**Специальная публикация NIST 800-53**

Пересмотр 5

# Меры обеспечения безопасности и приватности для информационных систем и организаций

**ОБЪЕДИНЁННАЯ ЭКСПЕРТНАЯ ГРУППА**

Эта публикация доступна бесплатно по адресу:

https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology
U.S. Department of Commerce

**NIST Специальная публикация 800-53**

**Специальная публикация NIST 800-53**

Пересмотр 5

# Меры обеспечения безопасности и приватности для информационных систем и организаций

**ОБЪЕДИНЁННАЯ ЭКСПЕРТНАЯ ГРУППА**

Эта публикация доступна бесплатно по адресу:

https://doi.org/10.6028/NIST.SP.800-53r5

**Сентябрь 2020**

ВКЛЮЧАЕТ ОБНОВЛЕНИЯ ПО СОСТОЯНИЮ НА 12-10-2020; СМ. СТР. XVII


Департамент торговли США
*Wilbur L. Ross, Jr., Министр*

Национальный институт стандартов и технологий
*Walter Copan, директор NIST и заместитель министра торговли по стандартам и технологиям*

## Полномочия

Эта публикация была разработана NIST в соответствии с его обязанностями, установленными в соответствии с Федеральным законом о модернизации информационной безопасности (FISMA), 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113 -283. NIST отвечает за разработку стандартов и руководств по информационной безопасности, включая минимальные требования к федеральным информационным системам. Такие стандарты и руководства по информационной безопасности не должны применяться к системам национальной безопасности без прямого санкционирования соответствующих федеральных должностных лиц, осуществляющих полномочия в отношении таких систем. Это руководство соответствует требованиям циркуляра Министерства управления и бюджета (ОМБ) A-130.

Ничто в этой публикации не должно использоваться в противоречие со стандартами и руководствами, определенными Министром торговли в соответствие с его законными полномочиями как обязательные для федеральных агентств. Ничто в этом руководстве также не должны интерпретироваться как изменяющие или заменяющие существующие полномочия министра торговли, директора ОМБ или любого другого федерального должностного лица. Эта публикация может использоваться неправительственными организациями на добровольной основе и это не попадает по действие авторского права в Соединенных Штатах. Вместе с тем NIST был бы признателен за упоминание.

Специальная публикация Национального института стандартов и технологий 800-53, редакция 5
Natl. Inst. Stand. Technol. Spec. Publ. 800-53, Rev. 5, 492 pages (сентябрь 2020)

CODEN: NSPUE2

Эта публикация доступна бесплатно по адресу:
https://doi.org/10.6028/NIST.SP.800-53r5

Некоторые коммерческие сущности, оборудование или материалы могут быть определены в настоящем документе для адекватного описания экспериментальной процедуры или концепции. Такая идентификация не подразумевает рекомендации или одобрение со стороны NIST и не подразумевает, что сущности, материалы или оборудование обязательно являются наилучшими из имеющихся по предназначению.

В этой публикации могут содержаться ссылки на другие публикации, которые в настоящее время разрабатываются NIST в соответствии с возложенными на него законными обязанностями. Информация в этой публикации, включая концепции, практику и методологии, может использоваться федеральными агентствами еще до завершения таких сопутствующих публикаций. Таким образом, до тех пор, пока каждая публикация не будет завершена, действующие требования, рекомендации и процедуры там, где они существуют, остаются в силе. Для целей планирования и перехода федеральные агентства имеют возможность постоянно отслеживать разработку этих новых публикаций в NIST.

Организации поощрены рассматривать все черновые публикации во время периодов для публичных комментариев и предоставлять обратную связь в NIST. Большинство публикаций NIST, кроме некоторых указанных выше, доступны в http://csrc.nist.gov/publications.

**Замечания по этой публикации могут быть представлены:**

Национальный институт стандартов и технологий
Attn: Отдел компьютерной безопасности, Лаборатория информационных технологий
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: Sec-cert@nist.gov

Все замечания подлежат опубликованию в соответствии с Законом о свободе информации (FOIA) [ФОИА96].

## Отчеты по технологиям компьютерных систем

Лаборатория информационных технологий (ITL) Национального института стандартов и технологий (NIST) содействует развитию экономики и общественного благосостояния США путем обеспечения технического лидерства для национальной инфраструктуры измерений и стандартов. ITL разрабатывает тесты, методы испытаний, справочные данные, доказательства реализации концепций и технический анализ в целях содействия разработке и продуктивному использованию информационных технологий (ИТ). В обязанности ITL входит разработка управленческих, административных, технических и физических стандартов и руководств для обеспечения эффективной с точки зрения затрат безопасности информации в федеральных информационных системах, не связанных с национальной безопасностью. В специальных публикациях серии 800 содержится информация об исследованиях, руководствах и усилиях ITL в области безопасности и приватности информационных систем, а также о ее совместных работах с промышленными, правительственными и научными организациями.

## Резюме

Эта публикация содержит каталог мер безопасности и приватности для информационных систем и организаций для защиты деятельности и активов организаций, людей, других организаций и Нации от различных угроз и рисков, включая враждебные атаки, человеческие ошибки, стихийные бедствия, структурные сбои, иностранные разведывательные структуры и риски для приватности. Эти меры безопасности являются гибкими и настраиваемыми и внедряются в качестве части общеорганизационного процесса управления рисками. Меры безопасности учитывают различные требования, вытекающие из потребностей предназначения и деятельности, законов, распоряжений правительства, директив, постановлений, политики, стандартов и руководств. Наконец, сводный каталог мер рассматривает безопасность и приватность с точки зрения функциональности (т.е. стойкости функций и механизмов, обеспечиваемых мерами безопасности) и с точки зрения доверия (т.е. с точки зрения степени уверенности в безопасности или приватности, обеспечиваемой мерами безопасности). Учет функциональных возможностей и доверия помогает обеспечить, чтобы продукты и системы информационных технологий, использующие эти продукты, были в достаточной степени доверенными.

## Ключевые слова

Доверие; доступность; компьютерная безопасность; конфиденциальность; контроль; кибербезопасность; FISMA; информационная безопасность; информационная система; целостность; персональная идентификационная информация; Закон о неприкосновенности частной жизни; меры обеспечения приватности; функции приватности; требования приватности; основа управления рисками; меры безопасности; функции безопасности; требования безопасности; система; безопасность системы.

## Выражение признательности

Эта публикация была подготовлена Межведомственной рабочей группой Совместной целевой группы. В состав группы входят представители гражданского, оборонного и разведывательного сообществ. Национальный институт стандартов и технологий хотел бы выразить признательность и благодарность старшим руководителям департамента торговли , департамента обороны , Офиса директора национальной разведки, Комитета по системам национальной безопасности и членам межведомственной рабочей группы, чьи целенаправленные усилия в значительной степени способствовали подготовке этой публикации.

### Министерство обороны

Dana Deasy
*Директор по информации (CIO)*

John Sherman
*Первый заместитель CIO*

Mark Hakun
*Заместитель CIO по кибербезопасности и DoD SISO*

Kevin Dulany
*Директор по политике и партнерству в области кибербезопасности*

### Офис директора национальной разведки

Matthew A. Kozma
*Директор по информации (CIO)*

Michael E. Waschull
*Заместитель директора по информации*

Клиффорд М. Коннер
*Группа кибербезопасности и IC CISO*

Свободный
*Директор Координационного центра по безопасности*

### Национальный институт стандартов и технологий

Charles H. Romine
*Директор лаборатории информационных технологий*

Kevin Stine
*Исполняющий обязанности советника ITLпо кибербезопасности*

Matthew Scholl
*Начальник Отдела компьютерной безопасности*

Kevin Stine
*Начальник отдела прикладной кибербезопасности*

Ron Ross
*Руководитель проекта реализации FISMA*

### Комитет по системам национальной безопасности

Mark G. Hakun
*Председатель*

Susan Dorr
*Сопредседатель*

Kevin Dulany
*Три-Председатель — ведомство обороны*

Крис Джонсон
*Три-Председатель — ведомство разведки*

Вики Мичетти
*Три-Председатель — гражданские агентства*

### Объединённая экспертная группа Рабочей группы

| | | | |
|---|---|---|---|
| Victoria Pillitteri<br>*NIST, руководитель JTF* | McKay Tolboe<br>*DoD* | Dorian Pappas<br>*Intelligence Community* | Kelley Dempsey<br>*NIST* |
| Ehijele Olumese<br>*Корпорация MITRE* | Lydia Humphries<br>*Боуз Аллен Гамильтон* | Daniel Faigin<br>*Аэрокосмическая корпорация* | Naomi Lefkovitz<br>*NIST* |
| Esten Porter<br>*Корпорация MITRE* | Julie Nethery Snyder<br>*Корпорация MITRE* | Christina Sames<br>*Корпорация MITRE* | Christian Enloe<br>*NIST* |
| David Black<br>*Корпорация MITRE* | Rich Graubart<br>*Корпорация MITRE* | Peter Duspiva<br>*Разведывательное ведомство* | Kaitlin Boeckl<br>*NIST* |
| Eduardo Takamura<br>*NIST* | Ned Goren<br>*NIST* | Andrew Regenscheid<br>*NIST* | Jon Boyens<br>*NIST* |

В дополнение к вышеуказанным, специальное выражение признательности адресуется Jeff Brewer, Jim Foti и NIST веб-команде за их выдающуюся административную поддержку. Авторы также хотят выделить Kristen Baldwin, Carol Bales, John Bazile, Jennifer Besceglie, Sean Brooks, Ruth Cannatti, Kathleen Coupe, Keesha Crosby, Charles Cutshall, Ja'Nelle DeVore, Jennifer Fabius, Jim Fenton, Hildy Ferraiolo, Ryan Galluzzo, Robin Gandhi, Mike Garcia, Paul Grassi, Marc Groman, Matthew Halstead, Kevin Herms, Scott Hill, Ralph Jones, Martin Kihiko, Raquel Leone, Jason Marsico, Kirsten Moncada, Ellen Nadeau, Elaine Newton, Michael Nieles, Michael Nussdorfer, Taylor Roberts, Jasmeet Seehra, Joe Stuntz, Jeff Williams, профессиональный персонал отдела компьютерной безопасности NIST и отдела прикладной кибербезопасности, и представителей Федерального совета CIO, Федерального совета CISO, Федерального совета по приватности, Межведомственной рабочей группы по уровням мер безопасности, Рабочей группы по сотрудничеству в области безопасности и приватности и Подкомитета по управлению рисками Федерального совета по приватности за их постоянное содействие в улучшение содержания публикации. Наконец, авторы с благодарностью отмечают содействия отдельных лиц и организаций в государственном и частном секторах как на национальном, так и на международном уровне, чьи вдумчивые и конструктивные комментарии улучшили общее качество, основательность и полезность этой публикации.

**ИСТОРИЧЕСКОЕ СОДЕЙСТВИЕ СПЕЦИАЛЬНОЙ ПУБЛИКАЦИИ NIST 800-53**

Авторы хотели отметить многих лиц, которые внесли свой вклад в предыдущие версии специальной публикации 800-53 с момента ее создания в 2005 году. Они включают Marshall Abrams, Dennis Bailey, Lee Badger, Curt Barker, Matthew Barrett, Nadya Bartol, Frank Belz, Paul Bicknell, Deb Bodeau, Paul Brusil, Brett Burley, Bill Burr, Dawn Cappelli, Roger Caslow, Corinne Castanza, Mike Cooper, Matt Coose, Dominic Cussatt, George Dinolt, Randy Easter, Kurt Eleam, Denise Farrar, Dave Ferraiolo, Cita Furlani, Harriett Goldman, Peter Gouldmann, Tim Grance, Jennifer Guild, Gary Guissanie, Sarbari Gupta, Priscilla Guthrie, Richard Hale, Peggy Himes, Bennett Hodge, William Hunteman, Cynthia Irvine, Arnold Johnson, Roger Johnson, Donald Jones, Lisa Kaiser, Stuart Katzke, Sharon Keller, Tom Kellermann, Cass Kelly, Eustace King, Daniel Klemm, Steve LaFountain, Annabelle Lee, Robert Lentz, Steven Lipner, William MacGregor, Thomas Macklin, Thomas Madden, Robert Martin, Erika McCallister, Tim McChesney, Michael McEvilley, Rosalie McQuaid, Peter Mell, John Mildner, Pam Miller, Sandra Miravalle, Joji Montelibano, Douglas Montgomery, George Moore, Rama Moorthy, Mark Morrison, Harvey Newstrom, Sherrill Nicely, Robert Niemeyer, LouAnna Notargiacomo, Pat O'Reilly, Tim Polk, Karen Quigg, Steve Quinn, Mark Riddle, Ed Roback, Cheryl Roby, George Rogers, Scott Rose, Mike Rubin, Karen Scarfone, Roger Schell, Jackie Snouffer, Ray Snouffer, Murugiah Souppaya, Gary Stoneburner, Keith Stouffer, Marianne Swanson, Pat Toth, Glenda Turner, Patrick Viscuso, Joe Weiss, Richard Wilsher, Mark Wilson, John Woodward, and Carol Woody.

## Уведомление о раскрытии патентной информации

*ПРИМЕЧАНИЕ: Лаборатория информационных технологий (ITL) обратилась с просьбой о том, чтобы держатели патентных заявок, использование которых может потребоваться для соответствия с рекомендациями или требованиями настоящей публикации, представили такие патентные заявки ITL. Однако обладатели патентов не обязаны отвечать на просьбы ITL о предоставлении патентов, и ITL не проводит поиск патентов, с целью определить, какие патенты, если таковые имеются, могут применяться к этой публикации.*

*В отношение запроса(ов) на выявление патентных формул, использование которых может потребоваться для соответствия руководству или требованиям настоящей публикации по состоянию на дату публикации и в последующем, ITL не было установлено таких патентных формул.*

*ITL не утверждает и не подразумевает, что не требуются лицензии для того, чтобы избежать нарушения патентов при использовании этой публикации.*

**УПРАВЛЕНИЕ РИСКАМИ**

Организации должны проявлять *должную осмотрительность* при управлении рисками информационной безопасности и приватности. Это достигается, в частности, путем создания комплексной программы которая использует гибкость, присущую публикациям NIST, для категорирования систем, выбора и внедрения мер обеспечения безопасности и приватности, отвечающих потребностям предназначения и деятельности, оценки эффективности мер безопасности, санкционирования систем для эксплуатации и постоянного мониторинга систем. Применение должной осмотрительности и внедрение надежных и всеобъемлющих программ управления рисками информационной безопасности и приватности может способствовать соответствию применимым законам, нормативным документам, правительственным постановлениям и общегосударственным политикам. Основы управления рисками и процессы управления рисками имеют важное значение для разработки, реализации и поддержания мер защиты, необходимых для удовлетворения соответствующих потребностей и текущих угроз деятельности и активам организации, отдельным лицам, другим организациям и Нации. Использование эффективных, базирующихся на риске, процессов, процедур, методов и технологий гарантирует что информационные системы и организации обладают необходимой доверенностью и отказоустойчивостью для поддержки основных функций предназначения и деятельности, критически важной инфраструктуры США и преемственности правительства.

**ОБЩИЕ ОСНОВЫ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ**

Работая с Министерством управления и бюджета над разработкой стандартов и руководств, требуемых FISMA, NIST консультируется с федеральными агентствами, правительствами штатов, местными и племенными правительствами, и организацисми частного сектора в целях улучшения информационной безопасности и приватности, избежания ненужного и дорогостоящего дублирования усилий, и содействует обеспечению того, чтобы его публикации дополняли стандарты и руководства, используемые для защиты систем национальной безопасности. В дополнение к всеобъемлющему и прозрачному процессу публичного рассмотрения и комментирования, NIST сотрудничает с Министерством управления и бюджета, Офисом директора национальной разведки, Министерством обороны, Комитетом по системам национальной безопасности, Федеральным советом по информационным технологиям и Федеральным советом по приватности по созданию основ управления рисками (RMF) для информационной безопасности и приватности для федерального правительства. Эта общая основа обеспечивает Федеральное правительство и его подрядчиков экономичными, гибкими и последовательными путями управления рисками безопасности и приватности для деятельности и активов организаций, отдельных лиц, других организаций и Нации. Эти основы обеспечивают базис для взаимного принятия свидетельств оценки безопасности и приватности и решений по санкционированию, а также способствуют обмену информацией и сотрудничеству. NIST продолжает работать с организациями государственного и частного секторов для установления сопоставлений и взаимосвязей между стандартами и руководствами, разработанными NIST и другими организациями. NIST предполагает использовать эти выявленные ими сопоставления и пробелы для улучшения каталога мер безопасности.

**РАЗРАБОТКА ИНФОРМАЦИОННЫХ СИСТЕМ, КОМПОНЕНТОВ И СЕРВИСОВ**

С учетом уделения повышенного внимания использованию доверенных, безопасных информационных систем и обеспечению безопасности цепочек поставок, важно, чтобы организации четко и конкретно выражали свои требования к безопасности и приватности с целью получения систем, компонентов и сервисов, необходимых для успешности их предназначения и деятельности. Соответственно, эта публикация предоставляет меры в семействах «Приобретение систем и услуг» (SA) и «Управление рисками цепочки поставок» (SR), которые предназначены для разработчиков. Область мер в этих семействах включает разработку информационных систем, системных компонентов и системных сервисов, а также связанных с ними разработчиков, независимо от того, проводится ли разработка внутри организации или за ее пределами через процессы заключения контрактов и приобретения. Затронутые меры в каталоге элементов управления включают в себя SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, SA-21, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9 и SR-11.

**ИНФОРМАЦИОННЫЕ СИСТЕМЫ - ШИРОКАЯ ПЕРСПЕКТИВА**

По мере того, как мы перемещаем компьютеры к «границам», строя все более сложный мир взаимосвязанных систем и устройств, безопасность и приватность продолжают доминировать в национальном диалоге. Существует настоятельная необходимость дальнейшего укрепления базовых систем, продуктов и сервисов, от которых мы зависим в каждом секторе критически важной инфраструктуры для обеспечения того, чтобы эти системы, продукты и сервисы были достаточно доверенными и обеспечивали необходимую устойчивость для поддержки интересов экономической и национальной безопасности Соединенных Штатов. Специальная публикация NIST 800-53, редакция 5, отвечает этой потребности, применяя упреждающий и системный подход к разработке и предоставлению широкому кругу организаций государственного и частного секторов всеобъемлющего набора мер защиты безопасности и приватности для всех типов вычислительные платформы, включая вычислительные системы общего назначения, киберфизические системы, облачные системы, мобильные системы, промышленные системы управления и устройства Интернета вещей (IoT). Меры защиты включают меры безопасности и приватности для защиты критически важной деятельности и активов организаций, а также приватности отдельных лиц. Цель состоит в том, чтобы сделать системы, от которых мы зависим, более устойчивыми к атакам, ограничить ущерб от этих атак, когда они происходят, сделать системы устойчивыми, живучими и защищающими приватность отдельных лиц.

**БАЗОВЫЕ УРОВНИ МЕР**

Базовые уровни мер, которые были ранее включены в Специальную Публикацию NIST 800-53, были перемещены в Специальную публикацию NIST 800-53B. SP 800-53B SP 800-53B содержит базовые уровни мер безопасности и приватности для федеральных информационных систем и организаций В нем содержатся руководства по адаптации базовых уровней мер и разработке оверлеев для поддержки требований заинтересованных сторон и их организаций. Инструкция CNSS 1253 содержит базовые уровни мер и руководство по категорированию безопасности и выбору мер безопасности для систем национальной безопасности.

**ИСПОЛЬЗОВАНИЕ ПРИМЕРОВ В ДАННОЙ ПУБЛИКАЦИИ.**

В данной публикации примеры используются для иллюстрации, пояснения или объяснения некоторых элементов в разделах, мерах и улучшениях мер. Эти примеры носят иллюстративный характер и не предназначены для сокращения или ограничения применения мер или улучшения мер организациями.

**ФЕДЕРАЛЬНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ ВЕДЕНИЯ УЧЁТНОЙ ДОКУМЕНТАЦИИ**

Процессы управления Федеральной учётной документацией связаны с определенными требованиями и мерами информационной безопасности и приватности. Например, сотрудники отдела документации могут управлять хранением учётной документации, в том числе, когда учётная документация будет удаляться. Взаимодействие с сотрудниками отделов документации по выбору и внедрению мер безопасности и приватности, связанных с управлением учётной документации, может обеспечить согласованность и эффективность и, в конечном итоге, укрепить позицию организации в области безопасности и приватности.

## Оглавление

**ГЛАВА ОДИН** ВВЕДЕНИЕ ..... 1
1.1 НАЗНАЧЕНИЕ И ПРИМЕНИМОСТЬ ..... 2
1.2 ЦЕЛЕВАЯ АУДИТОРИЯ ..... 3
1.3 ОБЯЗАННОСТИ ОРГАНИЗАЦИЙ ..... 3
1.4 СВЯЗЬ С ДРУГИМИ ПУБЛИКАЦИЯМИ ..... 5
1.5 ИЗМЕНЕНИЯ И РАСШИРЕНИЯ ..... 5
1.6 ОРГАНИЗАЦИЯ ПУБЛИКАЦИИ ..... 5
**ГЛАВА ДВА** ОСНОВЫ ..... 7
2.1. ТРЕБОВАНИЯ И МЕРЫ ..... 7
2.2. СТРУКТУРА И ОРГАНИЗАЦИЯ МЕР ..... 8
2.3. ПОДХОДЫ К РЕАЛИЗАЦИИ МЕР ..... 11
2.4. МУРЫ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ ..... 13
2.5. ДОВЕРЕННОСТЬ И ДОВЕРИЕ ..... 14
**ГЛАВА ТРИ** МЕРЫ ..... 16
**ССЫЛКИ** ..... 374
**ПРИЛОЖЕНИЕ А** ГЛОССАРИЙ ..... 394
**ПРИЛОЖЕНИЕ В** АКРОНИМЫ ..... 424
**ПРИЛОЖЕНИЕ С** РЕЗЮМЕ МЕР ..... 428

## Резюме

По мере того, как мы перемещаем компьютеры к «границам», строя все более сложный мир взаимосвязанных систем и устройств, безопасность и приватность продолжают доминировать в национальном диалоге. В своем отчете 2017 года *Целевая группа по киберзащите* [DSB 2017] Совета по оборонным наукам (DSB) дает отрезвляющую оценку текущих уязвимостей в критически важной инфраструктуре США и информационных системах, которые поддерживают деятельность, важную для предназначения, и активы в государственном и частном секторах.

