созданию безопасной системы. Действия по проверке и подтверждению соответствия должны проводиться отдельно и координироваться для обеспечения индивидуальной и совместной корректности и эффективности требований и политики.

Рисунок 14 иллюстрирует важность отношений согласованности, которые должны поддерживаться между взаимодействующими требованиями безопасности, политикой безопасности и механизмами безопасности.

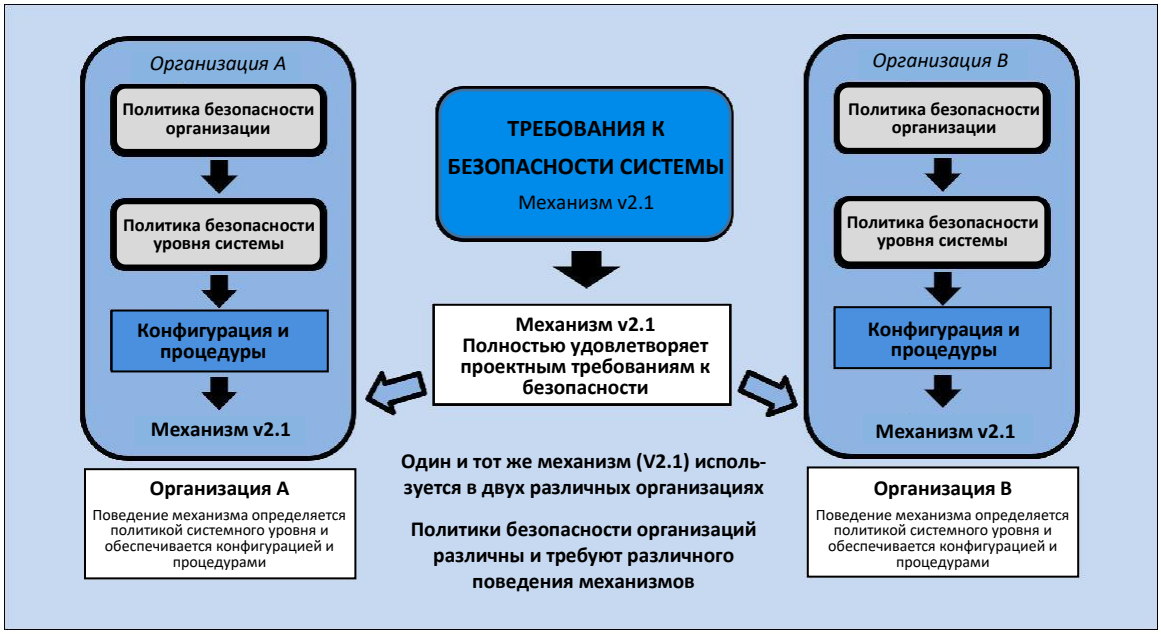

Рис. 14. Взаимосвязь между механизмами и реализацией политики безопасности

Следует отметить, что механизм безопасности, полностью удовлетворяющий требованиям безопасности системы, может считаться способным обеспечить выполнение политики безопасности, определенной для двух различных организаций. Каждая организация использует один и тот же механизм и настраивает его таким образом, чтобы обеспечить соблюдение правил политики безопасности организации. Однако, если бы организации поменялись механизмами и сохранили одинаковую конфигурацию механизма, они получили бы неопределенные результаты (если только их цели политики безопасности не требуют точно такой же конфигурации механизма). Из этого можно сделать следующие выводы:

- Требования касаются как мер защиты, которые должны обеспечиваться механизмами безопасности, так и ограничений, связанных с обеспечением безопасности, которые должны соблюдаться механизмами безопасности.
- Политика безопасности определяет поведение и результаты, которые считаются *безопасными*.
- Для того чтобы механизм считался безопасным, требования к возможностям механизма должны соответствовать правилам осуществление политики безопасности; механизм должен удовлетворять требованиям безопасности; и механизм должен быть сконфигурирован так, чтобы вести себя таким образом, как это определено политикой безопасности организации.

Приложение D. Проектирование доверенной безопасности

В этом приложении рассматривается подход и соображения по применению технических[63] концепций проектирования доверенных безопасных систем. Описанные концепции обеспечивают сбалансированный и интегрированный подход, который оптимально защищает от потери активов. Обсуждается подход к проектированию доверенных систем (раздел D.1), санкционированное и предполагаемое поведение и результаты работы системы (раздел D.2), порядок приоритетности при проектировании безопасности систем (раздел D.3) и соображения, касающиеся функционального проектирования и пространства компромиссов (раздел D.4).

Проектирование систем, основанное на принципах, усиливает утверждения о доверенности [2]. Концепции, содержащиеся в настоящем приложении, и принципы, содержащиеся в Приложении E, обеспечивают прочную основу для рассуждений о системе и позволяют продемонстрировать её доверенность. Применение концепций и принципов, а также использование других средств (например, стандартов, спецификаций, шаблонов проектирования, моделей политики безопасности, криптографических алгоритмов, протоколов безопасности, стойкости механизмов и неблагоприятных факторов) должно планироваться, соответствующим образом определяться и пересматриваться на протяжении всего жизненного цикла системы и в процессе разработки.

Наконец, потребности и соображения в отношение доверенности и доверия также служат основой для проектирование доверенной безопасности. В приложении F приводится дальнейшее обсуждение концепций доверенности и доверия.

ПРОЕКТИРОВАНИЕ ДОВЕРЕННОЙ БЕЗОПАСНОСТИ

Проектирование доверенной безопасности - это способ обеспечения уверенности заинтересованных сторон в том, что их противоречивые потребности в возможностях, проблемы, приоритеты и ограничения удовлетворены.

D.1. Подход к проектированию доверенной безопасности

Подход к проектированию доверенных безопасных систем предназначен для создания и поддержания способности предоставлять возможности системы на приемлемом уровне результативности[64], сводя к минимуму возникновение и масштабы потерь. Этот подход обеспечивает структуру системы для оптимального использования разработанных функций и устройств. Проект системы должен обеспечивать предполагаемое поведение и результаты, избегать непреднамеренного поведения и результатов, предотвращать потери и ограничивать потери при их возникновении. Проект доверенной безопасности включает в себя возможность к осведомленности о ситуации и запас[65] для учета

[63] Отметим, что элементы доверия, связанные с человеческим фактором, не рассматриваются. Система может быть доверенной, но пользователь может ей не доверять. Аналогично, пользователь может доверять системе, не заслуживающей доверия.

[64] Приемлемый уровень результативности лежит между минимальным порогом приемлемости и целью максимальной результативности. Этот уровень может варьироваться в различных эксплуатационных или системных состояниях и режимах (например, патрулирование в ясную погоду или в суровых погодных условиях), может варьироваться в зависимости от непредвиденных условий (например, нормальное, ухудшенное состояние) и может зависеть от оперативных приоритетов (например, поиск и спасение, розыск).

[65] Термин "*запас*" относится к резервному количеству, мере или степени, разрешенным или предоставляемым для непредвиденных или особых ситуаций. Добавки предоставляются с учетом факторов неопределенности и рисков. В инженерии систем используются два типа запасов: проектный и эксплуатационный. См. принцип проектирования «*Запас на случай потерь*».

неблагоприятных факторов, связанных с неизвестностью и неопределенностью, присущими системе и среде её эксплуатации. Возможности осведомленности о ситуации помогают определить ответственность за действия всех пользователей и субъектов (например, аудит, протоколирование, регистрация событий) и обнаружить предстоящие и фактические сбои (например, переход через порог установленных пределов). Принцип проектирования *«Обнаружение аномалий»* воплощает эту возможность.

Подход к проектированию включает следующие элементы:[66]

- Определение предполагаемого поведения и результатов для системы.[67]
- Определение состояний и условий системы, отражающих предполагаемое поведение и результаты.
- Определение состояний и условий системы, которые могут привести к потерям в системе.
- Выбор и изменение проекта системы для предотвращения потерь в той степени, в какой это практически возможно (предпочтительно), и ограничение потерь, которые действительно происходят (где, когда, и в необходимой и практически возможной степени).
- Повторение вышеуказанных элементов для понимания того, каким образом функции, служащие для предотвращения или ограничения потерь, могут не выполняться по намеренным или непреднамеренным причинам.

Рисунок 15 иллюстрирует шаги подхода к проектированию в контексте Основ инженерии безопасности систем, описанной в Главе 4.

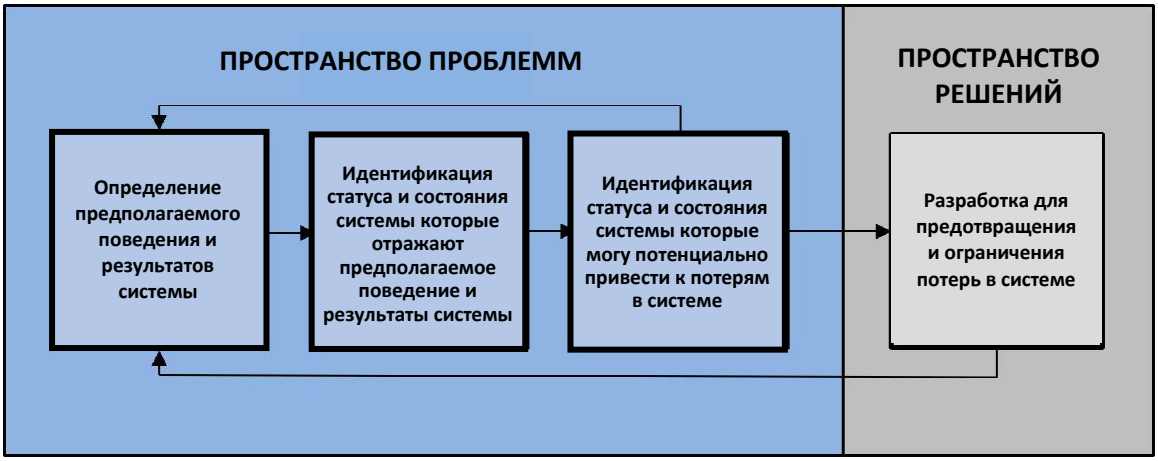

Рис. 15. Подход к проектированию в соответствии с Основами инженерии безопасности систем

Подход к доверенному проектированию включает как упреждающие, так и реактивные аспекты. Эти взаимоусиливающие аспекты обеспечивают защиту, необходимую для достижения только санкционированного и предполагаемого поведения и результатов. Упреждающий аспект приводит к появлению системных функций и действий системы, направленных на предотвращение и ограничение потерь до их возникновения, а реактивный аспект приводит к появлению действий системы по ограничению потерь и их последствий после возникновения потерь. Рис.16 иллюстрирует сбалансированную стратегию проектирования, которая включает упреждающие и реактивные аспекты.

[66] Эти шаги полезны при применении концепции управления системой для любого зависящего от потерь эмерджентного свойства (например, безопасности, устойчивости).
[67] Этот процесс повторяется при разработке систем по мере их декомпозиции. Последующие итерации будут применяться к элементам, составляющим интересующую нас систему (т.е. к подсистемам, сборкам и компонентам).

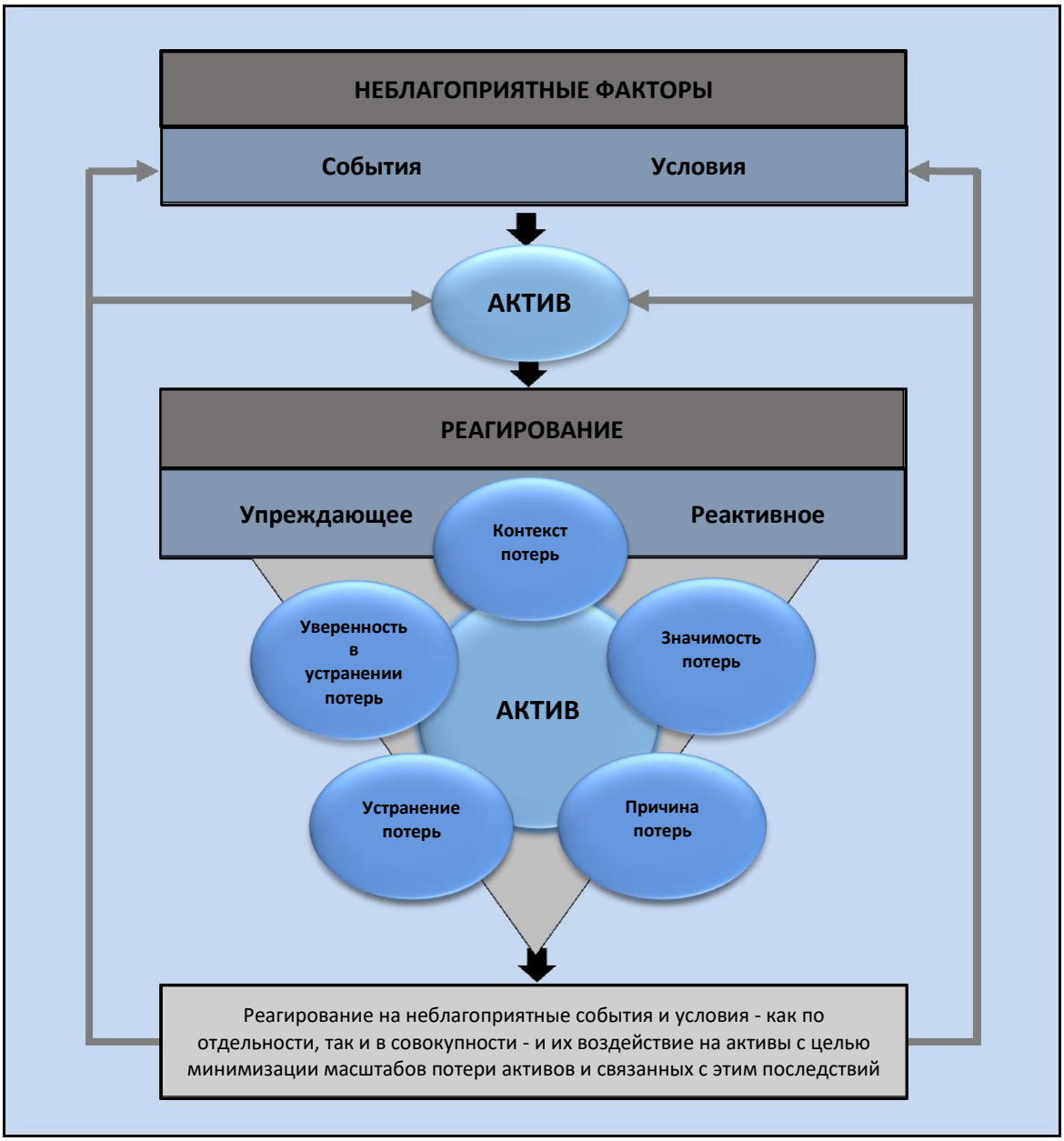

Рис. 16. Сбалансированная стратегия проектирования доверенных безопасных систем

Упреждающий аспект распознает условия, при которых могут происходить потери, и рассматривает сценарии до возникновения потерь (т.е. то, что может произойти). Если потеря всё же произойдет, её результаты будут ограничены благодаря особенностям системы и действиям, предпринятым заранее. Упреждающий аспект не зависит от каких-либо конкретных знаний об атаках и целях атакующих, а фокусируется на том, что возможно в течение жизненного цикла системы. Реактивный аспект признает пределы определенности в отношении того, что может произойти, и что новые, непредвиденные или иначе непредусмотренные неблагоприятные последствия будут иметь место, несмотря на упреждающее планирование и внедрение средств и методов контроля потерь и масштабов их последствий. Реактивный аспект способствует принятию обоснованных оперативных решений после начала эксплуатации системы и возникновения ситуации потерь, упреждающе обеспечивая операционную способность для устранения условий потерь и ликвидации потерь. Реактивный аспект дополняет упреждающий аспект обеспечивая информированную основу и средства для действий

внешней сущности (например, человека-оператора или системы), при возникновении сбоев. По существу, реактивный аспект представляет собой упреждающую инженерную деятельность по обеспечению реактивной способности.

Эффективный проект оптимизирует защиту от потерь в той мере, в какой это практически возможно, признавая при этом, что потери будут иметь место независимо от применяемых мер защиты. Решения по оптимизации в рамках упреждающих и реактивных подходов должны учитывать активы, заинтересованные стороны, интересы и цели. Для достижения надлежащего сочетания необходимо установить цели в области безопасности и провести выявление и анализ требований, с тем чтобы однозначно определить масштабы безопасности с точки зрения устранения сбоев и связанных с ними последствий в упреждающем и реактивном аспектах.

D.2. Проектирование с учетом эмерджентности

Предполагается, что система будет обеспечивать необходимые возможности, в соответствии с санкционированием, по назначению и при определенном уровне результативности. Она не должна предоставлять несанкционированные или непредусмотренные возможности. Одна из причин непредусмотренного поведения и результатов заключается в концепции *эмерджентности.* Эмерджентность относится к поведению и результатам, которые являются следствием того, как отдельные элементы системы образуют систему, выходя за рамки совокупности поведения и результатов отдельных элементов системы. Эта композиция рассматривается в принципе проектирования «*Структурированная декомпозиция и композиция*» и проиллюстрирована на Рис. 2.

Некоторые проявления желательны и продуктивны; другие проявления не желательны и не продуктивны, создавая неизвестные, непредвиденные или неблагоприятные последствия.[68] Разработка доверенных безопасных систем направлена на обеспечение только желательных проявлений. Суждения о доверенности основываются на предположении, что система может удовлетворить заявленные потребности в возможностях. Чтобы достичь этого, при проектировании необходимо учитывать эмерджентность на всех уровнях системной абстракции с точки зрения того, как система разбивается на составляющие ее элементы и как эти элементы системы объединяются для создания системы. Это отражено в принципе проектирования «*Композиционная доверенность*».

БЕЗОПАСНОСТЬ ЭМЕРДЖЕНТНА

Целью безопасности является обеспечения только санкционированного и предопределённого поведения и результатов в системе. Это требует фундаментального понимания того, как отдельные элементы системы объединяются в систему в целом. Системы проектируются на основе этого понимания, чтобы ограничить эмерджентное поведение и результаты, которые не определены заранее (включая желаемые и нежелательные неопределенные поведение и результаты).

[68] Эмерджентность может быть описана в терминах свойств, проявляемых сущностями, только если они относятся к целому, а не к какому-либо отдельному составляющему элементу.

D.3. Порядок приоритетности проектирования безопасности

Порядок приоритетности проектирования безопасности (SecDOP)[69] является подходом к проектированию целью которого является минимизация потенциальных потерь при проектировании системы. SecDOP подчеркивает важность создания безопасного структурного контекста для использования сконструированных элементов и устройств. Используя принципиальный инженерный подход, SecDOP устраняет восприимчивость, опасность и уязвимость, насколько это практически возможно, тем самым устраняя связанный с этим риск. В тех случаях, когда уязвимость, опасность или уязвимость не могут быть устранены, SecDOP снижает потенциал потерь до приемлемого уровня в пределах ограничений стоимости, сроков и результативности. SecDOP определяет альтернативные варианты проектирования в порядке уменьшения эффективности, что позволяет добиться максимальной отдачи от инвестиций.

Альтернативные варианты SecDOP:

- **Устранение возможности потерь за счет выбора проекта**

  Восприимчивость, опасность и уязвимость устраняются путем выбора альтернативного проекта или материала, который полностью устраняет восприимчивость, опасность и уязвимость и, таким образом, предотвращает потери.

  - *Пример:* Проект, выбранный для интересующей нас функции системы, приводит к минимальному числу внешних интерфейсов с другими системами и минимальному числу внутренних интерфейсов, обеспечивающих требуемые функции. Поскольку каждый интерфейс обладает потенциалом восприимчивости, опасности и уязвимости, выбор проекта с минимальным числом интерфейсов приводит к меньшей восприимчивости, опасности и уязвимости, чем проект, включающая дополнительные и ненужные внутренние и внешние интерфейсы.
  - *Примечание*: При выборе проекта также учитывается необходимость использования механизмов, обеспечивающих опосредованный доступ и доверенную связь, поскольку эти разрабатываемые функции и устройства необходимы для безопасной системы.

- **Снижение возможности потерь за счет изменения проекта**

  Если принятие альтернативного проекта или материала для устранения восприимчивости, опасности и уязвимости невозможно, рассмотрите изменения проекта или выбор материала, которые снизят частоту, потенциал, серьезность и/или масштабы потерь, вызванных восприимчивостью, опасностью или уязвимостью.

  - *Пример*: Выбранный проект имеет интерфейсы и, следовательно, имеет присущие ему восприимчивость, опасности и уязвимости, как в отношении взаимодействий с окружающей средой, так и в отношении взаимодействия внутри системы. Возможность потерь может быть уменьшена путем изменения проекта для сегментации функциональных возможностей, взаимодействующих с внешними сущностями и факторами, и влияющих на функциональность строго в пределах системы.
  - *Примечание*: Изменение проекта также учитывает необходимость внедрения механизмов, обеспечивающих опосредованный доступ и доверенную связь, поскольку эти конструктивные функции и устройства необходимы для безопасной системы.

[69] Порядок приоритетности при проектировании безопасности основан на «Порядке приоритетности при проектировании системы защиты» - оптимизированном подходе к проектированию системы защиты, описанном в [34]

- **Включение конструктивных функций или устройств для управления потенциальными потерями**

  Если предотвращение, ограничение или снижение потенциальных потерь за счет изменения проекта и выбора материала не представляется возможным или адекватным, используйте конструктивные функции и устройства для управления потерями, связанными с восприимчивостью, опасностью и уязвимостью. Как правило, конструктивные функции активно нарушают последовательность сценариев потерь и взаимодействия, а устройства снижают потенциал, серьезность и масштабы потерь.

  Два общих типа конструктивных элементов и устройств, используемых для устранения возможных потерь, связанных с интересующей системной функцией:

  - *Обязательные возможности и устройства безопасности*: Обязательные возможности и устройства безопасности применяют основополагающие принципы безопасности к интерфейсам. Например, каждый интерфейс должен иметь опосредованный доступ для управления доступом к и использованием возможностей и данных, предоставляемых интерфейсом.
  - *Специфические функциональные возможности и устройства*: Специфические функциональные возможности и устройства безопасности защищают от потерь, связанных со способностью проекта соответствовать функциональным требованиям и параметрам результативности. Конструктивные функции, такие как избыточные потоки данных и управления, а также избыточные элементы системы, могут дополнять выбор проекта для обеспечения требуемой защиты. Система также может иметь конструктивные функции, которые позволяют внешним сущностям вмешиваться в систему для устранения потенциала, серьезности или масштаба потерь.

- **Обеспечение видимости и обратной связи с внешними сущностями**

  Если изменение проекта, выбор материала и конструктивные элементы и устройства являются неосуществимыми или не позволяют адекватно снизить частоту, потенциал, серьезность или масштаб потерь, вызванных восприимчивостью, опасностью или уязвимостью, используйте конструктивные системы обнаружения и обратной связи, а также устройств предупреждения для оповещения внешних сущностей о наличии восприимчивого, опасного или уязвимого состояния; возникновения события, которое приведет к потерям; или о фактическом событии потерь. Внешние сущности включают оперативный персонал, системы мониторинга или другие системы, способные реагировать.

  - *Пример:* Функции обнаружения аномалий могут использоваться для предоставления информации о ситуации и предупреждения пользователей системы.
  - *Примечание:* Предоставленная информация и обратная связь не будут иметь ценности, если внешние сущности не в состоянии отреагировать на нее должным образом. Например, видимость и обратная связь должны предоставляться своевременно и должны иметь форму, которая может быть правильно интерпретирована.

- **Внедрение указателей, процедур, обучения и соответствующего оборудования**

  Внедряйте процедуры, обучение, указатели и надлежащее оборудование, в тех случаях, когда альтернативные проекты, изменения проекта, а также конструктивные возможности и устройства не применимы, а устройства предупреждения не могут адекватно уменьшить потенциал, серьезность или масштаб потерь, вызванных опасностью, восприимчивостью или уязвимостью. Процедуры и обучение включают надлежащие в себя предупреждения и предостережения и могут предписывать использование оборудования. Следует избегать использования указателей, процедур, обучения и оборудования в качестве единственного средства уменьшения потенциала, тяжести или масштаба потерь.

- *Пример*: Процедуры и обучение касаются правильного использования интересующей нас системной функции, использования опосредованных функций доступа, а также соответствующих предупреждений, предостережений и систем оповещения.

ОБ ИСПОЛЬЗОВАНИИ МЕР БЕЗОПАСНОСТИ

Обычная практика в некоторых сообществах заключается в выборе и наложении на системы мер безопасности (т.е. управленческих, оперативных и технических мер безопасности или контрмер) в качестве основного средства решения проблем безопасности [67] [68]. Но, как отмечается в [69], "Плохое проектирование безопасности систем очень трудно смягчить путем наложения мер безопасности, в то время как меры безопасности, наложенные на продуманный, безопасный проект, могут быть достаточно эффективными".

Порядок приоритетности проектирования безопасности, как часть практики разработки систем, помогает обеспечить надлежащую интеграцию *технических мер* и *эксплуатационных мер* безопасности.

D.4. Соображения по функциональному проектированию

В этом разделе описываются соображения по функциональному проектированию доверенных безопасных систем. Эти соображения включают в себя (1) гарантированные функции, которые обеспечивают осуществление управления, принятие решений по управлению и инфраструктуру управления; (2) критерии проектирования механизмов; (3) анализ сбоев в работе функций безопасности; (4) ситуационная осведомлённость; и 5) соображения, связанные с пространством компромиссов.

D.4.1. Роли для управления, связанного с безопасностью

Все функции способны влиять на поведение и результаты, выходящие за рамки их самих, и имеют значимость для безопасности.[70] Однако, некоторые функции имеют специальное предназначение для безопасности (например, функции, поддерживающие возможности аудита). В качестве примеров можно привести функции управления защитой.

Функции управления защитой обеспечивают или способствуют управлению, или иным образом непосредственно влияют на поведение и результаты системы или элементов системы. Эти функции могут быть охарактеризованы и оценены, используя следующие предназначения:

- *Функции принятия решений по управлению защит*ой: эти функции принимают решения по авторизации или выполняют другие действия для функций обеспечения управления защитой. Например, функция, которая принимает решение предоставить или запретить доступ к ресурсу на основании запроса (например, от функции обеспечения управления защитой).
- *Функции обеспечения управления защитой*: Эти функции обеспечивают соблюдение ограничений, гарантирующих, что система или элемент системы проявляют только разрешённое и

[70] Исторически термин "*значимость для безопасности*" использовался при проектировании и оценке безопасных систем для дифференциации роли функций системы, которые либо в отдельности, либо в комбинации проявляют поведение, дают результат или предоставляют возможность обеспечения применения авторизованного и предусмотренного поведения или результатов системы. Однако с точки зрения безопасности (раздел 3.8) и возможности потерь из-за недостатков и дефектов в любой функции системы, все функции имеют проблемы, связанные с потерями, и, следовательно, проблемы защиты.

предусмотренное поведение или результаты. Например, функция обеспечения управления защитой обеспечивает принятие решения о предоставлении или отказе в доступе к ресурсу.

- *Функции инфраструктуры управления защитой*: Эти функции поддерживают и помогают функциям обеспечения управления защитой и принятия решений по управлению защитой выполнять их предназначение. Эти функции также предоставляют данные, сервисы или выполняют операции, от которых зависят функции осуществления управления защитой и принятия решений по управлению защитой. Например, функция инфраструктуры управления защитой включает в себя механизмы безопасного хранения, защищенной связи и обнаружения аномалий.

Другие функции, включая функции управления для другого назначения, помимо защиты, могут потенциально негативно влиять на правильную работу функций управления защитой. Для целей безопасного проектирования и оценки эти функции обозначаются как другие функции системы. В идеале эти функции должны быть не вмешивающимися. Эта цель невмешательства может быть достигнута посредством доверия с ограничениями на требования, архитектуру, проект и использование этих функций.

Функции системы могут быть сопоставлены с одной или несколькими функциями принятия решений по управлению защитой, функциями осуществления управления защитой, функциями инфраструктуры управления защитой или другими функциями системы для целей проектирования и оценки безопасности. Это различие определяет принципиальный подход к проектированию, позволяющий с уверенностью ограничить взаимодействие между функциями. Такая уверенность может быть достигнута путем использования *доверительного управления системой*, применения критериев проектирования, описанных в разделе D.4.2, и оптимального размещения функции в архитектуре системы для ограничения побочных эффектов и взаимодействий, которые могут мешать функциям управления защитой.

Системный анализ может определить степень, в которой функции могут мешать другим функциям, включая определение любых необходимых действий для повышения доверия (Приложение F). Например, для удовлетворения ограничений по конкретному размеру или форм-фактору, функция системы, сопоставленная с функцией системы, обозначенной как "другая", может занимать тот же домен привилегий, что и функции обеспечения управления, принятия решений по управлению или инфраструктуры управления, тем самым повышая привилегированность этой функции системы. Если ограничений по размеру или форм-фактору не существует, было бы целесообразно локализовать эту функцию системы в другом месте, чтобы избежать предоставления ей повышенных привилегий. Это повысит доверие в том, что функции обеспечения, принятия решений и инфраструктуры изолированы от других частей системы и не окажут негативного влияния на ее поведение и не создадут возможности для атак.

D.4.2. Основные критерии проектирования механизмов

Для эффективного достижения целей доверенного проектирования безопасности механизмы (т.е. конструктивные элементы и устройства) должны соответствовать четырем основным критериям проектирования. Они должны быть не обходимыми, оцениваемыми, всегда вызываемыми и защищенными от несанкционированного доступа [35]. Как правило, проект любой функции управления, которая обеспечивает защиту, должна соответствовать этим критериям.[71] В таблице 3 кратко описаны основные критерии проектирования.

[71] Аргумент о том, что любая функция управления должна быть не обходимой, оцениваемой, всегда вызываемой и защищенной от несанкционированного доступа, следует из углубленного изучения теоретического анализа процессов систем (STPA), описанного в [36], в частности, из обсуждения причин отказа мер безопасности и способов устранения отказа.

Таблица 3. Основные критерии проектирования механизмов

ОСНОВНЫЕ КРИТЕРИИ ПРОЕКТИРОВАНИЯ	ОПИСАНИЕ
НЕ ОБХОДИМОСТЬ	Механизм не должен быть обходимым
ОЦЕНИВАЕМОСТЬ	Механизм должен быть достаточно маленьким и простым, чтобы его можно было оценить для получения достаточной уверенности в обеспечении защиты, соблюдении ограничений (или цели управления) и правильной реализации механизма. Оценка включает необходимый анализ и тестирование. (Чёткие абстракции, Уменьшение сложности, и Структурная декомпозиция и композиция)
ПОСТОЯННАЯ ЗАДЕЙСТВОВАНОСТЬ	Защита, обеспечиваемая механизмом или функцией, которые не всегда задействованы, не является непрерывной, и, поэтому, потеря может произойти, пока механизм или функция приостановлены или выключены. (Непрерывность защиты)
ЗАЩИЩЁННОСТЬ ОТ НЕСАНКЦИОНИРУ-ЕМОГО ДОСТУПА	Механизм или функция, а также данные, от которых зависит механизм или функция, не могут быть изменены несанкционированным образом.

Критерии проектирования, описанные выше, основаны на обобщенной концепции диспетчера доступа. Концепция диспетчера доступа[72] - это абстрактная модель необходимых и достаточных свойств, которыми должен обладать любой механизм, выполняющий функцию управления доступом через посредничество [21] [37]. Концепция диспетчера доступа является основополагающей концепцией управления доступом для проектирования систем с доверенным доступом. Она определяется как доверенная абстрактная машина, которая опосредует все виды доступа субъектов к объектам [38]. Будучи концепцией абстрактной машины, диспетчер доступа не рассматривает никакой конкретной реализации. Механизм проверки доступа, включающий в себя комбинацию аппаратных и программных средств, реализует концепцию диспетчера доступа для обеспечения основы посредничества в доступе для доверенной безопасной системы.

Обобщенная концепция диспетчера доступа и четыре основных критерия проектирования могут эффективно использоваться в качестве основы для проектирования отдельных элементов системы, совокупностей элементов, сетей и систем, где преднамеренные и непреднамеренные неблагоприятные факторы могут предотвратить возникновение потерь. Концепция диспетчера доступа определяет необходимость строгости проектной деятельности, соизмеримой с доверием к системе или ее составным элементам.[73] Эта концепция описывает абстрактную модель необходимых свойств, которые должны быть реализованы любым механизмом, претендующим на достижение ограничения или набора ограничений, и основу для определения степени удовлетворения этих свойств. Механизм, обеспечивающий успешное ограничение, состоит из двух частей: (1) средства для принятия решения об ограничении или отказе от ограничения и (2) обеспечения исполнения решения. Обеспечение исполнения решения должно в достаточной степени:

- Применять ограничения для достижения только разрешенного и предполагаемого поведения системы и результатов ее работы.
- Обеспечивать самозащиту от целенаправленных атак на механизм, обеспечивающий выполнение решения (включая применение основных критериев проектирования).

[72] Концепция диспетчера доступа описана в принципе «*Доверенное управление системой*» в Приложении Е.
[73] Концептуально концепция диспетчера доступа может быть распространена на любую функцию управления, которая должна обеспечивать соблюдение системных ограничений [39].

- Не допускать самопроизвольных, непредвиденных, ошибочных, небезопасных и недоверенных управляющих воздействий

Характеристики защиты механизмов должны учитывать, но не зависеть от подробного знания возможностей, средств и методов противника.

D.4.3. Анализ отказов функции безопасности

Принцип проектирования «*Защитный отказ*» гласит, что отказ конкретного элемента системы не должен приводить к недопустимым потерям или вызывать другой сценарий потерь. Отказ функции безопасности вызывает особую озабоченность, учитывая необходимость того, чтобы функции безопасности всегда вызывались и действовали правильно. Следовательно, во время проектирования системы необходимо провести анализ отказов для определения воздействия отказа функции безопасности на возможности системы.

При анализе отказов учитываются активы, на которые может повлиять отказ функции безопасности, и связанные с ними последствия потерь. При анализе отказов также учитывается распределение функций между элементами системы и то, как функция системы и комбинация элементов взаимодействуют с другими функциями системы и комбинациями элементов, независимо от конкретных событий и условий, которые могут привести к отказу. Принципы доверенного безопасного проектирования, изложенные в Приложении E, служат руководством и основой для анализа.

Результаты анализа отказов функций безопасности также определяют уровни доверия и цели, а также точность и строгость архитектуры, проекта и методов реализации, используемых для достижения этих целей. Вопросы обеспечения доверия рассматриваются в Приложении F.

НАУКА, ЛЕЖАЩАЯ В ОСНОВЕ БЕЗОПАСНОСТИ

"Каждое из этих [конструктивных] требований [к механизмам] имеет важное значение, поскольку без них механизм не может считаться безопасным. [Необходимость быть защищенным от несанкционированного доступа] очевидна, поскольку, если механизм подтверждения доступа может быть подделан, его способность к подтверждению рушится, как и любая надежда на достижение безопасности через него. [Третье] требование о постоянной задействованности механизма подтверждения доступа просто гласит, что если подтверждение доступа приостановлено (или должно быть приостановлено) для какой-либо группы программ, то эти программы должны рассматриваться как часть аппарата безопасности и быть [защищенными от несанкционированного доступа и поддающимися оценке]. Требование [оцениваемости] не менее важно. В нем указывается, что, поскольку механизм подтверждения доступа является механизмом обеспечения безопасности в системе, необходимо обеспечить возможность проверки правильности его функционирования во всех случаях и его постоянной задействованности. Если этого достичь невозможно, то нет возможности убедиться в том, что подтверждение доступа проводится правильно во всех случаях, и поэтому нет оснований для аттестации системы как защищенной."

-- **Андерсон, Джеймс**
Андерсон Отчет [37]

D.4.4. Ситуационная осведомлённость

Ситуационная осведомлённость является основополагающей целью средств обеспечения безопасности. То есть ситуационная осведомлённость необходима для достижения других целей безопасности и должна учитываться при проектировании. Например:

- Посреднический доступ требует ситуационной осведомлённости в случаях, когда правила предоставления доступа включают в себя время, последовательность, состояние и другие условия о системе и предыдущем доступе.
- Предотвращение и ограничение потерь осуществляется на основе исчерпывающих данных и информации о состояниях и условиях системы (*Обнаружение аномалии*).

Ситуационная осведомлённость требует способности точно обнаруживать, фиксировать, записывать и анализировать необходимые характеристики и детали поведения и действий системы с периодичностью и с детализацией, необходимой для принятия мер и/или информирования внешних сущностей для последующих действий.[74] Насколько это практически возможно, следует избегать ложноположительных и ложноотрицательных результатов.

С учетом потенциальных последствий компрометации возможностей ситуационной осведомлённости и неправомерного определения, используемые механизмы должны соответствовать основным критериям проектирования (раздел D.4.2) с соответствующей строгостью. Системные журналы аудита и другие системные записи часто нуждаются в строгой защите, такой как использование «*Распределённых привилегий*» для доступа и хранения журналов и записей в отдельной подсистеме *(Разделение доменов).*

D.4.5. Соображения по пространству компромиссов

Проектирование системы предполагает принятие решений о пространстве компромиссов. Принятие решений о защите активов основывается на определении оценки активов, при которой определяется критичность и приоритет активов (например, оценка положительного эффекта в достижении целей и отрицательного эффекта для любых потерь, связанных с активом). Критичность и приоритет, основанные на оценке, используются в инвестиционных решениях по типу, строгости и ожидаемой эффективности защиты *(Соразмерная защита).* Решения могут также определяться с учетом затрат и выгод для различных вариантов проекта.

Затраты, связанные с подходом к проектированию доверенной безопасности, включают в себя стоимость приобретения, разработки, интеграции, эксплуатации и поддержания средств безопасности; стоимость средств и функций безопасности с точки зрения их влияния на результативность системы; стоимость сервисов безопасности, используемых системой; стоимость разработки и управления документацией жизненного цикла и обучения; а также стоимость получения и поддержания целевого уровня доверия.

Стоимость анализа для обоснования утверждений о доверенности определённых вариантов проекта также является важным фактором пространства компромиссов. При наличии двух одинаково эффективных вариантов проекта, наиболее привлекательным из них может быть тот, который имеет более низкую относительную стоимость получения доверия, необходимого для демонстрации удовлетворения утверждениям о доверенности. Во всех случаях следует оценивать стоимость

[74] Общие действия организации включают (1) реагирование на аномалии, связанные с безопасностью, например, обучение пользователей или замену компонента системы, ответственного за нежелательное поведение системы, и (2) аудит действий системы, включая оценку подозрительных схем доступа, указывающих на внутренние угрозы, и удовлетворение требований к отчетности, таких как те, которые требуются от финансовых учреждений.

безопасности системы на уровне системы; и учитывать цели обеспечения доверенности и стоимость, обусловленные действиями по обеспечению доверия, необходимого для достижения целей обеспечения доверенности. Принципы доверенного проектирования, такие как *Соразмерная строгость* и *Соразмерная доверенность*, служат основой для анализа пространства компромиссов.

Преимущества того или иного варианта проектирования определяются его эффективностью в обеспечении требуемых возможностей защиты, доверенностью, которая может иметь место при нём, и потенциальными потерями, связанными с ним, учитывая ценность, критичность, подверженность риску и важность защищаемых активов. Оптимальный баланс между затратами и выгодами может быть достигнут за счет использования менее затратного сочетания проектных мероприятий и системных характеристик и функций, а не за счет использования одного дорогостоящего мероприятия, или элемента или функциональности безопасности. Более того, неблагоприятное воздействие на результативность может исключить некоторые варианты обеспечения безопасности.

СОХРАНЕНИЕ РИСКА

"Закон сохранения энергии гласит, что энергия не может быть ни создана, ни уничтожена, она может только изменяться в форме. Этот закон имеет много важных последствий в инженерии, в том числе подразумевая невозможность создания вечного двигателя... Существует параллельный псевдопринцип, который часто предлагается в полушутливой максиме: риск нельзя ни создать, ни уничтожить, его можно только перемещать. Это не универсальная истина, [но] стоит учитывать этот псевдопринцип, потому что часто изменения в проекте часто приводят к "сжиманию шарика риска", только чтобы обнаружить, что риск появляется в другом месте, возможно, в неожиданном месте в системе, что может привести к тому, что защищенная система будет менее безопасной, чем предполагалось при разработке".

-- **О. Сами Сайджари**
Разработка доверенных безопасных систем [62]

Приложение E. Принципы доверенного безопасного проектирования

В этом приложении описываются принципы проектирования, которые служат основой для разработки доверенных безопасных систем.[75] обеспечивают основу для аргументации относительно системы. Они не должны применяться в качестве *правил,* которые должны соблюдаться, а также не должны рассматриваться по приоритетности, последовательности или упорядоченности для предписывающего применения или использоваться в качестве основы для вынесения суждений о соответствии.

Использование принципов проектирования зависит от различных приоритетов и ограничений, которые могут ограничивать или исключать их применение в конкретном контексте.[76] Принципы могут вступать в противоречие с другими принципами, и это противоречие необходимо понимать. На практике эти принципы могут быть соблюдены или реализованы различными и зачастую одинаково эффективными способами. Использование конкретных принципов может меняться в ответ на изменения и расхождения в требованиях, архитектуре, проекте и приемлемости рисков. Поэтому их применение должно планироваться, соответствующим образом определяться и пересматриваться на протяжении всего процесса разработки.

КЛЮЧЕВАЯ ЦЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Важной целью обеспечения безопасности является снижение неопределенности в отношении возникновения и результатов нежелательных событий. Снижение неопределенности нежелательных событий достигается за счет максимально возможного устранения опасностей, подверженности и уязвимости. Там, где устранение их невозможно, их результаты должны контролироваться в максимально возможной степени. Применение принципов проектирования доверенных безопасных систем является средством устранения и контроля опасностей, подверженности и уязвимости, которые приводят к нежелательным событиям [39].

Принципы проектирования доверенной безопасности являются репрезентативными с точки зрения практики сообществ по защищенности, безопасности, надежности, живучести и устойчивости, а также специальных инженерных дисциплин, связанных с этими сообществами. В совокупности цели этих практик представляют собой *конечные цели*, которым должна удовлетворять система для доверенного контроля за неблагоприятными воздействиями. Принципы основаны на опыте исследований, разработок и применения, начиная с раннего внедрения механизмов в доверенные эксплуатируемые системы и заканчивая современными компонентами, средами и системами, и, как ожидается, останутся универсальными для новых, возникающих и развивающихся подходов. Концепции и теоремы из дисциплин, как информатика, вычислительная техника, инженерия систем, системы управления, отказоустойчивость, разработка программного обеспечения и математика, используемые в различных сообществах и специальностях, являются средствами достижения конечных целей.[77] Принципы проектирования доверенной безопасности приведены в таблице 4.

[75] NIST выражает признательность Центру исследований и изучения безопасности информационных систем Военно-морской аспирантуры и корпорации MITRE за значительный вклад в подготовку материалов для этого приложения. Содержание было основано на исследовательских отчетах главных исследователей из этих организаций [21] [39].

[76] Инженерные соображения, связанные с применением принципов разработки доверенных безопасных систем, описаны в [39].

[77] Например, доверенность требует, чтобы механизмы были оцениваемыми (раздел D.4.2). Следовательно, многие принципы касаются уменьшения сложности и управления ею, а также создания систем, которые легче поддаются оценке. Обсуждение того, как системы могут быть слишком сложными, чтобы их можно было проанализировать для обеспечения достаточного доверия, см. в [41].

ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ	ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ
Обнаружение аномалий	Наименьшее количество привилегии
Четкие абстракции	Наименьшее количество разделения
Соразмерная защита	Запас на случай потерь
Соразмерное реагирование	Опосредованный доступ
Соразмерная строгость	Минимальные доверенные элементы
Соразмерная доверенность	Минимизация возможности обнаружения
Композиционная доверенность	Настройки защиты по умолчанию
Непрерывная защита	Защищенный отказ
Эшелонированная защита	Защищенное восстановление
Распределение привилегий	Уменьшение сложности
Разнообразие (Динамичность)	Избыточность
Разделение доменов	Самообеспечение доверенности
Иерархическая защита	Структурная декомпозиция и композиция
Наименьшая функциональность	Подтверждённая доверенность
Наименьшее предоставление доступности	Доверенное управление системой

E.1. Обнаружение аномалий

Принцип: Любая существенная аномалия в системе или ее окружении обнаруживается своевременно, что позволяет принять эффективные ответные меры.

Примечание: Назначение обнаружения аномалий состоит в том, чтобы определить необходимость принятия корректирующих мер для устранения условий потерь, которые возникли или возникнут, если условия, влияющие на поведение системы, сохранятся. Обнаружение аномалий имеет решающее значение для достижения целей контроля потерь для предотвращения и ограничения потерь и их негативных последствий. Обнаружение таких аномалий требует мониторинга поведения и результатов работы системы, чтобы определить, когда происходят какие-либо отклонения от проектного замысла. Это также требует мониторинга условий в среде для определения или прогнозирования тех условий, которые могут вызвать аномалию в системе, если не будут предприняты корректирующие действия.

Аспект обнаружения аномалий «своевременным способом» отражает необходимость как можно раньше обнаружить возникающие условия потерь. Раннее обнаружение расширяет возможности для принятия ответных действий, таких как поэтапное реагирование, и гарантирует, что у ответных действий будет достаточно времени для достижения эффекта. Когда в определении ответных мер участвуют люди, раннее обнаружение позволяет принять более обоснованное решение о надлежащем реагировании.

Обнаружение аномалий может быть реализовано на различных уровнях абстракции (например, система, подсистема, узел, функция, механизм) и может происходить периодическим, апериодическим или управляемым событиями способом. Основой для обнаружения аномалий в системе является ожидание того, что поведение системы, результаты и взаимодействия, как ожидается, будут остаться последовательными, соответствовать некоторой норме или будут детерминированными во всех состояниях и режимах системы. К типам аномалий относятся те, которые связаны с результатами поведения системы; согласованностью состояний; непрерывностью функционирования; целостностью, корректностью и доверенностью элементов системы; конфигурацией системы; а также злоупотреблением или ненадлежащим использованием системы.

Основа для обнаружения аномалий в среде отличается от основы для обнаружения аномалий в системе, поскольку среда не находится под управлением системы. Среда представляет широкий спектр неблагоприятных воздействий на систему, и система проектируется таким образом, чтобы выполнять свои проектные задачи в определенных границах условий среды. Эти границы могут рассматриваться как «норма» для обнаружения аномалий, при которых условия среды, выходящие за рамки нормы или отражающие условия, выходящие за

рамки нормы, могут оказывать неблагоприятное воздействие на систему, что потребует запланированного реагирования для подготовки к надвигающимся трудностям или кризису.

Обнаружение аномалии требует фиксации данных для поддержки всех предполагаемых ответных действий на обнаруженную аномалию, включая данные, связанные с установлением авторства. Следовательно, точность данных, описывающих аномалию, должна быть соизмерима с последствиями сценариев потерь, связанных с аномалией, и неправильных ответных действий при устранении обнаруженной аномалии. Реакция на аномалию часто основывается на отнесении к уникально идентифицируемым сущностям, которые могут быть ответственными за нежелательные действия, поведение или результаты. Для сущностей, не являющихся людьми, корректирующие действия могут включать замену компонентов, ремонт или другие исправления. Для человеческих сущностей это может включать в себя обучение, коррекция поведения или дисциплинарные меры. Неправильное установление авторства может иметь нежелательные последствия, такие как неоправданный ремонт не того элемента системы при сохранении нежелательного состояния или неправомерное увольнение сотрудника. Строгость в установлении авторства определяется необходимостью доказательства того, что сущность несет ответственность за аномалию.

Для определения критериев надлежащего ответного действия или комплекса действий необходимы три аспекта выявления аномалий:

- *Основа для корректности:* Модель системы предоставляет основу, с которой можно сравнить фактическое поведение и результаты, чтобы уверенно сделать вывод о существовании аномалии, а также определить или спрогнозировать возникновение аномалии. Модели системы включают в себя нормальное, аварийное, деградированное и другие состояния/режимы работы системы и учитывают неблагоприятные факторы, которым подвергается система.

- *Сбор данных:* Системы собирают данные самоанализа в виде данных о работоспособности, состоянии, тестировании и других данных, отражающих фактическое поведение и результаты, включая прослеживаемость для поддержки установления авторства. Механизмы сбора данных включают инструментарий, мониторинг, протоколирование, аудит, самотестирование и встроенные тесты.

- *Интерпретация данных:* Интерпретация данных позволяет сделать выводы о неприемлемых или подозрительных событиях, которые произошли (например, об остановке или отказе), которые прогрессируют (например, приближаются к порогу состояния отказа) или которые, как ожидается, могут произойти (т.е. при отсутствии изменений может возникнуть состояние отказа), включая отслеживание ответственных сущностей для принятия соответствующих мер реагирования на события.

Следует проявлять осторожность при использовании конструктивных особенностей, которые могут препятствовать обнаружению аномалий. Было обнаружено, что плохо спроектированные линии защиты для глубокоэшелонированной обороны скрывают возникающие опасные состояния системы, особенно от наблюдателей-людей [40]. При проектировании системы необходимо минимизировать разницу между расчетными и фактическими состояниями и условиями системы.

Два подхода к обнаружению аномалий:

- *Самостоятельное обнаружение аномалии:* Сущность не зависит от другой сущности, чтобы обнаружить аномалию в рамках её предполагаемого проекта. Самостоятельное обнаружение аномалий обычно предполагает аксиоматическое или обусловленное средой предположение о её целостности. Как правило, доверенные элементы имеют возможность самостоятельного обнаружения аномалий. Это означает, что на самом высоком уровне доверенности сущность должен быть в состоянии в значимой степени оценивать свое внутреннее состояние и функциональность на различных этапах выполнения. Обнаруженные аномалии должны коррелировать с предположениями о доверенности, сделанными для сущности.

- *Зависимое обнаружение аномалии:* Представляющая интерес сущность зависит от другой сущности для некоторых или всех обнаруженных аномалий. Когда сущность, представляющая интерес, полагается на другую сущность для какой-либо части оценки, эта сущность должна быть, по крайней мере, такой же доверенной, как и сущность, представляющая интерес.

Ссылки: [20] [40] [43]

E.2. Четкие абстракции

Принцип: Абстракции, используемые для характеристики системы являются, простыми, четко определенными, точными, конкретными, необходимыми и достаточными.

Примечание: Абстракции могут помочь управлять сложностью системы [24]. Ясность в абстрактных представлениях системы способствует точному пониманию системы и того, как система функционирует для обеспечения требуемых возможностей. Четкие абстракции также снижают вероятность недопонимания или неправильного толкования того, что представлено абстракцией. Применение принципа четкой абстракции означает, что система имеет простые, четко определенные интерфейсы и функции, которые обеспечивают непротиворечивое и интуитивно понятное представление о данных и способах управления ими. Ясность (например, точность, чёткость, простота, необходимость, достаточность) интерфейсов системы в сочетании с точным определением функционального поведения интерфейсов способствует простоте анализа, контроля и тестирования, а также правильному и безопасному использованию системы. Примеры, отражающие применение этого принципа, включают исключение избыточных неиспользуемых интерфейсов; сокрытие информации;[78] и предотвращение семантической перегрузки интерфейсов или их параметров (например, отказ от использования одной функции для обеспечения различных функциональных возможностей в зависимости от того, как она используется).

Важно обеспечить надлежащую строгость при разработке системных абстракций в процессе проектирования. Ясность абстрактного представления системы требует использования четко определенного синтаксиса и семантики с последующими уточнениями, необходимыми для обеспечения того, чтобы представления были четко определенными, точными, необходимыми и достаточными. Четкие абстракции способствуют доверенности в анализе, проверке и правильном использовании системы. Абстракции могут быть достигнуты с помощью моделей, включая языки системного моделирования.

Ссылки: [2] [20] [21] [24]

E.3. Соразмерная защита

Принцип: Стойкость и тип защиты, обеспечиваемой элементу системы, соизмеримы с наиболее значительным неблагоприятным последствием, возникающим в результате отказа этого элемента.

Примечание: Стойкость и эффективность защиты элемента системы должны быть пропорциональны его значимости. По мере увеличения значимости защита этого элемента также должна увеличиваться в той же степени. Значимость определяется наиболее значительным неблагоприятным последствием, связанным с элементом системы или доверием, которое оказывается этому элементу. Защита может обеспечиваться в форме собственной самозащиты элемента системы, за счёт защиты, обеспечиваемой архитектурой системы, или за счёт защиты, обеспечиваемой другими элементами. Необходимая степень защиты не зависит от этих вариантов проектирования (или других, таких как распределенное и централизованное проектирование), которые иногда называют безопасной распределенной композицией [2]. Кроме того, уверенность в эффективности защиты, предоставляемой элементу системы, также должна возрастать соразмерно потребности. Этому служит принцип *Соизмеримой строгости*.

Ссылки: [2] [21]

E.4. Соразмерное реагирование

Принцип: При проектировании системы интенсивность планируемых действий по реагированию соответствует необходимой оперативности для борьбы с последствиями каждого сценария потерь.

[78] Термин "сокрытие информации", также называемый программированием, не зависящим от представления, является дисциплиной проектирования, призванной гарантировать, что внутреннее представление информации в одном компоненте системы не будет видно другому компоненту системы, вызывающему или привлекающему первый компонент, так что опубликованная абстракция не будет зависеть от того, как данные могут управляться внутри.

Примечание: При выборе реакции на обнаруженную аномалию учитываются три фактора, определяющие влияние реакции на потери и систему:

- Эффективность и интенсивность разработанных мер реагирования для непосредственного устранения аномалии и предотвращения или ограничения потерь.
- Прямой, остаточный или побочный эффект реагирования для системы.
- Возможности, которые остаются для принятия других мер реагирования, если выбранная реакция не достигает желаемого результата.

Реагирование может осуществляться с помощью комбинации ручных, полуавтоматических, полностью автоматических или автономных средств. При этом действия по реагированию зависят от определения того, какое реагирование необходимо, и от уведомления или сигнала, вызывающего действия по реагированию.

Соразмерные меры реагирования требуют рассмотрения взаимосвязи «реакция-эффект-последствия», связанной с конкретной потерей. В идеале, для любой конкретной потребности в мерах реагирования, однократное действие должно быть эффективным для решения проблемы потери и не должно иметь связанных с этим негативных последствий. На практике, из-за сложности и пределов определенности, действия по реагированию могут не дать желаемого эффекта, могут усугубить проблему или могут вызвать другую проблему. Требуемым балансом является тот, который определяет, будут ли действия по реагированию изначально более интенсивными или менее интенсивными, когда и каким образом. Серьезность проблемы и время, необходимое для эффективного реагирования, диктуют стратегию непрерывного реагирования, характеризующуюся двумя крайностями:

- *Дозированное реагирование:* - Дозированное реагирование первоначально является наименее интенсивным или эффективным действием, которое возможно для предотвращения продолжения или эскалации потерь, и осуществляется с учетом возможных побочных результатов, связанных с действиями по реагированию. Дозированное реагирование позволяет предпринимать все более интенсивные действия, если ситуация с потерями сохраняется или обостряется.

- *Ударное реагирование:* Ударное реагирование является наиболее агрессивным и эффективным действием для предотвращения продолжения или эскалации потерь и делает это без учета потенциальных побочных эффектов, связанных с действиями по реагированию. Ударное реагирование признает, что серьезность потерь оправдывает наиболее агрессивные действия, даже если этот вариант не предусматривает альтернатив, если он не принесет желаемого или ожидаемого эффекта, или приведет к возникновению других потерь.

Без своевременного выявления потенциальных потерь могут отсутствовать возможности для дозированного реагирования. Своевременное обнаружение способствует адекватному реагированию, что, в свою очередь, увеличивает возможности для дозированного реагирования.

Ссылки: [40]

E.5. Соразмерная строгость

Принцип: Строгость, связанная с проведением проектных работ, обеспечивает уверенность, необходимую для устранения наиболее значительных неблагоприятных последствий, которые могут возникнуть.

Примечание: Строгость определяет масштаб, глубину и детализацию проектных работ. Строгость - это средство обеспечения уверенности в результатах завершенных проектных работ. Как правило, повышение строгости приводит к повышению уверенности в результатах работ. Кроме того, повышение уверенности снижает неопределенность, что также может снизить риск или обеспечить лучшее понимание того, что следует предпринять для достижения снижения риска. Взаимосвязь между строгостью и критичностью данных и информации, используемой для принятия решений, учитывается в практике системного анализа [4].

Принцип соразмерной строгости помогает обеспечить учет концепции строгости в качестве равнозначного

фактора при оценке возможностей, побочных эффектов, затрат и сроков при планировании и проведении проектных работ, выборе методов и инструментов, а также при подборе персонала. Повышение строгости может привести к увеличению затрат на персонал, методы и инструменты, необходимые для выполнения сложных проектных работ, или к увеличению сроков выполнения работ с ожидаемой строгостью. Любое увеличение затрат, которое может возникнуть, может быть оправдано получением уверенности в результативности системы по ограничению потерь, а также в способности системы выполнять свои функции. Поэтому, строгость, связанная с проектной деятельностью, должна быть соизмерима со значимостью наиболее неблагоприятных последствий, связанных с этой деятельностью.

Ссылки: [2] [4]

E.6. Соразмерная доверенность

Принцип: Элемент системы заслуживает доверия на уровне, соизмеримом с наиболее значительными негативными последствиями, возникающими в результате выхода из строя этого элемента.

Примечание: Доверенный элемент постоянно проявляет свойства доверия в течение того времени, когда от него зависят другие элементы системы. Степень доверенности, необходимая для доверенного элемента, определяется теми сущностями, которые зависят от этого элемента. Необходима определенная основа для принятия решений о доверии и доверенности. Основа включает в себя выявление доверия, которое должно быть оказано элементу системы, выявление доверенности, которую демонстрирует элемент, и сравнение доверенности различных элементов системы. Этот принцип особенно актуален при рассмотрении систем и элементов со сложными цепочками зависимостей доверия.

Ссылки: [4] [20]

E.7. Композиционная доверенность

Принцип: Проект системы является доверенным для каждой совокупности взаимодействующих элементов системы.

Примечание: Доверенность совокупности составленных элементов системы не может быть принята на основании утверждений о доверенности каждого отдельного элемента в совокупности. Кроме того, нельзя считать, что доверенность совокупности составных доверенных элементов системы равна доверенности наименее доверенного элемента в совокупности. По определению, система представляет собой совокупность взаимодействующих элементов системы. Каждая функция системы является результатом эмерджентного поведения совокупности элементов системы. Аналогично, доверенность составленного набора элементов системы является эмерджентным свойством этой совокупности. Следовательно, доверенность составленного набора системных элементов (т.е. агрегата) для данной функции системы должна определяться путем рассмотрения агрегата как единого дискретного элемента. Принцип композиционной доверенности рассматривает вопрос о том, как можно аргументировать доверенность на уровне системы, учитывая то, как составные элементы системы образуют систему, придерживаясь принципов композиции.

Ссылки: [2] [4] [36] [42]

E.8. Непрерывная защита

Принцип: Защита, предусмотренная для элемента системы, должна быть эффективной и непрерывной в течение всего времени, когда требуется защита.

Примечание: Возможности защиты должны быть непрерывными во всех соответствующих состояниях, режимах и переходах системы, чтобы была уверенность в том, что система может эффективно обеспечивать требуемые возможности при одновременном управлении потерями. Непрерывная защита требует соблюдения следующих принципов:

- *Доверенное управление системой:* Каждое действие управления ограничено механизмом, который может защитить себя от несанкционированного доступа. Достаточная уверенность в корректности и полноте механизма может быть получена в результате анализа и тестирования.

- *Защищённый отказ* и *Защищённое восстановление:* Защищённое состояние сохраняется во время ошибок, сбоев, отказов и успешных атак, а также во время восстановления активов или возвращения к нормальному, ухудшенному или альтернативному режиму работы.

Непрерывная защита применяется ко всем конфигурациям, состояниям и режимам системы, а также к переходам между этими конфигурациями, состояниями и режимами. Проектирование системы должно обеспечивать, чтобы средства защиты были скоординированы и составлены таким образом, чтобы они не противоречили и взаимно дополняли друг друга во всех аспектах структуры системы, не связанных с поведением, и поведенческих аспектах функционирования системы и потоков данных.

Несмотря на то, что схема непрерывной защиты применяется в течение всего времени, в течение которого требуется защита, иногда функция защиты намеренно отключается (например, преднамеренный перевод в «пониженную готовность»[79]). Преднамеренное отключение/понижение защиты является исключительным случаем и, следовательно, не нарушает этот принцип. То есть принцип непрерывной защиты действует только в течение всего времени, когда защита требуется, а не когда она сознательно и намеренно отключена.[80]

Ссылки: [21]

E.9. Эшелонированная защита

Принцип: Потери предотвращаются или сводятся к минимуму путем использования нескольких скоординированных механизмов.

Примечание: Скоординированное развертывание нескольких защитных механизмов для системы помогает избежать единых точек отказа. Принцип эшелонированной защиты имеет три составляющие:

- В соответствии со сценариями потерь следует формировать несколько рубежей или барьеров защиты.
- Управление потерями не должно основываться на одном защитном элементе.
- Последовательные барьеры должны быть разнообразными по своей природе и включать технические, операционные и организационные барьеры [52].

Эшелонированная защита требует использования согласованных механизмов (активных) внутри структуры архитектуры (пассивных), что обеспечивает достижение характеристик глубины.[81] В идеале, начальные рубежи защиты предотвращают потери, в то время как последующие рубежи защиты блокируют эскалацию сценария потерь и/или сдерживают потери и потенциальные последствия, когда это необходимо. Стратегия эшелонированной защиты рассматривает сценарии потерь с точки зрения возможностей их предотвращения или сдерживания. Она также использует возможности использования активных или пассивных механизмов или ограничений для достижения целей управления потерями.

Координация механизмов эшелонированной защиты (т.е. сочетание координации структуры, данных и потоков управления) в сочетании с другими принципами проектирования (например, *Обнаружение аномалий*, *Соразмерное реагирование*) отражает стратегию проектирования, направленную на достижение заданных целей по предотвращению потерь.

Хотя при эшелонированной защите возможности защиты распределяются между многими компонентами, стратегия эшелонированной защиты может также рассматривать распределенный состав рубежей защиты.

---

[79] Пониженная готовность - это возможность обойти обычные блокировки критически важного оборудования (например, оборудования, которое не должно быть отключено, иначе функция предназначения не будет выполнена) в условиях противоборства [51].

[80] Однако, применение возможности преднамеренного отключения/понижения защиты требует дополнительных механизмов, устройств управления и соответствующего анализа для соблюдения ограничений, чтобы предотвратить непреднамеренную активацию возможности преодоления.

[81] Хотя в этом разделе речь идет только о механизмах, эшелонированная защита может включать в себя сочетание технических, операционных и организационных элементов. Подробнее об эшелонированной защите можно прочитать в [52].

Возможность защиты, обеспечиваемая одним компонентом системы, является потенциальной единой точкой отказа или узким местом для результативности системы. Это может также вызывать и другие проблемы. Распределенный состав защитного слоя может обеспечивать дополнительные возможности в рамках координации слоев.

Эшелонированная защита является, отчасти, формой принципа *Защищенного отказа.* Это помогает достичь цели, заключающейся в том, что отказ элемента системы не должен приводить к неприемлемым потерям. Однако она не позволяет достичь цели, заключающейся в том, что отказ элемента системы не должен приводить к другому сценарию потерь.

Ссылки: [2] [21] [40] [47]

E.10. Распределение привилегий

Принцип: Несколько уполномоченных сущностей осуществляют координацию, прежде чем будет разрешено выполнение операции в системе.

Примечание: Распределение привилегий[82] - это средство, требующее согласия и координации от нескольких сущностей при выполнении операции, тем самым предотвращая действие одной сущности в одиночку. Распределение привилегий разделяет, дробит или каким-либо другим способом распределяет привилегии, необходимые для выполнения операции, между несколькими сущностями. Такое распределение включает набор правил, условий и ограничений, которые описывают, как несколько сущностей должны взаимодействовать посредством позитивных действий, прежде чем запрошенная операция может быть продолжена и завершена. Правила, условия и ограничения могут отражать комбинации следующих факторов:

- *Одновременные действия*: Несколько различных авторизованных сущностей выполняют команду в течение заданного промежутка времени.
- *Последовательные действия:* Несколько различных сущностей взаимодействуют в линейной последовательности действий, где каждое последующее действие возможно только после успешного завершения предыдущего действия.
- *Параллельные действия:* Несколько сущностей выполняют одновременно последовательности действий, и успех достигается либо путем консенсуса результатов каждого параллельного действия, либо путем голосования среди участников.

Для преодоления распределенных привилегий требуется сговор для совершения несанкционированных или неправильных действий. В случае атаки распределение привилегий заставляет противника нацеливаться на все сущности, между которыми распределяются привилегии.

Ссылки: [21] [46]

E.11. Разнообразие (Динамичность)

Принцип: Проектирование системы обеспечивает необходимые возможности за счет изменения структуры, поведения, или потоков данных или управления.

Примечание: Проект системы, который содержит разнообразие, помогает избежать типовых отказов и вводит непредсказуемость для злоумышленников, тем самым усложняя им планирование и выполнение того, где, когда и как им проводить свои атаки. В то время как поведение системы, которое является результатом проектирования, может быть непредсказуемым с точки зрения противника, сам проект должен быть предсказуемым и проверяемым в достижении только намеченных результатов. Варианты разнообразия включают разнообразие структурных и архитектурных элементов проекта системы, функциональных и поведенческих элементов системы, интерфейсов и взаимосвязей между ними, потоков данных и управления, а также выбор технологий и компонентов. Разнообразие может заключаться в:

- Фиксированных или статических характеристиках системы (например, несколько экземпляров элемента системы, несколько каналов связи)

[82] Зальтцер и Шредер [46] первоначально назвали это разделением привилегий. Это также эквивалентно разделению обязанностей.

- Переменных или динамических характеристиках системы (например, реконфигурация, перемещение, обновление элементов системы; случайная маршрутизация данных по различным каналам связи от источника к месту назначения; возможность изменять аспекты поведения, структуры, данных или конфигурации системы случайным, но тем не менее поддающимся проверке способом)

Подход к проектированию, который включает в себя разнообразие в структуре, конфигурации, коммуникациях, протоколам и схожих или несхожих элементах системы (например, N-версии, гетерогенность), увеличивает неопределенность из-за повышенной сложности проекта, а также поведения и результатов, которые обусловлены эмерджентными эффектами, побочными эффектами и взаимодействием возможностей. Это обуславливает необходимость уверенности в том, что подход к проектированию обеспечит только разрешенное и намеченное функциональное поведение, даст только разрешённые и предполагаемые результаты и сделает это таким образом, который позволяет контролировать побочные эффекты, возникновение и взаимодействие возможностей.

Варианты разнообразия включают целенаправленно вносимые регулярные или нерегулярные изменения в систему (например, реализация концепции динамичности). Проект, включающий динамичность, может (1) усложнить планирование атаки противника, (2) уменьшить потенциал воздействия неблагоприятных факторов, не связанных с противоборством, (3) предоставит запас для обеспечения требуемых возможностей при одновременном снижении фактических потерь и (4) защитить от последствий атаки. Динамические изменения могут относиться либо к изменению цели, либо к изменению поведения цели при выполнении ею своих действий (например, скачкообразная перестройка частоты усложняет попытки перехвата или глушения сигналов в беспроводной связи).

Неопределенность и сниженная предсказуемость, связанные с использованием разнообразия и динамичности при проектировании, могут быть проблематичными в тех случаях, когда это препятствует или затрудняет обеспечение уверенности в том, что система будет функционировать и давать результаты только в том виде, в каком это установлено и предусмотрено. Важно различать, в чём заключается неопределённость: (1) неопределённость в том, как система достигает конечной цели (т.е. в средствах достижения цели) или (2) неопределенность в том, что цель будет достигнута (т.е. в достижении цели). Проект, в котором используется разнообразие и динамичность, должен быть основан на получении уверенности в том, что система будет давать только желаемые результаты, несмотря на неопределенность в том, как именно достигаются желаемые результаты. Это представляет собой специфику проектов, основанных на разнообразии и динамичности. Затраты на разнообразие (например, на оборудование, программное обеспечение, техническое обслуживание, обучение, гарантии) могут превышать ценность или эффективность, которые оно обеспечивает.

Ссылки: [20] [47] [45]

E.12. Разделение доменов

Принцип: Домены с отчётливо различными потребностями в защите разделяются физически или логически.

Примечание: Разделение доменов обеспечивает улучшенный контроль и, следовательно, защиту функций системы и потоков данных. Контроль в отношении разделенных доменов ограничивает степень, в которой сущность или домен подвергается влиянию или способны влиять на какую-либо другую сущность или домен, тем самым усиливая защиту домена. Это достигается посредством контроля информационных потоков и данных между доменами, а также контроля над использованием возможностей системы в разных доменах.

Различные потребности в защите, которые используются для определения доменов, могут рассматриваться с точки зрения защиты домена от влияния внешних сущностей (т.е. восприимчивость) и защиты внешних сущностей от ошибочного поведения, которое происходит внутри домена (т.е. локализация). Это различие может включать в себя отделение критических функций от менее критических, например, отделение функций управления полетом транспортного самолета от функций экологического контроля, которые поддерживают безопасную среду для перевозимого груза и пассажиров.

Исторически разделение доменов использовалось для обеспечения разделения ролей или привилегий. Например, система может отделять "административный" или "супервизорный" домен от "пользовательских" доменов. Административный домен доступен только системным администраторам с соответствующими

привилегиями, а конкретные административные функции могут выполняться только администраторами из административного домена. Аналогично, данные, предназначенные для доступа только администраторов и административных функций (например, конфигурации системы), хранятся и доступны только в этом домене, обеспечивая необходимую защиту данных.

Разделение доменов требует, чтобы домен содержался внутри его собственной защищенной подсистемы, так чтобы прямой доступ к элементам домена был возможен только с помощью процедур или функций защищенной подсистемы. Концепция изоляции позволяет реализовать разделение доменов. Изоляция ограничивает степень, с которой один домен может влиять на другие сущности или быть подверженным их влиянию. Проблема заключается в том, что элементы системы в пределах доменов иногда должны взаимодействовать с другими элементами и средой для обеспечения их возможностей. Каждый интерфейс, который является результатом проектных решений, может ослабить разделение доменов, но при одновременном выполнении требований к возможностям системы. Внешние запросы на ресурсы или функции в пределах защищенных подсистем обрабатываются на этих интерфейсах. Межсетевые экраны, диоды данных и междоменные решения (CDS) являются примерами механизмов, которые обеспечивают различные степени контроля взаимодействия между разделенными доменами.

Шифрование - это еще один механизм, часто используемый для разделения доменов. Например, связь между отдельными подсистемами в пределах домена может быть зашифрована ключом, который известен только подсистемам в пределах домена. Если общий модуль или подсистема хранения используется для нескольких доменов, шифрование может использоваться для ограничения доступа к информации доменом, который владеет ключом для расшифровки.

Ссылки: [21] [43]

E.13. Иерархическая защита

Принцип: Элемент системы не обязательно должен быть защищен от более доверенных элементов.

Примечание: Иерархическая защита является упрощающим допущением для компромиссных решений, помогающим определить, на что необходимо делать упор в обеспечении защиты и какова степень ее эффективности. Это упрощающее допущение делает уязвимыми элементы системы, которые зависят от более доверенных элементов. Это предположение основывается на подтвержденных утверждениях о доверии относительно более доверенного элемента и приемлемой неопределенности, связанной с поведением вне области проверенных утверждений о доверии. Например, системы могут включать в себя человеческий элемент, который часто является более доверенным элементом. Утверждения о доверенности человека нарушаются в случае злонамеренной инсайдерской угрозы. Степень, до которой любой элемент считается заслуживающим доверия, имеет пределы, и вне этих пределов этот элемент не должен считаться заслуживающим доверия. В вырожденном случае, наиболее доверенный элемент системы должен защищать себя от всех других элементов. Например, если ядро операционной системы считается наиболее доверенным компонентом в системе, оно должно защищать себя от менее доверенных приложений, которые она поддерживает. Однако приложения не нуждаются в защите от ядра операционной системы.

Ссылки: [2] [43]

E.14. Наименьшая функциональность

Принцип: Каждый элемент системы способен выполнять свои требуемые функции, но не более того.

Примечание: Подверженность и уязвимость неоправданно возрастают, когда элемент системы предоставляет больше функциональных возможностей, чем необходимо для достижения его целевого назначения. Наименьшая функциональность снижает потенциальную подверженность и уязвимость и уменьшает объём анализа доверенности элемента системы и возможных потерь. Самая строгая интерпретация наименьших функциональных возможностей заключается в запрете любых функций элемента системы, которые не требуются. Если это невозможно или нецелесообразно, ненужные функции элемента системы должны быть отключены, заблокированы или переведены в "безопасный" режим, который не позволяет функциям быть используемым. Во

всех остальных случаях для предотвращения доступа к ненужным функциям и их использования можно использовать опосредованный доступ.

Примером того, когда невозможно или нецелесообразно избегать ненужных функций, является использование готовых коммерческих компонентов (COTS). COTS компоненты обычно содержат функции, выходящие за рамки тех, которые необходимы для выполнения их целевого назначения. В таких случаях компоненты должны быть сконфигурированы так, чтобы было разрешено выполнять только те функции, которые необходимы для выполнения их назначения, и были запрещены или ограничены функции, которые не требуются для выполнения их назначения.

Ссылки: [2] [21]

E.15. Минимальное предоставление доступности

Принцип: Элементы системы и другие ресурсы доступны и способны выполнять свои проектные задачи только в течение того времени, на которое они необходимы.