*"... Целевая группа отмечает, что киберугрозы для критически важной инфраструктуры США опережают усилия по уменьшению широко распространенных уязвимостей, так что в течение следующего десятилетия, по крайней мере, Соединенные Штаты должны в значительной степени опираться на сдерживание, чтобы противостоять киберугрозам, создаваемым наиболее способными противниками США. Очевидно, что срочно необходим более активный и системный подход к киберзащите США "...*

Существует настоятельная необходимость дальнейшего укрепления базовых информационных систем, компонентов продуктов и сервисов, от которых зависит Нация в каждом секторе критически важной инфраструктуры для того, чтобы эти системы, компоненты и сервисы были достаточно доверенными и обеспечивали необходимую устойчивость для поддержания экономической и национальной безопасности Соединенных Штатов. Это обновление Специальной публикации (SP) NIST 800-53 отвечает на требование DSB, применяя превентивный и системный подход, чтобы разработать и сделать доступным для широкого круга организаций государственного и частного секторов всеобъемлющий набор защитных мер для всех типов вычислительных платформ, включая вычислительные системы общего назначение, киберфизические системы, облачные системы, мобильные устройства, устройства Интернета вещей (IoT), системы вооружения, космические системы, системы связи, системы экологического контроля, суперкомпьютеры и промышленные системы управления. Эти защитные меры включают реализацию мер безопасности и приватности в целях защиты критически важной деятельности и активов организаций и приватности отдельных лиц. Цель состоит в том, чтобы сделать информационные системы, от которых мы зависим, более устойчивыми к проникновению, ограничить ущерб от реализации атак, сделать системы киберустойчивыми и живучими и защитить частную жизнь людей.

Редакция 5 этой основной публикации NIST представляет собой многолетнюю работу по разработке следующей генерации мер обеспечения безопасности и приватности, которые потребуются для достижения вышеуказанных целей. Он включает в себя изменения, с тем чтобы сделать меры обеспечения более удобным для различных групп потребителей (например, предприятий, выполняющих функции предназначения и деятельности; инженерных организаций, разрабатывающие информационные системы, устройства Интернета вещей и системы; и отраслевых партнеров, создающие компоненты систем, продукты и сервисы). Наиболее значительные изменения в этой публикации включают:

- сделать меры более *ориентированным на результат*, исключив из описания меры сущность, ответственную за выполнение меры (т.е. информационную систему, организацию);
- интегрирование мер информационной безопасности и приватности в единый каталог мер для информационных систем и организаций;
- создание нового семейства мер управления рисками цепочек поставок;
- отделение *процессов* выбора мер от *мер*, что позволит использовать меры сообществам с различными интересами, включая системных инженеров, архитекторов систем безопасности, разработчиков программного обеспечения, архитекторов предприятий, инженеров по безопасности и приватности систем, а также владельцев предназначения или деятельности;

- Изъятие базовых мер и руководств по адаптации из публикации и включение их в NIST SP 800-53B, *Базовые меры для информационных систем и организаций*;
- уточнение взаимосвязи между требованиями и мерами и взаимосвязи между мерами безопасности и приватности; и
- Внедрение новых, современных мер (например, мер для поддержки киберустойчивости, поддержки проектирования безопасных систем и усиления управления и подконтрольности безопасности и приватности) на основе последних данных об угрозах и кибератаках.

При отделении процесса выбора мер от мер и переноса базовых мер было исключено значительное количество руководств и другого информационного материала, ранее содержавшегося в SP 800-53. Это содержание будет перенесено в другие публикации NIST, такие как SP 800-37 (Основы управления рисками) и SP 800-53B в течение следующего цикла обновления. В ближайшем будущем NIST также планирует представить содержание SP 800-53, SP 800-53A, и SP 800-53B на веб-портале, чтобы предоставить своим клиентам интерактивный онлайн-доступ ко всм мерам, базовым мерам, оверлеям и оценочной информации.

# Пролог

*"... В процессе управления рисками лидеры должны учитывать риск для интересов США от противников, использующих киберпространство в своих интересах и от наших собственных усилий по использованию глобальной природы киберпространства для достижения целей в военных, разведывательных и бизнес операциях"...*

*... "для разработки оперативных планов необходимо оценивать сочетание угроз, уязвимостей и воздействий с целью выявления важных тенденций и принятия решения о том, где следует прилагать усилия для ликвидации или сокращения возможностей угроз; устранение или уменьшение уязвимостей; и оценивать, координировать и разрешать всех операции в киберпространстве...*

*... "Руководители всех уровней несут ответственность за обеспечение готовности и безопасности в той же степени, что и в любой другой области…"*

НАЦИОНАЛЬНАЯ СТРАТЕГИЯ ДЕЯТЕЛЬНОСТИ В КИБЕРПРОСТРАНСТВЕ

ОФИС МИНИСТРА, ОБЪЕДИНЕННЫЙ КОМИТЕТ НАЧАЛЬНИКОВ ШТАБОВ, МИНИСТЕРСТВО ОБОРОНЫ США

---

*"Сети и информационные технологии изменяют жизнь в XXI веке, меняют способы взаимодействия людей, бизнеса и правительства. Значительные улучшения в области компьютеризации, хранения данных и коммуникаций создают новые возможности для повышения нашего социального благополучия; улучшение здравоохранения и медицинского обслуживания; устранение барьеров на пути образования и занятости; и повышают эффективность во многих секторах, таких как производство, транспорт и сельское хозяйство.*

*Перспектива этих новых приложений часто проистекает из их способности создавать, накапливать, передавать, обрабатывать и архивировать информацию в массовом масштабе. Однако значительное увеличение количества собираемой и сохраняемой личной информации в сочетании с возросшей способностью анализировать ее и объединять с другой информацией порождает обоснованное опасение в отношении приватности и способности сущностей ответственно управлять этими беспрецедентными объемами данных.... Ключевой задачей этой эпохи является обеспечение того, чтобы растущие возможности по созданию, сбору, хранению и обработке огромных объемов информации не наносили ущерба основным ценностям страны....*

*... "Когда системы обрабатывают персональную информацию, собирая, анализируя, генерируя, раскрывая, храня или иным образом используя эту информацию, они могут влиять на частную жизнь отдельных лиц. Разработчики систем должны учитывать отдельных лиц в качестве заинтересованных сторон в общей разработке решения.... Проектирование с учётом приватности должно увязывать пожелания людей в отношении приватности с системными требованиями и мерами таким образом, чтобы эффективно увязывать чаяния с развитием.... "*

НАЦИОНАЛЬНАЯ СТРАТЕГИЯ ИССЛЕДОВАНИЯ ПРИВАТНОСТИ

НАЦИОНАЛЬНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ СОВЕТ, ПРОГРАММА ИССЛЕДОВАНИЙ И РАЗРАБОТОК В ОБЛАСТИ СЕТЕЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

## Изменения

Эта таблица содержит изменения, которые были включены в SP 800-53, редакция 5. Изменения могут включать исправления, разъяснения или другие незначительные изменения в публикации, которые являются редакционными или существенными по своему характеру. Любые возможные обновления для этого документа, которые еще не опубликованы в обновлении или редакции с ошибками, включая дополнительные проблемы и возможные исправления, будут опубликованы по мере их выявления; посмотрите SP 800-53, Пересмотр 5 деталей

| DATE | TYPE | REVISION | PAGE |
|---|---|---|---|
| 12-10-2020 | Editorial | Acknowledgements (ODNI): Add “Matthew A. Kozma, Chief Information Officer” | iii |
| 12-10-2020 | Editorial | Acknowledgements (ODNI): Add “Michael E. Waschull, Deputy Chief Information Officer” | iii |
| 12-10-2020 | Editorial | Acknowledgements (ODNI): Add “Clifford M. Conner, Cybersecurity Group and IC CISO” | iii |
| 12-10-2020 | Editorial | Call Out Box: Change “Special Publication 800-53B contains control baselines” to “SP 800-53B contains security and privacy control baselines” | x |
| 12-10-2020 | Editorial | Chapter One (Footnote 7): Add “[SP 800-53A]” | 1 |
| 12-10-2020 | Editorial | Section 1.4: Delete “The controls have also been mapped to the requirements for federal information systems included in [OMB A- | 5 |
| 12-10-2020 | Editorial | Section 1.4 (Footnote 23): Delete “[OMB A-130] establishes policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services.” | 5 |
| 12-10-2020 | Editorial | Section 2.4 (first paragraph): Change “personally identifiable information (PII)” to “PII” | 13 |
| 12-10-2020 | Editorial | Control AC-1a.1.: Change “organization-level; mission/business process-level; system-level” to “Organization-level; | 18 |
| 12-10-2020 | Editorial | Control AC-1 Discussion: Change “security or privacy incidents” to “security incidents or breaches” | 18 |
| 12-10-2020 | Editorial | Control Enhancement AC-3(2) Discussion: Change “authorization duties to other individuals” to “authorization duties” | 23 |
| 12-10-2020 | Editorial | Control Enhancement AC-3(9) Discussion: Change “mitigating control” to “mitigation measure” | 26 |
| 12-10-2020 | Editorial | Control Enhancement AC-3(14) Related Controls: Add “, PT-6” | 28 |
| 12-10-2020 | Editorial | Control Enhancement AC-4(17): Change “organization, system, application, service, individual” to “organization; system; application; service; individual” | 33 |
| 12-10-2020 | Editorial | Control Enhancement AC-4(25): Change “Selection (one or more:” to “Selection (one or more):” | 34 |
| 12-10-2020 | Editorial | Control AC-12: Change “conditions,” to “conditions” | 43 |
| 12-10-2020 | Editorial | Control AC-14 Discussion: Change “assignment” to “assignment operation” | 44 |
| 12-10-2020 | Editorial | Control AC-19 Discussion: Change “the organizational network” to “its network” | 52 |

# ГЛАВА ОДИН
# ВВЕДЕНИЕ

НЕОБХОДИМОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ, СИСТЕМ, ОРГАНИЗАЦИЙ И ОТДЕЛЬНЫХ ЛИЦ

Современные информационные системы[1] могут включать в себя множество вычислительных платформ (например, промышленные системы управления, вычислительные системы общего назначение, киберфизические системы, суперкомпьютеры, системы оружия, системы связи, системы контроля окружающей среды, медицинские устройства, встроенные устройства, датчики и мобильные устройства, такие как смартфоны и планшеты). Все эти платформы имеют общую основу - компьютеры со сложным оборудованием, программным обеспечением и микропрограммным обеспечением, обеспечивающие возможности, поддерживающие основные функции предназначения и деятельности организаций.[2]

Меры безопасности - эти защитные меры или контрмеры, применяемые в рамках системы или организации для защиты конфиденциальности, целостности и доступности системы и ее информации, а также для управления рисками информационной безопасности.[3] Меры приватности - это административные, технические и физические защитные меры, используемые в системе или организации для управления рисками приватности и обеспечения соответствия применимым требованиям[4]. Требования безопасности и приватности вытекают из применимых законов, правительственных распоряжений, директив, нормативных документов, политик, стандартов и потребностей предназначения в обеспечение конфиденциальности, целостности и доступности обрабатываемой, хранимой или передаваемой, информации, а также в управлении рисками для приватности.

Выбор, разработка и реализация мер безопасности и приватности[5] являются важными задачами, которые имеют значительные последствия для деятельности[6] и активов организаций, а также для благосостояния отдельных лиц и Нации. При рассмотрении вопросов управления информационной безопасностью и приватностью организациям следует ответить на несколько ключевых вопросов:

- Какие меры безопасности и приватности необходимы для удовлетворения требований безопасности и приватности, а также для надлежащего управления рисками для предназначения/деятельности или рисками для людей?
- Были ли реализованы выбранные меры или имеется ли соответствующий план?
- Каков требуемый уровень доверия (т.е. основания для доверенности) тому, что выбранные меры том виде, в каком они разработаны и внедрены, эффективны?[7]

Ответы на эти вопросы даны не изолированно, а в контексте процесса управления рисками организации, который включает выявление, оценку, реагирование и мониторинг рисков

---

[1] *Информационная система* представляет собой набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, распределения, распространения или утилизации информации [OMB A-130].

[2] Термин *организация* описывает сущность любого размера, сложности или расположения в рамках организационной структуры (например, федеральное агентство или, в зависимости от обстоятельств, любой из его оперативных элементов).

[3] Два термина *информационная безопасность и безопасность* используются синонимично в данной публикации.

[4] *Меры безопасности и приватности* определяет [OMB A-130].

[5] Меры обеспечивают защитные меры и контрмеры в процессах проектирования безопасности и приватности систем для снижения риска в течение жизненного цикла разработки систем.

[6] Деятельность организации включает предназначение, функции, имидж и репутацию.

[7] Эффективность мер безопасности и приватности определяет степень, в которой меры осуществляются правильно, работают по назначению и дают желаемый результат в отношении соблюдения установленных требований безопасности и приватности [SP 800-53A].

безопасности и приватности, связанных с ее информацией и системами, на постоянной основе.[8] Меры безопасности и приватности в настоящей публикации, рекомендуются для использования организациями для удовлетворения их требований в информационной безопасности и приватности. Каталог мер можно рассматривать как инструментарий, содержащий набор защитных мер, контрмер, технологий и процессов реагирования на риски безопасности и приватности. Эти меры используются в качестве части четко определенного процесса управления рисками, который поддерживает программы организации по информационной безопасности и приватности. В свою очередь, эти программы информационной безопасности и приватности закладывают основу для успеха функций предназначения и деятельности организаций.

Важно, чтобы ответственные должностные лица понимали риски безопасности и приватности, которые могут отрицательно сказаться на деятельности и активах организации, людях, других организациях и Нации.[9] Эти должностные лица должны также понимать текущее состояние своих программ безопасности и приватности, а также мер, планируемых или существующих для защиты информации, информационных систем и организаций, с целью принятия обоснованных суждений и инвестиций для реагирования на выявленные риски приемлемым способом. Цель состоит в том, чтобы управлять этими рисками посредством выбора и реализации мер безопасности и приватности.

## 1.1 НАЗНАЧЕНИЕ И ПРИМЕНИМОСТЬ

Эта публикация устанавливает меры для систем и организаций. Меры могут быть реализованы в любой организации или системе, которая обрабатывает, хранит или передает информацию. Использование этих мер обязательно для федеральных информационных систем[10] в соответствии с Циркуляром A-130 [OMB A-130] Министерства управления и бюджета (OMB) и положениями Акта модернизации безопасности федеральной информации[11] [FISMA], которые требуют реализации минимальных мер для защиты федеральной информации и информационных систем.[12] Эта публикация, наряду с другими вспомогательными публикациями NIST, предназначена для помощи организациям в определении мер безопасности и приватности, необходимых для управления рисками и удовлетворения требований безопасности и приватности FISMA, Закона 1974 года о неприкосновенности частной жизни [PRIVACT], политик OMB (например, [OMB A-130]) и обозначенных, кроме того, Федеральными стандартами обработки информации (FIPS). Она обеспечивает достижение этой цели, предоставляя комплексный и гибкий каталог мер безопасности и приватности для удовлетворения текущих и будущих потребностей в защите, основанных на меняющихся угрозах, уязвимостях, требованиях и технологиях. Публикация также улучшает взаимодействие между организациями, предоставляя общий лексикон, который поддерживает обсуждение концепций безопасности, приватности и управления рисками.

---

[8] Основы управления рисками в [SP 800-37] являются примером комплексного процесса управления рисками.

[9] Сюда входят риски для критически важной инфраструктуры и ключевых ресурсов, описанные в [HSPD-7].

[10] *Федеральная информационная система* - информационная система, используемая или управляемая агентством, подрядчиком агентства или другой организацией от имени агентства.

[11] Информационные системы, которые были определены в качестве систем национальной безопасности в соответствии с определением, содержащимся в разделе 3542 Закона США № 44, не подпадают под действие требований [FISMA].Однако меры обеспечения, установленные в этой публикации, могут быть выбраны для систем национальной безопасности в соответствии с другими требованиями (например, Закон о неприкосновенности частной жизни 1974 года) или с одобрения федеральных должностных лиц, осуществляющих официальные полномочия в отношении таких систем. [CNSSP 22] и [CNSSI 1253] служат руководством для систем национальной безопасности. [DODI 8510.01] содержит руководство для Министерства обороны.

[12] Хотя меры, установленные в этой публикации, являются обязательными для федеральных информационных систем и организаций, другим организациям, таким как правительства штатов, местные и племенные правительства, а также организациям частного сектора, рекомендуется рассмотреть вопрос об использовании этих руководств в соответствующих случаях. Для получения информации о федеральных базовых мерах см. [SP 800-53B].

Наконец, меры не зависят от процесса, используемого для выбора этих мер. Процесс выбора мер может быть частью общего для организации процесса управления рисками, процесса проектирования систем [SP 800-160-1],[13] Основ управления рисками [SP 800-37], Основ кибербезопасности [NIST CSF] или основ приватности[NIST PF].[14] Критерии выбора мер могут определяться и основываться на многих факторах, включая потребности предназначения и деятельности, потребности в защите заинтересованных сторон, угроз, уязвимостей и требований к соблюдению федеральных законов, правительственных распоряжений, директив, нормативных документов, политик, стандартов и руководств. Сочетание каталога мер безопасности и приватности и процесса выбора мер на основе рисков может помочь организациям соблюдать установленные требования безопасности и приватности, обеспечивать адекватную безопасность своих информационных систем и защитить приватность отдельных лиц.

## 1.2 ЦЕЛЕВАЯ АУДИТОРИЯ

Эта публикация предназначена для широкой разнообразной аудитории, включая:

- лиц, несущих ответственность за системную, информационную безопасность, приватность или управление рисками и надзор, в том числе санкционирующих должностных лиц, директоров по информации, высших должностных лиц агентств по вопросам информационной безопасности и высших должностных лиц агентств по вопросам приватности;
- лиц, ответственных за разработку систем, включая владельцев предназначения, руководителей программ, системных инженеров, инженеров по безопасности систем, инженеров по приватности, разработчиков аппаратного и программного обеспечения, системных интеграторов и сотрудников по приобретениям или закупкам;
- лиц, выполняющих обязанности по материально-техническому обеспечению или распоряжению имуществом, включая руководителей программ, сотрудников по закупкам, системных интеграторов и управляющих недвижимостью;
- лиц, отвечающих за реализацию и деятельность по обеспечению безопасности и приватности, включая владельцев предназначения или деятельности, владельцев систем, владельцев или управляющих информацией, системных администраторов, специалистов по планированию непрерывности деятельности и сотрудников по безопасности или приватности систем;
- лиц, отвечающих за оценку и мониторинг безопасности и приватности, включая аудиторов, генеральных инспекторов, оценщиков систем, оценщиков мер, независимых проверяющих и лиц и лиц, осуществляющих подтверждение соответствия, и аналитиков; и
- Коммерческих сущностей, включая отраслевых партнеров, производящих компоненты продуктов и систем, создающих технологии безопасности и приватности или предоставляющих сервисы или возможности, которые поддерживают информационную безопасность или приватность.

## 1.3 ОБЯЗАННОСТИ ОРГАНИЗАЦИЙ

Управление рисками безопасности и приватности - это сложная, многогранная задача, требующая:

- четко определенных требований к безопасности и приватности для систем и организаций;
- использования заслуживающих доверия компонентов информационных систем на основе современных аппаратных средств, микропрограммного обеспечения и процессов разработки и приобретения программного обеспечения;

[13] Управление рисками является неотъемлемой частью проектирования систем, проектирования систем безопасности и проектирования приватности.

[14] [OMB A-130] требует, чтобы федеральные агентства реализовали Основы управления рисками NIST для выбора мер для федеральных информационных систем. [EO 13800] требует, чтобы федеральные агентства внедрили *Основы повышения кибербезопасности критически важной инфраструктуры* NIST для управления рисками кибербезопасности. Основы NIST также предназначены для нефедеральных организаций в качестве факультативных ресурсов.

- строгого планирования безопасности и приватности и управления жизненным циклом разработки;
- приложения принципов и практики обеспечения безопасности и приватности систем для безопасной разработки и интеграции компонентов систем в информационные системы;
- применение практики безопасности и приватности, которая надлежащим образом документирована и интегрирована в институциональные и оперативные процессы организаций и поддерживает их; и
- постоянного мониторинга информационных систем и организаций с целью определения текущей эффективности мер, изменений в информационных системах и средах деятельности, а также состояния безопасности и приватности в масштабах всей организации.

Организации постоянно оценивают риски безопасности и приватности для деятельностии активов организаций, людей, других организаций и Нации. Риски безопасности и приватности возникают в связи с планированием и выполнением организациями функций предназначения и деятельности, вводом в действие информационных систем или продолжением работы системы. Реалистичные оценки риска требуют глубокого понимания подверженности угрозам на основе конкретных уязвимостей в информационных системах и организациях, а также вероятности и потенциального неблагоприятного воздействия успешного использования таких уязвимостей этими угрозами.[15] Оценки риска также требуют понимания рисков[16] приватности.