Примечание: Минимальное предоставление доступности снижает подверженность. Оно ограничивает степень, в которой функции, ресурсы, данные и информация остаются присутствующими, доступными и пригодными для использования, когда они не требуются, тем самым уменьшая возможность их непреднамеренного или несанкционированного использования, модификации или активации.

Самая широкая интерпретация минимального предоставления доступности заключается в том, чтобы не устанавливать, не внедрять и не запускать элементы и ресурсы системы до тех пор, пока это не потребуется, и полностью удалять элементы системы или отключать элементы и ресурсы системы, когда они больше не требуются. Когда это невозможно или нецелесообразно, эти элементы и ресурсы системы должны быть полностью отключены, заблокированы или переведены в безопасный режим, чтобы предотвратить их функционирование или использование. Наконец, когда невозможно отключить, заблокировать или перевести в безопасный режим, доступ к этим элементам и ресурсам должен быть опосредован для ограничения времени и продолжительности их использования *(Опосредованный доступ).*

Для использования активного элемента или ресурса системы должны быть выполнены три условия, а два из этих условий применимы к неактивным элементам или ресурсам:

- *Наличие (активное и неактивное):* элемент или ресурс системы должен быть установлен, загружен, находиться в памяти (программное обеспечение) и настроен.

- *Доступность (активное и неактивное):* элемент или ресурс системы должен быть вызван, с ним необходимо взаимодействовать или управлять им.

- *Способность к функционированию (активное):* элемент или ресурс системы должен иметь способность выполнения (т.е. запущен, активирован или подготовлен) для предоставления сервиса или выполнения функции.

Минимальное предоставление доступности отражено в таких понятиях, как санация, стирание и очистка памяти и/или мест хранения; отключение, удаление и отсоединение сетевых портов, системных интерфейсов и сервисов, предоставляемых системными интерфейсами; отключение питания и отсоединение аппаратных средств, когда это не требуется; и инсталлирование экземпляров программного обеспечения непосредственно перед необходимостью и исключение экземпляров, когда они больше не требуется. Минимальное предоставление доступности имеет дополнительные преимущества, которые включают упрощение процессов:

- Очистки элемента системы для устранения поврежденных аспектов или побочных эффектов.
- Восстановления элемента системы в известное состояние (т.е. обновление).
- Минимизации времени, в течение которого элементы системы подвергаются воздействию среды, атакам и ошибочному поведению.

Когда элементы или ресурсы системы удаляются, а затем восстанавливаются по мере необходимости, должен быть доверенный образ элемента системы и доверенная возможность инсталлирования этого элемента системы для его использования в течение ограниченного времени.

Ссылки: [53]

E.16. Наименьшие привилегии

Принцип: Каждому элементу системы предоставляются привилегии, необходимые для выполнения определенных функций, но не более.

Примечание: Элементы системы могут быть реализованы такими сущностями, как аппаратное обеспечение, микропрограммное обеспечение, программное обеспечение и персонал. При проектировании система должна наделяться возможностью ограничивать область действий элемента системы. Это имеет два желательных эффекта: (1) влияние отказа, повреждения или неправильного использования элемента сводится к минимуму, и (2) упрощается анализ элемента системы. Проектирование, основывающееся на соображениях наименьших привилегий, приводит к достаточно мелкой градации привилегий и возможности для распределения мелко-градуированных привилегий между людскими и машинными элементами.

Применение принципа наименьших привилегий означает выделение элементу системы только тех привилегий, которые необходимы для того, чтобы этот элемент мог выполнять требуемые от него функции. Это может включать необходимость изменения, удаления, использования или настройки ресурса, а также авторизации, запуска/включения или остановки/отключения процесса [20].

Принцип наименьших привилегий может служить основой для использования других принципов, таких как применение *Разделения доменов* и *Структурированная декомпозиция и композиция.* То есть модули системы могут быть спроектированы таким образом, что только элементы системы, инкапсулированные в модуле, напрямую доступны или управляются функциями внутри модуля, что способствует реализации наименьших привилегий.

Ссылки: [2] [20] [21] [46]

E.17. Наименьшее совместное использование

Принцип: Ресурсы системы совместно используются элементами системы только при необходимости и как можно меньшим числом элементов.[83]

Примечание: Совместное использование с помощью общего механизма и других средств может повысить восприимчивость ресурсов системы (например, данных, информации, системных переменных, интерфейсов, функций, сервисов) к несанкционированному доступу, раскрытию, использованию или модификации и может отрицательно сказаться на возможностях, предоставляемых системой. По словам Зальцера и Шредера [46], "каждый совместно используемый механизм (особенно механизм, включающий совместно используемые переменные) представляет собой потенциальный путь передачи информации между пользователями и должен быть разработан с особой тщательностью, чтобы быть уверенным, что он непреднамеренно не нарушает безопасность ". Проектирование, применяющее наименьшее совместное использование, помогает уменьшить неблагоприятные последствия совместного использования системных функций, состояний, ресурсов и переменных различными элементами системы. Элемент системы, который нарушает общее состояние или общие переменные, потенциально может повредить другие элементы, поведение которых зависит от состояния. Минимизация совместного использования также помогает упростить проект и реализацию [54].

Два критерия обеспечивают основу для применения принципа наименьшего совместного использования: 1) совместное использование только при крайней необходимости и 2) минимизация совместного использования, если это допустимо. Первый критерий - это компромиссное решение, в котором сопоставляются затраты и выгоды от совместного использования ресурсов с увеличением подверженности, возникающей в результате совместного использования. Второй критерий - это ограничение степени совместного использования.

Ссылки: [2] [21] [46] [54] [55]

[83] Исторически хорошо известный принцип построения системы безопасности "наименьший общий механизм" является примером наименьшего совместного использования. Принцип наименьшего общего механизма описан в [55].

E.18. Запас на случай потерь

Принцип: Система проектируется для работы в пространстве состояний, достаточно удаленном от порогового значения, при котором возникают потери.

Примечание: Запасы на случай потерь определяются разницей между консервативным пороговым значением, при котором ожидается, что система будет работать в неблагоприятных условиях, и точкой, при которой неблагоприятные условия приводят к отказу. Запасы на случай потерь создаются проектными средствами, для поддержания условий эксплуатации и связанных с ними уровня неблагоприятных факторов на некотором расстоянии (т.е. консервативном пороге) от расчетного критического порога неблагоприятных воздействий или порога, приводящего к возникновению потерь. Запасы на случай потерь также позволяют увеличить время (1) обнаружения необходимости действий по реагированию *(Обнаружение аномалий*), (2) определения, каким должно быть реагирование (*Соразмерное реагирование)* и (3) завершения выбранных действий по реагированию. Когда существует неопределенность в отношении эффективности действий по реагированию, запасы на случай потерь должны обеспечивать время для оценки эффективности действий по реагированию, определения любых необходимых дополнительных действий и завершения любых выбранных действий.

Неопределенность может быть обусловлена средой эксплуатации, проектом и реализацией системы, использованием и поддержкой системы, а также неблагоприятными факторами, с которыми сталкивается система. Запасы на случай потерь эффективны для устранения неопределенности в отношении того, как и когда происходит событие, вызывающее потери. В частности, запасы на случай потерь эффективны для устранения неопределенности, связанной с:

- Грамотно разработанными и осуществленными атаками, включая атаки, которые сохраняются и эволюционируют с течением времени.
- Неизвестными, не поддающиеся количественной оценке и недооцененными предрасположенностями, угрозами, уязвимостями, опасностями и связанными с ними рисками.

Для проектов, в которых предусмотрены запасы на случай потерь, неопределенность в отношении неблагоприятных факторов затрудняет определение пороговых значений, приводящих к возникновению потерь. Запасы на случай потерь при проектировании должны определяться с учетом баланса между определенностью (т.е. тем, что произошло и может повториться) и неопределенностью (т.е. тем, что не произошло, но может произойти, или тем, что произошло, но может произойти и по-другому). Сценарии потерь, которые включают увеличение потерь и оценку критического порога возникновения потерь, полезны при принятии проектных решений, учитывающих запасы на случай потерь. Сценарии потерь также помогают определить пределы принятия решений, основанных на неблагоприятных факторах, из-за неопределенности в знаниях о неблагоприятных факторах (т. е. неблагоприятные факторы недостаточно известны, понятны или просто неизвестны).

Для определения запасов на случай потерь должен использоваться анализ чувствительности. К числу других факторов, влияющих на расчёт запасов на случай потерь, относятся сложность системы, использование новых технологий или старых технологий новыми способами, а также степень внедрения новых сред. Дополнительным фактором является возможность проведения всестороннего и эффективного тестирования. Ограничения на охват и эффективность тестирования системы для реальных, смоделированных или эмулированных неблагоприятных условий требуют увеличенных запасов на случай потерь, чтобы учесть остающуюся неопределенность. Размер запасов может со временем уменьшаться, по мере выявления и исправления неизвестных и недооцененных сценариев потерь. Размер запасов также может потребоваться увеличить с течением времени, по мере того как возможности вредоносного воздействия становятся все более изощренными.

Ссылки: [6] [23] [40] [45] [56] [57] [63]

E.19. Опосредованный доступ

Принцип: Весь доступ к элементам системы и операции с ними являются опосредованными.

Примечание: Опосредованный доступ является основополагающим принципом при проектировании безопасных систем. Назначением опосредованного доступа является:

- Установление ограничений на доступ к системе и ее использование
- Снижение вероятности увеличения потерь

- Уменьшение степени увеличения и распространения потерь

Опосредованный доступ основан на взаимодействии между сущностью и целевым элементом системы и имеет два аспекта:

- *Доступ к элементу системы*: Запрашивающая сущность имеет только санкционированный доступ к целевому элементу системы.

- *Использование элемента системы*: Запрашивающей сущности разрешено выполнять только санкционированные операции с целевым элементом системы.

Опосредованный доступ состоит из двух частей: (1) принятие решения о посредничестве в доступе на основе политики и (2) осуществление решения о посредничестве в доступе. Решение о посредничестве в доступе может включать в себя условные ограничения, которые дополнительно ограничивают доступ (например, роль, время суток, состояние или режим системы или продолжительность работы). Если доступ недостаточно опосредован, нет возможности ограничить взаимодействие элементов системы (включая человеческие и машинные элементы), чтобы обеспечить то, что в итоге будет только санкционированное поведение и запланированные результаты.

Опосредованный доступ достигается с помощью механизма управления опосредованным доступом. В основополагающих работах по компьютерной безопасности механизм эталонной проверки был определен как обобщенная форма любого механизма, который является реализацией концепции диспетчера доступа (раздел D.4.2). Диспетчер доступа обеспечивает доверенную проектную основу для демонстрации доверенности механизма опосредованного контроля доступа. Основные критерии проектирования (раздел D.4.2) представляют собой усовершенствованную версию обобщенной концепции диспетчера доступа. Опосредованный доступ может накладывать ограничения, описанные в принципах *Распределённые привилегии, Наименьшие привилегии и Наименьшее совместное использование.*

Являясь основной функцией безопасности, опосредованный доступ может привести к снижению производительности, если он будет неправильно спроектирован и реализован. Использование наименее общего механизма является одним из способов сокращения узких мест, такой подход называется *эффективным опосредованным доступом* [21].

Ссылки: [2] [21] [37] [40] [46] [58]

E.20. Минимум доверенных элементов

Принцип: Система содержит как можно меньше доверенных элементов системы.

Примечание: Минимизация доверенных элементов системы - это рассмотрение пространства компромиссов «Затраты – Выгоды», используемого для функционального распределения доверия в системе. Потребность в доверии связана с функцией, предоставляемой элементом системы, и эта потребность не зависит от любого распределения доверия между несколькими элементами в архитектуре. Таким образом, компромиссное решение заключается в том, как наилучшим образом распределить доверие между элементами системы с учетом функций, которые они предоставляют, и как элементы лучше всего распределяются по всей архитектуре, где распределение является обоснованной необходимостью. Минимизация доверенных элементов системы является одним из соображений при принятии такого решения.

Доверенные элементы, как правило, являются более дорогостоящими в изготовлении из-за повышенной строгости в процессах и работах проектирования. Они также требуют дополнительного анализа, чтобы оценить их доверенность. Минимизация числа доверенных элементов системы снижает стоимость анализа (т.е. уменьшает масштаб, объём и сложность анализа). Когда при минимизации доверенных элементов системы учитывается принцип *соразмерной защиты*, обеспечивается также экономическая эффективность анализа (т.е. стоимость анализа оправдывается требуемой степенью доверия).

Исторически сложилось так, что анализ взаимодействия между доверенными и недоверенными элементами системы является одним из наиболее важных аспектов проверки результативности безопасности системы на основе доверия. Если эти взаимодействия являются излишне сложными, то и безопасность системы будет также труднее установить, чем в системе, внутренние доверенные отношения которой просты и изящны. В целом, меньшее количество доверенных компонентов приводит к уменьшению внутренних отношений доверия и упрощению системы.

Ссылки: [2] [20] [43] [44]

E.21. Минимизация обнаруживаемости

Принцип: Проект системы сводит к минимуму обнаруживаемость системы настолько, насколько это практически возможно.

Примечание: Система, которую невозможно обнаружить, наблюдать и отслеживать противоборствующей угрозе или которая не подвержена такой угрозе, менее подвержена целенаправленной атаке. Минимизация обнаруживаемости определяет конструкторские решений, направленные на то, чтобы исключить или уменьшить такие факторы воздействия, как ненужные интерфейсы, точки доступа, следы и излучения, тем самым снижая подверженность действиям противоборствующих угроз. Интерфейсы и точки доступа могут подвергать систему воздействию преднамеренных (т.е. атак) и непреднамеренных (т.е. сбоев, ошибок, инцидентов, аварий) неблагоприятных воздействий. Тем не менее, интерфейсы и точки доступа необходимы для создания элементов системы, обеспечивающих требуемые возможности, а дублирование интерфейсов и точек доступа необходимо для предотвращения единых точек отказа. Проект системы должна балансировать потребность в интерфейсах с уязвимостью, возникающей в результате раскрытия, обнаружения и наблюдения интерфейса. Каждый интерфейс, как внутренний, так и внешний, представляет собой уязвимость, которую необходимо учитывать.

Минимизация обнаруживаемости снижает способность противника наблюдать и обнаруживать информацию о системе для разработки и выполнения атак. Это включает в себя обнаружение местоположения, присутствия и перемещения системы (например, по излучениям, сигнатурам или следам). Способы, с помощью которых система может быть обнаружена, включают в себя тепловое излучение, электромагнитное (ЭМ) излучение, звук, вибрации, отраженные радиолокационные волны или свет, реакцию на воздействие (например, реакцию на эхо-запрос протокола управления сообщениями Интернета [ICMP] или "ping"), а также программные следы и исключительные ситуации. Конкретные формы или средства для минимизации обнаруживаемости включают маскировку, скрытность, сигналы с низкой вероятностью перехвата/обнаружения (LPI/LPD) (для радиостанций) и скачкообразную перестройку частоты.

Ссылки: [53] [59] [60]

E.22. Настройки защиты по умолчанию

Принцип: Конфигурация системы по умолчанию обеспечивает максимальную эффективность защиты.

Примечание: Конфигурация системы включает параметры функций системы, данных, интерфейсов и ресурсов, которые определяют поведение системы и выдаваемые ей результаты. Настройки защиты по умолчанию гарантируют, что конфигурация и параметры системы "как поставляется" определяют приоритет достижения целей контроля потерь над способностью обеспечивать требуемые возможности и результативность системы без вмешательства человека. Настройки защиты по умолчанию требуют добросовестных действий для установления конфигурации и параметров системы, обеспечивающих требуемые возможности и результативность таким образом, чтобы обеспечить *Соразмерную защиту* от потерь. Настройки защиты по умолчанию для систем включают настройки для составляющих систему подсистем, компонентов и механизмов. Принципы *Защищённый отказ, Защищённое восстановление* и *Непрерывная защита* параллельно этому принципу обеспечивают возможности обнаружения и восстановления после отказа.

Ссылки: [2] [21] [46]

E.23. Защищённый отказ

Принцип: Отказ элемента системы не приводит ни к недопустимым потерям, ни к вызову другого сценария потерь.

Примечание: Защищённый отказ, обобщающий концепции отказоустойчивости и безотказной защиты, является аспектом непрерывной защиты, который гарантирует, что функция защиты не прерывается во время отказа и что последствия отказа ограничены. Для достижения намеченного эффекта должны быть удовлетворены два аспекта защищённого отказа:

- *Избегайте единых точек отказа:* Отказ одного элемента системы не должен приводить к недопустимым потерям. Недопустимые потери должны иметь место только в случае нескольких независимых неисправностей - принцип безопасности, известный как критерий одиночного отказа. Принцип *Эшелонированная защита* может помочь достичь этого аспекта защищённого отказа.

- *Избегайте распространения новых отказов:* Если не принимать меры, отказы в системе могут привести к распространяющимся, каскадным или скачкообразным последствиям для системы. Эти последствия могут быть устранены, если остальные средства защиты остаются эффективными, чтобы предотвратить возникновение дополнительных отказов.

Защищённый отказ применим к отдельным элементам системы, совокупностям элементов системы и системным абстракциям. Защищённый отказ направлен на ограничение эффекта отказа в той мере, в какой это практически возможно, и при этом сводит к минимуму возможность возникновения новых потерь. Защищённый отказ может ограничить степень развития связанных с отказом сценариев потерь, включая каскадные потери; инициировать другой сценарий потерь; или создайте новый сценарий потерь. Усилия по предотвращению или ограничению отказов могут сами по себе ухудшить результативность системы, что является одной из форм отказа. Таким образом, разработчикам систем может потребоваться рассмотреть компромисс между возможными негативными последствиями и результативностью системы.

Ссылки: [2] [21] [40] [47] [45]

E.24. Защищенное восстановление

Принцип: Восстановление элемента системы не приводит к недопустимым потерям.

Примечание: Защищённое восстановление является одним из *аспектов Непрерывной защиты,* который гарантирует, что возможности защиты не будут прерваны во время восстановления после фактического или прогнозируемого отказа. Защищённое восстановление применяется к отдельным элементам системы, совокупностям элементов системы и к системе в целом. В той мере, насколько это практически возможно, любое восстановление после прогнозируемого или фактического отказа для возобновления нормальной, ухудшенной, аварийной или альтернативной работы, или восстановления других потерь активов не должно (1) способствовать реализации сценария потерь, который является целью восстановления, (2) инициировать другие сценарии потерь или (3) создавать новые сценарии потерь. Практический аспект этого принципа заключается в том, что успешные усилия по восстановлению могут ухудшить результативность системы, что является формой потери. Защищённое восстановление является одним из аспектов стратегии реагирования для системы. Таким образом, соображения дозированное и ударного *Соразмерного реагирования* применяются для наилучшего удовлетворения потребности в защищённом восстановлении.

Ссылки: [2] [6] [20] [21]

E.25. Уменьшение сложности

Принцип: Проект системы должен быть настолько прост, насколько это практически возможно.

Примечание: Создаваемые системы часто бывают сложными. Некоторая степень сложности проектирования системы является неотъемлемой, неизбежной и должна быть принята. Целью этого принципа является обеспечение того, чтобы проект отражал степень, в которой сложность может быть разумно минимизирована (т.е. избегать ненужной сложности).

Сложность можно найти в структуре системы, интерфейсах, зависимостях, потоках данных и управления, а также во взаимодействии системы с ее средой эксплуатации. Сложность проистекает из того, как система разбивается на отдельные и совокупные составные элементы (например, подсистемы, узлы), и из того, как эти элементы через свое поведение и взаимодействие образуют функционирующую систему.

Более сложный проект увеличивает неопределенность. Такая неопределенность приводит к ошибкам и препятствует получению уверенности в понимании проекта. Сложный проект также более склонен к ошибочному толкованию при выполнении проектных работ по анализу, реализации и проверке на протяжении всего жизненного цикла системы [45]. Таким образом, снижение сложности проекта способствует уверенности в техническом понимании проекта, позволяя принимать более обоснованные компромиссные решения и уменьшая неопределенность при проектировании и последующей реализации проекта как системы.

Сложность также увеличивает трудности при выявлении и оценке сценариев потерь, подверженности и уязвимостей. Выводы о природе и влиянии уязвимостей могут быть сделаны с более высокой степенью доверия в случаях меньшей сложности проекта в отличие от случаев, когда проект чрезмерно сложен.

Принцип уменьшенной сложности можно также назвать принципом упрощения или наименьшего общего механизма.

Ссылки: [2] [40] [45] [46] [47]

E.26. Резервирование

Принцип: Проект системы обеспечивает требуемые возможности путем дублирования функций или элементов системы.

Примечание: Резервирование предполагает использование несколько одинаковых элементов системы, потоков данных и управления или путей, чтобы избежать единых точек отказа. Резервирование требует стратегии использования нескольких элементов системы по отдельности или в комбинации (например, балансировка нагрузки, переключение на резервный ресурс, одновременное использование, резервное копирование, голосование, согласование, консенсус).

Резервированные решения подвержены общему режиму отказов (т.е. единичное событие, приводит к отказу одних и тех же или эквивалентных элементов одинаковым образом). *Разнообразие* является средством решения проблем, связанных с общим режимом отказов.

Ссылки: [2] [20] [45] [47]

E.27. Самообеспечение доверенности

Принцип: Доверенность элемента системы достигается при минимальной зависимости от других элементов.

Примечание: В идеальном случае доверенность элемента системы достигается тогда, когда утверждение о доверенности не зависит от защиты со стороны другого элемента системы. Если элемент зависит от других элементов, чтобы удовлетворить его утверждения о доверенности, то доверенность этого элемента подвержена любой потере или ухудшению возможностей защиты, обеспечиваемых другим элементом. Соображения относительно степени, в которой элемент системы проявляет самообеспечение доверенности включают в себя:

- Цель обеспечения возможностей доверенности.
- Доверенность элемента системы в предоставлении возможностей.
- Степень, в которой возможности, обеспечиваемые элементом системы, зависят от другого элемента.
- Степень, в которой доверенность, связанная с возможностями, зависит от другого элемента системы.

Аргументы в пользу самообеспечения доверенности могут применяться на уровне отдельных элементов системы, на уровне совокупности элементов, на уровне системы или на уровне системы систем. Во всех случаях должно сохраняться различие между предоставляемыми возможностями и ответственностью за доверенность к этим возможностям (например, нельзя утверждать о самообеспеченной доверенности, если утверждения о защите доверия распределены между некоторыми другими сущностями и зависят от них). Аналогично, когда

возможности системы распределены между несколькими элементами системы, для самообеспеченной доверенности требуется, чтобы ожидания доверия для этих возможностей были правильно распределены между элементами, которые составляют распределенные возможности.

Суждение о том, что элемент системы является самообеспечивающим доверенность, основывается на способности элемента удовлетворять конкретному набору требований и связанных с ними допущений. Элемент, который является самообеспечивающим доверенность для одного набора требований и допущений, не обязательно является самообеспечивающим доверенность для других наборов требований и допущений. Любое изменение в требовании, удовлетворении требования или в допущениях, связанных с требованием, требует переоценки для определения того, что элемент остается самообеспечивающим доверенность.

Ссылки: [2]

E.28. Структурная декомпозиция и композиция

Принцип: Сложность системы для обеспечения требуемых возможностей управляется структурной декомпозицией системы и структурной композицией составляющих элементов.

Примечание: Структурная декомпозиция системы и последующая компоновка элементов системы основываются и определяются концепциями модульности, многоуровневости и частично упорядоченных зависимостей.

Модульность – это метод проектирования системы по принципу "*разделяй и властвуй*", то есть разделение системы на более мелкие, четко определённые взаимосвязанные компоненты и сборки, которые называются модулями. Модульность служит для разделения функций и структур данных на четко определенные логические единицы. Модульная декомпозиция может включать в себя распределение политик по системам в сети, распределение системных политик по уровням, разделение системных приложений на процессы с различными адресными пространствами и разделение процессов на субъекты с различными привилегиями на основе поддерживаемых аппаратным обеспечением доменов привилегий. Модульный проект может также распространяться на вопросы доверия, доверенности, привилегий и политики.

Многоуровневость - это группирование модулей в реляционную структуру с четко определенными интерфейсами, функциями, данными и потоками управления таким образом, чтобы граф зависимостей между слоями был линейно или частично упорядочен так, что более высокие уровни зависят только от более низких уровней [2]. Частично упорядоченные зависимости между модулями (например, если модуль A зависит от модуля B, то модуль B не может зависеть от модуля A) и многоуровневость системы вносят значительный вклад в простоту и согласованность проекта системы. Хотя частичное упорядочивание всех функций и процессов может быть невозможным, присущие им проблемы цикличности могут быть более легко решены, если ограничить циклические зависимости между уровнями и минимизировать их внутри каждого уровня. Частично упорядоченные зависимости также облегчают тестирование и анализ системы и обеспечивают строгую форму слабой связи (т.е. минимизацию взаимозависимостей между модулями).

Модульность и многоуровневость эффективны в управлении сложностью составной системы. Они обеспечивают средства для разложения системы на отдельные и агрегированные элементы для лучшего понимания системы с точки зрения ее структуры, потоков, взаимосвязей и того, как система обеспечивает требуемые возможности. Структурная композиция составляющих элементов должна также соответствовать принципу *композиционной доверенности*, чтобы обеспечить основу для поддержки утверждений о том, как система составлена на основе применения модульности, многоуровневости и частично упорядоченных зависимостей для достижения санкционированных и предусмотренных поведения и результатов.

Ссылки: [2] [20] [46] [48] [49]

E.29. Подтверждённая доверенность

Принцип: Суждения о доверенности системы основаны на свидетельствах того, что критерии доверенности были удовлетворены.

Примечание: Доверенность не должна предполагаться, а должна подтверждаться свидетельствами, которые ясно показывают, насколько сущность заслуживает доверия. Это помогает гарантировать, чтобы сущность никогда не пользовалась доверием сверх той меры, в которой она заслуживает доверия. Подход подтверждённой доверенности требует *Соразмерной строгости* с осторожным недоверием (т.е. элементы системы считаются виновными до тех пор, пока их невиновность не будет доказана).[84]

Для подтверждённой доверенности характерен проектный менталитет, при котором все компоненты, вовлеченные в контекст проектирования (то есть элемент системы и элементы, с которыми он взаимодействует), рассматриваются со взаимным подозрением [2] [20]. Такое взаимное подозрение отражает осторожное недоверие - чувство или мысль о том, что возможно или может произойти что-то нежелательное, ненужное или неожиданное. В проекте для каждого элемента системы должно быть отражено отсутствие доверия к взаимодействующим элементам или к самому себе. Это подозрение предполагает неработоспособность элемента и касается следующих случаев:

- *Подозрение в отношение взаимодействующих элементов (взаимная подозрительность):* Проектирование элемента, представляющего интерес для системы, основывается на нерезультативности элементов, с которыми она взаимодействует, и на том, как их нерезультативность может повлиять на поведение и результаты элемента, представляющего интерес. Проектирование с учётом взаимного подозрения усиливается применением принципа *Наименьших привилегий* ко всем сущностям (так, чтобы элемент выполнялся только с необходимыми привилегиями, уменьшая возможный ущерб), а также применением принципа *Наименьшего предоставления доступности* так, чтобы каждый элемент был минимально подвержен воздействию.

- *Самоподозрительность:* Проект для представляющего интерес элемента системы должен учитывать его собственную нерезультативность, не зависящую от какого-либо внешнего воздействия. Проектирование с учётом самоподозрительности может включать самоконтроль и встроенные действия, включая встроенное тестирование при инициировании элемента.

Такой подход заставляет проектировщика системы предполагать, что всё пойдёт не так, как надо, и тщательно искать свидетельства, которые демонстрируют эффективность проекта, когда что-то идёт не так, как надо. Соображения по поводу нерезультативности элемента системы включают в себя следующее:

- Ожидание того, что элементы будут вести себя и давать результаты, которые не соответствуют проектному замыслу.

- Ограничения, допущения и предварительные условия, связанные с достижением пороговых показателей результативности.

- Преднамеренные и непреднамеренные события и условия, обычно обозначаемые такими терминами, как неисправность, ошибка, отказ и компромисс

Ссылки: [2] [21] [50]

E.30. Доверенное управление системой

Принцип: Проект функций управления системой соответствует свойствам обобщенного диспетчера доступа.

Примечание: Принцип доверенного управления системой отражает обобщение концепции диспетчера доступа, чтобы обеспечить единую основу проектирования доверия для доверенных механизмов управления системой или механизмов обеспечения ограничений, которые составляются для обеспечения функций управления системой.

[84] Адаптировано из высказывания John Rushby, SRI International, о необходимости рассматривать программное обеспечение как «виновное, пока не доказана его невиновность» на семинаре Layered Assurance Workshop (LAW).

Концепция диспетчера доступа (Раздел D.4.2) является основополагающей концепцией управления доступом для проектирования безопасных систем. Она определяется как заслуживающая доверия абстрактная машина, которая опосредует все доступы субъектов к объектам. Как концепция абстрактной машины, диспетчер доступа не имеет отношения к какой-либо конкретной реализации. Механизм подтверждения доступа, представляющий собой комбинацию аппаратных средств и программного обеспечения, реализует концепцию диспетчера доступа для обеспечения основы посредничества в доступе для безопасной системы [37].

Концепция диспетчера доступа имеет несколько критериев, обеспечивающих проектное доверие к его реализации в качестве механизма подтверждения доступа:

- Механизм подтверждения доступа должен быть защищен от несанкционированного доступа чтобы гарантировать, что его целостность и достоверность не будут нарушены.

- Механизм подтверждения доступа должен всегда вызываем, и если это невозможно, то группа программ, для которой он предоставляет услуги подтверждения, должна рассматриваться как часть механизма подтверждения доступа и соответствовать первому и третьему требованиям.

- Механизм подтверждения доступа должен подвергаться тщательному анализу и тестированию, полнота которых может быть гарантирована (с целью убедиться в том, что механизм подтверждения доступа работает правильно во всех случаях).

Для доверенного управления системой добавляется четвертый критерий – невозможности обхода (Раздел D.4.2).

Успешное выполнение этих критериев предотвратит вмешательство внешних сущностей в механизм или контроллер защиты. Конкретно:

- Механизм или функция защиты не должны преодолеваться (т.е. механизм не должен обходиться).

- Механизм или функция защиты должны быть оцениваемыми (т.е. достаточно малыми и простыми, чтобы их можно было оценить для обеспечения достаточной уверенности в обеспечении защиты, соблюдения ограничений или достижения цели управления и корректной реализации механизма [Уменьшение сложности]).

- Механизм или функция защиты являются всегда вызываемыми, обеспечивающая непрерывную защиту.

- Механизм или функция защиты должны быть защищены от несанкционированного доступа (т.е. ни функции защиты, ни данные, от которых зависят функции, не могут быть изменены без санкционирования).

Доверенное управление системой также включает в себя концепции управления, защиты и безопасности для создания возможностей системы, которые в достаточной степени:

- Обеспечивают соблюдение ограничений для достижения только санкционированного и предполагаемого поведения и результатов системы.

- Обеспечивают самозащиту от целенаправленных атак на систему.

- Обеспечивают отсутствие самопроизвольно возникающих, ошибочных, незащищённых и небезопасных управляющих воздействий.

Такие возможности системы лежит в основе целей управления потерями и преобразует подход к проектированию так, чтобы не полагаться на детальное знание возможностей, средств и методов противника. Этот подход к проектированию может быть использован в способах, зависимых от атаки или независимых от атаки, исходя из пределов уверенности в том, что достоверно известно о противнике.

Доверенное управление системой служит также основой для проектирования отдельных элементов системы, совокупностей элементов, сетей и систем, в которых преднамеренные и непреднамеренные неблагоприятные факторы могут препятствовать достижению целей управления потерями. Этот принцип также обусловливает необходимость строгости в проектных работах, соизмеримой с доверием к элементам системы.

Ссылки: [21] [35] [37] [38]

Приложение F. Доверенность и доверие

Доверенность системы основана на концепции доверия. Доверие является основанием для обоснованной уверенности в том, что утверждение или набор утверждений были или будут выполнены [61]. Обоснованная уверенность вытекает из объективных свидетельств, которые снижают неопределенность до приемлемого уровня и при этом уменьшают связанный с этим риск (раздел F.2).[85] Свидетельства получаются с помощью методов проектной верификации и подтверждения.[86] Эти свидетельства должны быть актуальными, точными, достоверными и достаточными для того, чтобы эксперты по конкретным вопросам могли сделать обоснованные выводы и достичь консенсуса в отношении того, что утверждения удовлетворены. Взаимосвязь между свидетельствами и утверждениями может быть представлена различными способами. В разделе F.2 рассматриваются эти подходы.

> "Доверие, которое мы оказываем нашей цифровой инфраструктуре, должно быть пропорционально тому, насколько доверенной и прозрачной является эта инфраструктура, и тем последствиям, которые мы понесем, если это доверие будет потеряно".
>
> -- **Исполнительный указ (EO) о повышении национальной кибербезопасности [1]**
> Май 2021

F.1. Доверие и доверенность

Как обсуждается в разделе 2.3, доверие и доверенность являются основополагающими концепциями для разработки доверенных безопасных систем, принятия решений о предоставлении доверия и определения степени, в которой доверие предоставляется на основе продемонстрированной доверенности. Доверие - это уверенность в том, что сущность отвечает определенным ожиданиям и, следовательно, на нее можно положиться. Доверенность сущности нуждается в достаточных свидетельствах, подтверждающих утверждения о её доверенности. Доверенность демонстрируется на основании свидетельств, подтверждающих заявленное утверждение или суждение о том, что она достойна доверия [2] [20] [21].

Доверие к сущности может иметь место без основания или знаний о доверенности сущности. Это может произойти потому, что (1) нет альтернативы (например, индивидуум доверяет компонентам, участвующим в интернет-транзакции, не зная ничего о компонентах), (2) потребность в доверенности не существует, а возникает де-факто, или (3) другие причины (например, недопонимание или искажённое представление свидетельств) [58]. Поскольку решение о доверии сущности не обязательно основывается на суждении о доверенности, при принятии решения о доверии сущности должна учитываться значимость (т.е. последствия, эффекты и воздействия) того, что ожидания доверия не оправдаются. Для определения доверенности сущности используются критерии предоставления доверия. Доверие, предоставляемое без подтверждения требуемой доверенности, является существенным фактором риска.

F.1.1. Роль требований в обеспечении доверенности

Суждения о доверенности основываются на ожиданиях, которые должны быть выполнены сущностью,

[85] Сюда входят риски, связанные с некачественными, неправильными и необоснованными решениями.
[86] Эти методы включают в себя комбинации демонстраций, проверок, анализа и испытаний.

которой следует доверять. Ожидания в отношении доверенности системы, включая ее элементы, содержатся в требованиях к её возможностям, результативности, безопасности и других требованиях. Эти суждения имеет значение только в той степени, в которой требования, относящиеся к доверенности, точно отражают проблему, точно определяют решение и могут быть проверены как удовлетворяющие решению.

Требования к доверенности в отношении безопасности проистекают из потребностей в защите, приоритетов, ограничений и интересов, связанных со способностью системы обеспечивать разрешенное и предполагаемое поведение и результаты, справляться с неблагоприятными условиями и управлять потерями. Требования также касаются мер, используемых для оценки доверенности, а также доказательных данных и информации, необходимых для обоснования выводов о доверенности и предоставления доверия. Дисциплина разработки требований предоставляет методы, процессы, технологии и инструменты для этого.

> "Значимое утверждение о доверенности не может быть основано на изолированной демонстрации того, что система содержит возможности защиты, которые считаются эффективными или достаточными. Вместо этого выводы о возможности защиты должны основываться на свидетельствах того, что система была надлежащим образом определена, спроектирована и реализована со строгостью, необходимой для выполнения функции системного уровня способом, который считается доверенным и безопасным. " [2]

F.1.2. Проектные соображения

Проектирование доверенной безопасной системы требует применения принципиальных концепций и методов инженерии, подкрепленных свидетельствами, которые предоставляют доверие к тому, что все утверждения, относящиеся к безопасности системы удовлетворены (раздел F.2).[87] Некоторыми соображениями, которые относятся к достижению доверенности при проектировании системы, являются:

- **Композиция**

  Суждения о доверенности являются композиционными. Они должны соответствовать тому, как набор составных элементов обеспечивает возможности системы. Способ, которым система составляется из ее элементов, должен включать в себя принципы проектирования *Композиционной доверенности* и, насколько это практически возможно, *Структурной декомпозиции и композиции*.

- **Состояния, режимы и переходы**

  В идеале, реализация проекта системы должна приводить к тому, что система будет постоянно находиться в безопасных состояниях и режимах с безопасными переходами между состояниями и режимами (раздел 3.2). В реальности система будет иметь небезопасные и неопределенные (т.е. неизвестно, безопасные или небезопасные) состояния и режимы. Проект должен учитывать эти случаи и должен обеспечивать возможность перехода от небезопасных и неопределенных состояний и режимов к безопасным состояниям и режимам *(Защищённое восстановление).*

[87] Ограничения и утверждения выражаются в терминах функциональной корректности, стойкости функционирования, опасений по поводу утраты активов и последствий, а также возможностей защиты, обусловленных соблюдением стандартов или использованием конкретных процессов, процедур или методов.