Чтобы учесть интересы организации по оценке и определению рисков, требования безопасности и приватности удовлетворяются знаниями и пониманием стратегии управления рисками организации.[17] Стратегия управления рисками учитывает вопросы стоимости, календарного планирования, эффективности и цепочек поставок, связанные с проектированием, разработкой, приобретением, развертыванием, эксплуатацией, обеспечением и ликвидацией систем организаций. Процесс управления рисками затем применяется для управления рисками на постоянной основе.[18]

Каталог мер безопасности и приватности может эффективно использоваться для защиты организаций, отдельных лиц и информационных систем от традиционных и постоянно развивающихся угроз и рисков приватности, возникающих при обработке персональной идентификационной информации (PII) в различных эксплуатационных, экологических и технических сценариях. Меры могут использоваться для демонстрации соответствия различным требованиям государства, организаций или ведомств по безопасности и приватности. Организации несут ответственность за выбор соответствующих мер обеспечения безопасности и приватности. для правильной реализации мер и демонстрации эффективности мер в удовлетворении требований безопасности и приватности.[19] Меры безопасности и приватности могут также использоваться при разработке специализированных *базовых ребований или оверлеев* для уникальных или специализированных приложений по предназначению или деятельности, информационных систем, проблеммных угроз, сред эксплуатации, технологий или сообществ по интересам.[20]

---

[15] [SP 800-30] содержит руководства по процессу оценки рисков.

[16] [IR 8062] вводит концепции риска приватности.

[17] [SP 800-39] содержит руководство по процессам и стратегиям управления рисками.

[18] [SP 800-37] содержит комплексный процесс управления рисками.

[19] [SP 800-53A] содержит руководства по оценке эффективности мер.

[20] [SP 800-53B] содержит руководство по адаптации базовых мер безопасности и приватности и разработке оверлеев для удовлетворения конкретных потребностей и требований заинтересованных сторон и их организаций в области защиты.

Оценка рисков организаций частично используется для информирования о процессе выбора мер безопасности и приватности. Результатом процесса выбора является согласованный набор мер безопасности и приватности, учитывающий конкретные потребности предназначения или деятельности, согласующиеся с допустимостью рисков для организации.[21] Этот процесс в максимально возможной степени сохраняет адаптивность и гибкость, необходимые организациям для устранения все более сложных и враждебных угроз, требований предназначения и деятельности, быстро меняющихся технологий, сложных цепочек поставок и многих типов сред деятельности.

## 1.4 СВЯЗЬ С ДРУГИМИ ПУБЛИКАЦИЯМИ

В этой публикации определены меры, удовлетворяющие различным наборам требований безопасности и приватности, предъявляемым к информационным системам и организациям и соответствующим и дополняющим другие признанные национальные и международные стандарты информационной безопасности и приватности. Для разработки широко применимого и технически обоснованного набора мер для информационных систем и организаций в ходе подготовки этой публикации были рассмотрены многие источники. Эти источники включали требования и меры со стороны производственных, оборонных, финансовых, медицинских, транспортных, энергетических, разведывательных, промышленных и аудиторских сообществ, а также национальных и международных организаций по стандартам. Кроме того, меры в этой публикации используются сообществом по вопросам национальной безопасности в таких публикациях, как инструкция № 1253 [CNSSI 1253], с тем чтобы предоставить рекомендации по конкретным системам, определённым как системы национальной безопасности. Каждый раз, когда возможно, меры были сопоставлены с международными стандартами, чтобы обеспечить максимальное удобство использования и применимость.[22] Связь этой публикации с другими публикациями по управлению рисками, безопасности, конфиденциальности и другим публикациям можно найти на [IMP FISMA].

## 1.5 ИЗМЕНЕНИЯ И РАСШИРЕНИЯ

Описанные в этой публикации меры безопасности и приватность представляют собой современные меры защиты отдельных лиц, информационных систем и организаций. Эти меры периодически пересматриваются и прерабатываются с учетом опыта использования мер; новых или пересмотренных законов, правительственных распоряжений, директив, нормативных документов, политик и стандартов; изменения требований к безопасности и приватности; новых угроз, уязвимостей, методов атак и обработки информации; и наличия новых технологий.

Также ожидается, что меры безопасностью и приватностью в каталоге мер со временем будут изменяться по мере изъятия, пересмотра и добавления мер. Помимо необходимости изменений, потребность в стабильности решается путем введения требования о том, чтобы предлагаемые изменения в мерах безопасности и приватности проходили через строгий и прозрачный процесс публичного рассмотрения для получения обратной связи между государственным и частным секторами и достижения консенсуса в отношении таких изменений. Процесс проверки предоставляет технически обоснованный, гибкий и стабильный набор мер безопасности и приватности для организаций, использующих каталог мер.

## 1.6 ОРГАНИЗАЦИЯ ПУБЛИКАЦИИ

Остальная часть этой специальной публикации организована следующим образом:

[21] Санкционирующие должностные лица или их назначенные представители, принимая планы безопасности и приватности, соглашаться с мерами безопасности и приватности, предлагаемыми для удовлетворения требований безопасности и приватности, предъявляемых к организациям и системам.

[22] Таблицы соответствия доступны по адресу [SP 800-53 RES].

- Глава два описывает основные концепции, связанные с мерами безопасности и приватности, включая структуру мер, порядок организации мер в консолидированном каталоге, подходы к реализации мер, взаимосвязь между мерами безопасности и приватности, а также доверенность и доверие.
- **Глава три содержит** сводный каталог мер безопасности и приватности, включая раздел обсуждения, в котором разъясняется назначение каждой меры и приводится полезная информация, касающаяся реализации и оценки мер, перечень соответствующих мер для демонстрации взаимосвязей и зависимостей между мерами, а также перечень ссылок на вспомогательные публикации, которые могут оказаться полезными для организаций.
- **Ссылки, глоссарий, акронимы** и **резюме мер** предоставляют дополнительную информацию об использовании мер безопасности и приватности.[23]

[23] Если не указано иное, все ссылки на публикации NIST относятся к последнему варианту этих публикаций.

# ГЛАВА ДВА
# ОСНОВЫ

СТРУКТУРА, ТИПЫ И ОРГАНИЗАЦИЯ МЕР БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

В этой главе представлены основные понятия, связанные с мерами безопасности и приватности, включая взаимосвязь между требованиями и мерами, структура мер, организация мер в консолидированном каталоге мер, различные подходы к реализации мер для информационных систем и организаций, взаимосвязь между мерами безопасности и приватности, важность концепций доверенности и доверия для мер безопасности и приватности, и влияние мер на создание доверенных, безопасных и устойчивых систем.

## 2.1. ТРЕБОВАНИЯ И МЕРЫ

Важно понимать взаимосвязь между требованиями и мерами. В отношении федеральных политик информационной безопасности и приватности термин "*требование*" обычно используется для обозначения обязательств по обеспечению информационной безопасности и приватности, налагаемых на организации. Например, [OMB A- 130] устанавливает требования к информационной безопасности и приватности, которые федеральные агентства должны соблюдать при управлении информационными ресурсами. Термин "*требование*" может также использоваться в более широком смысле для выражения потребностей в защите конкретной системы или организации для заинтересованных сторон. Потребности заинтересованных сторон в защите и соответствующие требования к безопасности и приватности могут быть получены из многих источников (например, законы, правительственные распоряжения, директивы, нормативные документы, политики, стандарты, потребности предназначения и деятельности или оценки рисков). Термин "*требование*", используемый в настоящем руководстве, включает требования как законов, так и политик, а также выражение более широкого набора потребностей в защите заинтересованных сторон, которые могут быть получены из других источников. Все эти требования, применяемые к системе, помогают определить необходимые характеристики системы - включая безопасность, приватность и доверие.[24]

Организации могут разделить требования к безопасности и приватности на более детальные категории в зависимости от того, где требования используются в жизненном цикле разработки системы (SDLC) и для какого назначения. Организации могут использовать термин "*требование к возможностям*" для описания возможностей, которые система или организация должны предоставить для удовлетворения потребностей в защите заинтересованных сторон. Кроме того, организации могут ссылаться на системные требования, которые относятся к конкретным компонентам аппаратных средств, программного обеспечения и микропрограммного обеспечения системы, в качестве *требований к спецификациям*, т.е. на возможности, которые реализуют все или часть мер и которые могут быть оценены (т.е. как часть процессов проверки, подтверждения соответствия, тестирования и оценки). Наконец, организации могут использовать термин "*техническое задание*" для обозначения действий, которые должны быть выполнены при эксплуатации илипри разработке систем.

[24] Характеристики системы, влияющие на безопасность и приватность, различаются и включают тип и функцию системы в терминах ее основного назначения; состав системы в терминах ее технологий, механических, физических и человеческих элементов; режимы и состояния, в которых система выполняет свои функции и сервисы; критичность или важность системы и ее составных функций и сервисов; чувствительность данных или информации, обрабатываемых, хранимых или передаваемых; последствия потери, отказа или ухудшения способности системы правильно функционировать и обеспечивать собственную защиту (т.е. самозащиту); и денежную или иную стоимость [SP 800-160-1].

*Меры* можно рассматривать как описание предохранительных и защитных возможностей, подходящих для достижения конкретных целей организации в безопасности и приватности и отражающих потребности в защите заинтересованных сторон организации. Меры выбираются и внедряются организацией в соответствии с требованиями системы. Меры могут включать административные, технические и физические аспекты. В некоторых случаях выбор и реализация мер может потребовать дополнительной спецификации со стороны организации в форме производных требований или экземпляров значений параметров мер. Производные требования и значения параметров мер могут быть необходимы для обеспечения соответствующего уровня детализации реализации для конкретных мер в SDLC.

## 2.2. СТРУКТУРА И ОРГАНИЗАЦИЯ МЕР

Меры безопасности и приватности, описанные в этой публикации, имеют четко определенную организацию и структуру. Для простоты использования в процессе выбора и спецификации мер безопасности и приватности меры разделены на 20 *семейств*.[25] Каждое семейство содержит меры, относящиеся к конкретной теме семейства. Двухсимвольный идентификатор однозначно идентифицирует каждое семейство мер (например, PS для безопасности персонала). Меры безопасности и приватности могут включить аспекты политики, надзора, наблюдения, ручных процессов и автоматизированных механизмов, которые осуществляются системами или действиями людей. В таблице 1 перечислены семейства безопасности и приватности и связанные с ними идентификаторы семейств.

**ТАБЛИЦА 1: СЕМЕЙСТВА МЕР БЕЗОПАСНОСТИ И ПРИВАТНОСТИ**

| ID | СЕМЕЙСТВО | ID | СЕМЕЙСТВО |
|---|---|---|---|
| AC | Контроль доступа | PE | Физическая защита и защита окружающей среды |
| AT | Освоение и обучение | PL | Планирование |
| AU | Аудит и подотчетность | PM | Управление программами |
| CA | Оценка, санкционирование и мониторинг | PS | Безопасность персонала |
| CM | Управление конфигурацией | PT | Обработка и прозрачность ПИИ |
| CP | Планирование на случай непредвиденных ситуаций | RA | Оценка риска |
| IA | Идентификация и аутентификация | SA | Приобретение систем и сервисов |
| IR | Реагирование на инциденты | SC | Защита систем и коммуникаций |
| MA | Поддержка | SI | Целостность систем и информации |
| MP | Защита носителей информации | SR | Управление рисками |

Семейства мер содержат базовые меры и улучшения мер, которые непосредственно связаны с их базовыми мерами. Улучшения мер либо добавляют функциональность или специфичность к базовой мере, либо увеличивают стойкость базовой меры. Улучшения мер используются в системах и средах эксплуатации, требующих большей защиты, чем защита, обеспечиваемая базовыми

[25] Из 20 семейств контроля в NIST SP 800-53, 17 приведены в соответствие с минимальными требованиями безопасности в [FIPS 200].Семейства управления программами (PM), Обработка and Transparency (PT) и Supply Chain Risk Management (SR) рассматривают рассмотрения управления программами на уровне предприятия, приватности и рисков цепочки поставок, относящихся к федеральным мандатам, возникающим с момента [FIPS 200].

мерами. Необходимость отбора и внедрения организациями улучшений мер обусловлена потенциальными неблагоприятными воздействиями на организацию или индивидуумов, а также тем, что организации нуждаются в дополнениях к базовой функциональности мер или доверию на основе оценок рисков. Выбор и реализация улучшений мер *всегда* требует выбора и реализации базовых мер.

Семейства расположены в алфавитном порядке, а меры и улучшения мер в каждом семействе расположены в числовом порядке. Порядок семейств, меры и улучшения мер *не* подразумевает логической прогрессии, уровня приоритета или важности, или порядка, в котором должны быть реализованы меры или улучшения мер. Скорее, он отражает порядок, в котором они быть включены в каталог. Обозначения мер не используются повторно при удалении меры.

Меры обеспечения безопасности и приватности имеют следующую структуру: *базовый раздел меры*, *раздел обсуждения*, *раздел связанных мер*, *раздел улучшений мер* и *раздел ссылок*. На фиг.1 показана структура типичной меры.

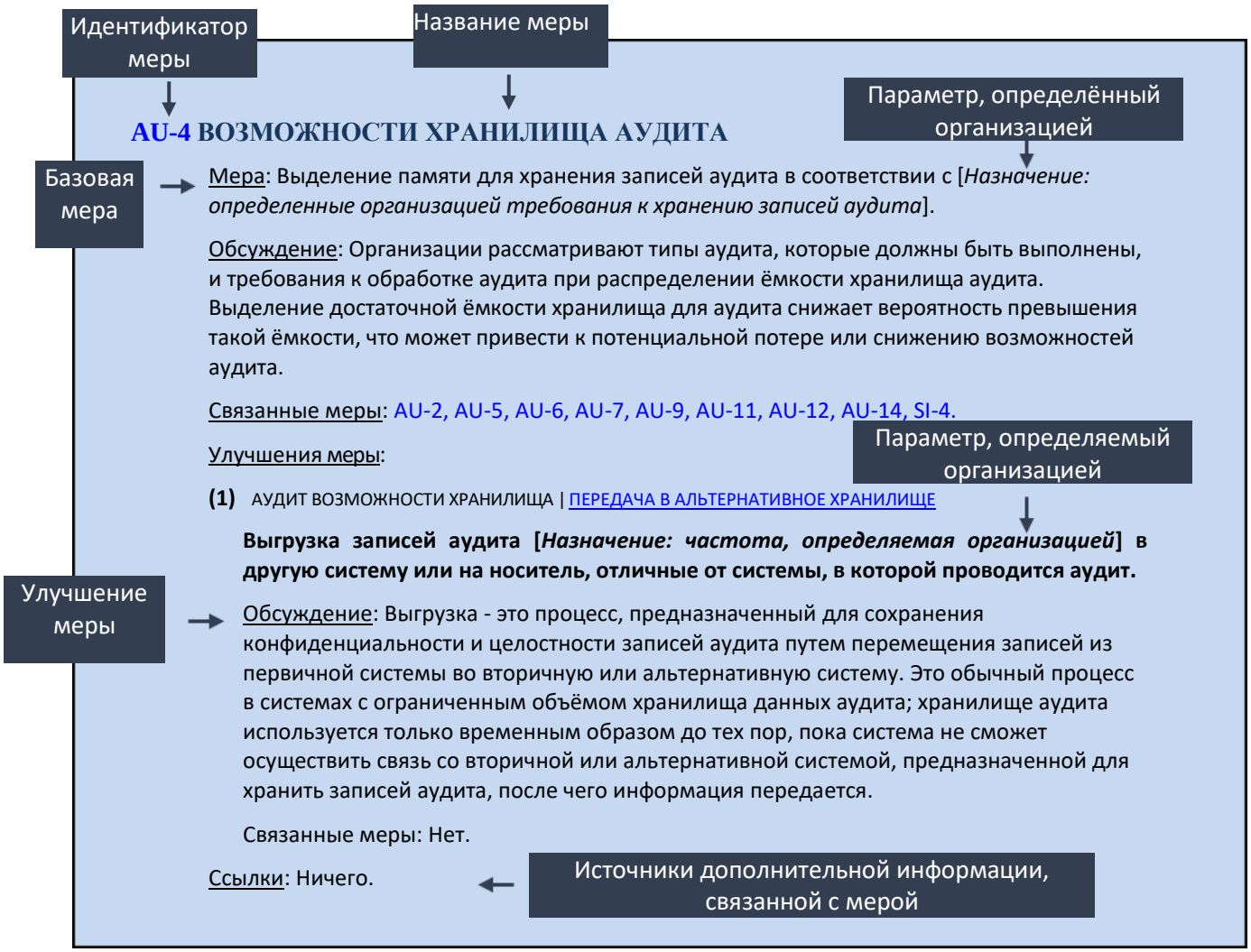


**РИСУНОК 1: СТРУКТУРА МЕРЫ**

Раздел «*Мера*» предписывает возможности по безопасности или приватности, которые должны быть реализованы. Возможности по безопасности и приватности достигаются за счет работ или действий, автоматизированных или неавтоматизированных, осуществляемых информационными

системами и организациями. Организации определяют ответственность за разработку, реализацию, оценку и мониторинг меры. Организации обладают гибкостью в реализации выбранных мер в любом способе, который удовлетворяет потребностям предназначению или деятельности организации в соответствии с законодательством, нармативными требованиями и политикой.

В разделе «*Обсуждение*» содержится дополнительная информация о мере. Организации могут использовать необходимую информацию при разработке, адаптации, внедрении, оценке или мониторинге меры. Информация содержит важные соображения для реализации мер на основе требований предназначения или деятельности, сред эксплуатации или оценки риска. Дополнительная информация также может объяснять назначение мер и часто включает примеры. Усовершенствования меры могут также включать в себя отдельный раздел обсуждения, когда информация обсуждения применима только к конкретному усовершенствованию меры.

В разделе «*Связанные меры*» представлен список мер из каталога мер, которые оказывают влияние или поддерживают реализацию конкретной меры или улучшения меры, касающиеся связанных возможностей безопасности или приватности, или на которые имеются ссылки в разделе обсуждения. Улучшения меры по своей сути связаны с их базовой мерой. Таким образом, связанные меры, на которые имеются ссылки в базовой мере, не повторяются в улучшениях меры. Однако могут существовать связанные меры, идентифицированные для улучшений меры, которые не упоминаются в базовой мере (т.е. связанная мера связана только с конкретным улучшением меры). Меры также могут быть связаны с усовершенствованиями других базовых мер. Когда мера обозначена как связанная мера, соответствующее обозначение делается в этой мере в её исходном местоположении в каталоге, чтобы проиллюстрировать двустороннюю связь. Кроме того, каждая мера в данном семействе по своей сути связана с мерой -1 (Политика и процедуры) в том же семействе. Поэтому взаимосвязь между мерой -1 и другими мерами в том же семействе не указана в разделе связанных мер для каждой меры.

В разделе «*Улучшения меры*» содержатся описания возможностей по безопасности и приватности, которые дополняют базовую меру. Улучшения меры пронумерованы последовательно в каждом мере, так что расширения могут быть легко идентифицированы при выборе улучшения для базовой меры. Каждое улучшение меры имеет короткий подзаголовок для указания предполагаемой функции или возможности, обеспечиваемой улучшением. В примере для AU-4, если выбрано улучшение меры, обозначение меры становится AU-4 (1). Числовое обозначение улучшения меры используется только для идентификации этого улучшения в пределах меры. Обозначение не указывает на стойкость улучшения меры, уровень защиты, приоритет, степень важности или какую-либо иерархическую связь между улучшениями. Улучшения меры не предназначены для независимого выбора. То есть, если выбрано улучшение меры, то также выбирается и реализуется соответствующая базовая мера.

Раздел «*Ссылки*» включает список применимых законов, политик, стандартов, руководств, вебсайтов и других полезных ссылок, которые имеют отношение к конкретной мере или улучшению меры.[26] Раздел ссылок также включает гиперссылки на публикации для получения дополнительной информации для разработки, реализации, оценки и мониторинга меры.

Для некоторых мер обеспечивается дополнительная гибкость, позволяя организациям определять конкретные значения для назначенных параметров, связанных с мерами. Гибкость достигается как часть процесса адаптации с использованием операций назначения и выбора, встроенных в меры и заключаются в скобки. Операции присвоения и выбора дают организациям возможность настраивать меры на основе требований безопасности и приватности организации. В отличие от операций

[26] Ссылки предоставляются для того, чтобы помочь организациям в понимании и реализации мер обеспечения за безопасностью и приватностью, и не предназначены для того, чтобы быть инклюзивными или полными.

назначения, которые обеспечивают полную гибкость в назначении значений параметров, операции выбора сужают масштаб потенциальных значений, предоставляя конкретный список параметров, из которых выбирают организации.

Определение параметров организации может осуществляться из различных источников, включая законы, правительственные распоряжения, директивы, нормативные документы, политики, стандарты, руководства, а также потребности предназначения или деятельности. Также важными факторами при определении значений параметров мер являются оценки рисков и допустимость рисков организации. После определения организацией значений для операций назначения и выбора они становятся частью меры. Определяемые организацией параметры мер, используемые в базовых мерах, также применяются к улучшениям мер, связанным с этими мерами. Эффективность реализации мер оценивается по полноте описания меры.

Помимо операций назначения и выбора, встроенных в меру, дополнительная гибкость достигается за счет действий «*итерация»* и *«уточнение»*. Итерация позволяет организациям использовать меру несколько раз с различными значениями назначения и выбора, давая возможность применения в различных ситуациях или при реализации нескольких политик. Например, организация может иметь несколько систем, реализующих меру, но с различными параметрами, установленными для устранения различных рисков для каждой системы и среды эксплуатации. Уточнение - это процесс предоставления для меры дополнительной информации о реализации. Уточнение также может быть использовано для ограничения области меры в сочетании с итерацией для охвата всех применимых областей (например, применение различных механизмов аутентификации к различным интерфейсам системы). Сочетание операций назначения и выбора и действий по итерации и уточнению при применении к мерам обеспечивает необходимую гибкость, позволяющую организациям удовлетворять широкий спектр требований безопасности и приватности на уровне организации, процесса предназначения и деятельности, а также на уровне внедрения системы.

**БЕЗОПАСНОСТЬ КАК ПРОБЛЕМА ПРОЕКТА**

«Обеспечение удовлетворительных мер безопасности в компьютерной системе - это… проблема проектирования системы. Для комплексной безопасности требуется сочетание аппаратных средств, программного обеспечения, средств связи, физических, кадровых и административно-процедурных мер безопасности… одних защитных мер по программному обеспечению недостаточно ».

***Отчет по программному обеспечению***
*Целевая группапо компьютерной безопасности, 1970 год*

## 2.3. ПОДХОДЫ К РЕАЛИЗАЦИИ МЕР

В Главе три определены три подхода к реализации мер безопасности : (1) *общий* (наследуемый) подход к реализации мер, (2) *системно ориентированный* подход к реализации мер, и (3) *гибридный* подход к реализации мер. Подходы к реализации мер определяют область применимости для мер, общая сущность или наследуемость мер, а также ответственность за разработку, внедрение, оценку и санкционирование мер. Каждый подход к реализации мер имеет конкретную цель и направленность, которые помогают организациям выбирать соответствующие меры безопасности, внедрять меры эффективным способом и удовлетворять требованиям безопасности и приватности. Конкретный подход к реализации мер может обеспечить снижение

затрат за счет использования возможностей безопасности и приватности в различных системах и средах эксплуатации.[27]

Общие меры безопасности - это меры безопасности, реализация которых выражается в возможности их *наследования* несколькими системами или программами. Мера считается наследуемой, когда система или программа получает защиту от реализованной меры, но разработка, реализация, оценка, авторизация и мониторинг меры осуществляется внутренней или внешней сущностью, отличной от сущности, ответственной за систему или программу. Возможности безопасности и приватности, обеспечиваемые общими мерами безопасности, могут быть унаследованы от многих источников, включая направления предназначения и деятельности, организации, анклавы, среды эксплуатации, сайты или другие системы или программы. Реализация мер безопасности в качестве общих мер безопасности может привести к появлению риска возникновения одной точки отказа.

Многие меры безопасности, необходимые для защиты информационных систем организации - в том числе многие меры физической и экологической защиты, меры безопасности персонала и меры реагирования на инциденты - наследуются и, следовательно, являются хорошими кандидатами на получение статуса общих мер. Общие меры безопасности могут также включать меры обеспечения на основе технологий, такие как меры обеспечения идентификации и аутентификации, мер обеспечения защиты границ, меры обеспечения контроля аудита и подконтрольности, а также меры контроля доступа. Затраты на разработку, реализацию, оценку, санкционирование и мониторинг могут быть амортизированы в нескольких системах, элементах организации и программах с использованием подхода реализации общих мер.

Меры безопасности, не реализованные в качестве общих мер, реализуются в виде *системно ориентированных* или *гибридных* мер безопасности. Меры безопасности, специфичные для системы, являются основной ответственностью владельца системы и санкционирующего должностного лица для данной системы. Реализация системно ориентированных мер безопасности, может привести к возникновению риска, если реализацованные меры будут не совместимы с общими мерами безопасности. Организации могут реализовать меру как *гибридную,* если одна часть меры является общей (наследуемой), а другая - специфичной для системы. Например, организация может реализовать меру CP-2, используя предварительно определенный шаблон для плана на случай непредвиденных обстоятельств для всех информационных систем организации с индивидуальной адаптацией плана владельцами систем, для использования в конкретных системах, где это необходимо. Разделение гибридных мер на общую (наследуемую) и системно лриентированную части части может варьироваться в зависимости от типов используемых информационных технологий, подхода, используемого организацией для управления ее мерами безопасности, и распределения обязанностей. Когда мера реализуется как гибридная мера, поставщик общих мер безопасности отвечает за обеспечение реализации, оценки и мониторинга *общей* части гибридной меры, а владелец системы отвечает за обеспечение реализации, оценки и мониторинга *системно ориентированной* части гибридной меры. Внедрение мер безопасности в качестве гибридных мер может создать риск, если ответственность за реализацию и текущее управление общей и системно ориентированной частями мер безопасности не определена.

Определение соответствующего подхода к реализации мер безопасности (т.е. общего, гибридного или системно ориентированного) зависит от контекста. Подход к реализации мер не может быть определен как общий, гибридный или системно ориентированный, просто основываясь на описании мер. Определение подхода к осуществлению мер может привести к значительной экономии для организаций расходов на реализацию и оценку и к более последовательному

[27] [SP 800-37] содержит дополнительное руководство по подходам к реализации мер (ранее называемым определениями мер) и по использованию различных подходов в *Основах управления рисками*.

применению мер безопасности в масштабах всей организации. Как правило, идентификация подхода к реализации мер безопасности является простой. Однако реализация требует значительного планирования и координации.

Планирование реализации подхода к мерам безопасности (т.е. общего, гибридного или системно ориентированного) лучше всего осуществлять на ранних этапах жизненного цикла разработки системы и согласовывать с сущностями, обеспечивающими меры безопасности [SP 800-37]. Например, если меры должны быть наследуемыми, требуется координация с наследующей сущностью для обеспечения того, чтобы мера удовлетворял его потребностям. Это особенно важно с учетом сущности параметров мер. Наследующая сущность не может предположить, что меры безопасности одинаковы, и уменьшить соответствующий риск для системы только потому, что идентификаторы мер (например, AC-1) одинаковы. Важно изучить параметры мер (например, операции назначения или выбора) при определении того, являются ли общие меры безопасности адекватным для снижения рисков для конкретной системы.

## 2.4. МУРЫ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

Выбор и реализация мер безопасности и приватности отражают цели программ информационной безопасности и приватности, а также способы управления этими программами их соответствующих рисков. В зависимости от обстоятельств эти цели и риски могут быть независимыми или дублирующими друг друга. Федеральные программы информационной безопасности отвечают за защиту информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения (т.е. несанкционированной работы или поведения системы) для обеспечения конфиденциальности, целостности и доступности. Эти программы также отвечают за управление рисками безопасности и обеспечение соответствия применимым требованиям безопасности. Федеральные программы приватности отвечают за управление рисками для физических лиц, связанными с созданием, сбором, использованием, обработкой, хранением, поддержкой, распространением, раскрытием или уничтожением (совместно именуемые "обработка") ПИИ и для обеспечения соответствия применимым требованиям приватности.[28] Когда система обрабатывает ПИИ, программа информационной безопасности и программа приватности несут совместную ответственность за управление рисками безопасности для ПИИ в системе. Из-за такого дублирования ответственности меры, выбранные организациями для управления рисками безопасности, будут, как правило, одинаковыми независимо от их назначения в качестве мер безопасности или приватности в базовых уровнях, программах или системных планах.

Также могут быть обстоятельства, при которых выбор и/или реализация мер или улучшений мер влияет на способность программы достигать свои цели и управлять своими соответствующими рисками. В разделе обсуждения мер могут быть выделены конкретные соображения безопасности и/или приватности, с тем чтобы организации могли принимать эти соображения во внимание при определении наиболее эффективного метода реализации мер. Однако эти соображения не являются исчерпывающими.

Например, организация может выбрать меру AU-3 (Содержание записей аудита) для поддержки мониторинга несанкционированного доступа к информационному активу, которая не включает ПИИ. Поскольку потенциальная утрата конфиденциальности информационного актива не влияет на

[28] Программы приватности могут также рассматривать риски для лиц, которые могут возникнуть в результате их взаимодействия с информационными системами, где обработка персональной информации может быть менее эффективной, чем влияние, которое система оказывает на поведение или работу людей. Такие результаты могут представлять собой риск для самостоятельности отдельных лиц, и организациям, возможно, потребуется предпринять шаги по управлению этими рисками в дополнение к рискам информационной безопасности и приватности.

приватность, основным фактором при выборе меры являются цели безопасности. Однако реализация меры в отношении мониторинга несанкционированного доступа может включать обработку ПИИ, что может привести к рискам приватности и повлиять на цели программы приватности. В разделе обсуждения, посвященном AU-3, рассматриваются факторы риска приватности, с тем чтобы организации могли принимать во внимание эти соображения, поскольку они определяют наилучший способ реализации мер. Кроме того, для поддержки управления рисками приватности можно выбрать улучшение меры AU-3 (3) (Ограничение элементов ПИИ).

Из-за перекрещивания во взаимосвязи между целями программы информационной безопасности и приватности и управлением рисками существует необходимость в тесном сотрудничестве между программами для выбора и внедрения соответствующих мер для обработки ПИИ информационных систем. Организации должны рассматривать вопрос о том, как поощрять и институционализировать взаимодействие между двумя программами для обеспечения достижения целей обеих дисциплин и надлежащего управления риски.[29]

## 2.5. ДОВЕРЕННОСТЬ И ДОВЕРИЕ

Доверенность систем, компонентов систем и системных услуг является важной частью стратегий управления рисками, разрабатываемых организациями.[30] *Доверенность,* в этом контексте, означает, что необходимо доверие к выполнению любых требований, которые могут быть необходимы для компонента, подсистемы, системы, сети, приложения, предназначения, функций деятельности, предприятия или других сущностей.[31] Требования к доверенности могут включать такие атрибуты, как надежность, функциональную надежность, производительность, отказоустойчивость, защищенность, безопасность, приватность и жизнеспособность при различных потенциальных неблагоприятных обстоятельствах в виде сбоев, опасностей, угроз и рисков приватности. Эффективные показатели доверенности имеют смысл только в том случае, если требования являются полными, четко определенными и могут быть точно оценены.

Двумя фундаментальными концепциями, влияющими на доверенность систем, являются *функциональность* и *доверие*. Функциональность определяется понятиями функций безопасности и приватности, функций, механизмов, сервисов, процедур и архитектур, реализованных в рамках систем и программ организации, а также сред, в которых работают эти системы и программы. Доверие - это мера уверенности в том, что функциональность системы реализована правильно, работает как предназначено и дает желаемый результат в отношении соответствия требованиям безопасности и приватности для системы – обладая, таким образом, способностью точно содействовать и применять установленные политики.

В общем, задача обеспечения значимого доверия тому, что система, вероятно, будет делать то, что от нее ожидается, может дополнительно решаться с помощью методов, которые упрощают или сужают анализ, например, путем повышения дисциплины, применяемой к архитектуре системы, проекту программного обеспечения, спецификациям, стилю кода и управлению конфигурацией. Меры безопасности и приватности обеспечивают функциональность и доверие. В некоторых мерах основное внимание уделяется функциональности, в то время как в других мерах основное внимание уделяется доверию. Некоторые меры могут поддерживать и функциональные возможности и доверие.

---

[29] Ресурсы для поддержки совместной работы по программе информационной безопасности и приватности доступны по адресу [SP 800-53 RES].

[30] [SP 800-160-1] содержит руководство по технике обеспечения безопасности систем и приложению принципов проектирования систем безопасности для достижения доверенности систем.

[31] См. [NEUM04].

Организации могут выбирать меры, связанные с обеспечением доверия, для определения работ по разработке системы, создания свидетельств по функциональности и поведению системы и отслеживания свидетельств для элементов системы, которые предоставляют такую функциональность или демонстрируют такое поведение. Свидетельства используются для того, чтобы получить определенную степень уверенности в том, что система удовлетворяет заявленным требованиям безопасности и приватности при поддержке функций предназначения и деятельности организаций. Меры относящиеся к доверию указаны в сводных таблицах мер в Приложении С

**СВИДЕТЕЛЬСТВА РЕАЛИЗАЦИИ МЕР**

Во время выбора и реализации мер важно, чтобы организации учитывали свидетельства (например, образцы, документацию), которые потребуются для поддержки текущих и будущих оценок мер. Такие оценки помогают определить правильно ли реализованы меры, применяются ли по предназначению, и удовлетворяют ли политикам безопасности и приватности – предоставляя, таким образом, важную информацию высшим руководителям для принятия обоснованных решений, *основанных на рисках*.

# ГЛАВА ТРИ
# МЕРЫ

МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ И УЛУЧШЕНИЯ МЕР

Этот каталог мер безопасности и приватности представляет защитные меры для систем, организаций и отдельных лиц.[32] Меры предназначены для облегчения управления рисками и соблюдения применимых федеральных законов, распоряжений, директив, нормативных документов, политик и стандартов. За редким исключением, меры безопасности и приватности в каталоге являются нейтральными с точки зрения политик, технологий и области применения, что означает, что меры сосредоточены на основных мерах, необходимых для защиты информации и приватности отдельных лиц на протяжении всего жизненного цикла информации. Несмотря на то, что меры обеспечения безопасности и приватности в основном нейтральны с точки зрения политик, технологий и области применения, это не означает, что меры не зависят от политик, технологий и области применения. Понимание политик, технологий и области применения необходимо для того, чтобы меры были актуальными при их внедрении. Использование каталога мер, нейтрального для политик, технологий и области применения, имеет много преимуществ. Он побуждает организации:

- уделять особое внимание функциям и возможностям безопасности и приватности, необходимым для успешного выполнения предназначения и деятельности, а также защите информации и приватности отдельных лиц, независимо от технологий, используемых в системах организаций;
- анализировать каждую меру безопасности и приватности на предмет её применимости к конкретным технологиям, средам эксплуатации, функциям предназначения и деятельности, а также заинтересованным сообществам; и
- определять политики безопасности и приватности в процессе адаптации мер с переменными параметрами.

В тех немногих случаях, когда конкретные технологии упоминаются в мерах, организации предупреждаются о том, что необходимость управления рисками безопасности и приватности может выходить за рамки требований одной меры, связанной с технологией. Дополнительные необходимые меры защиты получаются из других мер в каталоге. Федеральные стандарты обработки информации, специальные публикации и межведомственные/внутренние отчеты представляют рекомендации по выбору мер безопасности и приватности, которые снижают риск для конкретных технологий и отраслевых приложений, включая интеллектуальные сети, облака, здравоохранение, мобильные, промышленные системы управления и устройства Интернета вещей (IoT).[33] Публикации NIST приводятся в качестве ссылок в отношении конкретных мер в разделах 3.1-3.20.

Ожидается, что меры безопасности и приватности в каталоге со временем изменятся по мере изъятия, изменения и добавления мер. Для поддержания стабильности планов обеспечения безопасности и приватности, меры не перенумеровываются каждый раз при удалении мер. Вместо этого списки изъятых мер ведутся в каталоге мер в историческом порядке. Меры могут быть изъяты по различным причинам, в том числе когда функция или способность, обеспечиваемые мерой, включены в другую меру, мера является избыточной в отношении существующей меры или мера больше не считается необходимой или эффективной.

[32] Меры в этой публикации доступны в Интернете и могут быть получены в различных форматах. См. [NVD 800-53].
[33] Например, [SP 800-82] содержит руководство по управлению рисками и выбору мер для промышленных систем управления.

Новые меры разрабатываются на регулярной основе с использованием информации об угрозах и уязвимостях, а также информации о тактике, технологиях и процедурах, используемых противниками. Кроме того, разрабатываются новые меры, основанные на более глубоком понимании того, как уменьшить риски информационной безопасности для систем и организаций и риски для приватности отдельных лиц, возникающие в результате обработки информации. Наконец, новые меры разрабатываются на основе новых или изменяющихся требований в законах, правительственных постановлениях, нормативных документах, политиках, стандартах или руководствах. Предлагаемые изменения мер тщательно анализируются в течение каждого цикла пересмотра с учетом необходимости обеспечения стабильности мер и необходимости реагирования на изменяющиеся технологии, угрозы, уязвимости, типы атак и методы обработки. Цель состоит в том, чтобы со временем корректировать уровень информационной безопасности и приватности с учетом потребностей организаций и отдельных лиц.

Каталог мер безопасности и приватности приведен и исходной публикации на страницах 18 – 373.

# ССЫЛКИ

ЗАКОНЫ, ПОЛИТИКА, ДИРЕКТИВЫ, НОРМАТИВНЫЕ ДОКУМЕНТЫ, СТАНДАРТЫ И РУКОВОДСТВА[34]

Ссылки приведены в исходной публикации на страницах 374 – 393.

[34] Ссылки, приведенные в этом приложении, являются теми внешними публикациями, которые непосредственно поддерживают FISMA и проекты по приватности NIST. Дополнительные стандарты, руководства и межведомственные отчеты NIST также цитируются в данной публикации, в том числе ссылок в секциях применимости мер в третьей главе. Для получения доступа к этим публикациям приводятся прямые ссылки на веб-сайт NIST.

# ПРИЛОЖЕНИЕ А
# ГЛОССАРИЙ

ОБЩИЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Приложение А предоставляет определения для терминологии, используемой в Специальной публикации NIST 800-53. Где необходимо приводятся источники терминов, используемых в данной публикации. В случае отсутствия ссылок источником определения является Специальная публикация 800-53.

| | |
|---|---|
| **access control**<br>контроль доступа<br>[FIPS 201-2] | Процесс удовлетворения или отклонения конкретных запросов на получение и использование информации и соответствующих сервисов по обработке информации; и доступ к конкретным физическим объектам (например, федеральным зданиям, военным учреждениям и контрольно-пропускным пунктам). |
| **adequate security**<br>адекватная безопасность<br>[OMB A-130] | Безопасность, соразмерная с риском, следующим из потери, неправильного употребления или несанкционированного доступа к или модификации информации. Это включает в себя обеспечение того, что информация, размещенная от имени какого-либо агентства, и информационные системы и приложения, используемые этим агентством, функционировали эффективно и обеспечивали конфиденциальность, целостность и надлежащую защиту посредством применения экономичных мер безопасности. |
| **advanced persistent threat**<br>постоянная развивающаяся угроза<br>[SP 800-39] | Противник, который обладает высоким уровнем компетентности и существенными ресурсами, которые позволяют ему создавать возможности для достижения его целей при использовании множественных векторов атаки (например, кибернетическая, физическая и радиолектронное подавление). Эти цели, как правило, включают формирование и расширение точек опоры в инфраструктуре информационных технологий намеченных организаций с целью эксфильтрации информации, подрыва или воспрепятствования критическим аспектам предназначения, программ или структуры; или размещение их, чтобы выполнить эти цели в будущем. Постоянная развивающаяся угроза: (i) неоднократно преследует свои цели за длительный период времени; (ii) приспосабливается к усилиям защитников сопротивляться этому; и (iii) определяет, как поддерживать уровень взаимодействия, необходимый для выполнения её целей. |
| **agency**<br>агентство<br>[OMB A-130] | Любое исполнительное агентство или департамент, военное ведомство, корпорация федерального правительства, корпорация, контролируемая федеральным правительством, или другое учреждение в исполнительной ветви федерального правительства или любое независимое регулирующее агентство. См. *исполнительное агентство*. |
| **all Source Intelligence**<br>все источники разведки<br>[DODTERMS] | Разведывательные продукты и/или организации и действия, которые включают все источники информации, наиболее часто включая разведку людскими ресурсами, разведку получением снимков, измерительную и сигнатурную разведку, сигнальную |

| | |
|---|---|
| | разведку и открытые источники данных продукции конечной разведки. |
| **application**<br>приложение<br>[SP 800-37] | Программа, размещенная в информационной системе. |
| **assessment**<br>оценка | См. *control assessment* или *risk assessment*. |
| **assessment plan**<br>план оценки | Цели оценок мер безопасности и приватности и подробный путеводитель проведения таких оценок. |
| **assessor**<br>оценьщик | Лицо, группа или организация, ответственные за проведение оценки мер безопасности или приватности. |
| **assignment operation**<br>операция назначения | Параметр мер, позволяющий организации назначать специфическое, определяемое организацией значение для мер или улучшений мер (например, назначение списка ролей для оповещения или значение частоты тестирования).<br>*См. определяемые организацией параметры и выбираемые операции для мер*. |
| **assurance**<br>доверие<br>[ISO/ IEC 15026, адаптировано] | Основания для обоснованной уверенности в том, что утверждение о [безопасности или приватности] было или будет достигнуто.<br>*Примечание 1:* Доверие, как правило, получается относительно набора конкретных утверждений. Области и направленность таких утверждений могут различаться (например, утверждение безопасности, утверждения защищенности), а сами утверждения могут быть взаимосвязаны.<br>*Примечание 2:* Доверие получается с помощью технологий и методов, которые дают достоверные свидетельства для обоснования утверждений. |
| **attack surface**<br>поверхность атаки | Набор точек на границе системы, компонента системы или среды, в которую атакующий может попытаться проникнуть, воздействовать или извлечь данные из этой системы, компонента или среды. |
| **audit**<br>аудит<br>[CNSSI 4009] | Независимое рассмотрение и изучение записей и работ для оценки адекватности системных мер в целях обеспечения соответствия с установленными политиками и эксплуатационными процедурами. |
| **audit log**<br>журнал аудита<br>[CNSSI 4009] | Хронологическая запись действий информационной системы, включая записи доступа в систему и операций, выполнявшихся в установленный период. |
| **audit Record**<br>запись аудита | Отдельная запись в журнале аудита, относящаяся к аудитируемому событию. |
| **audit record reduction**<br>сокращение количества записей аудита | Процесс, который манипулирует собранной информацией аудита и организует её в сокращенном формате, который является более значимым для аналитиков. |
| **audit trail**<br>след аудита | Хронологическая запись, которая позволяет восстанавливать и изучать последовательность действий сопутствующих или приводящих к конкретной операции, процедуре или событию в связанной с безопасностью транзакции, от начала до окончательного результата. |

| | |
|---|---|
| **authentication**<br>аутентификация<br>[FIPS 200] | Проверка идентификационных данных пользователя, процесса или устройства, обычно как предпосылка к предоставлению доступа к ресурсам в системе. |
| **authenticator**<br>аутентификатор | Нечто, чем заявитель обладает и контролирует (обычно криптографический модуль или пароль), которое используется для аутентификации личности заявителя. Ранее это называлось токеном. |
| **authenticity**<br>аутентичность | Свойство, определяющее подлинность и возможность проверять и доверять; уверенность в законности передачи, сообщения или автора сообщения. См. *authentication*. |
| **authorization**<br>санкционирование<br>[CNSSI 4009] | Допуск к привилегиям, предоставленным пользователю, программе или процессу, или акт предоставления этих привилегий. |
| **authorization boundary**<br>граница санкционирования<br>[OMB A-130] | Все компоненты информационной системы, которая санкционирована для эксплуатации санкционирующим должностным лицом. Она не включает отдельно санкционированные системы, с которыми соединена информационная система. |
| **authorization to operate**<br>санкционирование на эксплуатацию<br>[OMB A-130] | Официальное управленческое решение, принимаемое высшим федеральным должностным лицом или лицами для того, чтобы разрешить эксплуатацию информационной системы и явно принять риск в отношении деятельности организации (включая предназначение, функции, имидж или репутацию), активов агентства, людей, других организаций и Нации, основанное на реализации согласованного набора мер безопасности и приватности. . Разрешение также распространяется на общие меры безопасности, унаследованные информационными системами агентства. |
| **authorizing official**<br>санкционирующее должностное лицо<br>[OMB A-130] | Высшее федеральное должностное лицо или руководитель с полномочием санкционировать (т.е. формально принять на себя ответственность за) эксплуатацию информационной системы или использование определенного набора общих мер безопасности на допустимом уровне риска в отношении деятельности агентства (включая предназначение, функции, имидж или репутацию), активов агентства, людей, других организаций и Нации. |
| **availability**<br>доступность<br>[FISMA] | Обеспечение своевременного и надежного доступа к и использования информации. |
| **baseline**<br>базовый набор | См. *control baseline.* |
| **baseline configuration**<br><br>[SP 800-128, Adapted] | Задокументированный набор спецификаций системы, или элемент конфигурации в системе, который был формально рассмотрен и согласован в данный момент времени и который может быть изменён только через процедуры контроля изменений. |
| **boundary**<br>граница<br>[CNSSI 4009] | Физический или логический периметр системы. См. также *границы разрешений* и *интерфейс*. |