- **Распространение отказов**

  В какой-то момент все системы отказывают. При возникновении отказа не должен инициироваться или вызываться другой сценарий отказа или создаваться новый сценарий отказа *(Защищённый отказ).* Проектирование без единых точек отказа *(Резервирование)*, включая отсутствие общего режима отказов *(Разнообразие)*, может помочь изолировать отказы элементов системы при обеспечении требуемых возможностей системы. Кроме того, реакция на отказ не должна приводить к потерям или другим отказам *(Защищённое восстановление).*

- **Обнаружение аномалий**

  Обнаружение аномалий обеспечивает осведомлённость о ситуации, которая позволяет системе принимать решения и рекомендовать корректирующие действия для учета фактических и потенциальных отклонений от принятых норм.

- **Компромиссы**

  Не каждый элемент системы обладает доверенностью, достаточной для его предназначения. Недостаток доверенности может быть результатом:

  - Проблем технической осуществимости и практичности.
  - Проблем стоимости и сроков того, что достижимо и практично.
  - Пределов определенности (т.е. то, что неизвестно, что не может быть известно и что недооценено [известно или может быть известно, но преждевременно отклонено]).

  Пространство компромиссов - это строгое применение принципов проектирования, которое обеспечивает основу для принятия необходимых проектных решений для максимального повышения доверенности отдельных элементов системы и совокупностей элементов. Например, при решении вопросов осуществимости и практичности затрат и сроков применяется принцип проектирования, заключающийся в минимизации количества элементов системы, которые должны быть доверенными *(Минимум доверенных элементов)*. Это уменьшает размер и область усилий и потенциально снижает расходы на получение свидетельств доверенности.

F.2. Доверие

Доверие является основанием для обоснованной уверенности в том, что утверждение или набор утверждений были или будут выполнены [61]. Доверие - это сложное и многомерное свойство системы, которое формируется с течением времени. Доверие должно планироваться, устанавливаться и поддерживаться в соответствии с системой на протяжении всего жизненного цикла системы.

Адекватные суждения о безопасности должны основываться на уровне уверенности в способности системы защитить себя от потери активов и связанных с этим последствий во всех формах неблагоприятных условий.[88] Они не могут основываться исключительно на одиночных усилиях, таких как демонстрация соответствия, функциональное тестирование или тестирование на проникновение. Суждения включают то, что система не может сделать, не будет делать или не может быть принуждена делать. Эти суждения о ненадлежащем поведении должны быть основаны на достаточной уверенности в способности системы правильно выполнять возложенные на неё функции при наличии и отсутствии неблагоприятных условий и делать это при её использовании в соответствии с проектным замыслом.

[88] Термин "неблагоприятные условия" относится к тем условиям, которые могут привести к потере активов (например, угрозы, атаки, уязвимости, опасности, сбои и воздействия).

Необходимая доказательная база для таких суждений получается из хорошо сформированных и всеобъемлющих действий, дающих свидетельства, которые касаются требований, проекта, свойств, возможностей, уязвимостей и эффективности функций безопасности. Эти действия включают сочетание демонстрации, инспекции, анализа, тестирования и других методов, необходимых для получения необходимых свидетельств. Свидетельства, полученные в результате этих действий, служат основой для квалифицированных тематических экспертов по интерпретации свидетельств в подтверждение сделанных утверждений о доверии, принимая во внимание другие возникающие свойства, которыми может обладать система.

ВИДИМАЯ БЕЗОПАСНОСТЬ

Доверие трудно, но необходимо.

"Я рассмотрел много материалов в этой книге, некоторые из них довольно сложные. Но самые трудные части я оставил на последок. Во-первых, это вопрос доверия "... [5].

Видимая безопасность - это функциональность безопасности, предоставляемая без соответствующего доверия, так что эта функциональность только кажется защищающей ресурсы, хотя на самом деле это не так. Видимая безопасность приводит к ложному чувству безопасности и, фактически, увеличивает риск из-за неопределенности поведения и результатов, вызванных функциональностью безопасности в присутствии и отсутствии неблагоприятных условий. Следует избегать видимой безопасности [62].

Соответствие требованиям - это форма "видимой безопасности". Хотя соответствие требованиям может играть важную информативную роль в суждениях о доверенности, суждения, основанные на соответствии требованиям, - как и другие формы видимой безопасности – не могут служить единственной доказательной основой для доверия и связанных с ней суждений о доверенности.

F.2.1. Утверждения о доверии к безопасности

С точки зрения безопасности высокоуровневые утверждения касаются отсутствия условий, которые приводят к потере активов, и связанных с этим последствий. В частности, это означает, что система будет надлежащим образом способствовать устранению условий, которые приводят к потере активов и связанным с этим последствий.

Высокоуровневые утверждения разбиваются структурированным образом на подутверждения о желаемых атрибутах доверенной безопасной системы. Подутверждения касаются требований, проекта, реализации, методов и неблагоприятных условий, которые демонстрируют, что система адекватно способствует обеспечению только санкционированного и предназначенного поведения и результатов системы. Эти подутверждения вытекают из интересов в отношении полноты и точности требований заинтересованных сторон и системы,[89] осуществления политики безопасности, надлежащей реализации проекта, надлежащей поддержки системы, удобства использования системы,[90] а также

[89] Требования не должны исключительно быть представлены как переформулирование функциональных требований и требований к результативности безопасности. Так делается лишь для того, чтобы предоставить доверие к тому, что требования безопасности удовлетворены, при неявном предположении, что требования корректны, обеспечивают адекватный охват и точно отражают потребности и проблемы заинтересованных сторон.

[90] Большинство системных сбоев связаны с человеческим фактором. Поэтому, доверие должно учитывать человеческие слабости [5]. Поведение оператора является продуктом среды (включая ее системы), в которой это происходит [36].

предотвращения, минимизации и смягчения последствий дефектов, ошибок и уязвимостей.[91] Могут существовать и другие подутверждения, включающие в себя способность проявлять предсказуемое поведение при работе в безопасных состояниях при наличии и отсутствии неблагоприятных условий и способность восстанавливаться из небезопасного состояния. Утверждения могут быть выражены в терминах функциональной корректности, стойкости функций и возможностей защиты, вытекающей из соблюдения стандартов и/или использования конкретных процессов, процедур и методов.

ИЗВЛЕКАЯ УРОКИ ИЗ ОПЫТА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по безопасности систем NASA [6] описывает соответствующие утверждения, которые должны быть удовлетворены с точки зрения высокоуровневого утверждения о том, что система является достаточно безопасной с подутверждениями, включающими то, что система спроектирована настолько безопасно, насколько это практически возможно, выполнена настолько безопасно, насколько это практически возможно, и эксплуатируется настолько безопасно, насколько это практически возможно.

F.2.2. Подходы к доверию

Существует три общих подхода к доверию. Эти подходы к доверию могут варьироваться в зависимости от типа свидетельств, способа получения свидетельств, строгости суждений, принимаемых на основе полученных свидетельств, и степени соответствия доверия потребностям принятия решений. От самого слабого к самому строгому, подходами к доверию являются аксиоматический, аналитический и синтетический.

- **Аксиоматическое доверие** (доверие посредством утверждения) основано на убеждениях, принятых на веру в отношении образца или процесса. Убеждения часто принимаются, потому что они не противоречат экспериментам или демонстрациям. Аксиоматическое доверие не подходит для сложных сценариев [62].
  - Демонстрация соответствия и согласованности - типы аксиоматического доверия. Хотя они и полезны, они не вполне подходят в качестве единственной основы доверия для сложных сценариев.
- **Аналитическое доверие** (доверие путем тестирования и анализа) основывается на тестировании или рассуждений для обоснования выводов о свойствах, представляющих интерес. Уверенность переносится от образца или процесса в доверие к некоторому методу анализа. Целесообразность создания аналитической основы зависит от объема работы, связанной с выполнением анализа, и от обоснованности любых предположений, лежащих в основе этого анализа. Аналитические методы наиболее уместны в модели, охватывающей все соответствующие виды использования и все интерфейсы к среде. То есть модель не должна игнорировать слишком много деталей.
  - Тестирование демонстрирует наличие, но не отсутствие ошибок и уязвимостей. Тестирование и анализ будут иметь неопределенность, которую нельзя игнорировать, особенно когда они не являются всеобъемлющими. Неопределенность способствует риску.
- **Синтетическое доверие** (доверие путем структурированных рассуждений) вытекает из метода составления «компонентов доверия» (т.е. доверие вытекает из способа синтеза составных частей).

[91] Не все уязвимости можно устранить до приемлемого уровня. Существует три класса уязвимостей в системах: (1) уязвимости, о существовании которых известно и которые либо устранены, либо сделаны несущественными, (2) уязвимости, о существовании которых известно, но которые недостаточно смягчены, и (3) неизвестные уязвимости, составляющие элемент неопределенности. То есть тот факт, что уязвимость не была выявлена, не должен давать повышенной уверенности в том, что уязвимость не существует. Определение влияния уязвимостей, имеющихся в поставленной системе, и риска, создаваемого этими уязвимостями, а также принятие неопределенности в отношении существования уязвимости, которая станет известна лишь со временем, являются важными аспектами, которые решаются с помощью доверия.

Это требует, чтобы доверие учитывалось на каждом этапе проектирования и реализации, от мельчайших компонентов до окончательной реализации подсистемы.

- Пример доверия, описанный в [30], является примером структурированного рассуждения (раздел 4.3). Структурированные рассуждения служат для заполнения пробелов, связанных с аксиоматическими и аналитическими подходами к доверию. Поскольку синтетическое доверие основано на экспертном суждении об имеющихся свидетельствах, оно не является полным. Тем не менее, синтетическое доверие позволяет еще больше снизить неопределенность и, таким образом, уменьшить риск.

Доверие зависит от качества свидетельств, используемых в аргументах, демонстрирующих, что утверждения о системе удовлетворены. Подтверждающие свидетельства могут быть получены либо непосредственно с помощью измерений, испытаний, наблюдений или инспекций, либо косвенно с помощью анализа, включая анализ данных, полученных в результате измерений, испытаний, наблюдений или инспекций. Свидетельства должны обладать достаточным качеством с точки зрения точности, достоверности, актуальности, строгости и количества. Точность, достоверность и актуальность свидетельств должны быть подтверждены до их использования. Например, некоторые свидетельства могут поддерживать аргументы в пользу стойкости функции, другие - в отношении негативных требований (т.е. того, что не произойдет), а третьи - в пользу качественных свойств.

КЕЙС ДОВЕРИЯ

Кейс доверия - это обоснованный, проверяемый образец, который создается в поддержку заявления о том, что утверждение верхнего уровня удовлетворено. Кейс доверия включает систематизированную аргументацию, свидетельства и явные предположения, которые поддерживают утверждение.

Кейс доверия содержит следующие элементы [30]:

- Одно или несколько утверждений о свойствах.
- Аргументы, логически связывающие свидетельства и любые предположения,
- Совокупность свидетельств.
- Обоснование выбора утверждения верхнего уровня и метод аргументации.

Кейсы доверия имеют многочисленные преимущества по сравнению с другими способами получения уверенности, например, в таких областях как понимание, информирование о необходимости распределения ответственности, организация информации и надежная должная осмотрительность. Эти преимущества были более значимыми в тех областях, где других методов для достижения высокой степени доверия было недостаточно. Кроме того, установлено, что кейсы доверия являются более эффективными для сложных и новых систем, а также систем, нуждающихся в высоком доверии.

В последние годы разработано множество формализаций и инструментов для построения кейсов доверия, в том числе Нотация структурирования целей (GSN) [64] и инструментарий NASA AdvoCATE: Assurance Case Automation Toolset [65].

F.2.3. Потребности в доверии

Доверие - это потребность, которая должна быть разработана и удовлетворена аналогично потребности в разработке возможностей системы для удовлетворения определенных потребностей в возможностях. Потребности в доверии для доверенных безопасных систем основаны на опасениях в потерях и неблагоприятных результатах из-за преднамеренных и непреднамеренных неблагоприятных ситуаций (*Соразмерная доверенность, Обоснованная доверенность, Соразмерная строгость*). Потребности в доверии включают в себя базу свидетельств для обоснования, степень строгости при получении и интерпретации свидетельств, а также выбор методов, инструментов и процессов, используемых в течение всего жизненного цикла системы. Аналогично потребностям в возможностях и результативности, потребности в доверии, ожидания, приоритеты и ограничения должны выражаться в требованиях к системе и достигаться, отслеживаться и поддерживаться в рамках работ по проектированию систем.

УВЕРЕННОСТЬ МОЖЕТ БЫТЬ ОТРИЦАТЕЛЬНОЙ

Свидетельства доверия могут подтвердить вывод о том, что заявленное утверждение не выполнено или что нет достаточных оснований для вывода о том, что утверждение поддерживается или не поддерживается. В любом случае уверенность является отрицательной по отношению к цели обоснования утверждения. То есть система или некоторая часть системы недостаточно доверена и ей не следует доверять в отношении ее определенной функции без дальнейших действий.

Потребности в доверии определяют тип и строгость свидетельств, связанные с работами, методами и инструментами, используемыми для получения свидетельств, в следующих случаях:

- *Что должно быть достигнуто в результате усилий по разработке системы*: Реализация проекта безопасной системы.
- *Средства осуществления усилий по разработке системы*: Методы, процессы и инструменты, используемые (в соответствии с целями строгости и доверия) для реализации проекта безопасной системы.
- *Результаты усилий по разработке системы*: Обоснованная эффективность реализации проекта безопасной системы.

Потребности в доверии могут различаться и представлять собой пространство компромиссов, которое должно регулироваться в соответствии с тем, как меняются потребности в возможностях и результативности. Степень строгости является основным средством изменения доверия. Как показано на рис. 17, существует прямая связь между степенью строгости и доверием, и оценкой заинтересованными сторонами результатов потери активов. Пространство компромиссов доверия включает следующие соображения:

- Стоимость, сроки и результативность.
- Архитектурные и проектные решения.
- Выбор технологий и решений.
- Выбор и применение методов и инструментов.
- Квалификация, необходимая для специалистов в данной области.

Анализ требований заинтересованных сторон и требований к системе определяет требуемую пороговую степень строгости. Если система практически не может соответствовать необходимой степени строгости, заинтересованные стороны должны иметь возможность определить, примут ли они связанный с этим риск.

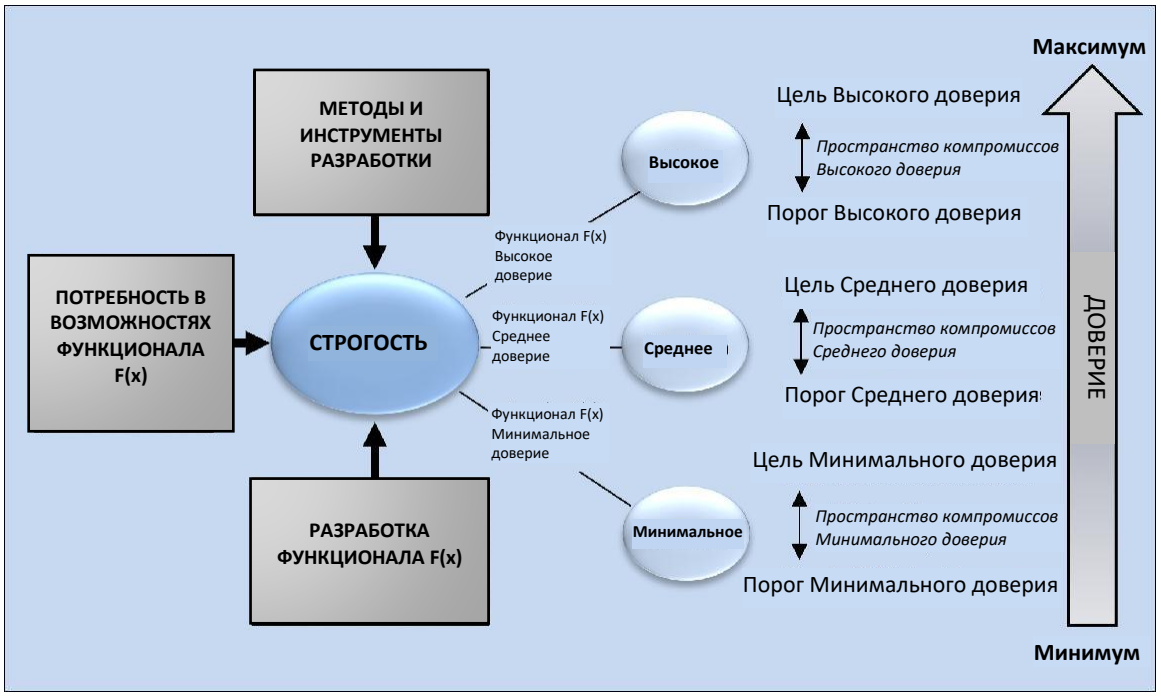

Рис. 17. Доверие и степень строгости в реализации потребностей в возможностях

Для достижения наивысшего уровня строгости в системах могут потребоваться формальные методы - методы, которые моделируют системы как математические сущности, что позволяет строго проверить свойства системы с помощью математических доказательств. Формальные методы зависят от формальных спецификаций (т.е. описаний на языке, словарь, синтаксис и семантика которого определены формально) и различных моделей, включая формальную модель политики безопасности (т.е. математически строгую спецификацию политики безопасности системы [Приложение C]).

Из-за связанных с этим затрат и сложности, формальные методы, как правило, ограничиваются проектными работами, в которых требуются только самые высокие уровни доверия, такие как формальное моделирование, спецификация и проверка политики безопасности, а также реализация, которая обеспечивает соблюдение политики (раздел D.4.2). В этом случае модель политики безопасности проверяется как полная в её области управления и как самосогласованная. Затем проверенная модель политики безопасности служит основой для проверки моделей проектирования и реализации механизмов, обеспечивающих принятие решений и выполнения этих решений.

Приложение G. Обзор процессов жизненного цикла системы

В этом приложении представлен обзор процессов жизненного цикла системы, приведенный в [4], устанавливается основа для углубленного охвата этих процессов в последующих приложениях и описываются соответствующие взаимосвязи между различными группами процессов и процессами (Раздел G.2).

G.1. Обзор процессов

Действия, выполняемые в течение жизненного цикла системы, группируются в Технические процессы (Приложение H), Технические процессы управления (Приложение I), Организационные процессы обеспечения проектирования (Приложение J) и Процессы согласования (Приложение K). В Приложениях H, I, J и K описаны соображения и вклад процессов жизненного цикла системы в достижение доверенных безопасных систем. В таблице 5 перечислены четыре группы процессов и процессы в каждой группе [4].

Таблица 5. Процессы жизненного цикла системы

ТЕХНИЧЕСКИЕ ПРОЦЕССЫ	ТЕХНИЧЕСКИЕ ПРОЦЕССЫ УПРАВЛЕНИЯ	ОРГАНИЗАЦИОННЫЕ ПРОЦЕССЫ РЕАЛИЗАЦИИ ПРОЕКТОВ	ДОГОВОРНЫЕ ПРОЦЕССЫ
- Анализ деятельности или предназначения (BA) - Определение потребностей заинтересованных сторон и требований (SN) - Определение требований к системе (SR) - Определение архитектуры системы (SA) - Определение проекта (DE) - Анализ системы (SA) - Реализация (IP) - Интеграция (B) - Проверка (VE) - Передача (TR) - Подтверждение соответствия (VA) - Эксплуатация (OP) - Поддержка (MA) - Ликвидация (DS)	- Планирование проекта (PL) - Оценка и управление проектом (PA) - Управление решениями (DM) - Управление рисками (RM) - Управление конфигурацией (CM) - Управление информацией (IM) - Измерение (MS) - Качество доверия (QA)	- Управление моделью жизненного цикла (LC) - Управление инфраструктурой (IM) - Управление портфелем (PM) - Управление персоналом - (HR) - Управление качеством (QM) - Управление знаниями (KM)	- Приобретение (AQ) - Снабжение (SP)

Соображения, связанные с безопасностью, и их вклад в жизненный цикл системы представлены в виде задач по обеспечению безопасности систем. Эти задачи соответствуют инженерным подходам к процессам жизненного цикла и основаны на фундаментальных принципах и концепциях безопасности и доверия, описанных в Главе два. Главе три, Главе четыре, Приложении C, Приложении D, Приложении E, и Приложении F. В задачах используются и применяются принципы, концепции, термины и практики разработки систем, чтобы облегчить согласованность их применения в рамках усилий по проектированию систем.

Процессы, работы и задачи жизненного цикла системы должны применяться по мере необходимости. Они не зависят от какой-либо конкретной методологии разработки системы, не ориентированы на нее и не предполагают их использования или необходимости в них. По замыслу процессы, их работы и задачи

могут применяться одновременно, итеративно или рекурсивно на любом уровне структурной иерархии системы с соответствующей точностью и строгостью и на любой стадии жизненного цикла системы в соответствии с моделями приобретения, проектирования систем или других процессов. Используя свои знания и опыт, специалисты-практики могут адаптировать процессы, работы и задачи жизненного цикла системы для достижения оптимизированных и эффективных результатов.[92] Используемые соображения включают:

- Как процессы жизненного цикла системы применяются в рамках моделей разработки, используемых организацией.
- Порядок или последовательность действий и задач в процессах жизненного цикла системы.
- Как результаты могут быть достигнуты способами, которые не строго соответствуют представлению процессов в данной публикации.
- Дополнительные работы и задачи, необходимые для достижения конкретных результатов.
- Размер, объём и сложность системы
- Необходимость учета конкретных технологий, методов или методик, используемых для разработки системы.

Адаптация процессов жизненного цикла системы позволяет команде разработчиков:

- Оптимизировать приложение процессов в соответствии с технологическими, программными, закупочными, технологическими, процедурными, этапов жизненного цикла системы или другими целями и ограничениями.
- Обеспечить одновременное приложение процессов подгруппами, сосредоточенными на различных частях одних и тех же усилий по разработке.
- Упростить применение процессов в соответствии с различными методологиями разработки систем, процессами и моделями (например, гибкими, спиральными, водопадами), которые могут использоваться в рамках одних усилий по разработке.
- Учитывать необходимость непредвиденного или иного управляемого событиями выполнения процессов для решения проблем и реагирования на изменения, происходящие во время разработки.

Хотя процессы и работы жизненного цикла взяты из [4], задачи в этой публикации не являются ни переформулированием, ни сопоставлением один к одному задач в [4]. В этой публикации основное внимание уделяется вкладу безопасности в процессы, и поэтому задачи названы для отражения этого вклада. В некоторых случаях были добавлены задачи для учёта диапазона результатов, применимых для достижения целей доверенной безопасной системы.

В описаниях процессов жизненного цикла системы предполагается, что имеется достаточно времени, финансирования, людских и материальных ресурсов для обеспечения полного применения процессов в рамках усилий по разработке систем. Процессы представляют собой *стандарт совершенства*, в рамках которого выполняется соответствующая адаптация для достижения реалистичных, оптимальных и экономически эффективных результатов в рамках ограничений, налагаемых на команду разработчиков.

[92] Адаптация может осуществляться как часть процесса планирования проекта в начале усилий по разработке систем, так и в произвольном порядке в любое время во время усилий по разработке, когда этого требуют ситуации и обстоятельства. Понимание основ инженерии безопасности систем (т.е. науки, лежащей в основе этой дисциплины) помогает определить процесс адаптации всякий раз, когда это происходит в течение жизненного цикла системы. Руководство INCOSE по проектированию систем содержит дополнительные рекомендации по адаптации процессов разработки систем [15].

Каждый из процессов жизненного цикла системы содержит набор работ и задач, которые приводят к результатам, ориентированным на безопасность.[93] В совокупности эти результаты создают систему и соответствующий набор свидетельств,[94] которые служат основой для:

- Обоснование безопасности и доверенности системы.
- Выявления и оценки рисков, связанных с безопасностью, с учетом интересов заинтересованных сторон в отношении использования системы для поддержки целей предназначения или деятельности.
- Внесения вклада в другие процессы, связанные с внедрением системы.
- Определения стратегий и действий в области эксплуатации и поддержки функционирования для устранения рисков, связанных с системой.

Описание каждого жизненного цикла системы содержит следующие разделы:

- *Назначение жизненного цикла:* описывает цель выполнения процесса.
- *Назначение безопасности:* Определяет, что процесс достигает с точки зрения безопасности.
- *Результаты по безопасности:* Представляет относящиеся к безопасности наблюдаемые результаты, ожидаемые от успешного выполнения процесса, и данные, генерируемые процессом.
- *Работы и задачи, относящиеся к безопасности:* Предоставляет набор связанных с безопасностью работ и задач, которые поддерживают достижение результатов в области безопасности для процесса.[95]

Описанные результаты достигаются персоналом, процессами и технологиями. Персонал выполняет работы и задачи на всех стадиях жизненного цикла системы для получения результатов, достигающих определенных целей безопасности. Ни одна роль персонала не отвечает за получение всех результатов, указанных в процессах жизненного цикла системы (т.е. процессы не зависят от конкретной роли). Таким образом, несколько ролей могут способствовать достижению конкретного результата.

Наконец, в этой публикации описываются соображения по разработке систем для получения указанных результатов. Однако конкретные роли или обязанности не определяются. Роли и обязанности персонала, выполняющего процессы жизненного цикла, определяют и распределяют организации. На рис. 18 представлен пример категорий персонала, каждая из которых имеет область полномочий, управления, ролей и обязанностей, которые в совокупности обеспечивают достижение результатов для данной категории. Результаты, достигнутые всеми категориями персонала, позволяют достичь определенных целей в области безопасности.

[93] Результаты являются основой для других процессов, в том числе внешних по отношению к усилиям по разработке (например, процессы жизненного цикла организации, связанные с заинтересованными сторонами, а также процессы сертификации, санкционирования или регулирования).

[94] Полнота, глубина, точность, достоверность и актуальность совокупности свидетельств являются факторами достижения желаемого уровня доверия. Цель состоит в том, чтобы совокупность свидетельств была достаточной для того, чтобы убедить заинтересованные стороны в том, что их потребности в доверии удовлетворены.

[95] Работы и задачи выполняются совместно в рамках различных ролей организации, включая разработку безопасности систем. Хотя в данной публикации основное внимание уделяется разработке безопасности систем, в ней не рассматриваются все аспекты каждого вида работ и задач.

Рис. 18. Типы персонала и ролей, поддерживающих процессы жизненного цикла

G.2. Отношения процесса

На рис. 19 показаны общие логические взаимосвязи между группами процессов жизненного цикла системы и процессами, которые могут использоваться в качестве основы и при необходимости изменяться в рамках адаптации [4].

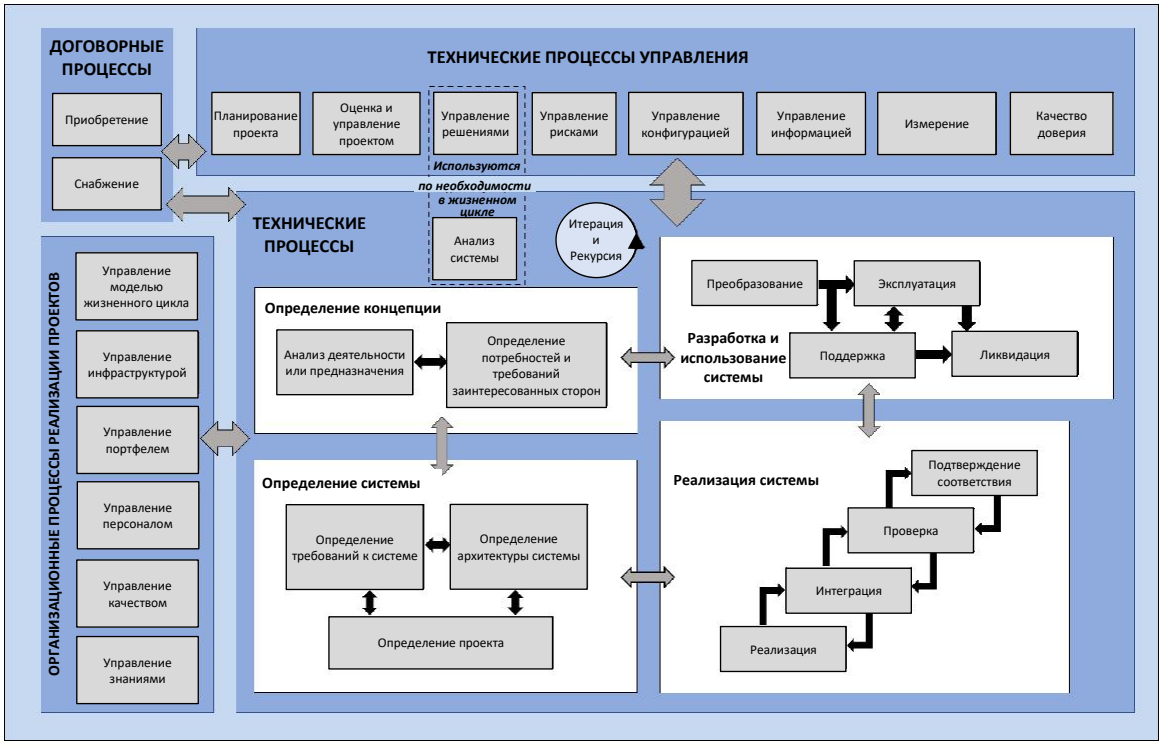

Рис. 19. Взаимосвязи между процессами жизненного цикла

Взаимосвязи процессов дополнительно проиллюстрированы *примерами использования* в [94]. Несколько известных примеров использования включают:

- *Заключение официального соглашения*
  - Соглашения между организациями, между проектами и для выполнения работ в рамках проекта.
  - Обычно это формальный договор между приобретателем и поставщиком, включая генерального подрядчика и его субподрядчиков.
- *Выполнение соглашения*
  - Процессы, необходимые для выполнения условий соглашения, включая информацию, которую организация-поставщик предоставляет организации-покупателю для обеспечения соблюдения условий соглашения.
- *Разработка системы, представляющей интерес*[96]
  - Взаимосвязи между техническими процессами (Приложение H).[97]

Дополнительную информацию о процессах жизненного цикла системы и их взаимосвязях предоставляют следующие источники: [4] [13] [15] [17] [18] [19] [27] [Процессы для систем с интенсивным использованием программного обеспечения обсуждаются в [86].

[96] Применение технических процессов для проектирования интересующей системы будет происходить рекурсивно для реализации подсистем и элементов системы. Дополнительные подробности см. в приложении A к [96].
[97] Этот пример использования часто поддерживает удовлетворение соглашения.

Приложение H. Технические процессы

Настоящее приложение содержит *Технические процессы из* [4] с учетом соображений безопасности и вклада в назначение, результаты, работы и задачи. Как отмечается в разделе G.2, применение этих процессов на любом этапе жизненного цикла описывается в [96], где приведен набор примеров этапов и результатов этапов для реализации технических процессов в рамках жизненных циклов систем и программного обеспечения.

H.1. Анализ деятельности или предназначения

Назначением процесса *«Анализ деятельности или предназначения»* является определение общей стратегической проблемы или возможности, характеристика пространства решения и определение потенциального класса(ов) решений, которые могут решить проблему или воспользоваться возможностью.

H.1.1. Назначение безопасности

- Определение аспектов безопасности, связанных со стратегическими проблемами или возможностями.
- Определение целей, проблем и ограничений безопасности, которые определяют потенциальный класс(ы) решений.

H.1.2. Результаты безопасности

- Определены аспекты безопасности стратегической проблемы или пространства возможностей.
- Охарактеризованы аспекты безопасности пространства решений.
- Определение предварительных концепций эксплуатации и других концепций на стадиях жизненного цикла основывается на аспектах безопасности пространства проблем или возможностей.
- Проанализированы класс(ы) альтернативных решений, учитывающие выявленные аспекты безопасности.
- Выбор предпочтительного класса(ов) альтернативных решений определяется аспектами безопасности пространства решений.
- Доступны вспомогательные системы или сервисы, необходимые для анализа аспектов безопасности деятельности или предназначения.
- Установлена прослеживаемость аспектов безопасности стратегических проблем и возможностей к предпочтительному(ым) классу(ам) альтернативных решений.

H.1.3. Работы и задачи безопасности

BA-1 ПОДГОТОВКА К АНАЛИЗУ ДЕЯТЕЛЬНОСТИ ИЛИ ПРЕДНАЗНАЧЕНИЯ

BA-1.1 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки анализа деятельности или предназначения.

BA-1.2 Определение и планирование вспомогательных систем или сервисов, необходимых для поддержки анализа аспектов безопасности, связанных с деятельностью или предназначением.

BA-1.3 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться при анализе деятельности или предназначения.

Ссылки: [4] [97]

BA-2 ОПРЕДЕЛЕНИЕ ПРОБЛЕМЫ ИЛИ ПРОСТРАНСТВА ВОЗМОЖНОСТЕЙ

BA-2.1 Анализ проблем или возможностей в контексте факторов пространства компромиссов, имеющих отношение к безопасности.

Примечание: Факторы пространства компромиссов, имеющие отношение к безопасности, анализируются в контексте всех факторов, включая факторы, связанные с допустимыми потерями. Результаты анализа служат основой для принятия решений о пригодности и осуществимости альтернативных вариантов.

BA-2.2 Определение аспектов безопасности проблемы или возможности предназначения, деятельности или эксплуатации, которые должны быть решены классом(ами) решений.

Примечание: Информация для получения представления о проблеме или возможности предназначения, деятельности или эксплуатации с точки зрения безопасности системы запрашивается у заинтересованных сторон. Аспекты безопасности включают цели, проблемы и ограничения безопасности.

Ссылки: [4] [30] [61] [97] [98] [99]

BA-3 ОПРЕДЕЛЕНИЕ ХАРАКТЕРИСТИК ПРОСТРАНСТВА РЕШЕНИЙ

BA-3.1 Определение аспектов безопасности предварительных концепций эксплуатации и других концепций на стадиях жизненного цикла.

Примечание 1: Концепции безопасности эксплуатации включают в себя режимы безопасной работы, сценарии эксплуатации и примеры использования, относящиеся к безопасности, а также безопасное использование в области предназначения или направления деятельности.

Примечание 2: Аспекты безопасности интегрированы в концепции жизненного цикла и используются для поддержки анализа осуществимости и оценки возможного альтернативного класса(ов) решений.

BA-3.2 Определение аспектов безопасности альтернативных классов решений.

Ссылки: [4] [71] [96] [97]

BA-4 ОЦЕНКА КЛАССОВ АЛЬТЕРНАТИВНЫХ РЕШЕНИЙ

BA-4.1 Оценка каждого класса альтернативных решений с учетом выявленных аспектов безопасности.

BA-4.2 Выбор предпочтительного класса (или классов) альтернативных решений на основе выявленных аспектов безопасности, факторов пространства компромиссов и других критериев, определенных организацией.

BA-4.3 Предоставление связанной с безопасностью обратной связи с концепциями жизненного цикла стратегического уровня для отражения выбранного класса(ов) решений.

Ссылки: [4] [71] [96] [97]

BA-5 УПРАВЛЕНИЕ АНАЛИЗОМ ДЕЯТЕЛЬНОСТИ ИЛИ ПРЕДНАЗНАЧЕНИЯ

BA-5.1 Обеспечение прослеживаемости аспектов безопасности, связанных с анализом деятельности или предназначения.

Примечание: Поддерживается двунаправленная прослеживаемость между выявленными аспектами безопасности и вспомогательными данными безопасности, связанными с проблемами и возможностями, предлагаемым классом или классами решения и стратегией организации.

BA-5.2 Предоставление связанных с безопасностью образцов, выбранных в качестве базовых.

Ссылки: [4] [71] [96]

H.2. Определение потребностей и требований заинтересованных сторон

Назначением процесса *«Определение потребностей и требований заинтересованных сторон»* является определение требований заинтересованных сторон к системе, которая может предоставить возможности, необходимые пользователям и другим заинтересованным сторонам в определенной среде.

H.2.1. Назначение безопасности

- Определение потребностей в защите, связанных с потребностями и требованиями заинтересованных сторон к системе, которая может защитить возможности, необходимые пользователям и другим заинтересованным сторонам в определенной среде.