| | |
|---|---|
| **boundary protection**<br>защита границ | Мониторинг и контроль коммуникаций на внешней границе системы, чтобы предотвратить и обнаружить злонамеренные и другие несанкционированные соединения с помощью устройств защиты границ. |
| **boundary protection device**<br>устройство защиты границ | Устройство (например, шлюз, маршрутизатор, межсетевой экран, сторож или зашифрованный туннель), которое облегчает разбирательство различных системных политик безопасности для подключенных систем или обеспечивает защиту границ. Граница может быть границей санкционирования для системы, границей сети организации или логической границей, определенной организацией. |
| **breach**<br>нарушение<br>[OMB M-17-12] | Потеря управления, компрометация, несанкционированное разглашение, несанкционированное приобретение или любое другое подобное событие, когда лицо, не являющееся авторизованным пользователем, получает доступ или потенциально получает доступ к персональной идентификационной информации; или авторизованный пользователь получает доступ к персональной идентификационной информации, которая не определена авторизацией. |
| **breadth**<br>широта [SP 800-53A] | Атрибут, связанный с методом оценки, который определяет область действия или охват объектов оценки, включенных в оценку. |
| **capability**<br>возможность | Сочетание взаимно усиливающих мер безопасности и/или приватности, реализуемых техническими, физическими и процедурными средствами. Такие меры обычно выбираются для достижения общей цели, связанной с информационной безопасностью или приватностью. |
| **central management**<br>центральное управление | Управление и реализация выбранных мер безопасности и связанных процессов в целом в организации. Центральное управление включает планирование, реализацию, оценку, санкционирование и мониторинг определенных организацией, централизованно управляемых мер и процессов безопасности. |
| **checksum**<br>контрольная сумма<br>[IETF 4949] | Значение, которое (a) вычисляется функцией, которая зависит от содержимого объекта данных, и (b) сохраняется или передается вместе с объектом для обнаружения изменений в данных. |
| **chief information officer**<br>директор по информации<br>[OMB A-130] | Высшее должностное лицо, которое консультирует и оказывает другую помощь руководителю агентства и другому высшему управленческому персоналу агентства для обеспечения приобретения ИТ и управления информационными ресурсами для агентства таким образом, чтобы достигались стратегические цели агентства и цели управления информационными ресурсами; и отвечает за обеспечение соблюдения агентством, а также своевременное, действенное и эффективное выполнение информационных политик и обязанностей по управлению информационными ресурсами, включая снижение нагрузки на общественность по сбору информации. |
| **chief information security officer**<br>директор по информационной безопасности | См. *senior agency information security officer.* |
| **classified information**<br>классифицированная информация | См. *classified national security information.* |

| | |
|---|---|
| **classified national security information**<br>классифицированная информация националной безопасности<br>[EO 13526] | Информация, которая была определена в соответствии с правительственным распоряжением (E.O.) 13526 или любым предшествующим распоряжением, требующим защиты от несанкционированного разглашения и помечена для указания ее классифицированного статуса в документальной форме. |
| **commodity service**<br>товарный сервис | Сервис информационной системы предоставляемый поставщиком коммерческих сервисов, как правило, большому и разнообразному набору потребителей. Организации, закупающие и/или получающие товарные сервисы, обладают ограниченной обозримостью структуры управления и эксплуатации поставщика, и хотя организация в состоянии согласовать соглашения об уровне обслуживания, организация, как правило, не имеет возможности требовать, чтобы поставщик реализовал конкретные меры безопасности и приватности. |
| **common carrier**<br>поставщик общих услуг связи | Телекоммуникационная компания, которая предлагает себя обществу для найма по предоставлению коммуникационных услуг связи. |
| **common control**<br>общая мера<br>[OMB A-130] | Мера безопасности или приватности, которая является наследуемой несколькими информационными системами или программами. |
| **common control provider**<br>поставщик общих мер<br>[SP 800-37] | Должностное лицо организации, ответственное за разработку, реализацию, оценку и мониторинг общих мер (то есть, мер безопасности или приватности, наследуемых системами). |
| **common criteria**<br>общие критерии<br>[CNSSI 4009] | Руководящий документ, который обеспечивает всесторонний, строгий метод для того, чтобы определить функциональные требования и требования доверия к безопасности для продуктов и систем. |
| **common secure configuration**<br>общая безопасная конфигурация<br>[SP 800-128] | Признанный стандартизированный и установленный эталон, который предусматривает конкретные безопасные установки конфигурации для данной платформы информационной технологии. |
| **compensating controls**<br>компенсационные меры | Меры безопасности или приватности, используемые вместо мер в базовых наборах мер, описанных в Специальной публикации NIST 800-53B, которые обеспечивают эквивалентную или сопоставимую защиту для информационной системы или организации. |
| **component**<br>компонент | См. *system component.* |
| **confidentiality**<br>конфиденциальность<br>[FISMA] | Сохранение установленных ограничений на доступ к и раскрытие информации, включая средства для защиты неприкосновенности частной жизни и конфиденциальной информации. |
| **configuration control**<br>управление конфигурацией<br>[SP 800-128] | Процесс контроля модификации аппаратных средств, встроенного микропрограммного обеспечения, программного обеспечения и документации, чтобы защитить информационную систему от ненадлежащих модификаций до, во время и после реализации системы. |
| **configuration item**<br>элемент конфигурации<br>[SP 800-128] | Объединение компонентов информационной системы, которое является назначенным для управления конфигурацией и рассматриваемое как отдельная сущность в процессе управления конфигурацией. |

| | |
|---|---|
| **configuration management**<br>управление конфигурацией<br>[SP 800-128] | Набор работ, направленных на то, чтобы определять и поддерживать целостность продуктов и систем информационных технологий, посредством контроля инициализации, изменения и мониторинга конфигурации этих продуктов и систем всюду по жизненному циклу разработки систем. |
| **configuration settings**<br>установки конфигурации<br>[SP 800-128] | Набор параметров, которые могут быть изменены в аппаратных средствах, программном обеспечении или встроенном микропрограммном обеспечении, влияющие на состояние безопасности и/или функциональность информационной системы. |
| **continuous monitoring**<br>непрерывный мониторинг<br>[SP 800-137] | Поддержание постоянной готовности поддерживать принятие решений по рискам организации. |
| **control**<br>мера | См. *security control or privacy control.* |
| **control assessment**<br>оценка мер<br>[SP 800-37] | Проверка или оценка мер в информационной системе или организации для определения того, в какой степени меры осуществляются правильно, работают по назначению и дают желаемый результат в отношении удовлетворения требований безопасности или приватности для системы или организации. |
| **control assessor**<br>оценщик мер | См. *assessor*. |
| **control baseline**<br>базовый набор мер<br>[SP 800-53B] | Заранее определенные наборы мер, специально собранные для удовлетворения потребностей в защите групп, организаций или сообществ по интересам. См. *базовый уровень приватности* или *базовый уровень безопасности.* |
| **control effectiveness**<br>эффективность мер | Показатель того, способствует ли мера безопасности или приватности снижению риска информационной безопасности или приватности. |
| **control enhancement**<br>улучшение мер | Расширение мер безопасности или приватности для создания дополнительных, но связанной функциональности мер, увеличения стойкости мер или повышения доверия к мерам. |
| **control inheritance**<br>наследование мер | Ситуация, в которой система или приложение получает защиту с помощью мер безопасности или приватности (или частей мер), которые разрабатываются, внедряются, оцениваются, авторизуются и контролируются сущностями, не являющимися ответственными за систему или приложение; сущностями, внутренними или внешними по отношению к организации, в которой находится система или приложение. См. *common control*. |
| **control parameter**<br>параметр меры | См. *organization-defined control parameter.* |
| **controlled area**<br>контролируемая зона | Любая область или пространство, для которого организация уверена, что обеспеченная физическая и процедурная защита |

| | |
|---|---|
| | достаточна, чтобы удовлетворить требованиям, установленным для защиты информации и/или информационной системы. |
| **controlled interface**<br>контролируемый интерфейс | Интерфейс системы с набором механизмов, которые проводят в жизнь политику безопасности и контролируют поток информации между взаимодействующими системами. |
| **controlled unclassified information**<br>контролируемая неклассифицированная информация<br>[32 CFR 2002] | Информация, которую правительство создает или которой владеет, или которую организация создает или владеет для правительства или от его имени, и которую закон, нормативный документ или общеправительственная политика требует или разрешает агентству обрабатывать с использованием мер защиты или распространения. При этом, CUI не включает классифицированную информацию или информацию, которой владеет и поддерживает в своих системах организация,не являющаяся субъектом исполнительной власти, которая не исходила, или не была создана или не принадлежала агентству исполнительной ветви власти или сущности, действующей от имени агентства. |
| **counterfeit**<br>подделка<br>[SP 800-161] | Несанкционированная копия или подмена, которая была идентифицирована, помечена и/или изменена источником, отличным от законно разрешенного источника элемента, и была искажена чтобы быть разрешенным элементом законно разрешенного источника. |
| **countermeasures**<br>контрмеры<br>[FIPS 200] | Действия, устройства, процедуры, методы или другие меры, снижающие уязвимость системы. Синоним мер безопасности и мер защиты. |
| **covert channel**<br>скрытый канал<br>[CNSSI 4009] | Непреднамеренный или несанкционированный внутрисистемный канал, который позволяет двум взаимодействующим объектам передавать информацию способом, который нарушает политику безопасности системы, но не превышает права доступа объектов. |
| **covert channel analysis**<br>анализ скрытых каналов<br>[CNSSI 4009] | Определение степени, с которой модель политики безопасности и последующие низко-уровневые описания программ могут допускать несанкционированный доступ к информации. |
| **covert storage channel**<br>скрытый канал памяти<br>[CNSSI 4009] | Особенность системы, которая позволяет одной сущности системы передавать информацию другой сущности путем прямой или косвенной записи в область памяти, которая позже прямо или косвенно считывается второй сущностью. |
| **covert timing channel**<br>скрытый канал синхронизации<br>[CNSSI 4009, Adapted] | Особенность системы, которая позволяет одной сущности системы передавать информацию другой сущности, модулируя его собственное использование системного ресурса таким образом, чтобы повлиять на время отклика системы, наблюдаемое второй сущностью. |
| **credential**<br>учётные данные<br>[SP 800-63-3] | Объект или структура данных, которые полномочно связывают идентичность посредством идентификатора или идентификаторов и (необязательно) дополнительных атрибутов, по крайней мере, с одним аутентификатором, которым владеет и управляет пользователь. |
| **critical infrastructure**<br>критическая инфраструктура<br>[USA PATRIOT] | Системы и активы, как физические, так и виртуальные, настолько жизненно важные для Соединенных Штатов, что неспособность или разрушение таких систем и активов окажут ослабляющее воздействие на безопасность, национальную экономическую |

| | |
|---|---|
| | безопасность, национальное общественное здравоохранение или защищенность или любую комбинацию этих вопросов. |
| **cross domain solution**<br>кросс-доменное решение<br>[CNSSI 1253] | Форма контролируемого интерфейса, который обеспечивает возможность для ручного и/или автоматического доступа и/или передачи информации между различными доменами безопасности. |
| **cryptographic module**<br>криптографический модуль<br>[FIPS 140-3] | Набор аппаратных средств, программного обеспечения и/или микропрограммного обеспечения, который реализует санкционированные функции безопасности (включая криптографические алгоритмы и генерацию ключей) и содержится в пределах криптографических границ. |
| **cybersecurity**<br>кибербезопасность<br>[OMB A-130] | Предотвращение ущерба, защита и восстановление компьютеров, систем электронной связи, сервисов электронной связи, проводной связи и электронной связи, включая содержащейся в них информации, для обеспечения её доступности, целостности, аутентичности, конфиденциальности и неотказуемости. |
| **cyberspace**<br>киберпространство<br>[CNSSI 4009] | Взаимозависимая сеть инфраструктур информационных технологий, включающая Интернет, телекоммуникационные сети, компьютерные системы, встраиваемые процессоры и контроллеры в критически важных отраслях. |
| **data action**<br>действия с данными<br>[IR 8062] | Системные действия, при которых обрабатывается персональная идентификационная информация. |
| **data mining**<br>интеллектуальный анализ данных | Аналитический процесс, который пытается найти корреляцию или образцы в больших наборах данных для целей обнаружения данных или знаний. |
| **de-identification**<br>деидентификация<br>[ISO 25237] | Общий термин для любого процесса удаления связи между набором идентификационных данных и субъектом данных. |
| **defense in breadth**<br>широкая защита<br>[CNSSI 4009] | Спланированный, систематизированный набор мультидисциплинарных действий, направленный на выявление, управление и снижение риска использования уязвимостей на каждой стадии жизненного цикла системы, сети или субкомпонента, включая проектирование и разработку; производство; упаковку; сборку; системную интеграцию; поставку; эксплуатацию; поддержку; и ликвидацию системы, сети или продукта. |
| **defense in depth**<br>глубокая защита | Стратегия информационной безопасности, объединяющая людей, технологии и оперативные возможности для создания разнообразных барьеров на различных уровнях и для различных предназначений организаций. |
| **depth**<br>глубина<br>[SP 800-53A] | Атрибут, связанный с методом оценки, который определяет строгость и уровень детализации, связанные с применением метода. |
| **developer**<br>разработчик | Общий термин, который включает разработчиков или производителей систем, компонентов систем или системных сервисов; интеграторов систем; поставщиков; и реселлеров |

| | |
|---|---|
| | продуктов. Разработка систем, компонентов или сервисов может осуществляться внутри организаций или через внешние сущности. |
| **digital media**<br>цифровой носитель информации | Форма электронных носителей, где данные хранятся в цифровой (как противоположность аналоговой) форме. |
| **discretionary access control**<br>дискреционный контроль доступа | Политика контроля доступа, которая применяется ко всем предметам и объектам в системе, когда политика определяет, что субъект, которому предоставлен доступ к информации, может выполнять одно или несколько следующих действий: передавать информацию другим субъектам или объектам; предоставлять свои полномочия другим субъектам; изменять атрибуты безопасности субъектов, объектов, систем или компонентов систем; выбирать атрибуты безопасности, которые должны быть связаны с вновь созданными или измененными объектами; или изменять правила, регулирующие контроль доступа. Мандатный контроль доступа ограничивает эти возможности. |
| **disassociability**<br>диссоциативность<br>[IR 8062] | Возможность обработки персональной идентификационной информации или событий без привязки к отдельным лицам или устройствам, выходящая за рамки оперативных требований к системе. |
| **domain**<br>домен | Среда или контекст, которые включают набор системных ресурсов и набор системных сущностей, которые имеют доступ к ресурсам, как определено общей политикой безопасности, моделью безопасности или архитектурой безопасности. См. домен безопасности. |
| **enterprise**<br>предприятие<br>[CNSSI 4009] | Организация с определенным предназначением/целью и определенными границами, использующая системы для выполнения этого предназначения, и с ответственностью за управление его собственными рисками и деятельностью. Предприятие может включать все или некоторые из следующих аспектов деятельности: приобретение, управление программами, людские ресурсы, управление финансами, безопасность, и системы, информацию и управление предназначением. См. organization. |
| **enterprise architecture**<br>архитектура предприятия<br>[OMB A-130] | Стратегическая основа информационных активов, которая определяет предназначение; информация, необходимая для выполнения предназначения; технологии, необходимые для выполнения предназначения; и переходные процессы для реализации новых технологий в ответ на изменение потребностей предназначения; и включает базовую архитектуру; целевую архитектуру; и план последовательности действий. |
| **environment of operation**<br>среда эксплуатации<br>[OMB A-130] | Физическое окружение, в котором информационная система обрабатывает, хранит и передает информацию. |
| **event**<br>событие<br>[SP 800-61, Уточненный] | Любое наблюдаемое явление в системе. |
| **executive agency**<br>исполнительное агентство<br>[OMB A-130] | Исполнительный департамент, определенный в 5 U.S.C., Раздел 101; военный департамент, определенный в 5 U.S.C., Раздел 102; независимое учреждение, как определено в 5 U.S.C., Раздел 104 (1); и полностью находящаяся в собственности Правительства корпорация, полностью попадающая под действие 31 U.S.C., Глава 91. |
| **exfiltration**<br>эксфильтрация | Несанкционированная передача информации из системы. |

| | |
|---|---|
| **external system (or component)**<br>внешняя система (или компонент) | Система или компонент системы, которая используется, но не является частью системы организации и в отношении которой организация не имеет прямого контроля за реализацией необходимых мер безопасности и приватности или оценки эффективности мер. |
| **external system service**<br>внешний сервис для системы | Системный сервис, предоставляемая внешним поставщиком сервисов в отношении которого организация не имеет прямого контроля за реализацией необходимых мер обеспечения безопасности и приватности или оценкой эффективности мер. |
| **external system service provider**<br>поставщик внешнего сервиса для системы | Поставщик внешних сервисов системы для организации через различные отношения между потребителем и производителем, включая совместные предприятия, деловые партнерства, механизмы аутсорсинга (т.е. через контракты, межведомственные соглашения, соглашения о направлениях деятельности), лицензионные соглашения и/или обмен по цепочкам поставок. |
| **external network**<br>внешняя сеть | Сеть не контролируемая организацией. |
| **failover**<br>отказоустойчивость | Возможность автоматического переключения (как правило, без вмешательства человека или предупреждения) на резервную или запасную систему после отказа или нештатного завершения работы ранее активной системы. |
| **federal information system**<br>федеральная информационная система<br>[OMB A-130] | Информационная система, используемая или управляемая исполнительным агентством, подрядчиком исполнительного агентства или другой организацией от имени исполнительного агентства. |
| **FIPS-validated cryptography**<br>криптография, проверенная по FIPS | Криптографический модуль, подтвержденный программой проверки криптографических модулей (CMVP) на соответствие требованиям, указанным в публикации FIPS 140-3 (с поправками). В качестве предварительного условия для проверки CMVP криптографический модуль должен использовать реализацию криптографического алгоритма, которая успешно прошла проверку в рамках Программы проверки криптографических алгоритмов (CAVP). См. *NSA-approved cryptography.* |
| **firmware**<br>встроенное микропрограммное обеспечение<br>[CNSSI 4009] | Компьютерные программы и данные, хранящиеся в аппаратном обеспечении - обычно в памяти только для чтения (ROM) или программируемой памяти только для чтения (PROM) - таким образом, что программы и данные не могут быть динамически записаны или изменены во время выполнения программ. См. *hardware* and *software*. |
| **hardware**<br>аппаратные средства<br>[CNSSI 4009] | Материальные физические компоненты системы. См. *software* and *firmware*. |
| **high-impact system**<br>система высокого воздействия<br>[FIPS 200] | Информационная система, в которой, по крайней мере, одной цели безопасности (то есть, конфиденциальности, целостности или доступности) назначено, в соответствии с FIPS Публикацией 199, значение потенциала воздействия «высокий». |
| **hybrid control**<br>гибридная мера<br>[OMB A-130] | Мера безопасности или приватности, которая реализована в информационной системе частично как общая мера безопасности и частично как специфичная для системы мера безопасности. |

| | |
|---|---|
| **identifier**<br>идентификатор<br>[FIPS 201-2] | Уникальные данные, используемые для представления личности человека и связанных с ней атрибутов. Имя или номер карты являются примерами идентификаторов.<br>Уникальная метка, используемая системой для обозначения конкретной сущности, объекта или группы. |
| **impact**<br>воздействие | Влияние потери конфиденциальности, целостности или доступности информации или системы на деятельность организации, ее активы, отдельных лиц, другие организации или нацию (включая интересы национальной безопасности США). |
| **impact value**<br>величина воздействия<br>[FIPS 199] | Оцененное наихудшее потенциальное воздействие, которое может быть результатом компрометации конфиденциальности, целостности или доступности информации, выраженная в значениях низкое, умеренное или высокое. |
| **incident**<br>инцидент<br>[FISMA] | Событие, которое фактически или неизбежно ставит под угрозу, без законных полномочий, конфиденциальность, целостность или доступность информации или информационной системы; или представляет собой нарушение или неизбежную угрозу нарушения закона, политики безопасности, процедур безопасности или политики приемлемого использования. |
| **industrial control system**<br>промышленная система управления<br>[SP 800-82] | Общий термин, охватывающий несколько типов систем управления, включая системы диспетчерского управления и сбора данных (SCADA), распределенные системы управления (DCS) и другие виды систем управления, такие как программируемые логические контроллеры (PLC), встречающиеся в промышленных секторах и критических инфраструктурах. Промышленная система управления состоит из комбинаций компонентов управления (например, электрических, механических, гидравлических, пневматических), которые действуют совместно для достижения промышленной цели (например, производство, транспортировка вещества или энергии). |
| **Information**<br>информация<br>[OMB A-130] | Любое сообщение или представление знаний, таких как факты, данные или мнения, в любой среде или форме, включая текстовые, числовые, графические, картографические, описательные, электронные или аудиовизуальные формы. |
| **information flow control**<br>контроль информационных потоков | Меры, гарантирующие, что передача информации внутри системы или организации не осуществляется в нарушение политики безопасности. |
| **information leakage**<br>утечка информации | Преднамеренная или непреднамеренная передача информации в недоверенную среду. |
| **information owner**<br>владелец информации<br>[SP 800-37] | Должностное лицо с установленными законом или исполнительными полномочиями в отношении определённой информации и ответственностью за установление мер безопасности по ее генерации, сбору, обработке, распространению и ликвидации. |
| **information resources**<br>информационные ресурсы<br>[OMB A-130] | Информация и связанные ресурсы, такие как персонал, оборудование, средства и информационные технологии. |
| **information security**<br>информационная безопасность<br>[OMB A-130] | Защита информации и систем от несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения, с целью обеспечения конфиденциальности, целостности и доступности. |

| | |
|---|---|
| **information security architecture**<br>архитектура информационной безопасности<br>[OMB A-130] | Встроенная, неотъемлемая часть архитектуры предприятия, которая описывает структуру и поведение для процессов безопасности предприятия, систем безопасности, персонала и подразделений организации, демонстрируя их соответствие с предназначением предприятия и стратегическими планами. |
| **information security policy**<br>политика информационной безопасности<br>[CNSSI 4009] | Совокупность директив, нормативных актов, правил и методов, которые предписывают, как организации должны управлять, защищать и распространять информацию. |
| **information security program plan**<br>План Программы информационной безопасности<br>[OMB A-130] | Официальный документ, содержащий обзор требований безопасности общей для организации программы информационной безопасности и описывающий меры управления программой и общие меры, существующие или планируемые для выполнения этих требований. |
| **information security risk**<br>риск информационной безопасности<br>[SP 800-30] | Риск для деятельности организации (включая предназначение, функции, имидж, репутацию), активов организации, отдельных лиц, других организаций и Нации вследствие наличия возможности для несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения информации и/или систем. |
| **information steward**<br>управляющий информацией<br>[SP 800-37] | Должностное лицо агентства с установленными законом или исполнительными полномочиями в отношении определенной информации и отвечающее за установление мер безопасности для ее создания, сбора, обработки, распространения и уничтожения. |
| **information system**<br>информационная система<br>[USC 3502] | Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, обмена, распространения или ликвидации информации. |
| **information technology**<br>информационная технология<br>[USC 11101] | Любые услуги, оборудование или взаимосвязанная система(ы) или подсистема(ы) оборудования, которые используются для автоматического получения, хранения, анализа, оценки, манипулирования, управления, перемещения, контроля, отображения, переключения, взаимообмена, передачи или приема данных или информации агентством. Для целей данного определения такие услуги или оборудование используются агентством напрямую или используются подрядчиком по контракту с агентством, который требует их использования; или в они используются значительной степени при реализации услуги или предоставлении продукта. Информационные технологии включают компьютеры, вспомогательное оборудование (включая периферийные устройства для обработки изображений, устройства ввода, вывода и хранения данных, необходимые для обеспечения безопасности и наблюдения), периферийное оборудование, предназначенное для управления центральным процессором компьютера, программное обеспечение, микропрограммы и аналогичные процедуры, услуги (включая облачные вычисления и услуги справочной службы или другие профессиональные услуги, которые поддерживают любой этап жизненного цикла оборудования или услуги), и связанные ресурсы. Информационные технологии не включают любое оборудование, которое |

| | |
|---|---|
| | приобретается подрядчиком в рамках контракта, который не требует его использования. |
| **information technology product**<br>продукт информационных технологий | См. *system component* |
| **information type**<br>тип информации<br>[FIPS 199] | Конкретная категория информации (например, приватная, медицинская, служебная, финансовая, следственная, чувствительная для подрядчиков, управления безопасностью), определенная организацией или, в некоторых случаях, конкретным законом, указом, директивой, политикой или нормативным документом. |
| **Insider**<br>инсайдер<br>[CNSSI 4009, уточнённый] | Любое лицо с авторизованным доступом к любому ресурсу организации, включая персонал, средства, информацию, оборудование, сети или системы. |
| **insider threat**<br>инсайдерская угроза<br>[CNSSI 4009, уточнённый] | Угроза того, что инсайдер, вольно или невольно, использует свой авторизованный доступ для нанесения ущерба безопасности деятельности и активам организации, отдельным лицам, другим организациям и Нации. Эта угроза может включать ущерб в результате шпионажа, терроризма, несанкционированного раскрытия информации о национальной безопасности, а также в результате потери или деградации ресурсов или возможностей организации. |
| **insider threat program**<br>Программа в отношении инсайдерских угроз<br>[CNSSI 4009, уточнённый] | Скоординированный набор возможностей, санкционированных организацией и используемых для сдерживания, обнаружения и смягчения последствий несанкционированного раскрытия информации. |
| **interface**<br>интерфейс<br>[CNSSI 4009] | Общая граница между независимыми системами или модулями, где происходит взаимодействие. |
| **integrity**<br>целостность<br>[FISMA] | Защита от ненадлежащего изменения или уничтожения информации, включающая обеспечение неотказуемости и подлинности информации. |
| **internal network**<br>внутренняя сеть | Сеть, в которой установление, поддержка и предоставление мер безопасности находится под прямым контролем сотрудников организации или подрядчиков. Криптографическая инкапсуляция или аналогичная технология безопасности, внедренная между конечными точками, контролируемыми организацией, обеспечивает тот же эффект (по крайней мере, в отношении конфиденциальности и целостности). Внутренняя сеть, как правило, принадлежит организации, но может контролироваться организацией и не принадлежать ей. |
| **label**<br>метка | См. *security label.* |
| **least privilege**<br>наименьшая привилегия<br>[CNSSI 4009] | Принцип, согласно которому архитектура безопасности разрабатывается таким образом, чтобы каждой сущности |

| | |
|---|---|
| | предоставлялись минимальные системные ресурсы и полномочия, необходимые ей для выполнения своих функций. |
| **local access**<br>локальный доступ | Доступ пользователя (или процесса, действующего от имени пользователя) к системе организации через прямое соединение без использования сети. |
| **logical access control system**<br>система логического контроля доступа | Автоматизированная система, контролирующая возможность доступа человека к одному или нескольким ресурсам компьютерной системы, таким как рабочая станция, сеть, приложение или база данных. Система логического контроля доступа требует подтверждения личности человека с помощью некоего механизма, например, PIN-кода, карты, биометрического или иного маркера. Она имеет возможность назначать разные привилегии доступа разным лицам в зависимости от их ролей и обязанностей в организации. |
| **low-impact system**<br>система низкого уровня воздействия<br>[FIPS 200] | Система, в который всем трём целям безопасности (то есть, конфиденциальности, целостности и доступности) назначено, в соответствии с FIPS Публикацией 199, значение потенциала воздействия «низкий». |
| **malicious code**<br>вредоносный код | Программное обеспечение или встроенное микропрограммное обеспечение, предназначенные для выполнения несанкционированного процесса, который может оказать негативное воздействие на конфиденциальность, целостность или доступность системы. Вирус, червь, троянский конь или другая сущность на основе кода, которая заражает хост. Шпионские программы и некоторые виды рекламного ПО также являются примерами вредоносного кода. |
| **managed interface**<br>управляемый интерфейс | Интерфейс в системе, обеспечивающий возможности защиты границ с помощью автоматизированных механизмов или устройств. |
| **mandatory access control**<br>мандатный контроль доступа | Политика управления доступом, которая однообразно применяется ко всем субъектам и объектам в системе. Субъект, которому предоставлен доступ к информации, ограничен в возможности: передавать информацию неавторизованным субъектам или объектам; предоставлять свои привилегии другим субъектам; изменять один или несколько атрибутов безопасности субъектов, объектов, системы или компонентов системы; выбирать атрибуты безопасности, которые будут связаны с вновь созданными или измененными объектами; или изменять правила управления доступом. Субъекты, определенные организацией, могут быть явно наделены привилегиями, определенными организацией (т.е. они являются доверенными субъектами), так что они не ограничены некоторыми или всеми вышеуказанными ограничениями. Мандатный контроль доступа является разновидностью недискреционного контроля доступа. |
| **marking**<br>маркировка | См. *security marking.* |
| **matching agreement**<br>соглашение о согласовании<br>[OMB A-108] | Письменное соглашение между агентством-получателем и агентством-источником (или не федеральным агентством), которое требуется в соответствии с Законом о приватности для сторон, участвующих в программе согласования. |
| **media**<br>носитель информации | Физические устройства или поверхности для записи, включая магнитные ленты, оптические диски, магнитные диски, |

| | |
|---|---|
| [FIPS 200] | микросхемы памяти высокого уровня интеграции и распечатки (исключая средства отображения), на которые записывается, хранится или печатается информация в системе. |
| **metadata**<br>метаданные | Информация, описывающая характеристики данных, включая структурные метаданные, описывающие структуру данных (т.е. формат данных, синтаксис, семантика), и описательные метаданные, описывающие содержание данных (т.е. метки безопасности). |
| **mobile code**<br>мобильный код | Программы или части программ, полученные из удаленных систем, переданные по сети и выполняемые в локальной системе без явной установки или выполнения получателем. |
| **mobile code technologies**<br>технологии мобильного кода | Программные технологии, предоставляющие механизмы для создания и использования мобильного кода. |
| **mobile device**<br>мобильные устройства | Портативное вычислительное устройство, которое имеет небольшой форм-фактор, чтобы его мог легко носить один человек; предназначено для работы без физического соединения (например, беспроводной передачи или приема информации); обладает локальным, несъемным хранилищем данных; и может работать в течение длительного времени от автономного источника питания. Мобильные устройства также могут включать в себя возможности голосовой связи, встроенные датчики, позволяющие устройству получать (например, фотографировать, снимать видео, записывать или определять местоположение) информацию, и/или встроенные функции для синхронизации локальных данных с удаленными местоположениями. В качестве примера можно привести смартфоны, планшеты и электронные книги. |
| **moderate-impact system**<br>система умеренного воздействия<br>[FIPS 200] | Система, в которой по крайней мере одной цели безопасности (т.е. конфиденциальности, целостности или доступности) назначено по FIPS Публикации 199 значение потенциала воздействия «умеренный», и ни одной цели безопасности не назначено значение потенциала воздействия «высокий». |
| **multi-factor authentication**<br>многофакторная аутентификация<br>[SP 800-63-3] | Система аутентификации или аутентификатор, которые требуют для успешной аутентификации более одного фактора аутентификации. Многофакторная аутентификация может осуществляться с помощью одного аутентификатора, предоставляющего более одного фактора, или комбинации аутентификаторов, предоставляющих различные факторы. |
| **multilevel security**<br>многоуровневая безопасность<br>[CNSSI 4009] | Концепция обработки информации с различной классификацией и категориями, которая одновременно разрешает доступ пользователями с различными уровнями допуска к информации и отказывает в доступе пользователям, которые не имеют разрешения. |
| **multiple security levels**<br>различные уровни безопасности | Возможность доверенной системы содержать и поддерживать разделение между ресурсами (в частности, хранимыми данными) различных доменов безопасности. |

[CNSSI 4009]

| | |
|---|---|
| **national security system**<br>система национальной безопасности<br>[OMB A-130] | Любая система (включая любую телекоммуникационную систему), используемая или эксплуатируемая агентством или подрядчиком агентства, или другой организацией от имени агентства - (i) функционирование, эксплуатация или использование которой включает разведывательную деятельность; включает криптологическую деятельность, связанную с национальной безопасностью; включает руководство и управление вооруженными силами; включает оборудование, являющееся неотъемлемой частью оружия или системы вооружения; или является критически важной для непосредственного выполнения военных или разведывательных задач (исключая систему, которая должна использоваться для стандартных административных и деловых приложений, например, приложений для расчета заработной платы, финансов, логистики и управления персоналом); или (ii) постоянно защищена процедурами, установленными для информации, которая была специально определена критериями, установленными Правительственным распоряжением или законом конгресса, как классифицированная в интересах национальной обороны или внешней политики. |
| **network**<br>сеть | Система, реализованная с помощью набора соединенных компонентов. Такие компоненты могут включать маршрутизаторы, концентраторы, кабели, телекоммуникационные контроллеры, центры распределения ключей и устройства технического контроля. |
| **network access**<br>сетевой доступ | Доступ пользователя (или процесса, действующего от имени пользователя) к системе через сеть, включая локальную сеть, глобальную сеть и Интернет. |
| **nonce**<br>однократно используемое число<br>[SP 800-63-3] | Значение, используемое в протоколах безопасности, которое никогда не повторяется с тем же ключом. Например, nonce, используемые в качестве вызовов в протоколах аутентификации "вызов-ответ", не повторяются до тех пор, пока не будут изменены ключи аутентификации. В противном случае существует вероятность атаки повторного использования. |
| **nondiscretionary access control**<br>не дискреционный контроль доступа | См. *mandatory access control.* |
| **nonlocal maintenance**<br>не местная поддержка | Действия поддержки, осуществляемые отдельными лицами, взаимодействующими через внутреннюю или внешнюю сеть. |
| **non-organizational user**<br>пользователь не из организации | Пользователь, который не является пользователем из организации (включая публичных пользователей). |
| **non-repudiation**<br>неотказуемость | Защита, направленная против людей, ложно отрицающих выполнение определенных действий, обеспечивающая возможность определить, совершил ли данный человек определенные действия, такие как создание информации, отправка сообщения, одобрение информации и получение сообщения. |

| | |
|---|---|
| **NSA-approved cryptography**<br>криптография, одобренная АНБ | Криптография, состоящая из одобренного алгоритма, реализации, одобренной для защиты классифицированной информации и/или контролируемой неклассифицированной информации в конкретной среде, и поддерживающей инфраструктуры управления ключами. |
| **object**<br>объект | Пассивная сущность, связанная с системой, включая устройства, файлы, записи, таблицы, процессы, программы, домены, содержащая или получающая информацию. Доступ к объекту (субъектом) подразумевает доступ к информации, которую он содержит. См. *subject*. |
| **operations security**<br>безопасность деятельности<br>[CNSSI 4009] | Систематизированный и проверенный процесс, посредством которого потенциальным противникам можно не дать возможность получить информацию о возможностях и намерениях, главным образом путём выявления, контроля и защиты неклассифицированных свидетельств планирования и выполнения чувствительных мероприятий. Процесс включает пять шагов: идентификация критической информации, анализ угроз, анализ уязвимостей, оценка рисков и применение соответствующих контрмер. |
| **organization**<br>организация<br>[FIPS 200, Adapted] | Сущность любого размера, сложности или положения в организационной структуре, включая федеральные агентства, частные предприятия, научные учреждения, правительства штатов, местные или племенные правительства или, в зависимости от обстоятельств, любые их операционные элементы. |
| **organization-defined control parameter**<br>параметр меры, определённый организацией | Переменная часть меры или улучшения меры, которая создается организацией во время процесса адаптации путем назначения определенного организацией значения или выбора значения из предопределенного списка, предоставленного как часть меры или улучшения меры. См. *assignment operation and selection operation.* |
| **organizational user**<br>пользователь организации | Сотрудник организации или человек, в отношение которого организация считает, что он имеет статус эквивалентный сотруднику, включая, например, подрядчик, приглашенный исследователь, человек, выделенный от другой организации. Политика и процедуры для того, чтобы предоставить людям статус эквивалентный сотруднику могут включать необходимые знания, отношение к организации и гражданство. |
| **overlay**<br>оверлей<br>[OMB A-130] | Спецификация мер безопасности или приватности, улучшений мер, дополнительного руководства и другой поддерживающей информации, используемой в процессе адаптации, которая предназначена для дополнения (и дальнейшего совершенствования) базовых мер безопасности. Спецификация оверлея может быть более или менее строгой, чем исходная спецификация базового набора мер безопасности, и может быть применена ко многим информационным системам. |
| **parameter** | См. *organization-defined control parameter.* |

| | |
|---|---|
| параметр | |
| **penetration testing**<br>тестирование проникновения | Методология тестирования, при которой оценщики, работающие, как правило, с конкретными ограничениями, пытаются обойти или преодолеть средства защиты системы. |
| **periods processing**<br>периодическая обработка | Режим работы системы, при котором информация различной чувствительности обрабатывается одной и той же системой в разное время, при этом между периодами система должным образом очищается или дезинфицируется. |
| **personally identifiable information**<br>персональная идентификационная информация<br>[OMB A-130] | Информация, которая может быть использована для идентификации или отслеживания личности человека, как отдельно, так и в сочетании с другой информацией, которая связана или может быть связана с конкретным человеком. |
| **personally identifiable information processing**<br>обработка персональной идентификационной информации<br>[ISO/IEC 29100, уточнённый] | Операция или набор операций, выполняемых над персональной идентификационной информацией, которые могут включать, но не ограничиваются, сбор, хранение, протоколирование, генерацию, преобразование, использование, раскрытие, передачу и утилизацию персональной идентификационной информации. |
| **personally identifiable information processing permissions**<br>разрешения на обработку персональной идентификационной информации | Требования к обработке персональной идентификационной информации или условия обработки персональной идентификационной информации. |
| **personnel security**<br>безопасность персонала | Дисциплина оценки поведения, добросовестности, рассудительности, лояльности, надежности и стабильности людей для выполнения обязанностей и ответственности, требующих доверенности. |
| **physical access control system**<br>система физического контроля доступа<br>[SP 800-116] | Электронная система, контролирующая возможность проникновения людей или транспортных средств на охраняемую территорию посредством аутентификации и авторизации в пунктах контроля доступа. |
| **plan of action and milestones**<br>план действий и вехи | Документ, в котором определены задачи, которые необходимо выполнить. В нем подробно описываются ресурсы, необходимые для выполнения элементов плана, этапы выполнения задач и запланированные даты завершения этапов. |
| **portable storage device**<br>переносное устройство хранения данных | Компонент системы, который может взаимодействовать с системой или сетью, добавляться в или удаляться из нее и основной функцией которого является хранение данных, включая текст, видео, аудио или изображения (например, оптические диски, внешние или съемные жесткие диски, внешние или съемные твердотельные диски, магнитные или оптические ленты, устройства флэш-памяти, карты флэш-памяти и другие внешние или съемные диски). |
| **potential impact**<br>потенциал воздействия<br>[FIPS 199] | Потеря конфиденциальности, целостности или доступности, можно ожидать, будет иметь ограниченное негативное воздействие (FIPS публикация 199 «низкое»); серьезное негативное воздействие (FIPS публикация 199 «умеренное»); или тяжелое или катастрофическое негативное воздействие (FIPS публикация 199 «высокое») на деятельность организации, активы организации или людей. |
| **privacy architecture**<br>архитектура приватности | Встроенная, неотъемлемая часть архитектуры предприятия, которая описывает структуру и поведение процессов защиты |

| | |
|---|---|
| [SP 800-37] | приватности предприятия, технических мер, персонала и подразделений организации, показывая их соответствие предназначению и стратегическим планам предприятия. |
| **privacy control**<br>меры приватности<br>[OMB A-130] | Административные , технические и физические меры защиты, используемые в агентстве для обеспечения соответствия применимым требованиям приватности и управления рисками приватности. |
| **privacy control baseline**<br>базовый набор мер приватности | Набор мер приватности, выбранных на основе критериев определения приватности, которые служат отправной точкой для процесса адаптации. |
| **privacy domain**<br>домен приватности | Домен в котором реализуется политика приватности. |
| **privacy impact assessment**<br>оценка воздействия на приватность<br>[OMB A-130] | Анализ того, как обрабатывается информация, чтобы убедиться в соответствии обработки применимым правовым, нормативным требованиям и требованиям политики в отношении приватности; определить риски и последствия формирования, сбора, использования, обработки, хранения, поддержания, распространения, раскрытия и утилизации информации в идентифицируемой форме в электронной информационной системе; изучение и оценка защитных и альтернативных процессов обработки информации для смягчения потенциальных проблем приватности. Оценка воздействия на приватность - это и анализ, и официальный документ с подробным описанием процесса и результатов анализа. |
| **privacy plan**<br>план приватности<br>[OMB A-130] | Официальный документ, в котором подробно описаны меры приватности, выбранные для информационной системы или среды применения, которые существуют или планируются для выполнения применимых требований приватности и управления рисками приватности, подробно описано, как меры были реализованы, а также описаны методы и метрики, которые будут использоваться для оценки мер. |
| **privacy program plan**<br>план Программы приватности<br>[OMB A-130] | Официальный документ, содержащий обзор программы приватности агентства, включая описание структуры программы приватности, ресурсов, выделенных на программу приватности, роли высшего должностного лица агентства по приватности и других должностных лиц и сотрудников по приватности, стратегических целей и задач программы приватности, а также имеющихся или планируемых мер управления программой и общих мер для выполнения применимых требований приватности и управления рисками приватности. |
| **privileged account**<br>привилегированная учетная запись | Системная учетная запись с разрешениями привилегированного пользователя. |
| **privileged command**<br>привилегированная команда | Инициированная человеком команда, выполняемая в системе, затрагивающая управление, мониторинг или администрирование системы, включая функции безопасности и связанную с ними информацию, имеющую отношение к безопасности. |