H.2.2. Результаты безопасности

- Определены заинтересованные стороны системы, имеющие отношение к безопасности.
- Определены проблемы безопасности заинтересованных сторон.
- Определены требуемые характеристики и контекст для безопасного использования возможностей для концепций жизненного цикла системы на этапах жизненного цикла системы.
- Определены активы и классы активов заинтересованных сторон.
- Охарактеризованы неблагоприятные условия окружающей среды.
- Определены приоритеты защиты активов.
- Определены потребности в защите заинтересованных сторон.
- Выявлены ограничения для системы, обусловленные безопасностью и основанные на безопасности.
- Приоритетные потребности в защите заинтересованных сторон преобразованы в требования заинтересованных сторон.
- Определены показатели эффективности и характеристики качества, ориентированные на безопасность.
- Заинтересованные стороны согласились с тем, что их потребности и ожидания в области защиты надлежащим образом отражены в требованиях.
- Имеются вспомогательные системы или сервисы, необходимые для определения аспектов безопасности потребностей и требований заинтересованных сторон.
- Установлена прослеживаемость требований заинтересованных сторон к заинтересованным сторонам и их потребностям в защите.

H.2.3. Работы и задачи безопасности

SN-1 ПОДГОТОВКА К ОПРЕДЕЛЕНИЮ ПОТРЕБНОСТЕЙ И ТРЕБОВАНИЙ ЗАИНТЕРЕСОВАННЫХ СТОРОН

SN-1.1 Определение заинтересованных сторон и их интересов в области безопасности.

Примечание 1: У всех заинтересованных сторон есть интересы в безопасности. Некоторые интересы известны явно и могут быть описаны; другие изначально неявны, не обязательно известны, и должны быть четко выражены в ходе обсуждения.

Примечание 2: К ним относятся заинтересованные стороны, представляющие органы, ответственные за принятие важных решений, регулирующие организации, организации по сертификации, санкционированию, принятию и аналогичные организации, наделенные конкретными полномочиями и ответственностью в области принятия решений, связанных с безопасностью.

SN-1.2 Определение стратегии определения потребностей и требований заинтересованных сторон в защите.

Примечание: Стратегия включает решение вопроса о том, каким образом должен быть достигнут консенсус в отношении потребностей и требований в области защиты среди заинтересованных сторон с противоположными интересами.

SN-1.3 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки определения потребностей и требований заинтересованных сторон.

SN-1.4 Определение и планирование вспомогательных систем или сервисов, необходимых для поддержки аспектов безопасности, связанных с определением потребностей и требований заинтересованных сторон.

SN-1.5 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться при определении потребностей и требований заинтересованных сторон.

Ссылки: [4] [30] [61] [86] [97] [98] [99] [100]

SN-2 РАЗРАБОТКА ЭКСПЛУАТАЦИОННОЙ И ДРУГИХ КОНЦЕПЦИЙ ЖИЗНЕННОГО ЦИКЛА

SN-2.1 Определение репрезентативного набора сценариев для определения требуемых возможностей и мер безопасности, соответствующих ожидаемым эксплуатационной и другим концепциям жизненного цикла.

Примечание: Концепции отражают поведение системы в предполагаемых средах эксплуатации. Сценарии также помогают определить изменения концепций жизненного цикла, обусловленные безопасностью.

SN-2.2 Характеристика аспектов безопасности сред эксплуатации и предполагаемых пользователей.

Примечание 1: Это включает в себя разделение того, что известно и что не известно о неблагоприятных условиях в средах эксплуатации.

Примечание 2: Это включает в себя ожидаемое доверие пользователей к решению проблем с внутренними угрозами. Если аспекты безопасности пользователей не могут быть получены или существует неопределенность пользователей в отношении доверия, это существенно повлияет на проект и процедуру эксплуатации, дополняющую проект.

SN-2.3 Определение взаимодействия между сущностями и системой, а также факторов безопасности, влияющих на взаимодействие.

Примечание: Взаимодействие между сущностями (например, персоналом, вспомогательными системами и взаимодействующими системами) и системой, а также факторы, влияющие на взаимодействие, должны быть поняты для обоснования проектных работ. К факторам, влияющим на взаимодействия, относятся среда интересующей системы и любой системы систем, к которой относится интересующая система, а также характеристика сущностей, с которыми система взаимодействует.

SN-2.4 Определение ограничений системного решения, связанных с безопасностью.

Ссылки: [4] [30] [31] [61] [91] [97] [98] [99] [100] [101] [102] [103] [104]

SN-3 ОПРЕДЕЛЕНИЕ ПОТРЕБНОСТЕЙ ЗАИНТЕРЕСОВАННЫХ СТОРОН

SN-3.1 Определение правил, отражающих санкционированные и предполагаемые взаимодействия, поведение и результаты.

Примечание: Правила определяются концепциями жизненного цикла и их контекстом.

SN-3.2 Определение активов и классов активов заинтересованных сторон.

SN-3.3 Определение проблем, связанных с потерями, для каждого идентифицированного актива и каждого класса активов.

SN-3.4 Расстановка приоритетов активов с учетом неблагоприятных последствий потери активов.

SN-3.5 Характеристика неблагоприятных факторов, присутствующих в среде.

Примечание: К средам, в которых система подвергается воздействию потенциальных неблагоприятных факторов, относятся среды тестирования, эксплуатации, поддержки и материально-технического обеспечения. По возможности следует избегать неблагоприятных факторов и принимать меры защиты от них.

SN-3.6 Определение неопределенности, связанной с каждым выявленным неблагоприятным фактором.

SN-3.7 Определение потребностей в защите заинтересованных сторон.

Примечание: Потребности в защите включают в себя критерии их успешности, такие как показатели эффективности (MOEs).

SN-3.8 Расстановка приоритетов и выбор наименьших потребностей в защите заинтересованных сторон.

SN-3.9 Регистрация и обоснование потребностей заинтересованных сторон в области защиты.

Ссылки: [4] [30] [31] [61] [91] [98] [99] [100] [101] [103]

SN-4 ПРЕОБРАЗОВАНИЕ ПОТРЕБНОСТЕЙ ЗАИНТЕРЕСОВАННЫХ СТОРОН В ТРЕБОВАНИЯ ЗАИНТЕРЕСОВАННЫХ СТОРОН

SN-4.1 Определение ограничений на системное решение, связанных с безопасностью.

SN-4.2 Определение требований заинтересованных сторон в соответствии с аспектами безопасности и потребностями в защите.

Ссылки: [4] [30] [31] [61] [86] [98] [99] [100] [105] [106] [107] [108] [109]

SN-5 АНАЛИЗ ПОТРЕБНОСТЕЙ И ТРЕБОВАНИЙ ЗАИНТЕРЕСОВАННЫХ СТОРОН

SN-5.1 Анализ набора требований заинтересованных сторон в отношении потребностей в защите.

Примечание: Требования заинтересованных сторон анализируются, чтобы определить, точно ли и всесторонне выражены потребности в защите как в отдельных требованиях, так и в совокупности требований. Потенциальные характеристики анализа включают в себя то, что требования являются (1) необходимыми, полными, краткими и не связанными с реализацией и (2) всесторонне учитывают потребности в защите.

SN-5.2 Определение показателей эффективности и доверия к безопасности, позволяющих оценить технические достижения и их относительную критичность.

Примечание: Определение относительной критичности мер (например, показателей эффективности) отражает технические достижения и приоритеты заинтересованных сторон.

SN-5.3 Обеспечение обратной связи с соответствующими заинтересованными сторонами от проанализированных требований для подтверждения того, что их потребности и ожидания в области защиты были надлежащим образом учтены и выражены.

SN-5.4 Решение проблем, связанных с требованиями заинтересованных сторон к защите.

Примечание: Любое изменение требований заинтересованных сторон означает необходимость заново оценить потребности в защите и определить, требуются ли какие-либо последующие изменения.

Ссылки: [4] [30] [31] [61] [79] [86] [98] [99] [100] [110]

SN-6 УПРАВЛЕНИЕ ОПРЕДЕЛЕНИЕМ ПОТРЕБНОСТЕЙ И ТРЕБОВАНИЙ ЗАИНТЕРЕСОВАННЫХ СТОРОН

SN-6.1 Получение четкого согласия на то, что требования заинтересованных сторон удовлетворительно учитывают потребности в защите.

SN-6.2 Регистрация данных о защите активов.

SN-6.3 Поддержка прослеживаемость между потребностями в защите заинтересованных сторон и требованиями заинтересованных сторон.

SN-6.4 Предоставление примеров, связанных с безопасностью, выбранных в качестве базовых.

Ссылки: [4] [86] [100]

H.3. Определение требований к системе

Назначение процесса *«Определение требований к системе»* заключается в преобразовании представление заинтересованных сторон и пользователей о желаемых возможностях в техническое описание решения, отвечающее потребностям пользователя по применению системы.

H.3.1. Назначение безопасности

- Обеспечить точное и полное представление потребностей заинтересованных сторон в защите (как указано в требованиях заинтересованных сторон) в требованиях к системе.

H.3.2. Результаты безопасности

- Определены аспекты безопасности описания системы, включая интерфейсы и функции системы, а также границы системного решения.
- Определены требования к системе, относящиеся к безопасности, и ограничения на проектирование, определяемые безопасностью.
- Определены показатели результативности безопасности.
- Проведен анализ аспектов безопасности требований к системе.
- Доступны вспомогательные системы или службы, необходимые для определения аспектов безопасности требований к системе.
- Установлена прослеживаемость аспектов безопасности требований к системе и соответствующих им ограничений, связанных с безопасностью, к требованиям заинтересованных сторон.

H.3.3. Работы и задачи безопасности

SR-1 ПОДГОТОВКА К ОПРЕДЕЛЕНИЮ ТРЕБОВАНИЙ К СИСТЕМЕ

SR-1.1 Определение аспектов безопасности предполагаемого поведения и результатов на функциональной границе системы.

Примечание: Предполагаемое поведение и свойства безопасности, которые должны быть реализованы на функциональной границе, учитывают характеристики предоставляемых или используемых возможностей, характеристики сущностей, которые взаимодействуют с интересующей нас системой на функциональной границе, и связанные с ними потребности в доверии.

SR-1.2 Определение доменов безопасности системы и их корреляции с функциональными границами системы.

SR-1.3 Определение аспектов безопасности стратегии определения требований к системе.

SR-1.4 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки определения требований к системе.

SR-1.5 Определение и планирование вспомогательных систем или сервисов, необходимых для поддержки определения аспектов безопасности требований к системе.

SR-1.6 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться при определении требований к системе.

Ссылки: [4] [30] [31] [61] [97] [98] [99] [100]

SR-2 ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ К СИСТЕМЕ

SR-2.1 Определение каждой функции безопасности, которую должна выполнять система.

Примечание: Функции безопасности определяются для всех состояний, режимов и условий эксплуатации и использования системы, включая связанные переходы между состояниями и режимами системы. Функции безопасности включают функции, ориентированные на обеспечение возможностей и работоспособности системы при сохранении присущих ей характеристик безопасности.

SR-2.2 Определение аспектов безопасности каждой функции, которую должна выполнять система.

Примечание: Это подразумевает отсутствие помех со стороны других функций системы (раздел D.4.1).

SR-2.3 Определение необходимых ограничений реализации, связанных с безопасностью.

Примечание: Ограничения на систему, определяемые безопасностью, обусловлены неблагоприятными факторами, неопределенностями и рисками с учетом целей результативности и потребностей в доверии. Эти ограничения определяются требованиями заинтересованных сторон, определением архитектуры системы и ограничениями решения на протяжении всего жизненного цикла.

SR-2.4 Определение необходимых ограничений на реализацию безопасности.

Примечание: Ограничения, связанные с реализацией безопасности, должны удовлетворять ожиданиям в отношении возможностей и результативности, не связанных с безопасностью.

SR-2.5 Определение и обоснований требований к безопасности системы.

Примечание: Требования к безопасности системы включают в себя требования к возможностям и функциональности, требования к результативности и эффективности безопасности, требования доверия к безопасности и ограничения на реализацию (результаты SR-2.3 и SR-2.4, выраженные в виде требований).

SR-2.6 Применение метаданных безопасности к требованиям безопасности системы.

Примечание: Метаданные обеспечивают идентификацию и прослеживаемость для поддержки анализа полноты и согласованности данных с целью определения влияния на безопасность при изменении требований.

Ссылки: [4] [30] [31] [61] [86] [97] [98] [99] [100] [105] [106] [107] [108] [109] [111] [112] [113]

SR-3 АНАЛИЗ ТРЕБОВАНИЙ К СИСТЕМЕ

SR-3.1 Анализ всего набора требований к системе с учетом соображений безопасности.

Примечание: Требования анализируются для обеспечения полного и правильного учета соображений защиты и ограничений безопасности. Приводится логическое обоснование, подтверждающее выводы анализа и дающее основание сделать вывод о том, что анализ имеет надлежащую перспективу и полностью соответствует сделанным предположениям. См. Приложение С.

SR-3.2 Определение показателей эффективности и доверия к безопасности, которые позволяют проводить оценку технических достижений.

Примечание: Каждый показатель результативности, определяемый безопасностью (например, показатель результативности и технический показатель результативности), анализируется, чтобы убедиться в том, что требования к системе выполнены, и что определены стоимость, сроки или риски результативности проекта, связанные с несоответствием требованиям.

SR-3.3 Предоставление обратной связи от проанализированных требований к системе к соответствующим заинтересованным сторонам для рассмотрений, связанных с безопасностью.

SR-3.4 Решение проблем безопасности, связанных с требованиями к системе.

Ссылки: [4] [30] [31] [61] [79] [86] [97] [98] [99] [100] [110]

SR-4 УПРАВЛЕНИЕ ТРЕБОВАНИЯМИ К СИСТЕМЕ

SR-4.1 Получение четкого согласия с тем, что требования к системе отражают потребности в защите.

SR-4.2 Фиксация ключевых решений и обоснований, касающиеся требований к безопасности системы.

SR-4.3 Поддержка прослеживаемости требований к системе к их аспектам, относящимся к безопасности.

Примечание: Поддерживается прослеживаемость требований к системе к потребностям в защите; требованиям заинтересованных сторон; элементам архитектуры; определениям интерфейсов; результатам анализа; методам проверки; выделенным, декомпозированным и производным требованиям (в формах требований к системе, элементам системы, защиты безопасности и ограничений, определяемых безопасностью); допустимости рисков и потерь; и достижению целей доверия и доверенности.

SR-4.4 Предоставление примеров, связанных с безопасностью, выбранных в качестве базовых.

Ссылки: [4] [30] [31] [61] [97] [98] [99] [100]

H.4. Определение архитектуры системы

Назначением процесса «*Определение архитектуры системы*» является создание альтернативных вариантов архитектуры системы, выбор одного или нескольких вариантов, которые отражают интересы заинтересованных сторон и удовлетворяют требованиям к системе, и выражение этого в виде набора согласованных представлений и моделей.

H.4.1. Назначение безопасности

- Создание концепций архитектуры и свойств альтернативных вариантов архитектуры системы для обеспечения защиты системы, которые отражают интересы заинтересованных сторон и отвечают требованиям системы.
- Выражение концепций архитектуры и свойств в виде набора согласованных представлений и моделей.
- Представление аспектов безопасности, используемых для выбора одного или нескольких вариантов архитектуры.

H.4.2. Результаты безопасности

- Уточнено поле проблемм с учетом интересов ключевых заинтересованных сторон в области безопасности.
- Достигнуто согласование архитектуры с применимыми политиками, директивами, целями и ограничениями в области безопасности.
- Концепции, свойства, характеристики, поведение, функции и ограничения, которые важны для принятия решений по архитектуре, связанные с безопасностью системы, распределены между сущностями архитектуры.
- Выявленные интересы защиты заинтересованных сторон учтены в архитектуре системы.
- Установлена прослеживаемость аспектов безопасности элементов архитектуры системы до ключевых архитектурно значимых требований заинтересованных сторон и системы.
- Разработаны аспекты безопасности представлений и моделей архитектуры системы.
- Определены аспекты безопасности элементов системы, их взаимодействий и интерфейсов.

H.4.3. Работы и задачи безопасности

AR-1 ПОДГОТОВКА К ОПРЕДЕЛЕНИЮ АРХИТЕКТУРЫ СИСТЕМЫ.

AR -1.1 Определение аспектов безопасности стратегии определения архитектуры системы.

AR -1.2 Определение набора существующих архитектур, относящихся к безопасности, или эталонных архитектур, которые могут иметь прямое применение и должны использоваться в качестве руководства для контроля.

AR -1.3 Определение аспектов безопасности основы(основ) описания архитектуры, точек зрения и шаблонов моделирования, которые будут использоваться при определении архитектуры системы.

AR -1.4 Определение специфичных для безопасности точек зрения и шаблонов моделирования для использования в процессе определения архитектуры системы.

AR -1.5 Определение целей и критериев оценки безопасности с учетом интересов ключевых заинтересованных сторон.

AR -1.6 Определение методов оценки безопасности и их интеграция с целями и критериями оценки.

AR -1.7 Сбор и анализ информации, связанной с оценкой безопасности.

AR -1.8 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки определения архитектуры системы.

AR -1.9 Определение и планирование вспомогательных систем или сервисов, необходимых для поддержки аспектов безопасности при определении архитектуры системы.

AR -1.10 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться при определении архитектуры системы.

Ссылки: [4] [30] [61] [71] [98] [99] [100] [117]

AR-2 СОЗДАНИЕ ВАРИАНТА(ОВ) АРХИТЕКТУРЫ СИСТЕМЫ

AR -2.1 Определение аспектов безопасности целей архитектуры и критических критериев успеха.

AR -2.2 Синтезирование потенциальных доверенных безопасных решений в пространстве решений.

AR -2.3 Характеристика аспектов доверенных безопасных решений и пространства компромиссов.

AR -2.4 Формулирование вариантов доверенных безопасных архитектур.

AR -2.5 Фиксация концепций и свойств доверенной безопасной архитектуры.

AR -2.6 Соотнесение вариантов архитектуры с другими архитектурами и соответствующими затрагиваемыми сущностями для обеспечения согласованности концепций и свойств доверенной безопасной архитектуры.

AR -2.7 Координация безопасного использования вариантов архитектур предполагаемыми пользователями.

AR -2.8 Разработка аспектов безопасности моделей и представлений вариантов архитектур.

Примечание: Ниже приведены некоторые типичные соображения:

- Определение контекста безопасности и границ безопасности системы с учётом интерфейсов и взаимодействий с внешними сущностями.
- Определение архитектурных сущностей и связей между сущностями, которые отвечают ключевым интересам защиты заинтересованных сторон и требованиям безопасности системы.
- Распределение концепций безопасности, свойств безопасности, характеристик безопасности, поведения безопасности, функций безопасности или ограничений безопасности между архитектурными сущностями.
- Составление совокупности взглядов, отражающих то, как архитектура учитывает интересы защиты заинтересованных сторон и отвечает требованиям безопасности заинтересованных сторон и системы.
- Согласование моделей и представлений архитектуры.

AR -2.9 Координация безопасного использования архитектуры предполагаемыми пользователями.

Ссылки: [4] [30] [61] [71] [98] [99] [100] [117]

AR-3 ОЦЕНКА ВАРИАНТОВ АРХИТЕКТУРЫ СИСТЕМЫ

AR -3.1 Анализ заслуживающих доверия концепций и свойств доверенной архитектуры и оценка ценности архитектуры для удовлетворения потребностей заинтересованных сторон в области безопасности.

AR -3.2 Характеристика вариантов архитектуры на основе доверенных результатов анализа безопасности.

AR -3.3 Формулирование выводов и рекомендаций оценки, относящихся к безопасности.

AR -3.4 Сбор и передача результатов оценки безопасности.

AR -3.5 Соотнесение архитектуры с другими архитектурами и соответствующими затронутыми сущностями, чтобы обеспечить согласованность архитектуры доверенной безопасной системы.

Ссылки: [4] [30] [61] [71] [98] [99] [117]

Связанные публикации: [100]

AR-4 УПРАВЛЕНИЕ РЕЗУЛЬТАТАМИ ОПРЕДЕЛЕНИЯ АРХИТЕКТУРЫ СИСТЕМЫ

AR -4.1 Достижение согласия по аспектам безопасности архитектуры.

AR -4.2 Фиксация ключевых решений по архитектуре системы, относящихся к безопасности, и их обоснование.

AR -4.3 Обеспечение прослеживаемости аспектов безопасности архитектуры системы.

AR -4.4 Предоставление образцов, относящихся к безопасности, выбранных в качестве базовых.

AR -4.5 Оказание поддержки усилиям организации по руководству и управлению архитектурой.

Ссылки: [4] [30] [61] [71] [98] [99] [100] [117]

H.5. Определение проекта

Назначением процесса «*Определение проекта»* является предоставление достаточных данных и информации о системе и ее элементах для реализации решения в соответствии с требованиями и архитектурой системы.

H.5.1. Назначение безопасности

- Предоставление достаточно подробных данных и информации об аспектах безопасности системы и ее элементов для реализации надежного безопасного решения в соответствии с требованиями системы и архитектуры.

H.5.2. Результаты безопасности

- Оценены аспекты безопасности альтернативных проектов элементов системы.
- Распределены требования к системе с учетом аспектов её безопасности.
- Определены интерфейсы безопасности и аспекты безопасности интерфейсов между элементами системы, составляющими систему.
- Определены проектные характеристики безопасности каждого элемента системы.
- Обеспечена доступность вспомогательных систем или служб для аспектов безопасности при определении проекта.
- Установлена прослеживаемость проектных характеристик безопасности.

H.5.3. Работы и задачи безопасности

DE-1 ПОДГОТОВКА К ОПРЕДЕЛЕНИЮ ПРОЕКТА

DE-1.1 Установление аспектов доверенной безопасности для стратегии определения проекта.

DE-1.2 Определение технологий безопасности, необходимых для каждого элемента системы, составляющего систему.

DE-1.3 Определение проблем безопасности, связанных с каждой технологией, требуемой для каждого элемента системы.

Примечание 1: Сюда входят проблемы безопасности, связанные с известными и потенциальными уязвимостями в цепочках поставок, связанных с приобретением технологий.

Примечание 2: У проблем могут быть связанные с ними риски, которые необходимо регистрировать и отслеживать.

DE-1.4 Определение необходимых категорий безопасности и доверенности характеристик системы, представленных в проекте.

DE-1.5 Определение принципов доверенного и безопасного развития проекта системы.

DE-1.6 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки определения проекта.

DE-1.7 Определение и планирование вспомогательных систем или сервисов, необходимых для поддержки аспектов безопасности при определении проекта.

DE-1.8 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться при определении проекта.

Ссылки: [4] [30] [61] [98] [99] [100]

DE-2 СОЗДАНИЕ ПРОЕКТА СИСТЕМЫ

DE-2.1 Распределение требований безопасности по элементам системы.

DE-2.2 Преобразование относящихся к безопасности архитектурных сущностей и взаимосвязей в элементы проекта.

DE-2.3 Преобразование архитектурных характеристик, относящихся к безопасности, в доверенные характеристики безопасного проекта.

Примечание: Характеристики включают или отражают ожидаемый уровень доверия.

DE-2.4 Определение необходимых средств обеспечения доверенного безопасного проекта.

DE-2.5 Изучение альтернативных вариантов доверенного безопасного проекта.

DE-2.6 Уточнение или определение аспектов безопасности интерфейсов между элементами системы и внешними сущностями.

Примечание: Детали определенных интерфейсах уточняются с учётом аспектов безопасности. К ним относятся безопасность и обусловленные безопасностью ограничения, применяемые к интерфейсам, взаимодействию и поведению между компонентами и с внешними сущностями, такими как взаимодействующие системы (раздел 2.1.2), периферийные устройства и люди, взаимодействующие с системой.

DE-2.7 Разработка аспектов безопасности образцов проекта.

Примечание 1. Образцы проекта включают общие спецификации и спецификации безопасности, таблицы данных, базы данных и документы.

Примечание 2: Образцы проекта включают в себя конфигурацию и процедуры, обеспечивающие поведение механизма безопасности, указанное в политике системного уровня и обеспечиваемое конфигурацией и процедурами (Приложение C.3).

DE-2.8 Фиксация аспектов проекта, связанных с безопасностью.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [106] [107] [108] [109]

DE-3 ОЦЕНКА ПРОЕКТА СИСТЕМЫ

DE-3.1 Проведение анализа каждого альтернативного варианта проекта системы по критериям, разработанным на основе ожидаемых свойств и характеристик доверенного безопасного проекта.

DE-3.2 Оценка каждого варианта проекта системы на предмет того, насколько хорошо он отвечает потребностям заинтересованных сторон в защите и аспектам безопасности требований к системе.

Примечание: Оценка включает в себя оценку конфигурации и процедур для обеспечения поведения механизма безопасности, определенного политикой на уровне системы и обеспечиваемого конфигурацией и процедурами (Приложение C.3).

DE-3.3 Объединение анализа и оценок безопасности в общей оценке для выбора предпочтительного проектного решения.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [109]

DE-4 УПРАВЛЕНИЕ РЕЗУЛЬТАТАМИ ОПРЕДЕЛЕНИЯ ПРОЕКТА

DE-4.1 Получение согласия по аспектам проекта, связанным с безопасностью.

DE-4.2 Сопоставление характеристик доверенного безопасного проекта с элементами системы.

DE-4.3 Регистрация решений по доверенному безопасному проекту и их обоснование.

DE-4.4 Поддержка прослеживаемости аспектов безопасности проекта системы.

Примечание: Прослеживаемость поддерживается между характеристиками доверенного безопасного проекта и архитектурными сущностями безопасности, требованиями к элементам системы, определениями интерфейсов, результатами анализа, а также методами или методиками проверки и подтверждения соответствия.

DE-4.5 Предоставление связанных с безопасностью образцов, выбранных в качестве базовых.

Ссылки: [4] [100] [106] [107] [108]

H.6. Анализ системы

Назначением процесса «*Анализ системы»* является обеспечение строгой основы информации и данных для технического понимания в целях содействия принятию решений и проведению технических оценок на протяжении всего жизненного цикла.

H.6.1. Назначение безопасности

- Создание строгой основы данных и информации для технического понимания аспектов безопасности в целях содействия принятию решений и проведению технических оценок на протяжении всего жизненного цикла.

H.6.2. Результаты безопасности

- Определены аспекты безопасности потребностей анализа системы.

- Подтверждены аспекты безопасности допущений и результатов анализа системы.
- Результаты системного анализа, представленные для всех решений или потребностей в технической оценке, включают аспекты безопасности.
- Доступны вспомогательные системы или службы для аспектов безопасности анализа системы.
- Установлена прослеживаемость аспектов безопасности результатов анализа системы.

H.6.3. Работы и задачи безопасности

SA-1 ПОДГОТОВКА К АНАЛИЗУ СИСТЕМЫ

SA-1.1 Определение аспектов безопасности стратегии анализа системы.

SA-1.2 Определение аспектов безопасности проблемы или вопроса, требующих анализа системы.

Примечание: Проблема или вопрос не обязательно могут определяться очевидными соображениями или аспектами безопасности или иметь их в своей основе.

SA-1.3 Определение заинтересованных сторон анализа системы, имеющих отношение к безопасности.

SA-1.4 Определение области, цели, уровня точности, уровня строгости и уровня доверия для аспектов безопасности анализа системы.

SA-1.5 Выбор методов для рассмотрения аспектов безопасности анализа системы.

SA-1.6 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки анализа системы.

SA-1.7 Определение и планирование вспомогательных систем или сервисов, необходимых для поддержки аспектов безопасности анализа системы.

SA-1.8 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться в анализе системы.

SA-1.9 Определение и подтверждение предположений, связанных с безопасностью.

Примечание 1: Сюда входят предположения, вытекающие из пределов определенности: что известно, что недостаточно известно и что неизвестно.

Примечание 2: Предположения, которые не могут быть подтверждены, представляют неопределенность и потенциальный риск.

SA-1.10 Планирование и сбор данных и исходных данных, необходимых для аспектов анализа, связанных с безопасностью.

Ссылки: [4] [30] [61] [98] [99] [100]

SA-2 ВЫПОЛНЕНИЕ АНАЛИЗА СИСТЕМЫ

SA-2.1 Применение выбранных методов анализа для выполнения необходимых аспектов анализа системы, относящихся к безопасности.

SA-2.2 Рассмотрение результатов анализа, связанных с безопасностью, на предмет качества и обоснованности.

Примечание: Результаты соотносятся с соответствующими и ранее выполненными анализами, имеющими отношение к безопасности. Доверенность результатов определяется в ходе рассмотрения.

SA-2.3 Подготовка выводов и рекомендаций по аспектам безопасности анализа системы.

Примечание: Проводятся консультации с экспертами в данной области, которые участвуют в формулировании выводов и рекомендаций.

SA-2.4 Фиксация результатов анализа аспектов безопасности системы.

Ссылки: [4] [86] [100] [106] [107] [108] [109]

SA-3 УПРАВЛЕНИЕ АНАЛИЗОМ СИСТЕМЫ

SA-3.1 Поддержание прослеживаемости аспектов безопасности результатов анализа системы.

Примечание: Двунаправленная прослеживаемость фиксирует взаимосвязь между аспектами безопасности результатов анализа системы, применяемыми методами, данными, используемыми для анализа, предположениями и контекстом, определяющим рассматриваемую проблему или вопрос.

SA-3.2 Предоставление связанных с безопасностью образцов, выбранные в качестве базовых.

Примечание: Сюда входят общие образцы и образцы, относящиеся к безопасности.

Ссылки: [4] [100] [106] [107] [108]

H.7. Реализация

Назначением процесса *«Реализация»* является реализация определенного элемента системы.

H.7.1. Назначение безопасности

- Преобразование требований к безопасности, архитектуры и проекта системы (включая интерфейсы) в действия, которые создают доверенный безопасный элемент системы в соответствии с практиками выбранной технологии реализации с использованием соответствующих технических специальностей или дисциплин, связанных и не связанных с безопасностью.

H.7.2. Результаты безопасности

- Определены связанные с безопасностью ограничения реализации, влияющие на требования, архитектуру или проект.
- Реализован доверенный безопасный элемент системы.
- Элементы системы безопасно упакованы и хранятся.
- Доступны вспомогательные системы или службы для обеспечения безопасности аспектов реализации.
- Установлена прослеживаемость аспектов безопасности реализованных элементов системы.

H.7.3. Работы и задачи безопасности

IP-1 ПОДГОТОВКА К РЕАЛИЗАЦИИ

IP-1.1 Определение доверенных безопасных аспектов стратегии реализации.

Примечание 1: Эти аспекты относятся ко всем элементам системы, которые приобретаются вновь, создаются вновь или используются повторно (*с* изменениями или без них). Если стратегия заключается в

повторном использовании, то проект определяет объем, источник, пригодность и доверенность повторно используемых элементов системы для новой цели. Стратегия реализации включает в себя процедуры, процессы изготовления, инструменты и оборудование, допуски, и неопределенности при проверке, которые могут привести к слабым местам и уязвимостям. В случае повторной реализации элементов системы (например, серийного производства, замены элементов системы) процедуры и процессы изготовления определяются для достижения стабильной и воспроизводимой производительности.

Примечание 2: Аспекты безопасности определяются целевым уровнем доверия, неопределенностями проверки безопасности и проблемами безопасности, связанными с логистикой, поставками и распределением компонентов.

IP-1.2 Определение связанных с безопасностью ограничений и целей реализации в требованиях к безопасности системы, характеристиках архитектуры и проекта, или методах реализации.

IP-1.3 Определение аспектов безопасности для вспомогательных систем, сервисов и материалов, необходимых для поддержки реализации.

IP-1.4 Определение и планирование вспомогательных систем, сервисов и материалов, необходимых для поддержки аспектов безопасности реализации.

IP-1.5 Получение или приобретение доступа к аспектам безопасности вспомогательных систем, сервисов и материалов, которые будут использоваться при реализации.

Ссылки: [4] [30] [61] [98] [99] [111] [112] [113]

IP -2 ВЫПОЛНЕНИЕ РЕАЛИЗАЦИИ

IP-2.1 Реализация или адаптация элементов системы в соответствии с аспектами безопасности стратегии внедрения и процедур внедрения, а также ограничениями, связанными с безопасностью.

Примечание: Элементы системы могут включать в себя:

- *Аппаратное и программное обеспечение:* Аппаратные и программные элементы либо приобретаются, либо изготавливаются.

  Изготовление оборудования и разработка программного обеспечения на заказ позволяют получить представление о деталях проекта и реализации. Эти знания нередко приводят к повышению доверия.

  Приобретенные аппаратные и программные элементы могут не дать возможности получить такое же глубокое представление о проекте и реализации и могут предложить больше функциональности и возможностей, чем требуется. Пределы того, что может быть известно о внутреннем устройстве элементов, приводят к уровню неопределенности в отношении уязвимости и максимального доверия, которое может быть достигнуто.

- *Встроенное программное обеспечение:* Встроенное программное обеспечение определяет свойства аппаратного и программного обеспечения. Элементы встроенного программного обеспечения могут быть получены или разработаны для реализации аспектов программного обеспечения, а затем изготовлены для реализации физической формы аппаратных аспектов. Поэтому, элементы встроенного программного обеспечения, должны соответствовать соображениям реализации безопасности как аппаратных, так и программных элементов.

- *Сервисы:* Элементы системы, реализованные путем получения или аренды сервисов, подчиняются тем же критериям, которые используются для приобретения оборудования, встроенного программного обеспечения и программного обеспечения, но также должны учитывать соображения безопасности, связанные с использованием и поддержкой ресурсов.

- *Ресурсы для использования и поддержки:* Соображения безопасности приобретённых или арендованных сервисов учитывают конкретные роли и обязанности отдельных лиц поставщика услуг/аренды и их способность учитывать все требования и ограничения безопасности, связанные с

поставкой, использованием и поддержанием арендуемых сервисов или возможностей.

IP-2.2 Перевод, при необходимости, элемента системы в безопасное состояние для использования в будущем.

Примечание: Это включает защиту элемента во время хранения и транспортировки, а также упаковку и маркировку элемента.

IP-2.3 Фиксация объективных свидетельств соответствия элементов системы требованиям безопасности системы.

Ссылки: [4] [30] [61] [86] [98] [99] [109] [111] [112] [113]

IP -3 УПРАВЛЕНИЕ РЕЗУЛЬТАТАМИ РЕАЛИЗАЦИИ

IP-3.1 Фиксация аспектов безопасности результатов реализации и всех встречающихся аномалий.

IP-3.2 Поддержание прослеживаемости аспектов безопасности реализованных элементов системы.

Примечание: Поддерживается двунаправленная прослеживаемость аспектов безопасности реализованных элементов системы с требования к безопасности системы, представлениями о безопасности архитектуры, проектом безопасности и требованиями к интерфейсам безопасности.

IP -3.3 Предоставление связанных с безопасностью образцов, выбранных в качестве базовых.

Ссылки: [4] [30] [61] [98] [99]

H.8. Интеграция

Назначением процесса «*Интеграция*» является синтезирование набора элементов системы в реализованную систему, удовлетворяющую требованиям к системе.

H.8.1. Назначение безопасности

- Синтезирование набора элементов системы в реализованную доверенную безопасную систему, удовлетворяющую требованиям к системе.

H.8.2. Результаты безопасности

- Определены связанные с безопасностью ограничения интеграции, влияющие на требования, архитектуру, проект или интерфейсы и взаимодействия.
- Разработаны подходы и контрольные точки для правильной безопасной активации идентифицированных интерфейсов и функций системы в исходное или установленное безопасное состояние.
- Доступны вспомогательные системы или сервисы для аспектов интеграции, связанных с безопасностью.
- Интегрирована доверенная безопасная система, состоящая из реализованных элементов системы.
- Проверены аспекты безопасности внешних интерфейсов системы (система - внешняя среда) и внутренних интерфейсов системы (между реализованными элементами системы).
- Выявлены аспекты безопасности результатов интеграции и аномалий.

- Установлена прослеживаемость аспектов безопасности элементов интегрированной системы.

H.8.3. Работы и задачи безопасности

IN-1 ПОДГОТОВКА К ИНТЕГРАЦИИ

IN-1.1 Идентификация и определение контрольных точек для правильной безопасной активации и целостности интерфейсов и выбранных функций системы по мере синтеза элементов системы.

IN-1.2 Определение аспектов стратегии интеграции, связанных с безопасностью.

Примечание: Интеграция выполняется для достижения доверенных безопасных результатов с использованием таких аспектов, как безопасные последовательности сборки и контрольные точки для элементов системы на основе установленных приоритетов, при минимизации времени и затрат на интеграцию и обеспечении соответствующей обработки рисков.

IN-1.3 Определение связанных с безопасностью ограничений и целей интеграции, которые должны быть включены в требования к системе, архитектуру или проект.

IN-1.4 Определение аспектов безопасности для вспомогательных систем, сервисов и материалов, необходимых для поддержки интеграции.

IN-1.5 Определение и планирование вспомогательных систем, сервисов и материалов, необходимых для поддержки аспектов интеграции, связанных с безопасностью.

IN-1.6 Получение или приобретение доступа к аспектам безопасности вспомогательных систем, сервисов и материалов, используемых при интеграции.

Ссылки: [4] [30] [61] [81] [98] [99] [100] [111] [112] [113]

IN-2 ВЫПОЛНЕНИЕ ИНТЕГРАЦИИ

IN-2.1 Проверка доступности и согласованности интерфейсов в соответствии с аспектами безопасности, указанными в определениях интерфейсов и графиках интеграции.