| | |
|---|---|
| **privileged user**<br>привилегированный пользователь<br>[CNSSI 4009] | Пользователь, который уполномочен (и поэтому, является доверенным) выполнять функции, связанные с безопасностью, которые обычные пользователи выполнять не уполномочены. |
| **protected distribution system**<br>защищенная система передачи<br>[CNSSI 4009] | Проводная линия или оптоволоконная система, содержащая адекватные меры защиты и/или противодействия (например, акустические, электрические, электромагнитные и физические), позволяющие использовать ее для передачи незашифрованной информации через зону меньшей чувствительности или контроля. |
| **provenance**<br>происхождение | Хронология возникновения, развития, владения, местонахождения и изменений системы или системного компонента и связанных с ними данных. Она также может включать персонал и процессы, используемые для взаимодействия или внесения изменений в систему, компонент или связанные данные. |
| **public key infrastructure**<br>инфраструктура открытых ключей<br>[CNSSI 4009] | Архитектура, организация, методы, практика и процедуры, которые в совокупности поддерживают внедрение и работу криптографической системы с открытым ключом на основе сертификатов. Структура, созданная для выпуска, обслуживания и отзыва сертификатов открытых ключей. |
| **purge**<br>уничтожение<br>[SP 800-88] | Метод санации, при котором применяются физические или логические методы, делающие невозможным восстановление целевых данных с помощью современных лабораторных методов. |
| **reciprocity**<br>соглашение о взаимности<br>[SP 800-37] | Соглашение между участвующими организациями о принятии оценок безопасности друг друга для повторного использования системных ресурсов и/или о принятии оцененное состояние безопасности друг друга в качестве общей информации. |
| **records**<br>записи<br>[OMB A-130] | Вся зарегистрированная информация, независимо от формы или характеристик, сделанная или полученная Федеральным агентством в соответствии с Федеральным законом или в связи с ведением публичной деятельности и сохраненная или предназначенная для сохранения этим агентством или его законным правопреемником в качестве свидетельства организации, функций, политики, решений, процедур, операций или других работ правительства Соединенных Штатов или из-за информационной ценности данных в них. |
| **red team exercise**<br>учения красной команды | Учения, отражающие реальные условия, которые проводятся как имитация попытки противника скомпрометировать процессы предназначения или деятельности организации и обеспечить всестороннюю оценку возможностей безопасности организации и ее систем. |
| **reference monitor**<br>диспетчер доступа | Набор проектных требований к механизму проверки доступа, который, как ключевой компонент операционной системы, обеспечивает соблюдение политики управления доступом ко всем субъектам и объектам. Механизм проверки доступа всегда вызван (т.е. полностью посредничающий), устойчив к взлому и достаточно |

| | |
|---|---|
| | мал, чтобы подвергаться анализу и тестам, полнота которых может быть гарантирована (т.е. проверяем). |
| **regrader**<br>регрейдер<br>[CNSSI 4009] | Доверенный процесс, явно уполномоченный на переклассификацию и перемаркировку данных в соответствии с определенным исключением политики. Недоверенные или неавторизованные процессы подвержены таким действиям в соответствии с политикой безопасности. |
| **remote access**<br>удаленный доступ | Доступ пользователя (или процесса, действующего от имени пользователя) к системе организации через внешнюю сеть. |
| **remote maintenance**<br>удаленная поддержка | Действия поддержки, проводимые людьми, взаимодействующими через внешнюю сеть. |
| **replay attack**<br>атака подменой<br>[SP 800-63-3] | Атака, при которой злоумышленник может воспроизвести ранее перехваченные сообщения (между законным Заявителем и Верификатором), чтобы выдать себя за этого Заявителя Верификатору или наоборот. |
| **replay resistance**<br>устойчивость к подмене | Защита от перехвата переданной информации аутентификации или контроля доступа и ее последующей повторной передачи с целью получения несанкционированного эффекта или несанкционированного доступа. |
| **resilience**<br>устойчивость<br>[OMB A-130] | Способность информационной системы работать в неблагоприятных условиях или при большой нагрузке, даже если она находится в деградированном или ослабленном состоянии, сохраняя при этом основные операционные возможности, и восстанавливаться до эффективного операционного состояния в сроки, соответствующие потребностям предназначения. |
| **restricted data**<br>данные ограниченного доступа<br>[ATOM54] | Все данные, касающиеся (i) проектирования, производства или использования атомного оружия; (ii) производства специальных ядерных материалов; или (iii) использования специальных ядерных материалов в производстве энергии, но не включающие данные, деклассифицированные или исключенные из категории данных ограниченного доступа в соответствии с разделом 142 [Закона об атомной энергии 1954 года]. |
| **risk**<br>риск<br>[OMB A-130] | Мера степени, в которой сущности угрожает потенциальное обстоятельство или событие, и обычно является функцией: (i) неблагоприятного воздействия или величины ущерба, который возникнет, если обстоятельство или событие произойдет; и (ii) вероятности возникновения. |
| **risk assessment**<br>оценка риска<br>[SP 800-39]<br>[IR 8062, уточнено] | Процесс выявления рисков для деятельности организации (включая предназначение, функции, имидж, репутацию), активов организации, отдельных лиц, других организаций и Нации, возникающих в результате эксплуатации системы.<br><br>Управление рисками включает анализ угроз и уязвимостей, а также анализ неблагоприятных последствий для отдельных лиц, возникающих в результате обработки информации, и учитывает меры по смягчению последствий, обеспечиваемые |

| | |
|---|---|
| | запланированными или уже существующими мерами безопасности и приватности. Синоним - *risk analysis*. |
| **risk executive (function)** ответственный за риски (функция) [SP 800-37] | Лицо или группа в организации, которые помогают обеспечить, чтобы соображения, связанные с риском безопасности по отдельным системам, включая решения по авторизации для этих систем, рассматривались с точки зрения всей организации в отношении общих стратегических целей и задач организации при выполнении ее функций предназначения и деятельности; и управление рисками, связанными с отдельными системами, согласовано в рамках всей организации, отражает устойчивость организации к рискам и рассматривается наряду с другими рисками организации, влияющими на успех предназначения или деятельности. |
| **risk management** управление рисками [OMB A-130] | Программа и вспомогательные процессы управления рисками для деятельности агентства (включая предназначение, функции, имидж, репутацию), активов агентства, отдельных лиц, других организаций и Нации, и включает: установление контекста для деятельности, связанной с рисками; оценку рисков; реагирование на риски после их определения; и мониторинг рисков во времени. |
| **risk mitigation** снижение рисков [CNSSI 4009] | Определение приоритетов, оценка и внедрение соответствующих мер/контрмер по снижению рисков, рекомендованных в процессе управления рисками. |
| **risk response** реагирование на риски [OMB A-130] | Принятие, предотвращение, смягчение, распределение или передача рисков для деятельности агентства, активов агентства, отдельных лиц, других организаций или Нации. |
| **risk tolerance** терпимость риска [SP 800-39] | Уровень риска или степень неопределенности, приемлемые для организации. |
| **role-based access control** ролевой контроль доступа | Управление доступом на основе ролей пользователей (т.е. наборе разрешений на доступ, которые пользователь получает на основе явного или неявного принятия на себя определенной роли). Ролевые разрешения могут наследоваться через иерархию ролей и обычно отражают разрешения, необходимые для выполнения определенных функций в организации. Данная роль может относиться к одному или нескольким лицам. |
| **runtime** время выполнения | Период, в течение которого выполняется компьютерная программа. |
| **sanitization** санация [SP 800-88] | Процесс, обеспечивающий невозможность доступа к целевым данным на носителе информации для заданного уровня усилий. Очистить, уничтожить и разрушить - это действия, которые можно предпринять для санации носителей информации. |
| **scoping considerations** соображения по сфере применения | Часть руководства по адаптации, которая предоставляет организациям конкретные соображения по применимости и внедрению мер безопасности и приватности в базовые наборы мер. Соображения включают политику или нормативное регулирование, технологии, физическую инфраструктуру, распределение компонентов системы, публичный доступ, |

| | |
|---|---|
| | масштабируемость, общий контроль, эксплуатационные или экологические условия, а также цель безопасности. |
| **security**<br>безопасность<br>[CNSSI 4009] | Состояние, возникающее в результате создания и поддержания защитных мер, которые позволяют организации выполнять свою миссию или критически важные функции, несмотря на риски, связанные с угрозами использования систем. Защитные меры могут включать в себя сочетание сдерживания, уклонения, предотвращения, обнаружения, восстановления и исправления, которые должны стать частью подхода организации к управлению рисками. |
| **security attribute**<br>атрибуты безопасности | Абстракция, представляющая основные свойства или характеристики сущности в отношении защиты информации. Обычно ассоциируется с внутренними структурами данных, включая записи, буферы и файлы в системе, и используется для реализации политик контроля доступа и управления потоками; отражает специальные инструкции по распространению, обработке или распределению; или поддерживает другие аспекты политики информационной безопасности. |
| **security categorization**<br>категорирование безопасности | Процесс определения категории безопасности для информации или системы. Методологии определения категории безопасности описаны в Инструкции CNSS 1253 для систем национальной безопасности и в Публикации FIPS 199 для систем, не относящихся к национальной безопасности. См. *security category*. |
| **security category**<br>категория безопасности<br>[OMB A-130] | Характеристика информации или информационной системы, основанная на оценке потенциального воздействия, которое потеря конфиденциальности, целостности или доступности такой информации или информационной системы окажет на деятельность агентства, активы агентства, отдельных лиц, другие организации и Нацию. |
| **security control**<br>мера безопасности<br>[OMB A-130] | Мера защиты или контрмера, предписанная для информационной системы или организации для защиты конфиденциальности, целостности и доступности системы и ее информации. |
| **security control baseline**<br>базовый уровень мер безопасности<br>[OMB A-130] | Набор минимальных мер безопасности, определенных для информационной системы с низким, умеренным или высоким уровнем воздействия. |
| **security domain**<br>домен безопасности<br>[CNSSI 4009] | Домен, реализующий политику безопасности и администрируемый отдельным органом. |
| **security functionality**<br>функциональность безопасности | Характеристики, функции, механизмы, услуги, процедуры и архитектуры, относящиеся к безопасности, реализованные в информационных системах организации или средах, в которых применяются эти системы. |
| **security functions**<br>функции безопасности | Аппаратное, программное или микропрограммное обеспечение системы, отвечающее за реализацию политики безопасности системы и поддерживающее изоляцию кода и данных, на которых основана защита. |

| | |
|---|---|
| **security impact analysis**<br>анализ воздействия на безопасность [SP 800-128] | Анализ, проводимый квалифицированным персоналом в организации для определения степени влияния изменений в системе на уровень безопасности системы. |
| **security kernel**<br>ядро безопасности<br>[CNSSI 4009] | Аппаратные, микропрограммные и программные элементы доверенной вычислительной базы, реализующие концепцию диспетчера доступа. Ядро безопасности должно опосредовать все доступы, быть защищенным от модификации и проверяемым на корректность. |
| **security label**<br>метка безопасности | Средства, используемые для связи набора атрибутов безопасности с конкретным информационным объектом как часть структуры данных для этого объекта. |
| **security marking**<br>маркирование безопасности | Средства, используемые для связи набора атрибутов безопасности с объектами в удобочитаемой форме, чтобы обеспечить организации реализацию основанных на процессе политик информационной безопасности. |
| **security objective**<br>цель безопасности<br>[FIPS 199] | Конфиденциальность, целостность или доступность. |
| **security plan**<br>план безопасности | Формальный документ, который предоставляет обзор требований безопасности для информационной системы или программы информационной безопасности и описывает имеющиеся или планируемые меры безопасности для выполнения этих требований. План безопасности системы описывает компоненты системы, входящие в ее состав, среду, в которой работает система, способы реализации требований безопасности, а также взаимодействие связи с другими системами.<br>См. *system security plan*. |
| **security policy**<br>политика безопасности<br>[SP 800-160-1, уточнено] | Набор критериев для предоставления сервисов безопасности. Набор правил, регулирующих все аспекты поведения системы и компонентов системы, относящихся к безопасности. |
| **security policy filter**<br>фильтр политики безопасности | Аппаратный и/или программный компонент, выполняющий одну или несколько следующих функций: проверка содержимого, чтобы установить тип данных представленного содержимого; проверка содержимого для анализа представленного содержимого и проверки его соответствия заданной политике; проверка вредоносного содержимого для оценки содержимого на наличие вредоносного кода; проверка подозрительной активности для оценки или выполнения содержимого безопасным способом, например, в песочнице или детонационной камере, и мониторинга подозрительной активности; или обеззараживание, очистка и преобразование содержимого, которые изменяют представленное содержимое для соответствия заданной политике. |

| | |
|---|---|
| **security requirement**<br>требование безопасности<br>[FIPS 200, уточнено] | Требование, предъявляемое к информационной системе или организации, которое вытекает из применимых законов, приказов, директив, нормативных документов, политик, стандартов, процедур или потребностей предназначения/деятельности для обеспечения конфиденциальности, целостности и доступности информации, которая обрабатывается, хранится или передается.<br>*Примечание: Требования безопасности могут использоваться в различных контекстах от высокоуровневых действий, связанных с политикой, до низкоуровневых действий, связанных с реализацией, в области разработки систем и технических дисциплинах.* |
| **security service**<br>сервис безопасности<br>[SP 800-160-1] | Возможность или функция безопасности, предоставляемые сущностью, поддерживающей одну или несколько целей безопасности. |
| **security-relevant information**<br>информация, связанная с безопасностью | Информация в системе, которая может потенциально влиять на применение функций безопасности или предоставление сервисов безопасности таким образом, что это может иметь результат в отказе проведения в жизнь политики безопасности системы или поддержки изоляции кода и данных. |
| **selection operation**<br>операция выбора | Параметр меры, который позволяет организации выбрать значение из списка предопределенных значений, предоставленных как часть меры или улучшения меры (например, выбор для ограничения действия или запрета действия).<br>См. *assignment operation* и *organization-defined control parameter.* |
| **senior agency information security officer**<br>высшее должностное лицо агентства по информационной безопасности | Должностное лицо, ответственное за выполнение обязанностей Директора по информации в соответствии с FISMA и служащее основным связующим звеном Директора по информации с санкционирующими должностными лицами агентства, владельцами информационной системы и сотрудниками безопасности информационной системы.<br>*Примечание: организации, подчиненные федеральным агентствам, могут использовать термин Высшее должностное лицо по информационной безопасности или Директор по информационной безопасности, чтобы обозначить людей, занимающих позиции с обязанностями, подобными Высшему должностному лицу агентства по информационной безопасности.* |
| **senior agency official for privacy**<br>высшее должностное лицо агентства по приватности<br>[OMB A-130] | Высшее должностное лицо, назначенное руководителем каждого агентства, которое несет ответственность за приватность в масштабах всего агентства, включая реализацию мер защиты приватности; соблюдение федеральных законов, нормативных актов и политики, касающихся приватности; управление рисками приватности в агентстве; а также центральную роль в разработке и оценке законодательных, нормативных и других предложений политики агентства. |
| **senior information security officer**<br>высшее должностное лицо по информационной безопасности | См. *Senior Agency Information Security Officer.* |
| **sensitive compartmented information** | Классифицированная информация, касающаяся или полученная из источников, методов или аналитических процессов разведки, |

| | |
|---|---|
| закрытая чувствительная информация [CNSSI 4009] | которая требуется для обработки в рамках официальных систем управления доступом, установленных директором Национальной разведки. |
| **service-oriented architecture** сервис-ориентированная архитектура | Набор принципов и методологий проектирования и разработки программного обеспечения в виде взаимодействующих сервисов. Эти сервисы представляют собой четко определенные бизнес-функции, которые строятся как программные компоненты (т.е. дискретные фрагменты кода и/или структуры данных), которые могут повторно использоваться для различных целей. |
| **shared control** совместная мера | Мера безопасности или приватности, которая реализуется в информационной системе частично как общая мера, а частично как мера для конкретной системы. См. *hybrid control*. |
| **software** программное обеспечение [CNSSI 4009] | Компьютерные программы и связанные с ними данные, которые могут быть динамически записаны или изменены в процессе выполнения. |
| **spam** спам | Злоупотребление электронными системами обмена сообщениями для беспорядочной рассылки незапрашиваемых массовых сообщений. |
| **special access program** программа специального доступа [CNSSI 4009] | Программа, установленная для конкретного класса классифицированной информации, которая налагает требования защиты и доступа, которые превышают обычно требуемые для информации на таком уровне классификации. |
| **split tunneling** раздельное туннелирование | Процесс, позволяющий удаленному пользователю или устройству установить не удаленное соединение с системой и одновременно общаться через другое соединение с ресурсом во внешней сети. Этот метод доступа к сети позволяет пользователю получить доступ к удаленным устройствам и одновременно получить доступ к неконтролируемым сетям. |
| **spyware** шпионское программное обеспечение | Программное обеспечение, которое тайно или скрытно устанавливается в информационную систему для сбора информации о людях или организациях без их ведома; разновидность вредоносного кода. |
| **subject** субъект | Лицо, процесс или устройство, порождающие информацию, для передачи между объектами или изменения состояния системы.<br>Также см. *object*. |
| **subsystem** подсистема | Основное подразделение или компонент информационной системы, состоящее из информации, информационных технологий и персонала, которое выполняет одну или более конкретные функции. |
| **supplier** поставщик | Организация или физическое лицо, заключающее соглашение с приобретателем или интегратором на поставку продукта или услуги. Сюда входят все поставщики в цепочке поставок, разработчики или производители систем, компонентов систем или системных услуг; системные интеграторы; продавцы; реселлеры продукции; и сторонние партнеры. |
| **supply chain** цепочка поставок | Связанный набор ресурсов и процессов между несколькими уровнями организаций, каждая из которых является |

| | |
|---|---|
| | приобретателем, который начинается с поиска поставщиков продукции и услуг и продолжается на протяжении всего их жизненного цикла. |
| **supply chain element**<br>элемент цепочки поставок | Организации, подразделения или инструменты, используемые для исследования и разработки, проектирования, производства, приобретения, поставки, интеграции, эксплуатации и обслуживания, а также утилизации систем и компонентов систем. |
| **supply chain risk**<br>риск цепочки поставок | Потенциал ущерба или компрометации, возникающий в результате рисков безопасности поставщиков, их цепочек поставок, а также их продукции или услуг. Риски цепочки поставок включают риски, угрозы и уязвимости, связанные с продуктами и услугами, проходящими через цепочку поставок, а также риски, угрозы и уязвимости цепочки поставок. |
| **supply chain risk assessment**<br>оценка риска цепочки поставок | Систематическое изучение рисков цепочки поставок, вероятности их возникновения и потенциальных последствий. |
| **supply chain risk management**<br>управление риском цепочки поставок | Систематический процесс управления рисками, угрозами и уязвимостями цепочки поставок по всей цепочке поставок и разработка стратегий реагирования на риски, возникающие в результате деятельности поставщика, поставляемых продуктов и услуг или цепочки поставок. |
| **system**<br>система<br>[CNSSI 4009] | Любая организованная совокупность ресурсов и процедур, объединенных и регулируемых взаимодействием или взаимозависимостью для выполнения набора определенных функций.<br>*Примечание: Системы также включают специализированные системы, такие как системы промышленного управления, системы телефонной коммутации и АТС, а также системы экологического контроля.* |
| [ISO 15288] | Сочетание взаимодействующих элементов, организованных для достижения одной или нескольких заявленных целей.<br>*Примечание 1: Существует множество типов систем. Примеры включают: информационные системы общего и специального назначения; командные системы, системы управления и связи; криптографические модули; центральные процессоры и графические процессорные платы; промышленные системы управления; системы управления полетом; системы управления оружием, целеуказанием и огнем; медицинские приборы и системы лечения; системы финансовых, банковских и торговых операций; системы социальных сетей.*<br>*Примечание 2: Взаимодействующие элементы в определении системы включают аппаратные средства, программное обеспечение, данные, людей, процессы, объекты, материалы и физические объекты природного происхождения.*<br>*Примечание 3: Система систем входит в определение системы.* |
| **system component**<br>компонент системы<br>[SP 800-128] | Дискретный идентифицируемый актив информационной технологии, который представляет собой строительный блок системы и может включать аппаратное, программное и микропрограммное обеспечение. |
| **system of records**<br>система записей<br>[USC 552] | Группа любых записей, находящихся под контролем какого-либо агентства, из которых информация извлекается по имени человека или по какому-либо идентифицирующему номеру, символу или другой идентифицирующей особенности, присвоенной человеку. |

| | |
|---|---|
| **system of records notice**<br>уведомление о системе записей [OMB A-108] | Уведомление(я), публикуемое(ые) агентством в *Федеральном регистре* при создании и/или изменении системы записей, описывающее существование и характер системы. |
| **system owner (or program manager)**<br>владелец системы (или руководитель программы) | Должностное лицо, ответственное в общем за закупку, разработку, интеграцию, модификацию, эксплуатацию и обслуживание системы. |
| **system security officer**<br>сотрудник безопасности системы<br>[SP 800-37] | Лицо, на которое возложена ответственность за поддержание соответствующего состояния безопасности применения системы или программы. |
| **system security plan**<br>план безопасности системы | См. *security plan* |
| **system service**<br>системный сервис | Возможность, предоставляемая системой, которая облегчает обработку, хранение или передачу информации. |
| **system-related security risk**<br>риск безопасности, связанный с системой<br>[SP 800-30] | Риск, возникающий в результате потери конфиденциальности, целостности или доступности информации или систем и учитывающий воздействие на организацию (включая активы, предназначение, функции, имидж или репутацию), отдельных лиц, другие организации и Нацию. См. *risk*. |
| **system-specific control**<br>мера, специфическая для системы<br>[OMB A-130] | Мера безопасности или приватности для информационной системы, которая реализуется на уровне системы и не наследуется никакой другой информационной системой. |
| **systems engineering**<br>проектирование систем<br>[SP 800-160-1] | Инженерная дисциплина, в задачи которой входит создание и выполнение междисциплинарного процесса для обеспечения удовлетворения потребностей заказчиков и всех других заинтересованных сторон высококачественным, надежным, экономически эффективным и планомерным способом на протяжении всего жизненного цикла системы. |
| **systems security engineering**<br>проектирование безопасности систем<br>[SP 800-160-1] | Специальная инженерная область, тесно связанная с проектированием систем. В ней применяются научные, инженерные принципы и принципы обеспечения доверия к безопасности информации для создания доверенных систем, удовлетворяющих требованиям заинтересованных сторон в пределах установленной допустимой степени риска. |
| **tailored control baseline**<br>адаптированный базовый уровень мер | Набор мер, который является результатом применения руководства по адаптации к базовому уровню мер. См. *tailoring*. |
| **tailoring**<br>адаптация | Процесс, посредством которого базовые уровни мер безопасности изменяются путем: определения и назначения общих мер, приложения объектовых особенностей при применении и реализации базовых мер, выбора компенсирующих мер безопасности, назначения конкретных значений определенным организацией параметрам мер безопасности, дополнения базовых наборов дополнительными мерами безопасности или улучшениями мер, а также предоставления дополнительной уточняющей информации для реализации мер. |