IN-2.2 Выполнение действий по устранению любых проблем, связанных с согласованностью или доступностью.

IN-2.3 Безопасное объединение реализованных элементов системы в соответствии с запланированными последовательностями.

IN-2.4 Безопасная интеграция конфигураций элементов системы до тех пор, пока не будет безопасно синтезирована вся система.

IN-2.5 Проверка ожидаемых результатов интерфейсов, взаимосвязей, выбранных функций и характеристик безопасности.

Ссылки: [4] [86] [100] [109] [111] [112] [113]

IN-3 УПРАВЛЕНИЕ РЕЗУЛЬТАТАМИ ИНТЕГРАЦИИ

IN-3.1 Фиксация аспектов безопасности результатов интеграции и всех встречающихся аномалий.

Примечание: Анализ аномалий определяет корректирующие действия, которые могут повлиять на возможности защиты системы и уровень доверия, который можно получить.

IN-3.2 Обеспечение прослеживаемости аспектов безопасности интегрированных элементов системы.

Примечание: Поддерживается двунаправленная прослеживаемость аспектов безопасности интегрированных элементов системы с требованиями к безопасности системы, представлениями о безопасности архитектуры, проектом безопасности и требованиями к интерфейсам безопасности.

Прослеживаемость обеспечивает свидетельства, которые поддерживают утверждения о доверии и доверенности.

IN-3.3 Предоставление связанных с безопасностью образцов, выбранных в качестве базовых.

Ссылки: [4] [30] [61] [98] [99] [100]

H.9. Проверка

Назначением процесса «*Проверка*» является предоставление объективных свидетельств того, что система, элемент системы или образец соответствуют заданным требованиям и характеристикам.

H.9.1. Назначение безопасности

- Предоставление объективных свидетельств того, что система, элемент системы или образец (например, требования к системе, описание архитектуры или описание проекта) соответствует заданным требованиям и характеристикам безопасности.
- Выявление связанных с безопасностью аномалий[98] в любом образце, реализованных элементах системы или процессах жизненного цикла и предоставление необходимой информации для определения путей устранения таких аномалий.

H.9.2. Результаты безопасности

- Определены связанные с безопасностью ограничения проверки, влияющие на требования, архитектуру или проект.
- Доступны вспомогательные системы или сервисы для аспектов безопасность проверки.
- Проверены аспекты безопасности системы, элемента системы или образца.
- Представлены данные, относящиеся к безопасности, которые предоставляют информацию для корректирующих действий.
- Представлены объективные свидетельства того, что реализованная система соответствует требованиям безопасности и аспектам безопасности архитектуры и проекта.
- Выявлены аспекты безопасности результатов проверки и аномалии.
- Установлена прослеживаемость аспектов безопасности проверенных элементов системы.

H.9.3. Работы и задачи безопасности

VE-1 ПОДГОТОВКА К ПРОВЕРКЕ

VE-1.1 Определение аспектов безопасности в рамках области проверки и соответствующие действия по проверке безопасности.

Примечание: Область включает систему, элементы системы, элементы информации или образцов, которые будут проверены на соответствие применимым требованиям, характеристикам безопасности или другим свойствам безопасности. Описание каждого действия по проверке включает в себя то, что будет проверяться (например, реальная система, модель, макет, прототип, процедура, план или другой

[98] Аномалии включают в себя поведение и результаты, которые наблюдаются, но не соответствуют предусмотренным.

информационный элемент), метод проверки (включая эмуляцию любых неблагоприятных условий) и ожидаемый результат, определенный критериями успеха. Критерии безопасности могут отражать соображения стойкости функции/механизма, устойчивости к вмешательству, неправильному использованию или злоупотреблению, устойчивости к проникновению, уровня доверия, отсутствия недостатков, слабых мест и отсутствия неопределенного поведения и результатов.

VE-1.2 Определение ограничений, которые потенциально могут ограничить осуществимость действий по проверке, ориентированных на безопасность.

Примечание: Ограничения включают техническую осуществимость; доступность квалифицированного персонала и средств обеспечения проверки; доступность достаточных, актуальных и достоверных данных об угрозах; применяемую технологию (включая эмуляцию неблагоприятных условий); размер и сложность элемента системы или образца; а также стоимость и время, отведенные на проверку.

VE-1.3 Выбор подходящих методов проверки безопасности и соответствующих критериев успеха для каждого действия по проверке безопасности.

Примечание: Методы и технологии выбираются для получения свидетельств, необходимых для достижения ожидаемых результатов с желаемым уровнем доверия.

VE-1.4 Определение аспектов безопасности стратегии проверки.

Примечание: Это включает в себя подход, используемый для включения соображений безопасности во все действия по проверке с учётом компромиссов между областью, глубиной и строгостью, необходимыми для достижения желаемого уровня доверия и заданных ограничений.

VE-1.5 Определение связанных с безопасностью ограничений и целей, которые вытекают из аспектов безопасности стратегии проверки и должны быть включены в требования к системе, архитектуру и проект.

VE-1.6 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки проверки.

VE-1.7 Определение и планирование вспомогательных систем или сервисов, необходимых для поддержки аспектов безопасности проверки.

VE-1.8 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться при проверке.

Ссылки: [4] [30] [31] [61] [86] [[97] [98] [99] [100] [119] [120] [121] [122]

VE-2 ВЫПОЛНЕНИЕ ПРОВЕРКИ

VE-2.1 Определение аспектов безопасности процедур проверки, каждая из которых поддерживает одно или несколько действий по проверке.

Примечание: Процедуры определяют назначение проверки с точки зрения безопасности, критерии успеха (ожидаемые результаты), применяемый метод проверки, необходимые вспомогательные системы (например, средства, оборудование) и условия среды для выполнения каждой процедуры проверки (например, ресурсы, квалифицированный персонал, эмуляция неблагоприятных условий).

VE-2.2 Выполнение процедур проверки безопасности.

Ссылки: [4] [86] [97] [100] [109]

VE-3 УПРАВЛЕНИЕ РЕЗУЛЬТАТАМИ ПРОВЕРКИ

VE-3.1 Регистрация аспектов безопасности результатов проверки и любых обнаруженных аномалий.

VE-3.2 Получение согласования от санкционирующего органа на то, что система, элемент системы или образец соответствуют установленным требованиям безопасности системы.

Примечание: Могут существовать несколько органов санкционирования с обязанностями, связанными с безопасностью.

VE-3.3 Обеспечение прослеживаемости аспектов безопасности проверки.

Примечание: Поддерживается двунаправленная прослеживаемость между проверенными аспектами безопасности элементов системы и требованиями к безопасности системы, архитектурой, проектом и интерфейсами. Эта прослеживаемость включает в себя результаты проверки или свидетельства, такие как аномалии, отклонения или соответствие требованиям, связанным с безопасностью.

VE-3.4 Предоставление связанных с безопасностью образцов, выбранных в качестве базовых.

Ссылки: [4] [30] [61] [98] [99] [100] [109]

H.10. Передача

Назначением процесса *«Передача»* является создание возможности для системы по предоставлению сервисов, определенных требованиями заинтересованных сторон в среде эксплуатации.

H.10.1. Назначение безопасности

- Сохранение проверенных характеристик безопасности системы во время упорядоченной и плановой передачи системы к функционированию в намеченной среде, которая может быть новой или измененной средой.

H.10.2. Результаты безопасности

- Определены связанные с безопасностью ограничения передачи, влияющие на требования к системе, архитектуру или проект.
- Доступны вспомогательные системы или службы для аспектов безопасности передачи.
- Подготовленный объект информатизации удовлетворяет критериям безопасности.
- Система установлена в эксплуатационной среде и может выполнять заданные функции доверенным и безопасным способом.
- Операторы, пользователи и другие заинтересованные стороны, необходимые для использования и поддержки системы, обучены возможностям, механизмам и функциям безопасности системы.
- Определены связанные с безопасностью результаты и аномалии передачи.
- Установленная система активирована и готова к доверенной безопасной эксплуатации.
- Установлена прослеживаемость аспектов безопасности элементов передачи.

H.10.3. Работы и задачи безопасности

TR-1 ПОДГОТОВКА К ПЕРЕДАЧЕ

TR-1.1 Определение аспектов безопасности стратегии передачи.

Примечание: Стратегия передачи включает в себя все относящиеся к безопасности работы от доставки и установки на объекте информатизации до развертывания и ввода системы в эксплуатацию, а также все заинтересованные стороны, имеющие отношение к безопасности, включая операторов. Стратегия также включает в себя роли и обязанности по обеспечению безопасности, соображения по средствам безопасности, безопасную доставку и приёмку, планы возврата в исходное состояние в непредвиденных ситуациях, обучение по вопросам безопасности, аспекты безопасности при выполнении демонстрационных задач по приемке развёртывания, проверке готовности к безопасной эксплуатации, начале безопасной эксплуатации, критерии успешности безопасного перехода, права безопасного доступа, права на данные, и интеграцию с другими планами. Ввод системы в эксплуатацию рассматривается наряду с безопасным выводом из эксплуатации старой системы при ее наличии. В этом случае процессы передачи и утилизации используются одновременно.

TR-1.2 Выявление и определение любых необходимых изменений средств или объекта информатизации, связанных с безопасностью.

TR-1.3 Определение связанных с безопасностью ограничений и целей из аспектов безопасности передачи, которые должны быть включены в требования к системе, архитектуру и проект.

TR-1.4 Определение и организация обучения по вопросам безопасности операторов, пользователей и других заинтересованных сторон**,** необходимых для использования и поддержки системы.

TR-1.5 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки передачи.

TR-1.6 Определение и планирование вспомогательных систем или сервисов, необходимых для поддержки аспектов безопасности передачи.

TR-1.7 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться при передаче.

TR-1.8 Определение аспектов безопасности и организация безопасной доставки и приема элементов системы и вспомогательных систем.

Ссылки: [4] [30] [61] [98] [99]

TR-2 ВЫПОЛНЕНИЕ ПЕРЕДАЧИ

TR-2.1 Подготовка объекта эксплуатации в соответствии с требованиями к безопасной установке.

TR -2.2 Безопасная доставка системы для установки в нужное место и время.

Примечание: Безопасная доставка включает различные формы, средства и методы, которые обеспечивают сквозную транспортировку элементов системы, чтобы гарантировать, что они не будут изменены во время транспортировки. Предметы и упаковки доставляются только предполагаемому получателю, что может приводить к увеличению времени доставки для обеспечения дополнительной безопасности.

TR -2.3 Установка системы в эксплуатационной среде в соответствии со стратегией безопасной установки и установление безопасных взаимодействий с её средой.

TR -2.4 Демонстрация доверенной безопасной установки системы.

Примечание: Процедуры установки и подключения должны быть надлежащим образом проверены, чтобы обеспечить уверенность в том, что достигнута запланированная конфигурация системы во всех режимах и состояниях системы. Это включает завершение приемочных испытаний, определенных в соглашениях. Эти испытания включают в себя аспекты безопасности, связанные с физическими соединениями между

системой и средой.

TR -2.5 Проведение обучения по вопросам безопасности для операторов, пользователей и других заинтересованных сторон, необходимых для использования и поддержки системы.

TR -2.6 Выполнение безопасной активации и проверки системы.

Примечание: Безопасная активация и проверка показывают, что система может быть инициализирована в начальное безопасное рабочее состояние для всех определенных режимов работы и учитывает все соединения с другими системами через физические, виртуальные и беспроводные интерфейсы.

TR -2.7 Демонстрация того, что установленная система может выполнять требуемые функции доверенным и безопасным способом.

TR -2.8 Демонстрация того, что функции безопасности, предоставляемые системой, и результаты функций безопасности являются устойчивыми к вспомогательным системам.

TR -2.9 Рассмотрение доверенности безопасности системы на предмет ее готовности к эксплуатации.

Примечание: Результаты установки, эксплуатации и проверки вспомогательных систем рассматриваются для определения того, являются ли производительность и эффективность безопасности достаточным основанием для использования по назначению.

TR -2.10 Ввод системы в эксплуатацию для безопасного применения.

Примечание: Это включает предоставление поддержки безопасности для пользователей и операторов во время ввода системы в эксплуатацию.

Ссылки: [4] [86]

TR-3 УПРАВЛЕНИЕ РЕЗУЛЬТАТАМИ ПЕРЕДАЧИ

TR -3.1 Регистрация аспектов безопасности результатов передачи и всех обнаруженных аномалий.

TR -3.2 Регистрация аспектов безопасности эксплуатационных инцидентов и проблем и отслеживание их решения.

TR -3.3 Обеспечение прослеживаемости аспектов безопасности передаваемых элементов системы.

Примечание: Поддерживается двунаправленная прослеживаемость между всеми выявленными аспектами безопасности и вспомогательными данными, связанными со стратегией передачи и требованиями к системе, архитектурой и проектом системы.

TR -3.4 Предоставление связанных с безопасностью образцов, выбранных в качестве базовых.

Ссылки: [4]

H.11. Подтверждение соответствия

Назначение процесса *«Подтверждение соответствия»* заключается в том, чтобы предоставить объективные свидетельства того, что система, при использовании, соответствует целям деятельности или предназначения и требованиям заинтересованных сторон, и может использоваться по назначению в предполагаемой среде эксплуатации.

H.11.1. Назначение безопасности

Предоставить объективные свидетельства того, что система, при использовании, удовлетворяет потребностям в защите, связанным с целями деятельностями или предназначения, и требованиям заинтересованных сторон, тем самым обеспечивая её целевое использование в намеченной среде эксплуатации доверенным и безопасным способом.

H.11.2. Результаты безопасности

- Определены критерии подтверждения соответствия безопасности.
- Подтверждена доступность сервисов безопасности, необходимых заинтересованным сторонам.
- Определены связанные с безопасностью ограничения подтверждения соответствия, влияющие на требования к системе, архитектуру или проект.
- Проверены аспекты безопасности системы, элемента системы или образца.
- Доступны системы или сервисы, отвечающие за аспекты безопасности при подтверждении соответствия.
- Выявлены результаты подтверждения соответствия и аномалии, ориентированные на безопасность.
- Представлены объективные свидетельства успешного подтверждения соответствия аспектов безопасности.
- Установлена прослеживаемость подтверждённых аспектов безопасности системы, элементов системы и образцов.

H.11.3. Работы и задачи безопасности

VA-1 ПОДГОТОВКА К ПОДТВЕРЖДЕНИЮ СООТВЕТСТВИЯ

VA-1.1 Определение аспектов безопасности в области подтверждения соответствия и соответствующих действий по подтверждению соответствия безопасности.

Примечание: Аспекты безопасности подтверждения соответствия сосредоточены на потребностях, интересах и связанных с ними требованиях безопасности заинтересованных сторон в защите. Эта область включает в себя элементы системы, всю систему или любой образец, который влияет на уверенность заинтересованных сторон в системе и решение принять систему как доверенную для ее предполагаемого использования.

VA-1.2 Определение ограничений, которые могут ограничить выполнимость действий по подтверждению соответствия безопасности.

Примечание: Ограничения могут включать в себя уровень доверия и доступность деятельности или предназначения заинтересованных сторон для поддержки работ по подтверждению соответствия; доступность достаточных, актуальных и достоверных данных об угрозах; ограничения на выполнение работ по подтверждению соответствия в реальных эксплуатационных условиях по всем режимам деятельности и предназначения и связанных с ними состояниях и режимах системы; применяемые технологии; размер и сложность элемента или образца системы; и стоимость и время, отведенные на работы по подтверждению соответствия.

VA-1.3 Выбор соответствующих методов подтверждения соответствия безопасности и соответствующих критериев успеха для каждого действия по подтверждению соответствия безопасности.

Примечание: Включает в себя эмуляцию неблагоприятных условий, включая проверку на проникновение и имитацию злоупотреблений и неправомерного использования.

VA-1.4 Разработка аспектов безопасности стратегии подтверждения соответствия.

Примечание: Аспекты безопасности стратегии подтверждения соответствия касаются подхода, предусматривающего включение соображений безопасности во все действия по подтверждению соответствия с учётом компромиссов между областью, глубиной и строгостью, необходимыми для достижения желаемого уровня доверия и заданными ограничениями.

VA-1.5 Определение для системы ограничений, связанных с безопасностью, которые вытекают из аспектов безопасности стратегии подтверждения соответствия, которые должны быть включены в потребности заинтересованных сторон в защите, и требования, преобразованные из этих потребностей.

Примечание: Эти ограничения связаны с четкостью и точностью выражения потребностей и требований для достижения желаемого уровня доверия с определенностью и повторяемостью.

VA-1.6 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки подтверждения соответствия.

VA-1.7 Определение и планирование вспомогательных систем или сервисов для поддержки аспектов безопасности подтверждения соответствия.

VA-1.8 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться для поддержки подтверждения соответствия.

Ссылки: [4] [30] [61] [86] [97] [98] [99] [100] [118]

VA-2 ВЫПОЛНЕНИЕ ПОДТВЕРЖДЕНИЯ СООТВЕТСТВИЯ

VA-2.1 Определение аспектов безопасности процедур подтверждения соответствия, каждая из которых поддерживает одно или набор действий по подтверждению соответствия.

Примечание: Это включает в себя определение методов или технологий подтверждения соответствия, которые будут использоваться, квалификации лиц, проводящих подтверждение соответствия, и любого специализированного оборудования, которое может потребоваться, для имитации неблагоприятных условий среды.

VA-2.2 Выполнение процедур подтверждения соответствия безопасности.

Примечание 1: Действия по подтверждению соответствия, ориентированные на безопасность, в ходе выполнения процедур подтверждения соответствия, способствуют демонстрации того, что система является достаточно доверенной.

Примечание 2: Выполнение действий по подтверждению соответствия, ориентированных на безопасность, включает фиксацию результата от выполнения процедуры, сравнения полученного результата с ожидаемым результатом, определения степени соответствия элемента и принятия решения о приемлемости соответствия, если остаётся неопределенность.

Ссылки: [4] [86] [97] [100] [118]

VA-3 УПРАВЛЕНИЕ РЕЗУЛЬТАТАМИ ПОДТВЕРЖДЕНИЯ СООТВЕТСТВИЯ

VA-3.1 Регистрация аспектов безопасности результатов подтверждения соответствия и всех обнаруженных аномалий.

Примечание: Регистрируемые результаты подтверждения соответствия включают аспекты несоответствия, аномалии или проблемы, потенциально связанные с безопасностью. Эти результаты служат основой для анализа, чтобы определить причины и выполнить корректирующие или улучшающие действия. Корректирующие действия могут влиять на аспекты безопасности определения архитектуры системы, проекта, требований к безопасности системы и связанных с ними ограничений, уровень доверия, который может быть получен, и/или стратегию реализации, включая ее аспекты безопасности.

VA-3.2 Регистрация характеристик безопасности эксплуатационных инцидентов и проблем и отслеживание их разрешения.

Примечание: Инциденты, возникающие в среде эксплуатации системы, регистрируются и впоследствии соотносятся с действиями и результатами подтверждения соответствия. Это важный контур обратной связи для непрерывного совершенствования разработки доверенных безопасных систем.

VA-3.3 Получение согласия на то, что критерии подтверждения соответствия безопасности соблюдены.

VA-3.4 Поддержание прослеживаемости аспектов безопасности подтверждения соответствия.

Примечание: Поддерживается двунаправленная прослеживаемость аспектов безопасности проверенных элементов системы с учетом потребностей заинтересованных сторон в защите, интересов безопасности и требований безопасности. Прослеживаемость демонстрирует полноту процесса подтверждения соответствия и предоставляет свидетельства, подтверждающие доверие и доверенность утверждений.

VA-3.5 Предоставление связанных с безопасностью образцов, выбранных в качестве базовых.

Ссылки: [4] [30] [61] [98] [99] [100]

H.12. Эксплуатация

Назначение процесса «*Эксплуатация*» заключается в использовании системы для предоставления сервисов.

H.12.1. Назначение безопасности

- Информировать об аспектах безопасности требований и ограничений для безопасной эксплуатации системы и отслеживать аспекты безопасности продуктов, сервисов и результативности эксплуатируемой системы.
- Выявление и анализ аномалий в эксплуатации, связанных с безопасностью.

H.12.2. Результаты безопасности

- Определены аспекты безопасности ограничений на эксплуатацию, влияющие на требования, архитектуру или проект системы.
- Доступны вспомогательные системы, сервисы и материалы для аспектов безопасности эксплуатации.
- Имеется обученный и квалифицированный персонал, способный безопасно эксплуатировать систему.
- Поставляются продукты или сервисы системы, отвечающие требованиям безопасности заинтересованных сторон.
- Отслеживаются аспекты безопасности функционирования системы в процессе эксплуатации.
- Заинтересованным сторонам оказывается поддержка в области безопасности.

H.12.3. Работы и задачи безопасности

OP-1 ПОДГОТОВКА К ЭКСПЛУАТАЦИИ

OP-1.1 Определение аспектов безопасности стратегии эксплуатации.

Примечание 1: Это включает в себя подход, позволяющий обеспечить непрерывную безопасную эксплуатацию и использование системы и ее сервисов безопасности, а также оказание поддержки компонентам эксплуатации по устранению аномалий, выявленных в ходе эксплуатации и использования системы. Это также включает:

- Рассмотрение возможностей, доступности, сроков, и безопасности продуктов или сервисов по мере их внедрения, регулярной эксплуатации и ликвидации (включая эксплуатацию в непредвиденных ситуациях).
- Кадровую стратегию и требования к квалификации персонала в области безопасности, включая все требования, относящиеся к обучению безопасности и соответствию персонала.
- Аспекты безопасности, касающиеся критериев обновления и пере-приёмки системы, а также календарных планов, позволяющих вносить изменения, которые поддерживают аспекты безопасности существующих или усовершенствованных продуктов или сервисов.
- Подход к реализации режимов эксплуатации в концепции эксплуатации системы, включая нормальную и аварийную работу.
- Безопасные подходы для непредвиденных, деградированных, альтернативных, учебных и других режимов работы, а также к переходам внутри режимов и между ними с учетом устойчивости в неблагоприятных условиях.
- Эксплуатационные меры, позволяющие получить представление об уровнях безопасности при функционировании.
- Подход к обеспечению ситуационной осведомлённости для определения последствий, имеющих отношение к безопасности.

Примечание 2: Это включает в себя планирование обеспечения безопасности при запуске системы, остановке системы, выключении системы, работе системы в режиме обучения, безопасную реализацию обходных процедур для восстановления работы, выполнение операций отката и восстановления, работу в некотором ухудшенном режиме или альтернативных режимах для особых условий. При необходимости оператор выполняет соответствующие действия для перевода в работу в непредвиденных условиях и, возможно, выключения питания системы. Работа в непредвиденных условиях выполняется в соответствии с заранее установленными процедурами для такого случая.

Примечание 3: Может возникнуть необходимость в планировании определенных режимов работы, для которых функции и сервисы безопасности сокращаются или исключаются для обеспечения более важных функций и сервисов системы или для выполнения определенного технического обслуживания или периодического тестирования. Должны использоваться заранее определенные процедуры для входа и выхода из таких режимов.

OP-1.2 Определение ограничений и целей, вытекающих из аспектов безопасности эксплуатации, которые должны быть включены в требования, архитектуру и проект системы.

OP-1.3 Определение аспектов безопасности вспомогательных систем и сервисов, необходимых для поддержки эксплуатации.

OP-1.4 Определение и планирование вспомогательных систем или сервисов, необходимых для поддержки аспектов безопасности эксплуатации.

OP-1.5 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться при эксплуатации.

OP-1.6 Выявление или определение требований к обучению и квалификации в области безопасности для поддержки персонала, необходимого для безопасной эксплуатации системы.

Примечание: Квалификация и обучение по безопасности включают в себя ролевую и функционально ориентированную компетентность, квалификацию, сертификацию и другие критерии для безопасной эксплуатации и использования системы во всех ее определенных режимах или состояниях.

OP-1.7 Назначение обученного и квалифицированного персонала, необходимого для безопасной эксплуатации системы.

Ссылки: [4] [86] [100] [111] [112] [113] [114]

OP-2 ОСУЩЕСТВЛЕНИЕ ЭКСПЛУАТАЦИИ

OP-2.1 Безопасное использование системы в намеченной среде эксплуатации.

OP-2.2 Применение материалов и других ресурсов, необходимых для безопасной эксплуатации системы и поддержания возможностей её продуктов и сервисов.

Примечание 1: Материалы и ресурсы предоставляются в рамках логистических мероприятий. Логистика рассматривается как часть процесса поддержки.

Примечание 2: Эксплуатирующий персонал может выполнять работы по модификации и поддержке системы, например, обновление программного обеспечения.

OP-2.3 Мониторинг эксплуатации системы на предмет отклонений от предполагаемого поведения и результатов.

Примечание: Это включает в себя: (1) управление соблюдением стратегии эксплуатации и эксплуатационных процедур (операций, проводимых персоналом), (2) мониторинг того, что система эксплуатируется безопасным способом и соответствует нормативным документам, процедурам и директивам, и (3) мониторинг аномалий, которые могут не быть непосредственно наблюдаемыми, таких как поведение системы, и могут быть или не быть явно связанными с безопасностью.

OP-2.4 Использование мер, определенных в стратегии, и их анализ для подтверждения того, что результативность системы безопасности находится в пределах допустимых параметров.

Примечание: Мониторинг системы включает в себя рассмотрение того, находится ли её результативность в пределах установленных пороговых значений безопасности (границ потерь), допустимы ли периодические инструментальные показания, а также приемлемо ли время обслуживания и реагирования. Отзывы и предложения операторов являются полезным вкладом в повышение аспектов безопасности эксплуатационных характеристик системы.

OP-2.5 Выявление и регистрация случаев, когда безопасность системы или результативность обслуживания не соответствуют допустимым параметрам.

Ссылки: [4] [30] [61] [86] [98] [99] [100]

OP-3 УПРАВЛЕНИЕ РЕЗУЛЬТАТАМИ ЭКСПЛУАТАЦИИ

OP-3.1 Регистрация результатов безопасных операций и любых обнаруженных аномалий.

Примечание: К аномалиям относятся те, которые связаны со стратегией эксплуатации, работой вспомогательных систем, осуществлением эксплуатации и неправильным определением системы, все из которых могут быть вызваны проблемами безопасности или могут привести к проблемам безопасности.

OP-3.2 Регистрация аспектов безопасности эксплуатационных инцидентов и проблем и отслеживание их разрешения.

OP-3.3 Поддержание прослеживаемости аспектов безопасности элементов эксплуатации.

OP-3.4 Предоставление связанных с безопасностью образцов, выбранные в качестве базовых.

Ссылки: [4] [30] [61] [98] [99] [100]

OP-4 ЗАИНТЕРЕСОВАННЫЕ СТОРОНЫ ПОДДЕРЖКИ

OP-4.1 Оказание помощи в вопросах безопасности и консультаций заинтересованным сторонам если требуется.

Примечание: Помощь и консультации включают предоставление или рекомендации по источникам для обучения по вопросам безопасности, аспектам безопасности документации, устранению уязвимостей, информированию по проблемам безопасности и другие услуги поддержки, которые позволяют эффективно и безопасно использовать продукт или сервис.

OP-4.2 Регистрация и отслеживание запросов и последующие действия для поддержки безопасности.

OP-4.3 Определение степени, в которой аспекты безопасности поставляемых продуктов и сервисов удовлетворяют потребности заинтересованных сторон.

Ссылки: [4] [86] [100]

H.13. Поддержка

Назначением процесса «*Поддержка*» является поддержание способности системы предоставлять продукт или услугу.

H.13.1. Назначение безопасности

- Установление аспектов безопасности требований и ограничений для безопасного поддержания способности системы предоставлять продукт или услугу.

  Примечание: Безопасная поддержка включает в себя все мероприятия по поддержке и логистике, связанные с упаковкой, обработкой, хранением и транспортировкой заменяемых элементов системы.

H.13.2. Результаты безопасности

- Определены аспекты безопасности ограничений поддержки и логистики, влияющие на требования, архитектуру или проект системы.
- Доступны вспомогательные системы или сервисы, необходимые для обеспечения безопасных аспектов поддержки и логистики системы.
- Обеспечен безопасный доступ к заменяемым, отремонтированным или модифицированным элементам системы.
- Сообщено о необходимости принятия необходимых мер по поддержке и логистике, связанных с безопасностью.
- Определены связанные с безопасностью отказы и данные жизненного цикла, включая сопутствующие затраты.

H.13.3. Работы и задачи безопасности

MA-1 ПОДГОТОВКА К ПОДДЕРЖКЕ И ЛОГИСТИКЕ

MA-1.1 Определение аспектов безопасности стратегии поддержки.

Примечание: Стратегия поддержки направлена на сохранение безопасных возможностей и результативности поставляемой системы. Аспекты безопасности стратегии поддержки, как правило, включают:

- Безопасный переход системы и элементов системы в режим или состояние безопасной поддержки, а также безопасный возврат к эксплуатации.

- Подход, гарантирующий, что в систему не будут внедрены материалы и элементы системы, которые не соответствуют установленному качеству, происхождению и функциональности (например, контрафактные).
- Уровень квалификации и персонала, необходимый для проведения ремонта, замены и восстановления, с учетом требований к персоналу поддержки и любого соответствующего законодательства, касающегося здоровья, охраны труда, безопасности и окружающей среды.
- Меры по поддержке, которые обеспечивают понимание аспектов безопасности уровней результативности, эффективности и производительности.

MA-1.2 Определение аспектов безопасности логистической стратегии.

Примечание: Логистическая стратегия определяет конкретные соображения безопасности, необходимые для выполнения логистики на протяжении всего жизненного цикла. Это, как правило, включает в себя:

- Логистику приобретений, которая помогает обеспечить учет последствий для безопасности на ранней стадии разработки.
- Эксплуатационную логистику, помогающую гарантировать, что необходимые материалы и ресурсы будут безопасно предоставлены в надлежащем количестве и качестве и в нужном месте и времени; соображения по безопасному предоставлению материалов и ресурсов, включают идентификацию и маркировку, упаковку, распространение, обработку и выделение ресурсов.
- Критерии безопасности для мест хранения и условий хранения, а также число и тип сменных элементов безопасности системы, ожидаемый частота их замены, срок хранения и периодичность обновления.

MA-1.3 Определение связанных с безопасностью ограничений и целей, вытекающих из аспектов безопасности поддержки и логистики, которые должны быть включены в системные требования, архитектуру и проект.

MA-1.4 Определение компромиссов таким образом, чтобы аспекты безопасности системы и связанные с ними действия по поддержке и логистике привели к решению, которое является доверенным, безопасным, доступным, работоспособным, поддерживаемым и устойчивым.

Примечание: Стоимость безопасной поддержки и логистики должна учитываться в рамках стоимости срока службы системы.

MA-1.5 Определение аспектов безопасности для вспомогательных систем, продуктов и сервисов, необходимых для сопровождения поддержки и логистики.

MA-1.6 Определение и планирование вспомогательных систем, продуктов и сервисов, необходимых для обеспечения аспектов безопасности поддержки и логистики.

MA-1.7 Получение или получение доступа к аспектам безопасности вспомогательных систем, продуктов и сервисов, используемых в поддержке и логистике.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113] [114] [115]

MA-2 ВЫПОЛНЕНИЕ ПОДДЕРЖКИ

Примечание: необходимость выполнения поддержки может быть обусловлена необходимостью устранения явных проблем безопасности, инцидентов или отказов. Все действия по поддержке должны выполняться безопасным способом при понимании того, что некоторые действия могут оказывать непосредственное влияние на уровень безопасности системы.

MA-2.1 Мониторинг и пересмотр требований заинтересованных сторон, а также отчетов о инцидентах и проблемах для определения связанных с безопасностью корректирующих, профилактических, адаптивных, аддитивных или совершенных потребностей в поддержке.

Примечание: К потребностям в поддержке, связанным с безопасностью, относятся те, которые являются прямыми (например, выявленный инцидент с безопасностью) или косвенными (например, соображения по безопасному решению проблем в поддержке) потребностями.

MA-2.2 Регистрация аспектов безопасности инцидентов и проблем поддержки и отслеживание их безопасного разрешения.

MA-2.3 Анализ влияния изменений, вносимых действиями по поддержке на аспекты безопасности системы и элементов системы.

MA-2.4 Безопасное восстановление системы до безопасного рабочего состояния при возникновении неисправностей, приводящих к отказу системы.

Примечание: Безопасное восстановление означает, что само действие поддержки не ухудшает безопасный статус или состояние системы.

MA-2.5 Безопасное устранение аномалий (например, дефектов, ошибок и неисправностей) и замена или обновление элементов системы.

MA-2.6 Проведение профилактической поддержки путем безопасной замены или обслуживания элементов системы до отказа.

MA-2.7 Безопасное выполнение адаптивной, аддитивной или перфективной поддержки при необходимости**.**

Ссылки: [4] [30] [61] [86] [98] [99] [100] [114] [115]

MA-3 ОСУЩЕСТВЛЕНИЕ ЛОГИСТИЧЕСКОГО СОПРОВОЖДЕНИЯ

MA-3.1 Выполнение аспектов безопасности логистики приобретений.

MA-3.2 Выполнение аспектов безопасности эксплуатационной логистики.

MA-3.3 Реализация механизмов безопасной логистики, необходимых в течение жизненного цикла.

Примечание 1: Эти механизмы обеспечивают безопасную упаковку, обработку, хранение и транспортировку.

Примечание 2: Эти механизмы помогают в предотвращении и обнаружении подделки, фальсификации, замены и перенаправления.

MA-3.4 Подтверждение того, что аспекты безопасности логистических действий реализованы.

Примечание: Аспекты безопасности логистических действий удовлетворяют как интересам защиты логистики, так и необходимости соблюдения норм ремонта, уровней пополнения и плановых календарных планов.

Ссылки: [4] [30] [61] [98] [99] [100] [111] [112] [113] [114] [115]

MA-4 УПРАВЛЕНИЕ РЕЗУЛЬТАТАМИ ПОДДЕРЖКИ И ЛОГИСТИКИ

MA 4.1 Фиксация аспектов безопасности результатов поддержки и логистики, а также всех встречающихся аномалий.

MA-4.2 Регистрация инцидентов и проблем, связанных с безопасностью поддержки и логистики, и отслеживание их безопасного разрешения.

MA-4.3 Выявление и регистрация связанных с безопасностью тенденций инцидентов, проблем, а также действий по поддержке и логистике.

MA-4.4 Поддержание прослеживаемости аспектов безопасности поддержки и логистики.

MA-4.5 Предоставление связанных с безопасностью образцов, выбранные в качестве базовых.

MA-4.6 Мониторинг удовлетворенности клиентов аспектами безопасности системы, поддержки и логистики.

Ссылки: [4] [30] [61] [98] [99] [100] [114] [115] [116]

H.14. Ликвидация

Назначением процесса «*Ликвидация*» является завершение существования элемента системы или системы для конкретного целевого использования, надлежащее обращение с замененными или ликвидированными элементами и любыми отходами и надлежащее удовлетворение выявленных критических потребностей в ликвидации (например, в соответствии с соглашением, политикой организации или в отношении экологических, юридических аспектов, аспектов безопасности или защиты).

H.14.1. Назначение безопасности

- Обеспечение аспектов, необходимые для безопасного завершения существования элемента системы или системы для определенного использования, а также для безопасного сохранения или уничтожения связанных данных и информации.

H.14.2. Результаты безопасности

- Определены ограничения безопасной ликвидации, влияющие на системные требования, архитектуру, проект и реализацию.
- Доступны вспомогательные системы или сервисы для обеспечения безопасности ликвидации.
- Элементы системы уничтожены, хранятся, восстановлены или утилизированы в соответствии с требованиями безопасности.
- Среда надежно возвращена в исходное безопасное или согласованное безопасное состояние.
- Предоставлены отчёты по аспектам безопасности действий по утилизации и анализу.

H.14.3. Работы и задачи безопасности

DS-1 ПОДГОТОВКА К ЛИКВИДАЦИИ

DS-1.1 Определение аспектов стратегии ликвидации, связанных с обеспечением безопасности.

Примечание: Аспекты безопасности касаются безопасного завершения функций и сервисов системы, преобразования системы и среды в приемлемое безопасное состояние, решения проблем безопасности и передачи системы и элементов системы для будущего использования. Стратегия ликвидации определяет подходы, календарные планы, ресурсы, конкретные соображения безопасной ликвидации, а также эффективность и полноту действий по безопасной ликвидации и отчуждению.

- *Перманентное завершение функционирования системы и предоставления сервисов:* Аспекты безопасности касаются удаления, вывода из эксплуатации или уничтожения связанных с ними элементов системы при сохранении состояния безопасности любых оставшихся функций и сервисов.
- *Преобразование системы и среды в приемлемое состояние:* Аспекты безопасности касаются любых изменений, вносимых в систему, ее применение и среду, для обеспечения того, чтобы удовлетворить потребности и проблемы заинтересованных сторон в защите с помощью оставшихся частей системы и предоставляемых ею функций и сервисов. Когда вся система ликвидирована, аспекты безопасности касаются изменений в окружающей среде, чтобы вернуть ее в исходное или согласованное безопасное состояние.
- *Устранение проблем безопасности материалов, данных и информации:* Аспекты безопасности касаются защиты чувствительных компонентов, технологий, данных и информации, выведенных из использования, демонтированных, сохраненных, подготовленных к повторному использованию или уничтоженных. Эти аспекты могут включать в себя продолжительность уровня/состояния защиты, понижения уровня, возможность высвобождения и критерии, определяющие санкционированный доступ и использование в течение периода хранения. Потребности в защите при ликвидации определяются заинтересованными сторонами и соглашениями и могут регулироваться нормативными требованиями, ожиданиями и ограничениями.
- *Перевод системы и элементов системы для будущего использования:* Аспекты безопасности касаются перевода системы или элементов системы для будущего использования в измененной или адаптированной форме, включая перенос и возврат к эксплуатации. Аспекты безопасности могут включать в себя ограничения, пределы или другие критерии, позволяющие восстановить функции и сервисы систем в течение определенного времени или обеспечить ориентированную на безопасность совместимость с будущими вспомогательными системами и другими системами. Эти аспекты могут также включать периодические инспекции для учета состояния безопасности и готовности к возврату в эксплуатацию элементов хранимой системы, соответствующих данных и информации, а также всех материалов, поддерживающих эксплуатацию и работоспособность. Аспекты безопасности относятся ко всем функциям и сервисам системы и не ограничиваются только безопасностью функций и сервисов системы, ориентированных на защиту.

DS-1.2 Определение связанных с безопасностью ограничений и целей ликвидации, в зависимости от системных требований, архитектуры и конструктивных особенностей, а также методов реализации.

DS-1.3 Определение аспектов безопасности для вспомогательных систем или сервисов, необходимых для поддержки ликвидации.

DS-1.4 Определение и планирование обеспечивающих систем или сервисов, необходимых для поддержки аспектов безопасности, связанных с ликвидацией.

DS-1.5 Получение или приобретение доступа к аспектам безопасности вспомогательных систем или сервисов, которые будут использоваться при ликвидации.

DS-1.6 Спецификация критериев безопасности для защитного оборудования, мест хранения, проверок и сроков хранения (если система должна храниться).

DS-1.7 Определение аспектов безопасности превентивных методов для предотвращения повторного поступления в цепочку поставок ликвидированных элементов и материалов, которые не подлежат перепрофилированию, восстановлению или повторному использованию.

Ссылки: [4] [86] [100]

DS-2 ВЫПОЛНИЕ ЛИКВИДАЦИИ

DS-2.1 Безопасная деактивация системы или элемента системы, чтобы подготовить их к безопасному выводу из эксплуатации.

Примечание: Деактивация выполняется для сохранения безопасного состояния системы.

DS-2.2 Безопасное удаление системы, элемента системы или отходов из использования или производства для надлежащей безопасной ликвидации и принятия соответствующих мер.

DS-2.3 Безопасный перевод операционного персонала системы или элемента системы, попадающих под ликвидацию, и фиксация соответствующих знаний о безопасной эксплуатации.

DS-2.4 Безопасный демонтаж системы или элемента системы в управляемые элементы, для облегчения их безопасного извлечения для повторного использования, переработки, восстановления, ремонта, архивирования или уничтожения.

Примечание: Безопасный демонтаж сохраняет характеристики безопасности элементов системы, которые не удаляются.

DS-2.5 Безопасная обработка элементов системы и их частей, не предназначенных для повторного использования, таким образом, чтобы они не попадали обратно в цепочку поставок.

DS-2.6 Проведение безопасной очистки и уничтожения элементов системы и образцов жизненного цикла.

Примечание 1: Регулирующие соглашения, законы и нормативные документы определяют соответствующие средства для очистки и уничтожения данных, информации и элементов системы, которые содержат данные и информацию, а также сроки хранения до начала очистки и уничтожения.

Примечание 2: Методы очистки и уничтожения включают удаление, криптографическое стирание, физическую модификацию и физическое разрушение.

Примечание 3: Методы и технологии очистки и разрушения могут быть специфичными для данных, информации и типов элементов системы.

Ссылки: [4] [86] [100]

DS-3 ЗАВЕРШЕНИЕ ЛИКВИДАЦИИ

DS-3.1 Убеждение в том, что после утилизации не существует факторов безопасности, наносящих ущерб.

DS-3.2 Возврат среды в исходное безопасное состояние или в безопасное состояние, указанное в соглашении.

DS-3.3 Безопасная архивация данные и информации, собранных в течение всего срока службы системы, для проведения аудитов и проверок в случае долгосрочных угроз здоровью, безопасности и окружающей среде, а также для того, чтобы будущие создатели и пользователи системы могли безопасно создавать базу знаний на основе прошлого опыта.

DS-3.4 Предоставление связанных с безопасностью образцов, выбранные в качестве базовых.

Ссылки: [4] [100]

Приложение I. Процессы технического управления

Это приложение содержит *процессы технического управления* из [4] с учетом соображений безопасности и вклада в назначение, результаты, работы и задачи.

I.1. Планирование проекта

Назначением процесса *«Планирование проекта»* является разработка и координация эффективных и осуществимых планов.

I.1.1. Назначение безопасности

- Определение и координация аспектов безопасности эффективных и осуществимых планов.

I.1.2. Результаты безопасности

- Определены цели безопасности, планы, относящиеся к безопасности, и аспекты безопасности других планов.
- Определены релевантные для безопасности роли, обязанности, подотчётность и полномочия в рамках проекта.
- Определены аспекты безопасности для критериев результативности и технических достижений.
- Выделены ресурсы и сервисы, необходимые для достижения целей в области безопасности.
- Активированы планы выполнения аспектов проекта, связанных с безопасностью.

I.1.3. Работы и задачи безопасности

PL-1 ОПРЕДЕЛЕНИЕ ПРОЕКТА

PL-1.1 Определение аспектов безопасности целей и ограничений проекта.

Примечание: Цели и ограничения включают стратегические цели безопасности, доверие и доверенность, а также пороговые значения потерь и нормативные требования. Каждая цель, связанная с безопасностью, определяется с таким уровнем детализации, который позволяет выбирать, адаптировать и осуществлять соответствующие процессы и действия.

PL-1.2 Определение аспектов безопасности в области проекта в соответствии с соглашениями.

Примечание: Это включает в себя соответствующие действия, необходимые для удовлетворения аспектов безопасности критериев принятия решений и успешного завершения проекта.

PL-1.3 Определение и поддержка представлений безопасности модели жизненного цикла проекта, которая состоит из этапов, с использованием установленных моделей жизненного цикла организации.

PL-1.4 Установление соответствующих аспектов безопасности в структуре разбивки работ.

Примечание: Каждый элемент разбиения структуры работы, имеющий отношение к безопасности, описывается с уровнем детализации, который соответствует выявленным рискам безопасности и требуемой наглядности.

PL-1.5 Определение и поддержка аспектов безопасности процессов, которые будут применяться к проекту.

Примечание: Критерии включения, входные данные, ограничения последовательности процессов, а также атрибуты показателей эффективности и/или показателей результативности могут иметь аспекты безопасности.

Ссылки: [4] [30] [61] [86] [96] [98] [99] [100] [111] [112] [113] [123]

PL-2 ПЛАНИРОВАНИЕ ПРОЕКТА И ТЕХНИЧЕСКОЕ УПРАВЛЕНИЕ

PL-2.1 Определение и поддержание аспектов безопасности календарного плана проекта на основе управленческих и технических целей, а также сметы работ.

Примечание: Это включает аспекты безопасности, влияющие на определение продолжительности, взаимосвязей, зависимостей и последовательности работ; вехи результатов; используемые ресурсы; рассмотрения (включая привлечение специалистов по вопросам безопасности); и календарный план резервов для управления рисками в области безопасности, необходимых для своевременного завершения проекта.

PL-2.2 Определение аспектов безопасности критериев достижения результатов для этапов принятия решений жизненного цикла, сроков поставки и основных зависимостей от внешних входных и выходных данных.

Примечание: Сюда входят критерии, определенные нормативными, сертификационными, оценочными и прочими органами.

PL-2.3 Определение аспектов безопасности критериев эффективности проекта.

PL-2.4 Определение затрат проекта, связанных с безопасностью, и планирование бюджета.

PL-2.5 Определение ролей, обязанностей, подотчётности и полномочий, связанных с безопасностью.

Примечание: Это включает определение организации проекта, подбор персонала и повышение квалификации персонала в области безопасности. Полномочия, в зависимости от обстоятельств, включают в себя юридически ответственные должности и отдельных лиц. Эти полномочия, относящиеся к безопасности, включают в себя санкционирование проекта безопасности, проверку безопасности и разрешение на эксплуатацию, а также сертификацию, аккредитацию или санкционирование.

PL-2.6 Определение аспектов безопасности необходимой инфраструктуры и сервисов.

Примечание: Это включает определение возможностей, необходимых для инфраструктуры и сервисов безопасности, их доступности и распределения по задачам проекта. Инфраструктура безопасности включает в себя объекты (например, чувствительные разделенные информационные объекты (SCIF) и изолированные сети), специфическую стойкость механизмов, обеспечивающих доступ, междоменные решения, инструменты, средства связи и информационные технологии.

PL-2.7 Планирование аспектов безопасности при приобретении материалов и предоставляемых системных сервисов, поставляемых вне проекта.

PL-2.8 Разработка и распространение плана по аспектам безопасности проекта и технического управления и реализации, включая рассмотрения безопасности, учитывающие соображения безопасности.

Примечание: Соображения безопасности и планирование учёта этих соображений отражаются в «Плане управления системным проектированием», «Планах управления проектированием программным обеспечения» и аналогичных планах.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

PL-3 ЗАПУСК ПРОЕКТА

PL-3.1 Получение санкционирования по аспектам безопасности проекта.

PL-3.2 Отправка запросов и получение подтверждений в отношении необходимых ресурсов для выполнения аспектов безопасности проекта.

PL-3.3 Реализация аспектов безопасности планов проекта.

Ссылки: [4] [86] [100]

I.2. Оценка и контроль проекта

Назначение процесса «Оценка и контроль проекта» заключается в оценке того, являются ли планы согласованными и осуществимыми; определении статуса проекта, технического и технологического процесса; и непосредственное исполнение для обеспечения того, чтобы результаты работы соответствовали прогнозируемым бюджетам в соответствии с планами и календарными планами для достижения технических целей.

I.2.1. Назначение безопасности

- Оценка согласованности и осуществимости аспектов безопасности планов и планов обеспечения безопасности.
- Определение состояния проекта, технических характеристик и результативности процесса обеспечения безопасности.
- Непосредственное выполнение для обеспечения того, чтобы показатели безопасности находились в пределах прогнозируемых бюджетов в соответствии с планами и календарными планами для достижения целей безопасности и других технических целей.

I.2.2. Результаты безопасности

- Определены аспекты безопасности показателей эффективности или результатов оценки.
- Роли, обязанности, подотчетность, полномочия и ресурсы, относящиеся к безопасности, оценены на предмет их адекватности.
- Выполняется рассмотрение технического прогресса по аспектам безопасности.
- Анализируются отклонения в аспектах безопасности выполнения проекта от планов.
- Соответствующие заинтересованные стороны информируются об аспектах безопасности, связанных со статусом проекта.
- В тех случаях, когда результаты или реализация проекта не соответствуют целям безопасности принимаются корректирующие действия.
- При необходимости инициируются аспекты безопасности перепланирования проекта.
- Санкционируются аспекты безопасности действий по проекту, связанные с переходом (или нет) от одной запланированной вехи или события к следующим.

I.2.3. Работы и задачи безопасности

PA-1 ПЛАН ОЦЕНКИ И КОНТРОЛЯ ПРОЕКТА

PA-1.1 Определение аспектов безопасности стратегии оценки и контроля проекта.

Примечание 1: Сюда входят планируемые методы и временные рамки оценки безопасности, а также необходимые рассмотрения по управлению безопасностью и техническим аспектам.

Примечание 2: Аспекты безопасности стратегии оценки и контроля проекта определяются ожиданиями регуляторных, сертификационных и санкционирующих органов.

Ссылки: [4] [30] [61] [98] [99] [100]

PA-2 ОЦЕНКА ПРОЕКТА

PA-2.1 Оценка соответствия аспектов безопасности целей и планов проекта контексту проекта.

PA-2.2 Оценка аспектов безопасности управленческих и технических планов поставленным целям для определения их адекватности и осуществимости.

PA-2.3 Оценка аспектов безопасности проекта и технического состояния на соответствие планам для определения отклонений в фактических и прогнозируемых затратах, календарном плане и результативности.

PA-2.4 Оценка адекватности ролей, обязанностей, подотчётности и полномочий, связанных с безопасностью.

Примечание: Это включает оценку достаточности компетенций персонала для осуществления проектных ролей и выполнения задач проекта.

PA-2.5 Оценка аспектов безопасности, связанных с достаточностью и доступностью ресурсов.

PA-2.6 Оценка прогресса с использованием измеренных достижений в области безопасности и аспектов безопасности, связанных с завершением этапов.

Примечание: Это включает сбор и оценка связанных с безопасностью данных о трудовых ресурсах, материалах, затратах на обслуживание и технических показателях, а также других технических данных о целях безопасности. Эти показатели сопоставляются с показателями достижения результатов в области безопасности, включая проведение оценок эффективности для определения адекватности формирующейся системы для выполнения требований безопасности.

PA-2.7 Проведение необходимых управленческих и технических рассмотрений, аудитов и инспекций, связанных с аспектами безопасности проекта.

Примечание: Пересмотры, аудиты и инспекции являются официальными или неофициальными и проводятся для определения готовности к переходу на следующий этап или к выполнению следующего контрольного показателя с точки зрения безопасности, для обеспечения достижения целей проекта и технических целей в области безопасности, а также для получения обратной связи от заинтересованных сторон, имеющих отношение к безопасности.

PA-2.8 Монитор аспектов безопасности критически важных процессов и новых технологий.

Примечание: Это включает *в* себя определение и оценку зрелости технологий с точки зрения безопасности, а также возможность внедрения технологий для достижения целей безопасности.

PA-2.9 Подготовка рекомендаций на основе результатов измерения уровня безопасности и другой информации о проекте, имеющей отношение к безопасности.

Примечание: Результаты измерений анализируются для выявления отклонений, вариаций или нежелательных тенденций, связанных с безопасностью, от плановых значений, и для выработки рекомендаций по корректирующим, профилактическим, адаптивным, дополняющим или улучшающим действиям, связанным с безопасностью.

PA-2.10 Регистрация и предоставление информации о состоянии безопасности и результатах оценки.

PA-2.11 Мониторинг аспектов безопасности выполнения процессов в рамках проекта.

Примечание: Это включает *в* себя анализ мер по обеспечению безопасности процессов и рассмотрение тенденций, связанных с безопасностью, в отношении целей проекта.

Ссылки: [4] [30] [61] [86] [98] [99] [100]

PA-3 КОНТРОЛЬ ЗА ПРОЕКТОМ

PA-3.1 Инициирование действий, необходимых для решения выявленных проблем безопасности.

PA-3.2 Инициирование необходимых аспектов безопасности при перепланировании проекта.

Примечание: Перепланирование инициируется при изменении аспектов безопасности целей или ограничений проекта, или при обнаружении недопустимых допущений планирования, относящихся к безопасности.

PA-3.3 Инициирование необходимых действий по внесению изменений, когда по контракту происходят изменения в стоимости, сроках или качестве из-за влияния на безопасность требований покупателя или поставщика.

Примечание: Влияние на безопасность не всегда очевидно, когда запрос не связан с безопасностью или не ориентирован на безопасность.

PA-3.4 Выдача рекомендаций, по переходу проекта к следующему этапу или событию, если это оправдано, на основе достижения важных для безопасности вех или критериев события.

Ссылки: [4] [86] [100] [111] [112] [113]

I.3. Управление принятием решений

Назначение процесса «*Управление принятием решений*» состоит в том, чтобы обеспечить структурированную аналитическую основу для объективного выявления, характеристики и оценки набора альтернатив для принятия решения в любой момент жизненного цикла и выбора наиболее выгодного курса действий.

I.3.1. Назначение безопасности

- Определение, анализ, характеристика и оценка аспектов безопасности альтернативных решений.
- Рекомендация наиболее выгодного курса действий с учетом требований безопасности.

I.3.2. Результаты безопасности

- Определены аспекты безопасности решений, требующих альтернативного анализа.
- Определены и оценены аспекты безопасности альтернативных вариантов действий.
- Выбран предпочтительный вариант действий с учетом требований безопасности.
- Определены аспекты безопасности решения проблем, обоснования решений и допущений.

I.3.3. Работы и задачи по безопасности

DM-1 ПОДГОТОВКА К ПРИНЯТИЮ РЕШЕНИЙ

DM-1.1 Определение аспектов безопасности стратегии управления принятием решений.

Примечание: Стратегия управления принятием решений включает определение ролей, обязанностей, подотчетности и полномочий, связанных с безопасностью. Она также включает определение конкретных категорий решений по вопросам безопасности и схему назначения приоритетов. Решения, касающиеся безопасности, часто принимаются в результате оценки эффективности безопасности, технического компромисса, проблемы безопасности, которую необходимо решить, реакции на риск безопасности, который превышает приемлемый порог, или новой возможности.

DM-1.2 Определение аспектов безопасности обстоятельств и необходимости принятия решения.

DM-1.3 Определение заинтересованных сторон, обладающих соответствующими экспертными знаниями в области безопасности, для поддержки усилий по принятию решений.

Ссылки: [4] [86] [100]

DM-2 АНАЛИЗ ИНФОРМАЦИИ О ПРИНЯТИИ РЕШЕНИЯ

DM-2.1 Выбор и декларирование аспектов безопасности стратегии управления решениями для каждого решения.

Примечание: Это включает уровень строгости, необходимый для обеспечения безопасности, а также необходимый анализ данных и системы.

DM-2.2 Определение желаемое значение результатов безопасности и измеримых атрибутов безопасности критериев выбора.

Примечание: Определяется желаемое значение для всех поддающихся количественной оценке критериев безопасности и пороговые значения, при превышении которых атрибут будет неудовлетворительным.

DM-2.3 Определение аспектов безопасности пространства компромиссов и альтернативных вариантов.

Примечание: Если существует много альтернатив, аспекты безопасности должны быть качественно проверены, чтобы уменьшить альтернативы управляемому числу для дальнейшего подробного системного анализа.

DM-2.4 Оценка каждой альтернативы по критериям безопасности.

Ссылки: [4] [86] [100]

DM-3 ПРИНЯТИЕ РЕШЕНИЙ И УПРАВЛЕНИЕ ИМИ

DM-3.1 Определение предпочтительной альтернативы для каждого решения, связанного с безопасностью и основанного на безопасности.

DM-3.2 Регистрация связанных с безопасностью и базирующихся на безопасности решений, обоснований решения и допущений.

DM-3.3 Регистрация, отслеживание, оценка и информирование об аспектах безопасности решений, связанных с безопасностью и основанных на безопасности.

Примечание: Аспекты безопасности проблем или возможностей и альтернативные варианты действий, которые позволят устранить их последствия, включая те, которые имеют последствия для безопасности, регистрируются, классифицируются и сообщаются.

Ссылки: [4] [86] [100]

I.4. Управление рисками

Назначением процесса «*Управление рисками*» является постоянное выявление, анализ, устранение и мониторинг рисков.

I.4.1. Назначение безопасности

- Постоянное выявление, анализ, устранение и мониторинг рисков, связанных с неопределенностью достижения целей безопасности, а также влияния мер по обеспечению безопасности на достижение целей системы.

I.4.2. Результаты безопасности

- Выявлены риски, связанные с безопасностью.
- Проведен анализ рисков, связанных с безопасностью.
- Выбраны способы обработки рисков, относящиеся к безопасности.
- Применены меры по устранению рисков, связанных с безопасностью.
- Риски, связанные с безопасностью, оцениваются на постоянной основе для оценки изменений в статусе и прогрессе устранения.
- Риски, связанные с безопасностью, регистрируются и сохраняются в профиле рисков.

I.4.3. Работы и задачи безопасности

RM-1 ПЛАНИРОВАНИЕ УПРАВЛЕНИЯ РИСКАМИ

RM-1.1 Определение аспектов безопасности стратегии управления рисками.

Примечание 1: Сущность риска безопасности включает в себя преднамеренные и непреднамеренные случайные события, рассмотрения предполагаемого поведения и результатов, функций (безопасности и других функций) и потенциальных последствий реализации риска безопасности. Случайными событиями могут быть комбинации событий в среде эксплуатации и событий в системной среде.

Примечание 2: Определяются аспекты безопасности процесса управления рисками, подход к управлению рисками, критерии рисков, меры, параметры, шкала оценок и альтернативы устранения. Это включает в себя аспекты безопасности процесса управления рисками на всех уровнях цепочки поставок (например, поставщики, субподрядчики) и способы их включения в процесс управления рисками по проекту.

Примечание 3: Стратегия может включать проблемы безопасности (т.е. риски с вероятностью возникновения равной 1) и возможности (т.е. риски с положительными результатами) в рамках области и подхода. Аспекты возможностей включают критерии возможностей, показатели, параметры, шкалу оценок и альтернативы устранения.

RM-1.2 Определение и регистрация контекста безопасности процесса управления рисками.

Примечание 1: Это включает в себя определение заинтересованных сторон, имеющих отношение к безопасности, и описание их точек зрения, категорий рисков, а также технических и управленческих целей, предположений и ограничений.

Примечание 2: Возможности обеспечения безопасности обеспечивают потенциальные выгоды для системы или проекта. В контексте безопасности учитываются воздействия на безопасность, заключающиеся в том, что такая возможность не предоставляется, и риск безопасности того, что такая возможность не обеспечивает результатов.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [124] [125]

RM-2 УПРАВЛЕНИЕ ПРОФИЛЕМ РИСКОВ

RM-2.1 Определение и регистрация пороговых значений и условий рисков безопасности.

Примечание: Пороговые значения рисков безопасности определяют уровни, на которых рассматриваются соответствующие стратегии устранения.

RM-2.2 Формирование и ведение аспектов безопасности профиля рисков.

Примечание: В профиле риска регистрируются каждый риск безопасности и возможность, включая описание риска безопасности или возможности, регистрация параметров риска или возможности, приоритет, основанный на критериях риска или возможности, а также текущее состояние риска или возможности, их устранение и стратегия на случай непредвиденных обстоятельств. Профиль риска обновляется при изменении состояния отдельного риска безопасности или возможности.

RM-2.3 Предоставление заинтересованным сторонам аспектов безопасности соответствующего профиля рисков.

Примечание: Периодичность представления профиля рисков и его аспектов безопасности определяется в плане проекта.

Ссылки: [4] [86] [100] [124] [125]

RM-3 АНАЛИЗ РИСКОВ

RM-3.1 Определение рисков безопасности в категориях, описанных в контексте управления рисками.

Примечание: Риски безопасности обычно выявляются с помощью различных видов анализа безопасности и других видов анализа (например, анализ безопасности, доверия, результативности и эффективности); оценок технологии, архитектуры, интеграции и готовности; отчетов об измерениях; и исследований компромиссов. Кроме того, риски безопасности часто выявляются с помощью анализа мер, связанных с целями безопасности системы (например, показателей эффективности или показателей результативности, относящихся к безопасности).

RM-3.2 Измерение каждого выявленного риска безопасности.

RM-3.3 Оценка каждого риск безопасности в соответствии с пороговыми значениями риска.

RM-3.4 Определение и регистрация рекомендуемых стратегий и мер устранения для каждого риска, связанного с безопасностью, который превышает пороговое значение риска.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [124] [125]

RM-4 ОТНОШЕНИЕ К РИСКАМ, ПРЕВЫШАЮЩИМ ПОРОГ РИСКА

RM-4.1 Определение рекомендуемых альтернатив для обработки рисков безопасности.

RM-4.2 Определение мер для установления эффективности устранения рисков безопасности.

RM-4.3 Внедрение выбранных методов устранения рисков безопасности.

Примечание: Реализованная альтернатива должна быть такой, для которой заинтересованные стороны, имеющие отношение к вопросам безопасности, считают, что принятые меры сделают риск, связанный с безопасностью, приемлемым.

RM-4.4 Координация действий по управлению для выбранных способов устранения рисков безопасности.

Ссылки: [4] [86] [100] [124] [125]

RM-5 МОНИТОРИНГ РИСКОВ

RM-5.1 Постоянный мониторинг всех рисков, связанных с безопасностью, и контекста управления рисками безопасности.

Примечание: Изменения в рисках, связанных с безопасностью, и способах их устранения могут привести к переоценке. Первоначальные планы устранения для рисков, связанных с безопасностью, могут включать предварительно спланированные дополнительные действия, когда риск возрастает или недостаточно снижается, несмотря на попытки устранения.

RM-5.2 Реализация и мониторинг мер по оценке эффективности обработки рисков, связанных с безопасностью.

RM-5.3 Постоянный мониторинг появления новых рисков, связанных с безопасностью, и источников рисков на протяжении всего жизненного цикла.

Примечание: Это включает в себя мониторинг известных изменений в неблагоприятных факторах.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [124] [125]

I.5. Управление конфигурацией

Назначением процесса «*Управление конфигурацией*» является управление системой, элементами системы и конфигурациями в течение всего жизненного цикла.

I.5.1. Назначение безопасности

- Включение соображений безопасности в безопасное управление системой, элементами системы и конфигурациями в течение всего жизненного цикла.

I.5.2. Результаты безопасности

- Конфигурации элементов системы управляются безопасно.
- Установлены аспекты безопасности базовых значений конфигурации.
- Изменения в элементах, находящихся под управлением конфигурации, надежно контролируются.
- Доступны аспекты безопасности информации о состоянии конфигурации.
- Завершены необходимые проверки конфигурации по аспектам безопасности.
- Утверждены аспекты безопасности версий системы.

I.5.3. Работы и задачи по безопасности

CM-1 ПОДГОТОВКА К УПРАВЛЕНИЮ КОНФИГУРАЦИЕЙ

CM-1.1 Определение стратегии безопасного управления конфигурацией.

Примечание: К ней относятся:

- Связанные с безопасностью роли, обязанности, подотчетность и полномочия

- Критерии безопасного управления изменениями элементов, находящихся под управлением конфигурацией, включая удаление, доступ, выпуск и контроль
- Соображения безопасности, критерии и ограничения для местоположений, условий и среды хранения
- Критерии или события для начала безопасного управления конфигурацией и безопасного поддержания базовых уровней эволюционирующих конфигураций
- Аспекты безопасности стратегии аудита и обязанности по оценке постоянной целостности и безопасности информации определения конфигурации
- Критерии и ограничения для безопасного управления изменениями, планируемые контрольные списки конфигурации и контрольные списки конфигурации безопасности, нормативные и экстренные запросы на изменение, а также процедуры безопасного управления изменениями
- Обеспечение координации между заинтересованными сторонами, покупателями, поставщиками, цепочкой поставок и другими взаимодействующими организациями

CM-1.2 Определение безопасного подхода к архивированию и извлечению элементов конфигурации, образцов управления конфигурацией, и данных.

Примечание: Сюда входят правила, регулирующие безопасное хранение, доступ и использование.

Ссылки: [4] [74] [86] [100] [126] [127]

CM-2 ВЫПОЛНЕНИЕ ИДЕНТИФИКАЦИИ КОНФИГУРАЦИИ

CM-2.1 Определение аспектов безопасности элементов и образцов системы, которые должны находиться под управлением конфигурацией.

CM-2.2 Определение аспектов безопасности данных конфигурации, подлежащих управлению.

CM-2.3 Установление аспектов безопасности идентификаторов для элементов, находящихся под управление конфигурацией.

CM-2.4 Определение аспектов безопасности базовых уровней на протяжении всего жизненного цикла.

CM-2.5 Получение применимого соглашения с заинтересованными сторонами по аспектам безопасности для установления базовых уровней.

CM-2.6 Утверждение и отслеживание аспектов безопасности версий системы или элементов системы.

Примечание 1: Аспекты безопасности версии - это относящиеся к безопасности соображения санкционирования использования системы или элементов системы для определенного назначения с ограничениями, относящимися к безопасности, или без них. Примерами являются версии для тестирования или эксплуатационного использования.

Примечание 2: Версии, как правило, включают набор изменений, вносимых с помощью технических процессов. Санкционирование версии, как правило, включает в себя принятие проверенных и утвержденных изменений и любых воздействий на безопасность изменений.

Ссылки: [4] [86] [100] [111] [112] [113]

CM-3 УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ В КОНФИГУРАЦИИ

CM-3.1 Определение и регистрация аспектов безопасности запросов на изменения и запросов на несоответствие.

Примечание 1: Сюда входят запросы на отклонение, отказ или разрешение.

Примечание 2: Изменения или несоответствия могут быть основаны на причинах, отличных от безопасности или не имеющих очевидного отношения *к* безопасности.

CM-3.2 Определение аспектов безопасности действий по координации, оценке и принятию решений по запросам на изменение или запросов на несоответствие.

Примечание: Выявленные аспекты безопасности координируются и оцениваются по всем критериям оценки результативности и эффективности, а также критериям планов проекта, стоимости, преимуществ, рисков, качества и календарного плана.

CM-3.3 Представление запросов на рассмотрение и санкционирование безопасности.

Примечание: Контрольные списки могут быть ориентированы или не ориентированы на безопасность. При работе с контрольными списками, не связанными с безопасностью, необходимо проверить, нет ли в запросе аспектов, связанных с безопасностью.

CM-3.4 Отслеживание и управление аспектами безопасности утвержденных изменений базового уровня, запросов на изменения и запросов на несоответствие.

Ссылки: [4] [86] [100]

CM-4 ВЫПОЛНЕНИЕ УЧЕТА СОСТОЯНИЯ КОНФИГУРАЦИИ

CM-4.1 Разработка и поддержание относящейся к безопасности информации о состоянии управления конфигурацией для элементов системы, базовых уровней, утвержденных изменений и версий.

Примечание: Информация включает в себя решения по сертификации безопасности, аккредитации, санкционированию или одобрению для системы, элемента системы, базового уровня или версии.

CM-4.2 Сбор, хранение и регистрация данных управления конфигурацией, относящихся к безопасности.

Ссылки: [4] [86] [100]

CM-5 ВЫПОЛНЕНИЕ ОЦЕНКИ КОНФИГУРАЦИИ

CM-5.1 Определите необходимость в действиях по проверкам и аудитам конфигурации безопасности и управления конфигурацией.

CM-5.2 Убедитесь, что конфигурация продукта или сервиса соответствует требованиям к конфигурации, относящимся к безопасности.

Примечание: Это выполняется путем сравнения требований к безопасности, ограничений и исключений (несоответствий) с результатами формальных действий по проверке.

CM-5.3 Мониторинг безопасного внедрения утвержденных изменений конфигурации.

CM-5.4 Выполнение действий по проверке и аудитам конфигурации безопасности и управления конфигурацией и для определения аспектов безопасности базовых уровней продукта.

Примечание: Это включает аспекты безопасности аудита функциональной конфигурации (FCA), которые ориентированы на функциональные и эксплуатационные возможности, и аудита физической конфигурации (PCA), которые ориентированы на соответствие системы элементам информации об эксплуатации и конфигурации.

CM-5.5 Регистрация аспектов безопасности аудита управления конфигурацией и другие результаты оценки конфигурации, а также элементов действий по удалению.

Ссылки: [4] [86] [100]

I.6. Управление информацией

Назначение процесса «*Управление информацией*» - генерирование, получение, подтверждение, преобразование, сохранение, извлечение, распространение и распределение информации среди определённых заинтересованных сторон.

I.6.1. Назначение безопасности

- Рассмотрение аспектов безопасности управления информацией.

I.6.2. Результаты безопасности

- Определена информация, относящаяся к безопасности и подлежащая управлению.
- Определены средства защиты информации.
- Определены аспекты безопасности представления информации.
- Информация безопасно управляется.
- Определяются аспекты безопасности состояния информации.
- Информация доступна определённым заинтересованным сторонам безопасным способом.

I.6.3. Работы и задачи безопасности

IM-1 ПОДГОТОВКА К УПРАВЛЕНИЮ ИНФОРМАЦИЕЙ

IM-1.1 Определение аспектов безопасности стратегии управления информацией.

Примечание: Аспекты безопасности включают в себя информацию о заинтересованных сторонах, техническую и другую информацию. Эти аспекты касаются безопасности, приватности и интеллектуальной собственности.

IM-1.2 Определение аспектов безопасности информационных элементов, которые будет осуществляться управление.

IM-1.3 Определение полномочий и обязанностей в отношении аспектов безопасности управления информацией.

Примечание: Должное внимание уделяется законодательству, безопасности и приватности (например, правам собственности, ограничениям соглашений, правам доступа, правам на данные и интеллектуальной собственности). При наличии ограничений или условий информация соответствующим образом идентифицируется. Персонал, знакомый с такими элементами информации, информируются об их обязательствах и обязанностях, связанных с обеспечением безопасности.

IM-1.4 Определение аспектов безопасности содержания, форматов, структуры и стойкости защиты элементов информации.

Примечание 1: Аспекты безопасности относятся к информации, находящейся в состоянии покоя (т.е. постоянного или непостоянного хранения), при передаче между источником/точкой отправления и пунктом назначения и находящейся в процессе преобразования.

Примечание 2: Аспекты безопасности основываются на критериях применимых законов, политик, директив, постановлений и патентов.

IM-1.5 Определение аспектов безопасности действий по поддержке информации.

Ссылки: [4] [86] [100] [128]

IM-2 УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ

IM-2.1 Безопасное получение, разработка или преобразование идентифицированных элементов информации.

Примечание: Получение, разработка и преобразование элементов информации включает маркировку элементов по потребностям в их защите (например, классификацию).

IM-2.2 Безопасное хранение элементов информации и их учетных записей, а также запись состояния безопасности информации.

IM-2.3 Безопасная публикация, распространение или предоставление доступа к информации и элементам информации определённым заинтересованным сторонам.

IM-2.4 Безопасное архивирование заданной информации.

Примечание: Носители информации, местоположение и защита информации выбираются в соответствии *с* указанными периодами хранения и извлечения, соглашениями, законодательством и политикой безопасности организации.

IM-2.5 Безопасное удаление нежелательной, недействительной или неподтвержденной информации.

Ссылки: [4] [86] [100] [128] [129]

I.7. Измерение

Назначением процесса «*Измерение*» является сбор, анализ и представление объективных данных и информации для поддержки эффективного управления и демонстрации качества продуктов, сервисов и процессов.

I.7.1. Назначение безопасности

- Сбор, анализ и предоставление данных и информации, касающихся безопасности, для поддержки эффективного управления и демонстрации качества продуктов, сервисов и процессов.

I.7.2. Результаты безопасности

- Определены потребности в информации, имеющей отношение к безопасности.
- Определён или разработан соответствующий набор мер безопасности на основе потребностей в информации, имеющей отношение к безопасности, и потребностей в защите информации.
- Обеспечивается надежное управление необходимыми данными.
- Проводится анализ данных, относящихся к безопасности, и интерпретация результатов.
- Результаты измерений предоставляют объективную информацию, которая поддерживает решения, касающиеся безопасности.

I.7.3. Работы и задачи безопасности

MS-1 ПОДГОТОВКА К ИЗМЕРЕНИЮ

MS-1.1 Определение аспектов безопасности стратегии измерения.

MS-1.2 Описание характеристик организации, имеющих отношение к измерению безопасности.

MS-1.3 Определение и установление приоритетности информационных потребностей, связанных с безопасностью.

Примечание: Потребности основаны на целях защиты, рисках и других относящихся к безопасности элементах, связанных с проектными решениями.

MS-1.4 Выберите и спецификация мер, удовлетворяющих требованиям безопасности информации.

MS-1.5 Определение процедур сбора, анализа, доступа и отчетности по данным, имеющим отношение к безопасности.

MS-1.6 Определение критериев безопасности для оценки элементов информации и процесса измерения.

Примечание: Все критерии для элемента информации, связанного с безопасностью, являются релевантными для безопасности.

MS-1.7 Определение аспектов безопасности для предоставления систем или сервисов, необходимых для поддержки измерений.

MS-1.8 Определение и планирование предоставления систем или сервисов, необходимых для поддержки аспектов безопасности измерения.

MS-1.9 Приобретение или получение доступа к аспектам безопасности вспомогательных систем или сервисов, используемых при измерении.

Ссылки: [4] [86] [130] [79] [97]

MS-2 ВЫПОЛНЕНИЕ ИЗМЕРЕНИЙ

MS-2.1 Интеграция процедур генерации, сбора, анализа и отчетности по данным, имеющим отношение к безопасности, в соответствующие процессы.

MS-2.2 Интеграция процедур безопасной генерации, сбора, анализа и отчетности по данным в соответствующие процессы.

MS-2.3 Сбор, хранение и проверка данных, относящихся к безопасности.

MS-2.4 Безопасный сбор, хранение и проверка данных.

MS-2.5 Анализ данных, относящихся к безопасности, и разработка элементов информации, относящихся к безопасности.

MS-2.6 Регистрация результаты измерений безопасности и информирование пользователей измерений.

Примечание: Результаты измерения безопасности предоставляются заинтересованным сторонам и персоналу проекта для поддержки принятия решений и управления рисками, а также для инициирования корректирующих действий и улучшений.

Ссылки: [4] [79] [86] [97] [130]

I.8. Обеспечение доверия

Назначением процесса «*Обеспечение доверия*» - помочь гарантировать эффективное приложение к проекту процесса *«Управление качеством*» в организации.

Перепечатано с разрешения IEEE, Copyright IEEE 2015, Все права защищены.

I.8.1. Назначение безопасности

- Обеспечение эффективного приложения процесса «*Управление качеством*» в организации к аспектам безопасности проекта.

  Примечание: Аспекты безопасности для «*Обеспечение доверия*» должны учитывать принципы доверия, подробно описанные в Приложении F.2.

I.8.2. Результаты безопасности

- Реализованы аспекты безопасности процедур обеспечения доверия, включая критерии безопасности и методы оценки обеспечения доверия.
- Оценка продуктов, сервисов и процессов проекта выполняется в соответствии с политиками, процедурами и требованиями по управлению качеством в области безопасности.
- Результаты оценок безопасности предоставляются соответствующим заинтересованным сторонам.
- Устраняются инциденты, связанные с безопасностью.
- Рассматриваются приоритетные проблемы, связанные с безопасностью.

I.8.3. Работы и задачи безопасности

QA-1 ПОДГОТОВКА К ОБЕСПЕЧЕНИЮ ДОВЕРИЯ

QA-1.1 Определение аспектов безопасности стратегии обеспечения доверия.

Примечание: Аспекты безопасности основываются на политиках, целях и процедурах управления качеством и согласуются с ними, а также включают:

- Процедуры обеспечения доверия к безопасности проекта
- Роли, обязанности, подотчетность и полномочия в области обеспечения безопасности
- Действия по обеспечению безопасности, соответствующие каждому процессу жизненного цикла
- Действия по обеспечению безопасности, соответствующие каждому поставщику (включая субподрядчиков)
- Необходимые действия по проверке, подтверждению соответствия, мониторингу, измерению, проверке и тестированию, относящиеся к конкретному продукту или сервису
- Критерии безопасности для принятия продукта или сервиса

QA-1.2 Обеспечение независимости обеспечения доверия к безопасности от других процессов жизненного цикла.

Ссылки: [4] [30] [61] [86] [98] [99] [106] [107] [108] [131]

QA-2 ПРОВЕДЕНИЕ ОЦЕНКИ ПРОДУКТОВ ИЛИ СЕРВИСОВ

QA-2.1 Оценка продуктов и сервисов на соответствие установленным критериям безопасности, контрактам, стандартам и нормативным документам.

QA-2.2 Выполнение аспектов безопасности при проверке и подтверждении соответствия результатов процессов жизненного цикла для определения соответствия установленным требованиям.

Ссылки: [4] [30] [61] [86] [98] [99] [131]

QA-3 ВЫПОЛНЕНИЕ ОЦЕНКИ ПРОЦЕССОВ

QA-3.1 Оценка процессов жизненного цикла проекта на соответствие установленным критериям качества безопасности.

QA-3.2 Оценка инструментов и сред, поддерживающих или автоматизирующих процесс на соответствие установленным критериям качества безопасности.

QA-3.3 Оценка процессов поставщика на соответствие требованиям безопасности процессов.

Примечание: Рассматриваются такие элементы, как аспекты безопасности среды разработки, технологические меры, требуемые от поставщиков, или процессы по рискам, которые поставщики должны использовать.

Ссылки: [4] [30] [61] [86] [98] [99] [111] [112] [113] [131]

QA-4 УПРАВЛЕНИЕ ЗАПИСЯМИ И ОТЧЕТАМИ ПО ОБЕСПЕЧЕНИЮ ДОВЕРИЯ

QA-4.1 Создание записей и отчетов, связанных с аспектами безопасности действий по обеспечению доверию.

QA-4.2 Безопасное ведение, хранение и распространение записей и отчетов.

QA-4.3 Определение аспектов безопасности инцидентов и проблем, связанных с оценками продуктов, сервисов и процессов.

Ссылки: [4] [30] [61] [86] [98] [99] [131]

QA-5 РАССМОТРЕНИЕ ИНЦИДЕНТОВ И ПРОБЛЕМ

QA-5.1 Регистрация, анализ и классификация аспектов безопасности инцидентов.

Примечание: Инциденты группируются (классифицируются) по таким критериям, как тип, область действия и последствия.

QA-5.2 Устранение аспектов безопасности инцидентов или повышение аспектов безопасности инцидентов до уровня проблем.

QA-5.3 Регистрация, анализ и классификация аспектов проблем, связанных с безопасностью.

QA-5.4 Отслеживание аспектов безопасности при определении приоритетов и реализации методов устранения проблем.

Примечание: Это включает в себя как решение проблем, связанных с безопасностью, так и аспекты безопасности при решении общих проблем.

QA-5.5 Регистрация и анализ аспектов безопасности инцидентов и проблем.

QA-5.6 Информирование заинтересованных сторон о состоянии аспектов безопасности инцидентов и проблем.

QA-5.7 Отслеживание аспектов безопасности инцидентов и проблем до их закрытия.

Ссылки: [4] [30] [61] [98] [99] [131]

Приложение J. Организационные процессы реализации проектов

В этом приложении приведены *«Организационные процессы, обеспечивающие реализацию проектов»* из [4], с учетом соображений безопасности и вклада в цели, результаты, мероприятия и задачи.

J.1. Управление моделью жизненного цикла

Назначением процесса «*Управление моделью жизненного цикла*» является определение, поддержание и помощь в обеспечении доступности политик, процессов жизненного цикла, моделей жизненного цикла и процедур для использования организацией в соответствии со сферой применения данного международного стандарта.

J.1.1. Назначение безопасности

- Обеспечение учета потребностей и соображений безопасности в политиках, процессах жизненного цикла, моделях жизненного цикла и процедурах, используемых организацией.

J.1.2. Результаты безопасности

- Соображения безопасности отражены в политиках и процедурах управления и развертывания моделей и процессов жизненного цикла организации.
- Определены роли, обязанности, подотчётность и полномочия в области безопасности в рамках политик, процессов, моделей и процедур жизненного цикла.
- Выбор политик, процессов жизненного цикла, моделей жизненного цикла и процедур для использования организацией определяется потребностями и соображениями безопасности.
- Оцениваются потребности и соображения безопасности для политик, процессов жизненного цикла, моделей жизненного цикла и процедур для использования организацией.
- Внедрены приоритетные улучшения процессов, моделей и процедур, имеющие отношение к безопасности.

J.1.3. Работы и задачи безопасности

LM-1 СОЗДАНИЕ ПРОЦЕССОВ ЖИЗНЕННОГО ЦИКЛА

LM-1.1 Разработка политик и процедур управления и развертывания процессов, соответствующих аспектам безопасности стратегий организации.

Примечание: Политики и процедуры могут быть ориентированы на безопасность, основаны на безопасности или могут иметь аспекты, связанные с обеспечением безопасности.

LM-1.2 Определение аспектов безопасности процессов жизненного цикла, реализующих требования [4] и согласующихся со стратегиями организации.

LM-1.3 Определение ролей, обязанностей, подотчётности и полномочий в области безопасности для облегчения реализации аспектов безопасности процессов жизненного цикла и стратегического управления жизненными циклами.

LM-1.4 Определение аспектов безопасности критериев, контролирующих ход выполнения в течение жизненного цикла.

Примечание: Сюда входят критерии безопасности для результатов, контрольных точек, а также критерии входа/выхода для этапов и точек принятия решений.

LM-1.5 Установление критериев безопасности для стандартных моделей жизненного цикла для организации, включая критерии результатов для каждого этапа.

Примечание: Модель жизненного цикла включает, при необходимости, один или несколько этапов, причем каждый этап имеет аспекты безопасности, соответствующие его цели и результатам. Модель собрана в виде последовательности этапов, которые перекрываются или повторяются в зависимости от сферы охвата системы, представляющей интерес, величины, сложности, изменяющихся потребностей и возможностей (включая потребности и возможности в области защиты).

Ссылки: [4] [30] [61] [86] [98] [99] [100] [132]

LM-2 ОЦЕНКА ПРОЦЕССА ЖИЗНЕННОГО ЦИКЛА

LM-2.1 Мониторинг аспектов безопасности выполнения процессов в организации.

Примечание: Это включает в себя анализ технологических мер и пересмотр тенденций в области безопасности в отношении стратегических критериев безопасности, обратную связь с проектами относительно эффективности и действенности процессов, а также мониторинг исполнения в соответствии с нормативными документами и политиками организации.

LM-2.2 Проведение пересмотров аспектов безопасности моделей жизненного цикла, используемых в проектах.

Примечание: Сюда входит подтверждение пригодности, адекватности и эффективности моделей жизненного цикла, используемых в проекте. Эти пересмотры должна проводиться периодически и определяться событиями (например, по завершении крупных этапов проекта).

LM-2.3 Выявление связанных с безопасностью возможностей улучшения исходя из результатов оценки.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [134]

LM-3 СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА

LM-3.1 Определение приоритетов и планирование возможностей повышения безопасности.

LM-3.2 Реализация возможностей повышения безопасности и информирование соответствующих заинтересованных сторон.

Примечание: Сюда входят регулирующие, сертифицирующие, аккредитующие, принимающие и аналогичные заинтересованные стороны.

Ссылки: [4] [30] [61] [86] [98] [99] [100]

J.2. Управление инфраструктурой

Назначением процесса «*Управление инфраструктурой*» является предоставление инфраструктуры и сервисов проектам для поддержки целей организации и проекта на протяжении всего жизненного цикла.

J.2.1. Назначение безопасности

- Определение потребностей в защите для аспектов инфраструктуры и сервисов, которые поддерживают цели организации и проекта.

J.2.2. Результаты безопасности

- Определены потребности в защите инфраструктуры.
- Определены возможности безопасности и ограничения элементов инфраструктуры.
- Получены элементы инфраструктуры, удовлетворяющие спецификациям безопасности инфраструктуры.
- Доступна безопасная инфраструктура.
- Внедрены приоритетные усовершенствования в области безопасности инфраструктуры.

J.2.3. Работы и задачи безопасности

IF-1 СОЗДАНИЕ ИНФРАСТРУКТУРЫ

IF-1.1 Определение потребности в защите инфраструктуры безопасности.

Примечание: Аспекты безопасности потребностей в ресурсах инфраструктуры рассматриваются в контексте других проектов и ресурсов в рамках организации. Также определяются ограничения безопасности, которые влияют на предоставление инфраструктурных ресурсов и сервисов для проекта и контролируют их.

IF-1.2 Определение, получение и предоставление инфраструктурных ресурсов и сервисов, удовлетворяющих требованиям защиты для безопасного внедрения и поддержки проектов.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

IF-2 ПОДДЕРЖАНИЕ ИНФРАСТРУКТУРЫ

IF-2.1 Оценка степени, в какой поставляемые инфраструктурные ресурсы удовлетворяют требованиям защиты проекта.

IF-2.2 Определение и предоставление улучшений безопасности или изменений в ресурсах инфраструктуры по мере изменения требований проекта.

Примечание: Любое несоответствие между требованиями безопасности проекта и безопасностью, обеспечиваемой инфраструктурными ресурсами, может привести к пробелам в доверии.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

J.3. Управление портфелем

Назначение процесса «*Управление портфелем*» проектов заключается в том, чтобы инициировать и поддерживать необходимые, достаточные и подходящие проекты для достижения стратегических целей организации.

J.3.1. Назначение безопасности

- Определение соображений безопасности для проектов, отвечающих стратегическим целям организации.

J.3.2. Результаты безопасности

- Определены аспекты безопасности стратегических венчурных возможностей, инвестиций или потребностей.

- Определены аспекты проектов, связанные с безопасностью.
- Выделены ресурсы и бюджеты на аспекты безопасности каждого проекта.
- Определены обязанности по управлению проектом, ответственность и полномочия по обеспечению безопасности.
- Поддерживаются проекты, отвечающие критериям безопасности в соглашениях и требованиям безопасности заинтересованных сторон.
- Проекты, которые не соответствуют критериям безопасности в соглашениях или не удовлетворяют требованиям безопасности заинтересованных сторон, переориентированы или прекращены.
- Проекты, в которых завершено выполнение аспектов соглашений, касающихся безопасности, и отвечающие требованиям безопасности заинтересованных сторон, закрыты.

J.3.3. Работы и задачи безопасности

PM-1 ОПРЕДЕЛЕНИЕ И САНКЦИОНИРОВАНИЕ ПРОЕКТОВ

PM-1.1 Определение потенциальных новых или измененных возможностей или задач по обеспечению безопасности.

Примечание: Стратегия организации, концепция эксплуатации, а также анализ пробелов или возможностей рассматриваются с целью выявления пробелов, проблем или возможностей, связанных с безопасностью.

PM-1.2 Определение аспектов безопасности потенциальных новых или измененных возможностей или задач.

Примечание: Стратегия организации, концепция эксплуатации, а также анализ пробелов или возможностей рассматриваются с целью выявления пробелов, проблем или возможностей, связанных с безопасностью.

PM-1.3 Определение приоритетов, выбор и внедрение новых бизнес-возможностей, предприятий или начинаний с учетом целей и интересов безопасности.

PM-1.4 Определение аспектов безопасности проектов, обязанностей и полномочий.

Примечание: Сюда входят критерии собственности, конфиденциальности и приватности проекта.

PM-1.5 Определение аспектов безопасности ожидаемых целей, задач и результатов каждого проекта.

Примечание: Сюда входят критерии собственности, конфиденциальности и приватности проекта.

PM-1.6 Определение и распределение ресурсов для достижения аспектов безопасности целей и задач по проекту.

PM-1.7 Определение аспектов безопасности любых меж-проектных интерфейсов и зависимостей, которые должны управляться или поддерживаться каждым проектом.

Примечание: Сюда входят интерфейсы и зависимости со вспомогательными системами и службами, а также все связанные данные и информацию.

PM-1.8 Определение аспектов безопасности требований к отчетности по проекту и рассмотрение контрольных точек, регулирующих выполнение каждого проекта.

PM-1.9 Санкционирование каждому проекту начинать выполнение планов проекта, включая его аспекты безопасности.

Ссылки: [4] [30] [61] [86] [98] [99] [100]

PM-2 ОЦЕНКА ПОРТФЕЛЯ ПРОЕКТОВ

PM-2.1 Оценка аспектов безопасности проектов для подтверждения текущей жизнеспособности.

Примечание: Это включает в себя следующее:

- Проект продвигается к достижению установленных целей и задач в области безопасности.
- Проект соответствует директивам безопасности проекта.
- Проект осуществляется в соответствии с аспектами безопасности, предусмотренными политиками, процессами и процедурами жизненного цикла проекта.
- Проект остается жизнеспособным, о чем свидетельствует сохраняющаяся потребность в услугах по обеспечению безопасности, практической реализации безопасных продуктов и приемлемые инвестиционные выгоды, обусловленных безопасностью.

PM-2.2 Продолжение осуществления проектов, которые успешно продвигаются с учетом аспектов безопасности проектов.

PM-2.3 Переориентация проектов, которые, как можно ожидать, будут успешно продвигаться при соответствующем перенаправлении с учетом безопасности.

Ссылки: [4] [86] [100]

PM-3 ЗАВЕРШЕНИЕ ПРОЕКТОВ

PM-3.1 Если это предусмотрено соглашением, принимаются меры по отмене или приостановке проектов для которых недостатки или риски для безопасности организации перевешивают выгоды от продолжения инвестиций.

PM-3.2 После завершения соглашения по аспектам безопасности продуктов или сервисов выполняются действия по закрытию проектов.

Примечание: Закрытие осуществляется в соответствии с политиками безопасности, процедурами и соглашением организации.

Ссылки: [4] [86] [100]

J.4. Управление персоналом

Назначение процесса «*Управление персоналом*» заключается в том, чтобы обеспечить организацию необходимыми людскими ресурсами и поддерживать их компетентность способом, согласующемся со стратегическими потребностями.

J.4.1. Назначение безопасности

- Определение критериев безопасности для необходимых людских ресурсов и поддержание их компетентности в соответствии со стратегическими потребностями.

J.4.2. Результаты безопасности

- Определены квалификации, необходимые для обеспечения безопасности в рамках проектов. В проекты включаются сотрудники, обладающие необходимой квалификацией в области безопасности.

- Развиваются, поддерживаются или совершенствуются квалификации персонала, связанные с безопасностью.
- Разрешаются кадровые конфликты, имеющие отношение к безопасности.

J.4.3. Работы и задачи безопасности

HR-1 ОПРЕДЕЛИТЕ КВАЛИФИКАЦИИ

HR-1.1 Определение необходимых квалификаций в области безопасности на основе текущих и ожидаемых проектов.

HR-1.2 Определение и регистрация квалификаций персонала, связанных с обеспечением безопасности.

Ссылки: [4] [86] [100] [132] [109] [133]

HR-2 РАЗВИТИЕ КВАЛИФИКАЦИЙ

HR-2.1 Разработка плана развития квалификаций, необходимых для обеспечения безопасности.

Примечание: Квалификации, относящиеся к безопасности, включают в себя основные и специальные компетенции.

HR-2.2 Получение ресурсов для обучения, переподготовки или наставничества, связанных с безопасностью.

HR-2.3 Обеспечение запланированного развития квалификаций по вопросам безопасности.

HR-2.4 Ведение учета развития квалификаций, связанных с безопасностью.

Ссылки: [4] [86] [100] [109] [132]

HR-3 ПРИОБРЕТЕНИЕ И ПРЕДОСТАВЛЕНИЕ КВАЛИФИКАЦИЙ

HR-3.1 Привлечение квалифицированного персонала при выявлении дефицита квалификаций, связанных с обеспечением безопасности.

HR-3.2 Поддержание и управление резервом квалифицированного персонала по вопросам безопасности, необходимого для осуществления текущих проектов.

HR-3.3 Распределение персонала на основе требований проекта, связанных с обеспечением безопасности, и потребностей в развитии персонала.

HR-3.4 Мотивация персонала имеющего квалификации, связанные с безопасностью, (например, с помощью механизмов карьерного роста и вознаграждения).

HR-3.5 Разрешение аспектов безопасности, связанных с конфликтами персонала в рамках проектов или между ними.

Примечание: Конфликты между проектами и внутри проектов могут включать в себя кадровые возможности, доступность, конфликты квалификации и личные конфликты.

Ссылки: [4] [86] [133]

J.5. Управление качеством

Назначением процесса «*Управление качеством*» является обеспечение того, чтобы продукты, сервисы и результаты процесса управления качеством отвечали целям качества организации и проекта и достижение удовлетворенности клиентов.

J.5.1. Назначение безопасности

- Определение целей организации и проекта в области качества безопасности и критериев, используемых для определения того, соответствуют ли продукты, услуги и результаты процесса управления качеством этим целям безопасности.

  Примечание: Аспекты обеспечения безопасности для управления качеством должны учитывать принципы доверия, подробно описанные *в* Приложении F.2.

J.5.2. Результаты безопасности

- Определены и внедрены политики, стандарты и процедуры управления качеством безопасности организации.
- Установлены критерии и методы оценки качества безопасности.
- Проектам предоставляются ресурсы и информация для поддержки деятельности и мониторинга мероприятий по обеспечению качества безопасности проектов.
- Анализируются аспекты безопасности результатов оценки качества.
- Политики и процедуры управления качеством безопасности совершенствуются на основе результатов проектов и организации.

J.5.3. Работы и задачи безопасности

QM-1 ПЛАНИРОВАНИЕ УПРАВЛЕНИЯ КАЧЕСТВОМ

QM-1.1 Определение аспектов безопасности политики, стандартов и процедур управления качеством.

QM-1.2 Определение обязанностей и полномочий по внедрению управления качеством безопасности.

QM-1.3 Определение критериев и методов оценки качества безопасности.

QM-1.4 Предоставление ресурсов, данных и информации для управления качеством безопасности.

Ссылки: [4] [30] [61] [86] [98] [99] [130]

QM-2 ОЦЕНКА УПРАВЛЕНИЯ КАЧЕСТВОМ

QM-2.1 Сбор и анализ результатов оценки доверия к качеству в соответствии с определенными критериями оценки качества безопасности.

QM-2.2 Оценка удовлетворенности клиентов.

QM-2.3 Проведение периодических пересмотров действий по доверию к качеству проектов на соответствие политикам, стандартам и процедурам управления качеством безопасности.

QM-2.4 Мониторинг состояния повышения качества безопасности процессов, продуктов и сервисов.

Ссылки: [4] [30] [61] [86] [98] [99] [130]

QM-3 ВЫПОЛНЕНИЕ КОРРЕКТИРУЮЩИХ И ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ ПО УПРАВЛЕНИЮ КАЧЕСТВОМ

QM-3.1 Планирование корректирующих действий при невыполнении целей управления качеством безопасности.

QM-3.2 Планирование превентивных действий при наличии достаточного риска того, что цели управления качеством безопасности не будут достигнуты.

QM-3.3 Мониторинг аспектов безопасности корректирующих и превентивных действий до их завершения и информирование заинтересованных сторон.

Ссылки: [4] [30] [61] [86] [98] [99] [130]

J.6. Управление знаниями

Назначением процесса «*Управления знаниями*» является создание возможностей и активов, которые позволяют организации использовать возможности для повторного применения существующих знаний.

J.6.1. Назначение безопасности

- Дать организации возможности для повторного применения существующих знаний в области безопасности.

J.6.2. Результаты безопасности

- Определена таксономия для применения знаний, относящихся к безопасности.
- Упорядочены знания, квалификации и активы организации в области безопасности.
- Доступны знания, квалификации и активы для обеспечения безопасности организации.
- Информация о знаниях, квалификациях и активах в области безопасности в организации распространяется по всей организации.
- Анализируются данные об использовании управления знаниями о безопасности.

J.6.3. Работы и задачи безопасности

КМ 1 ПЛАНИРОВАНИЕ УПРАВЛЕНИЯ ЗНАНИЯМИ

КМ 1.1 Определение аспектов безопасности стратегии управления знаниями.

Примечание: Аспекты безопасности стратегии управления знаниями включают:

- Области знаний и технологии в области безопасности и их потенциал для повторного применения знаний
- Планы получения и поддержания знаний, квалификаций и активов в области безопасности в течение срока их полезного использования
- Типы знаний по безопасности, квалификаций в области безопасности и активов знаний по безопасности, подлежащих сбору и хранению
- Критерии для получения, квалифицирования и исключения знаний в области безопасности, квалификаций в области безопасности и активов знаний по безопасности

- Процедуры контроля за изменениями в знаниях по безопасности, квалификациях в области безопасности и активах знаний по безопасности
- Планы, механизмы и процедуры защиты, контроля и доступа к классифицированным или чувствительным данным и информации
- Механизмы безопасного хранения и безопасного извлечения

КМ 1.2 Определение знаний, квалификаций и активов знаний для обеспечения безопасности, которыми необходимо управлять.

КМ 1.3 Определение проектов, которые могут воспользоваться преимуществами приложения знаний, квалификаций и активов знаний в области безопасности.

Ссылки: [4] [86] [100] [132] [133]

КМ 2 СОВМЕСТНОЕ ИСПОЛЬЗОВАНИЕ ЗНАНИЙ И КВАЛИФИКАЦИЙ В РАМКАХ ОРГАНИЗАЦИИ

КМ 2.1 Создание и ведение классификаторов для фиксации и обмена знаниями и квалификациями в области безопасности.

Примечание: Эти классификаторы включают в себя экспертные знания по безопасности, общую безопасность и области знаний и квалификаций по безопасности, а также извлеченные уроки.

КМ 2.2 Сбор или приобретение знаний и квалификаций в области безопасности.

КМ 2.3 Обеспечение доступности знаний и квалификаций в области безопасности для всей организации.

Ссылки: [4] [86] [100]

КМ 3 СОВМЕСТНОЕ ИСПОЛЬЗОВАНИЕ АКТИВОВ ЗНАНИЙ В РАМКАХ ОРГАНИЗАЦИИ

КМ 3.1 Создание таксономии активов знаний по безопасности для организации.

Примечание: Таксономия включает в себя следующее:

- Определение границ областей безопасности и их связей друг с другом
- Определение границ областей, имеющих отношение к безопасности (например, защита), и их взаимосвязи друг с другом
- Модели областей, которые отражают основные общие и различные характеристики, возможности, концепции и функции, относящиеся к безопасности

КМ 3.2 Разработка или приобретение активов знаний по безопасности.

Примечание: Активы знаний по безопасности включают в себя элементы систем или их представления (например, многоразовые библиотеки кодов, эталонные архитектуры безопасности), элементы архитектуры или дизайна (например, архитектура безопасности или образцы проектирования безопасности), процессы, критерии безопасности или другую техническую информацию (например, учебные материалы), связанную со знаниями в области безопасности и извлеченными уроками.

КМ 3.3 Обеспечение безопасного доступа организации ко всем активам знаний.

Ссылки: [4] [71] [86] [100]

КМ 4 УПРАВЛЕНИЕ ЗНАНИЯМИ, КВАЛИФИКАЦИЯМИ И АКТИВАМИ ЗНАНИЙ

КМ-4.1 Поддержание знаний, квалификаций и активов знаний в области безопасности.

КМ 4.2 Мониторинг и регистрация использования знаний, квалификаций и активов в области безопасности.

КМ 4.3 Периодическая переоценка актуальности аспектов безопасности технологий и рыночных потребностей в активах знаний по безопасности.

Ссылки: [4] [86] [100]

Приложение К. Согласительные процессы

Настоящее приложение содержит «*Согласительные процессы*» из [4] с учетом соображений безопасности и содействия для назначений, результатов, работ и задач.

К.1. Приобретение

Назначением процесса «*Приобретение*» является получение продукта или сервиса в соответствии с требованиями приобретателя.

К.1.1. Назначение безопасности

- Получение продукта или сервиса в соответствии с требованиями безопасности приобретателя.

К.1.2. Результаты безопасности

- Запрос на поставку включает критерии безопасности.
- Выбран один или несколько поставщиков, удовлетворяющих критериям безопасности.
- Между приобретателем и поставщиком установлено соглашение, содержащее критерии безопасности.
- Согласованы продукт или сервис, соответствующие критериям безопасности в соглашении.
- Соблюдены аспекты безопасности обязательств покупателя, определенные в соглашении.

К.1.3. Работы и задачи безопасности

AQ-1 ПОДГОТОВКА К ПРИОБРЕТЕНИЮ

AQ-1.1 Определение аспектов стратегии обеспечения безопасности в отношении того, как будет осуществляться приобретение.

Примечание: Эта стратегия описывает или ссылается на модель жизненного цикла, меры по снижению рисков и проблем безопасности, календарный план этапов, относящихся к безопасности, защиту активов приобретателя и поставщика и критерии выбора, относящиеся к безопасности, если поставщик является внешним по отношению к приобретающей организации. Она также включает ключевые факторы безопасности и связанные с безопасностью характеристики приобретения, такие как обязанности и обязательства; конкретные модели, методы или процессы; формальность; уровень критичности; и приоритетность обеспечения безопасности в рамках соответствующих компромиссных факторов.

AQ-1.2 Подготовка запроса на продукт или сервис с требованиями безопасности.

Примечание: Запрос включает критерии безопасности для деловой практики, которым должен соответствовать поставщик, список участников конкурса с надлежащей квалификацией в области безопасности и критерии безопасности, которые будут использоваться для выбора поставщика.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

AQ-2 ОБЪЯВЛЕНИЕ О ПРИОБРЕТЕНИИ И ВЫБОР ПОСТАВЩИКА

AQ-2.1 Безопасная передача запроса на поставку продукта или сервиса потенциальным поставщикам.

AQ-2.2 Выбор одного или нескольких поставщиков, удовлетворяющих критериям безопасности.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

AQ-3 ЗАКЛЮЧЕНИЕ И ПОДДЕРЖКА СОГЛАШЕНИЯ

AQ-3.1 Разработка и утверждение соглашения с поставщиком, включающего критерии принятия мер безопасности.

Примечание: Это соглашение может быть в разной степени формальным. В соответствии с уровнем формальности, соглашение устанавливает требования безопасности, этапы безопасной разработки и поставки, проверку безопасности, подтверждение соответствия безопасности и аспекты безопасности условий принятия, требований к процессам (например, управление конфигурацией, управление рисками и измерение), а также управление правами на данные и интеллектуальную собственность. Аспекты соглашения, связанные с обеспечением безопасности, также включают применение всех вышеперечисленных положений к субподрядчикам и другим вспомогательным организациям поставщика.

AQ-3.2 Определение необходимых изменений соглашения, имеющих отношение к безопасности.

AQ-3.3 Оценка влияния изменений в соглашении на безопасность.

Примечание: Основания для изменения соглашения могут быть связаны или не связаны с безопасностью. Однако, независимо от причины изменения, это может повлиять на безопасность.

AQ-3.4 Обновление, при необходимости, критерии безопасности в соглашении с поставщиком.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

AQ-4 КОНТРОЛЬ ЗА ВЫПОЛНЕНИЕМ СОГЛАШЕНИЙ

AQ-4.1 Оценка выполнения аспектов соглашения, связанных с обеспечением безопасности.

Примечание: Это включает подтверждение того, что все стороны выполняют свои обязательства по обеспечению безопасности в соответствии с соглашением.

AQ-4.2 Безопасное предоставление данных, необходимых поставщику, и своевременный способ решение проблем.

Ссылки: [4] [86] [100] [111] [112] [113]

AQ-5 ПРИЁМКА ПРОДУКТА ИЛИ СЕРВИСА

AQ-5.1 Подтверждение соответствия поставляемого продукта или сервиса аспектам соглашения, касающимся безопасности.

AQ-5.2 Безопасное предоставление платежа или другого согласованного возмещения.

AQ-5.3 Принятие продукта или сервиса от поставщика или другой стороны в соответствии с критериями безопасности, указанными в соглашении.

AQ-5.4 Закрытие соглашения в соответствии с критериями безопасности соглашения.

Ссылки: [4] [86] [100] [111] [112] [113] [118]

K.2. Поставка

Назначением процесса «*Поставка*» является предоставление приобретателю продуктов или сервисов, соответствующих согласованным требованиям.

K.2.1. Назначение безопасности

- Предоставление приобретателю продуктов или сервисов, соответствующих согласованным требованиям к безопасности.

K.2.2. Результаты безопасности

- Реакция на запрос приобретателя учитывает требования к безопасности приобретателя.
- Соглашение, заключенное между приобретателем и поставщиком, включает требования безопасности.
- Предоставлены продукты или сервисы, удовлетворяющие требованиям безопасности приобретателя.
- Обязательства по обеспечению безопасности поставщика, определенные в соглашении, выполнены.
- Ответственность за приобретенный продукт или сервис, как предписано соглашением, безопасно передана.

K.2.3. Работы и задачи безопасности

SP-1 ПОДГОТОВКА К ПОСТАВКЕ

SP -1.1 Определение аспектов безопасности, связанных с потребностью приобретателя в продуктах или сервисах.

SP -1.2 Определение аспектов безопасности стратегии поставок.

Примечание: Стратегия описывает или ссылается на аспекты безопасности модели жизненного цикла, меры по снижению рисков и проблем, а также календарный план важных для безопасности этапов. Она также включает ключевые факторы, имеющие отношение к безопасности, и характеристики приобретения, такие как обязанности и обязательства, конкретные модели, относящиеся к безопасности, методы или процессы, имеющие отношение к безопасности, уровень критичности, формальность и приоритет соответствующих компромиссных факторов.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

SP-2 ОТВЕТ НА ЗАПРОС НА ПОСТАВКУ ПРОДУКТОВ ИЛИ СЕРВИСОВ

SP -2.1 Оценка запроса на продукт или сервис для определения возможности обеспечения безопасности и способов реагирования.

SP -2.2 Подготовка ответа, удовлетворяющего критериям безопасности в запросе.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

SP-3 ЗАКЛЮЧЕНИЕ И ПОДДЕРЖКА СОГЛАШЕНИЯ

SP -3.1 Согласование и утверждение соглашения с приобретателем, включающего критерии принятия безопасности.

Примечание 1: Это включает управление конфигурацией, отчетность о рисках, отчетность о мерах безопасности и анализ мер безопасности; требования к безопасности; безопасность разработки; проверку безопасности; подтверждение соответствия безопасности; процедуры и критерии принятия мер

безопасности; принятие, разрешение и санкционирование регулирующего органа; процедуры транспортировки, обработки, доставки и хранения; защиту безопасности и приватности и ограничения на использование, распространение и уничтожение данных, информации и интеллектуальной собственности; процедуры и критерии обработки исключений, имеющих отношение к безопасности; процедуры управления изменениями в соглашениях; и процедуры расторжения соглашений.

Примечание 2: Аспекты безопасности соглашения также включают применение всего вышеперечисленного к планам использования субподрядчика.

SP -3.2 Определение необходимых изменений соглашения, имеющих отношение к безопасности.

SP -3.3 Оценка влияния необходимых изменений в соглашении на безопасность.

Примечание: Основанием для внесения изменений в соглашение могут быть, а могут и не быть соображения безопасности. Однако, независимо от того, на какой основе вносятся изменения, они могут повлиять на безопасность. Оценка необходимых изменений с точки зрения безопасности позволяет выявить их значимость для безопасности и определить влияние с точки зрения планов, календарного плана, стоимости, технических возможностей, качества, доверия и доверенности.

SP -3.4 Обновление, при необходимости, критериев безопасности в соглашении с приобретателем.

Ссылки: [4] [30] [61] [86] [98] [99] [100] [111] [112] [113]

SP-4 ВЫПОЛНЕНИЕ СОГЛАШЕНИЯ

SP -4.1 Выполнение аспектов безопасности соглашения в соответствии с установленными планами проекта.

Примечание: Поставщик иногда принимает или соглашается использовать процессы приобретателя, включая процессы, относящиеся к безопасности.

SP -4.2 Оценка исполнения аспектов соглашения, связанных с обеспечением безопасности.

Примечание: Это включает подтверждение того, что все стороны выполняют свои обязанности по обеспечению безопасности в соответствии с соглашением.

Ссылки: [4] [86] [100] [111] [112] [113]

SP-5 ПОСТАВКА И ПОДДЕРЖКА ПРОДУКТА ИЛИ СЕРВИСА

SP -5.1 Поставка продукта или сервиса в соответствии с критериями безопасности соглашения.

SP -5.2 Оказание помощи приобретателю в обеспечении безопасности в соответствии с соглашением.

SP -5.3 Безопасное принятие и подтверждение оплаты или иного согласованного возмещения.

SP -5.4 Передача продукта или сервиса приобретателю или другой стороне в соответствии с требованиями безопасности в соглашении.

Примечание: Сюда входит передача аппаратных средств, программного обеспечения и чувствительной, служебной и классифицированной информации.

SP -5.5 Закрытие соглашения в соответствии с критериями безопасности соглашения.

Ссылки: [4] [86] [100] [111] [112] [113] [118]

Приложение L. Журнал регистрации изменений

L.1. Изменения по сравнению с NIST SP 800-160 Том 1

Эта публикация включает следующие изменения по сравнению с первоначальным изданием (ноябрь 2016 года; обновлено 21 марта 2018 года):

- Обеспечивается новый фокус на принципах и концепциях проектирования доверенных безопасных систем, с разделением содержания по нескольким переработанным начальным главам
- Подробные процессы жизненного цикла системы и соображения безопасности перемещены в отдельные приложения для удобного использования
- Оптимизированы принципы проектирования доверенных безопасных систем за счет исключения двух предыдущих категорий принципов проектирования
- Включено новое введение в процессы жизненного цикла систем и описание ключевых связей между этими процессами.
- Разъяснены ключевые термины по проектированию систем и технике обеспечения безопасности
- Упрощены структуры процессов жизненного цикла систем, работ, задач и ссылок
- Предоставлены дополнительные ссылки на международные стандарты и технические руководства для более эффективной поддержки аспектов безопасности процесса проектирования систем

L.2. Сводка по обновлению ошибок

В таблице 6 показаны изменения, внесенные в эту публикацию. Обновления с ошибками могут включать исправления, разъяснения или другие незначительные изменения в публикации, которые носят редакционную или существенную сущность. Любые возможные обновления для этого документа, которые еще не опубликованы в обновлении по ошибкам или в официальной редакции, включая дополнительные проблемы и возможные исправления, будут опубликованы по мере их выявления. См. сведения о публикации для этого отчета.
Текущий выпуск этой публикации не содержит обновлений с ошибками.

Таблица 6. Журнал изменений

Идентификатор публикации	Дата	Тип редактирования	Изменение	Местоположение