| | |
|---|---|
| **tampering**<br>фальсификация<br>[CNSSI 4009] | Преднамеренное, но несанкционированное действие, приводящее к изменению систем, компонентов систем, их предполагаемого поведения или данных. |
| **threat**<br>угроза<br>[SP 800-30] | Любое обстоятельство или событие, способное негативно повлиять на деятельность организации, ее активы, отдельных лиц, другие организации или Нацию через систему посредством несанкционированного доступа, уничтожения, раскрытия, модификации информации и/или отказа в обслуживании. |
| **threat assessment**<br>оценка угроз<br>[CNSSI 4009] | Формальное описание и оценка угрозы для информационной системы. |
| **threat modeling**<br>моделирование угроз<br>[SP 800-154] | Форма оценки риска, которая моделирует аспекты атаки и защиты логической сущности, такой как часть данных, приложение, хост, система или среда. |
| **threat source**<br>источник угрозы<br>[FIPS 200] | Намерение и метод, направленные на преднамеренное использование уязвимости, или ситуация и метод, которые могут случайно вызвать уязвимость. См. *threat agent* |
| **transmission**<br>трансмиссия<br>[CNSSI 4009] | Состояние, возникающее при электронной передаче информации из одного места в одно или несколько других мест. |
| **trusted path**<br>доверенный путь | Механизм, посредством которого пользователь (через устройство ввода данных) может напрямую взаимодействовать с функциями безопасности системы с необходимым доверием для поддержки политики безопасности системы. Этот механизм может быть активирован только пользователем или функциями безопасности системы и не может быть имитирован недоверенным программным обеспечением. |
| **trustworthiness**<br>доверенность<br>[CNSSI 4009] | Атрибут человека или предприятия, обеспечивающий уверенность других в квалификации, возможностях и надежности данной сущности для выполнения конкретных задач и возложенных на неё обязанностей. |
| **trustworthiness (system)**<br>доверенность (системы) | Степень, до которой информационная система (включая компоненты информационных технологий, используемые для создания системы), как можно ожидать, сохранит конфиденциальность, целостность и доступность информации, обрабатываемой, хранимой или передаваемой системой, во всем спектре угроз. Считается, что доверенная информационная система работает в пределах установленных уровней риска, несмотря на нарушения в окружающей среде, человеческие ошибки, структурные отказы и целенаправленные атаки, которые, как ожидается, будут происходить в среде ее функционирования. |
| **user**<br>пользователь | Человек, или (системный) процесс, действующий от имени человека, уполномоченный на доступ к информационной системе. См. *organizational user u non-organizational user.* |

| | |
|---|---|
| **virtual private network**<br>виртуальная частная сеть<br>[CNSSI 4009] | Защищенный канал информационной системы, использующий туннелирование, меры безопасности и трансляцию адресов конечных точек, создающий впечатление выделенной линии. |
| **vulnerability**<br>уязвимость<br>[SP 800-30] | Недостаток в информационной системе, процедурах безопасности системы, внутренних мерах безопасности или реализации, который может быть использован или инициирован источником угрозы. |
| **vulnerability analysis**<br>анализ уязвимостей | См. *vulnerability assessment* |
| **vulnerability assessment**<br>оценка уязвимостей<br>[CNSSI 4009] | Систематизированное изучение информационной системы или продукта для определения адекватности мер безопасности, выявления недостатков безопасности, получения данных, на основе которых можно прогнозировать эффективность предлагаемых мер безопасности и подтверждения адекватности таких мер после внедрения. |

# ПРИЛОЖЕНИЕ B
# АКРОНИМЫ

ОБЩИЕ СОКРАЩЕНИЯ

| | |
|---|---|
| **ABAC** | Attribute-Based Access Control - Контроль доступа на основе атрибутов |
| **API** | Application Programming Interface - Интерфейс прикладного программирования |
| **APT** | Advanced Persistent Threat - Постоянная развивающаяся угроза |
| **BGP** | Border Gateway Protocol - Протокол пограничного шлюза |
| **BIOS** | Basic Input/Output System - Базовая система ввода/вывода |
| **CA** | Certificate Authority/Certificate Authorities - Орган сертификации/Органы сертификации |
| **CAC** | Common Access Card - Карта общего доступа |
| **CAVP** | Cryptographic Algorithm Validation Program - Программа проверки криптографических алгоритмов |
| **CD** | Compact Disc - Компакт-диск |
| **CD-R** | Compact Disc-Recordable – Перезаписываемый компакт-диск |
| **CIPSEA** | Confidential Information Protection and Statistical Efficiency Act - Закон о защите конфиденциальной информации и эффективности статистики |
| **CIRT** | Computer Incident Response Team - Команда реагирования на компьютерные инциденты |
| **CISA** | Cybersecurity and Infrastructure Security Agency - Агентство по кибербезопасности и инфраструктурной безопасности |
| **CMVP** | Cryptographic Module Validation Program - Программа подтверждения соответствия криптографических модулей |
| **CNSSD** | Committee on National Security Systems Instruction – Инструкция комитета по системам национальной безопасности |
| **CNSSI** | Chief Privacy Officer – Директор по приватности |
| **CNSSP** | Committee on National Security Systems Policy – Политика комитета по системам национальной безопасности |
| **CONOPS** | Concept of Operations - Концепция операций |
| **CUI** | Controlled Unclassified Information - Контролируемая некласифицированная информация |
| **CVE** | Common Vulnerabilities and Exposures - Общие уязвимости и воздействия |
| **CVSS** | Common Vulnerability Scoring System - Общая система оценки уязвимостей |
| **CWE** | Common Weakness Enumeration – Перечень общих недостатков |
| **DHCP** | Dynamic Host Configuration Protocol - Протокол динамической конфигурации хоста |
| **DMZ** | Demilitarized Zone – Демилитаризованная зона |
| **DNS** | Domain Name System – Система доменных имен |

| | |
|---|---|
| **DNSSEC** | Domain Name System Security Extensions - Расширения безопасности системы доменных имен |
| **DoD** | Department of Defense - Министерство обороны |
| **DSB** | Defense Science Board - Научный совет по вопросам обороны |
| **DVD** | Digital Versatile Disc - Многоцелевой цифровой диск |
| **DVD-R** | Digital Versatile Disc-Recordable – Перезаписываемый многоцелевой цифровой диск |
| **EAP** | Extensible Authentication Protocol - Расширяемый протокол аутентификации |
| **EMP** | Electromagnetic Pulse - Электромагнитный импульс |
| **EMSEC** | Emissions Security – Эмиссионная безопасность |
| **FASC** | Federal Acquisition Security Council - Федеральный совет по безопасности закупок |
| **FBCA** | Federal Bridge Certification Authority - Федеральный орган по сертификации мостов |
| **FCC** | Federal Communications Commission - Федеральная комиссия по связи |
| **FICAM** | Federal Identity, Credential and Access Management - Федеральное управление идентификацией, учетными данными и доступом |
| **FIPPs** | Fair Information Practice Principles - Принципы честной информационной практики |
| **FIPS** | Federal Information Processing Standards - Федеральные стандарты обработки информации |
| **FISMA** | Federal Information Security Modernization Act - Федеральный закон о модернизации информационной безопасности |
| **FOCI** | Foreign Ownership, Control, or Influence - Иностранное владение, управление или влияние |
| **FOIA** | Freedom of Information Act - Закон о свободе информации |
| **FTP** | File Transfer Protocol - Протокол передачи файлов |
| **GMT** | Greenwich Mean Time - Гринвичское среднее время |
| **GPS** | Global Positioning System - Глобальная система позиционирования |
| **GSA** | General Services Administration - Администрация общих сервисов |
| **HSPD** | Homeland Security Presidential Directive - Президентская директива по безопасность отечества |
| **HTTP** | Hypertext Transfer Protocol - Протокол передачи гипертекста |
| **ICS** | Industrial Control System – Индустриальная система управления |
| **IEEE** | Institute of Electrical and Electronics Engineers - Институт инженеров по электронике и радиотехнике |
| **I/O** | Input/Output – ввод/вывод |
| **IOC** | Indicators of Compromise - Показатели компромисса |
| **IoT** | Internet of Things – Интернет вещей |
| **IP** | Internet Protocol – Протокол Интернет |
| **IR** | Interagency Report or Internal Report - Межведомственный отчет или внутренний отчет |

| | |
|---|---|
| **ISAC** | Information Sharing and Analysis Centers - Центры обмена информацией и анализа |
| **ISAO** | Information Sharing and Analysis Organizations - Организации обмена информацией и анализа |
| **IT** | Information Technology – Информационная технология |
| **ITL** | Information Technology Laboratory - Лаборатория информационных технологий |
| **MAC** | Media Access Control - Контроль доступа к носителям |
| **MLS** | Multilevel Secure – Многоуровневая безопасность |
| **MTTF** | Mean Time To Failure - Среднее время до отказа |
| **NARA** | National Archives and Records Administration - Национальное управление архивов и документации |
| **NATO** | North Atlantic Treaty Organization - Организация Североатлантического договора |
| **NDA** | Non-Disclosure Agreement – Соглашение о неразглашении |
| **NIAP** | National Institute of Standards and Technology – Национальный институт стандартов и технологий |
| **NOFORN** | Not Releasable to Foreign Nationals - Не разрешеный для передачи иностранным гражданам |
| **NSA** | National Security Agency - Агентство национальной безопасности |
| **NVD** | National Vulnerability Database - Национальная база данных уязвимостей |
| **ODNI** | Office of the Director of National Intelligence - Офис Директора национальной разведки |
| **OMB** | Office of Management and Budget - Министерство управления и бюджета |
| **OPM** | Office of Personnel Management - Управление по работе с персоналом |
| **OPSEC** | Operations Security – Эксплуатационная безопасность |
| **OVAL** | Open Vulnerability and Assessment Language - Открытый язык оценки и анализа уязвимостей |
| **PDF** | Portable Document Format - Формат переносимого документа |
| **PDS** | Position Designation System - Система обозначения должностей |
| **PII** | Personally Identifiable Information – Персональная идентификационная информация |
| **PIN** | Personal Identification Number – Персональный идентификационный номер |
| **PIV** | Personal Identity Verification – Подтверждение соответствия персональных идентификационных данных |
| **PIV-I** | Personal Identity Verification-Interoperable - Подтверждение соответствия персональных идентификационных данных-интерперабельность |
| **PKI** | Public Key Infrastructure - Инфраструктура публичных ключей |
| **RBAC** | Role-Based Access Control - Ролевой контроль доступа |
| **RD** | Restricted Data – Данные ограниченного доступа |
| **RFID** | Radio-Frequency Identification - Радиочастотная идентификация |
| **RFP** | Request For Proposal - Запрос предложений |

| | |
|---|---|
| **RPKI** | Resource Public Key Infrastructure - Ресурс инфраструктуры открытых ключей |
| **SAP** | Special Access Program - Программа специального доступа |
| **SCAP** | Security Content Automation Protocol - Автоматизированный протокол контента безопасности |
| **SCIF** | Sensitive Compartmented Information Facility - Объект чувствительной закрытой информации |
| **SCRM** | Supply Chain Risk Management - Управление рисками цепочки поставок |
| **SDLC** | System Development Life Cycle - Жизненный цикл разработки систем |
| **SIEM** | Security Information and Event Management - Управление информацией и событиями в области безопасности |
| **SME** | Subject Matter Expert -Эксперт по предметным вопросам |
| **SMTP** | Simple Mail Transfer Protocol - Простой протокол передачи почты |
| **SOC** | Security Operations Center - Центр управления безопасностью |
| **SP** | Special Publication - Специальная публикация |
| **STIG** | Security Technical Implementation Guide - Руководство по техническому внедрению системы безопасности |
| **SWID** | Software Identification - Программная идентификация |
| **TCP** | Transmission Control Protocol - Протокол управления передачей |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol - Протокол управления передачей / интернет-протокол |
| **TIC** | Trusted Internet Connections – Доверенные интернет соединения |
| **TLS** | Transport Layer Security - Безопасность транспортного уровня |
| **TPM** | Trusted Platform Module - Модуль доверенной платформы |
| **TSP** | Telecommunications Service Priority - Приоритизация телекоммуникационных сервисов |
| **UEFI** | Unified Extensible Firmware Interface - Унифицированный расширяемый интерфейс микропрограммного обеспечения |
| **UPS** | Uninterruptible Power Supply - Источник бесперебойного питания |
| **USGCB** | United States Government Configuration Baseline – Базовый уровень конфигурации правительства Соединенных Штатов |
| **USB** | Universal Serial Bus - Универсальная последовательная шина |
| **UTC** | Coordinated Universal Time - Всемирное координированное время |
| **VoIP** | Voice over Internet Protocol - Голосовой интернет-протокол |
| **VPN** | Virtual Private Network - Виртуальная частная сеть |
| **WORM** | Write-Once, Read-Many - Запись - один раз, чтение - много |
| **XML** | Extensible Markup Language - Расширяемый язык разметки |

# ПРИЛОЖЕНИЕ C
# РЕЗЮМЕ МЕР

ОБОЗНАЧЕНИЕ РЕАЛИЗУЕМЫХ, УДАЛЕННЫХ МЕР И МЕР ДОВЕРИЯ

В таблицах C-1- C-20 приводится сводная информация о мерах по обеспечению безопасности и приватности и улучшениях мер в Главе Три. Каждая таблица фокусируется на отдельном семействе мер.

- мера или улучшение меры, которые были удалены из каталога мер, обозначается символом "W" и пояснением к мере или улучшению меры в светло-сером тексте.
- мера или улучшение меры, которое обычно реализуется информационной системой с помощью технических средств, обозначается "S" в столбце реализации.
- мера или улучшение меры, которое обычно реализуется организацией (т.е. людьми посредствам нетехнических средств), обозначается "O" в столбце реализации.[35]
- мера или улучшение меры, которое может быть реализовано организацией, системой или их комбинацией, обозначаются "O/S".
- обозначение "V" меры или улучшения меры в столбце доверия, указывает на то, что усиление меры или улучшения меры способствует возникновению оснований для доверия тому, что утверждение о безопасности или приватности было или будет достигнуто.[36]

Каждая мера и улучшение меры в таблицах C-1- C-20 имеет гиперссылку на текст для этой меры и улучшения меры в Главе Три.

Семейства мер содержат базовые меры и улучшения мер, которые непосредственно связаны с их базовыми мерами. Улучшения мер либо добавляют функциональность или специфичность к базовой мере, либо увеличивают стойкость базовой меры. В обоих случаях улучшения меры используются в системах и средах эксплуатации, которые требуют большей защиты, чем обеспечивается базовой мерой. Такая повышенная защита необходима в связи с потенциальными неблагоприятными воздействиями на организации и людей или в тех случаях, когда организациям требуются дополнения к функциям базовых мер или доверию, основанные на оценках риска организаций. Для использования улучшения меры всегда требуется использование базовой меры.

Семейства расположены в алфавитном порядке, а меры и улучшения мер в каждом семействе расположены в числовом порядке. Алфавитный или числовой порядок семейств, мер и улучшений мер не подразумевает ни какого типа назначения приоритетов, уровня важности или порядка, в котором должны быть реализованы меры или улучшения мер.

[35] Указание на то, что определенная мера или улучшение меры внедряется системой или организацией в таблицах C-1 - C-20 является условным. Организации имеют возможность гибко внедрять выбранные меры и улучшения мер наиболее экономичным и эффективным способом, одновременно соблюдая цель этих мер или улучшений мер. В некоторых ситуациях мера или улучшение меры могут быть реализованы системой, организацией или комбинацией этих двух сущностей.

[36] Доверие является критически важным аспектом при определении доверенности систем. Доверие - это мера уверенности в том, что функции безопасности и приватности, особенности, практика, политики, процедуры, механизмы и архитектура систем организации точно опосредуют и обеспечивают соблюдение установленных политик безопасности и приватности.

## ТАБЛИЦА C-1: СЕМЕЙСТВО КОНТРОЛЯ ДОСТУПА

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **AC-1** | **Политика и процедуры** | O | √ |
| **AC-2** | **Управление аккаунтом** | O | |
| AC-2 (1) | АВТОМАТИЗИРОВАННОЕ УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ СИСТЕМЫ | O | |
| AC-2 (2) | АВТОМАТИЗИРОВАННОЕ ВРЕМЕННОЕ И АВАРИЙНОЕ УПРАПВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ | S | |
| AC-2 (3) | ОТКЛЮЧЕНИЕ УЧЕТНЫХ ЗАПИСЕЙ | S | |
| AC-2 (4) | АВТОМАТИЗИРОВАННЫЕ ДЕЙСТВИЯ АУДИТА | S | |
| AC-2 (5) | ВЫХОД ИЗ СИСТЕМЫ БЕЗ ДЕЙСТВИЙ | O/S | |
| AC-2 (6) | ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ ПРИВИЛЕГИЯМИ | S | |
| AC-2 (7) | ПРИВИЛЕГИРОВАННЫЕ УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ | O | |
| AC-2 (8) | ДИНАМИЧЕСКОЕ ВЕДЕНИЕ УЧЕТНЫХ ЗАПИСЕЙ | S | |
| AC-2 (9) | ОГРАНИЧЕНИЯ НА ИСПОЛЬЗОВАНИЕ ОБЩИХ И ГРУППОВЫХ УЧЕТНЫХ ЗАПИСЕЙ | O | |
| AC-2 (10) | ИЗМЕНЕНИЕ УЧЁТНЫХ ДАННЫХ ОБЩЕЙ И ГРУППОВОЙ УЧЕТНОЙ ЗАПИСИ | W: Включено в состав AC-2k. | |
| AC-2 (11) | УСЛОВИЯ ИСПОЛЬЗОВАНИЯ | S | |
| AC-2 (12) | МОНИТОРИНГ УЧЕТНЫХ ЗАПИСЕЙ ДЛЯ НЕТИПИЧНОГО ИСПОЛЬЗОВАНИЯ | O/S | |
| AC-2 (13) | ОТКЛЮЧЕНИЕ УЧЕТНЫХ ЗАПИСЕЙ ДЛЯ ЛИЦ С ВЫСОКИМ РИСКОМ | O | |
| **AC-3** | **Осуществление доступа** | S | |
| AC-3 (1) | ОГРАНИЧЕННЫЙ ДОСТУП К ПРИВИЛЕГИРОВАННЫМ ФУНКЦИЯМ | W: Включено в состав AC-6. | |
| AC-3 (2) | ДВОЙНАЯ АВТОРИЗАЦИЯ | S | |
| AC-3 (3) | ОБЯЗАТЕЛЬНЫЙ КОНТРОЛЬ ДОСТУПА | S | |
| AC-3 (4) | ДИСКРЕЦИОННЫЙ КОНТРОЛЬ ДОСТУПА | S | |
| AC-3 (5) | ИНФОРМАЦИЯ, ВАЖНАЯ ДЛЯ БЕЗОПАСНОСТИ, | S | |
| AC-3 (6) | ЗАЩИТА ПОЛЬЗОВАТЕЛЬСКОЙ И СИСТЕМНОЙ ИНФОРМАЦИИ. | W: Включено в MP-4 и SC -28 | |
| AC-3 (7) | РОЛЕВОЙ КОНТРОЛЬ ДОСТУПА | O/S | |
| AC-3 (8) | АННУЛИРОВАНИЕ РАЗРЕШЕНИЙ ДОСТУПА | O/S | |
| AC-3 (9) | КОНТРОЛИРУЕМЫЙ ВЫПУСК | O/S | |
| AC-3 (10) | ПРОВЕРЕННОЕ ПЕРЕОПРЕДЕЛЕНИЕ МЕХАНИЗМОВ КОНТРОЛЯ ДОСТУПА. | O | |
| AC-3 (11) | ОГРАНИЧЕНИЕ ДОСТУПА К ОПРЕДЕЛЕННЫМ ТИПАМ ИНФОРМАЦИИ | S | |
| AC-3 (12) | УТВЕРЖДЕНИЕ И ОБЕСПЕЧЕНИЕ ДОСТУПА К ПРИЛОЖЕНИЯМ. | S | |
| AC-3 (13) | КОНТРОЛЬ ДОСТУПА НА ОСНОВЕ АТРИБУТОВ. | S | |
| AC-3 (14) | ИНДИВИДУАЛЬНЫЙ ДОСТУП | S | |
| AC-3 (15) | ДИСКРЕЦИОННЫЙ И МАНДАТНЫЙ КОНТРОЛЬ ДОСТУПА | S | |
| **AC-4** | **Осуществление информационных потоков** | S | |
| AC-4 (1) | АТРИБУТЫ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ ОБЪЕКТОВ | S | |
| AC-4 (2) | ОБРАБОТКА ОБЛАСТЕЙ | S | |
| AC-4 (3) | ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМ ПОТОКОМ. | S | |
| AC-4 (4) | УПРАВЛЕНИЕ ПОТОКОМ ЗАШИФРОВАННОЙ ИНФОРМАЦИИ. | S | |
| AC-4 (5) | ТИПЫ ДАННЫХ ДЛЯ ВСТРАИВАЕМЫХ СИСТЕМ | S | |
| AC-4 (6) | МЕТАДАННЫЕ | S | |
| AC-4 (7) | МЕХАНИЗМЫ ОДНОСТОРОННИХ ПОТОКОВ | S | |
| AC-4 (8) | ФИЛЬТРЫ ПОЛИТИКИ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ | S | |
| AC-4 (9) | ЧЕЛОВЕЧЕСКИЕ ОБЗОРЫ | O/S | |
| AC-4 (10) | ВКЛЮЧЕНИЕ И ОТКЛЮЧЕНИЕ ФИЛЬТРОВ ПОЛИТИКИ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ | S | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| AC-4 (11) | КОНФИГУРАЦИЯ ФИЛЬТРОВ ПОЛИТИКИ БЕЗОПАСНОСТИ ИЛИ ПРИВАТНОСТИ | S | |
| AC-4 (12) | ИДЕНТИФИКАТОРЫ ТИПОВ ДАННЫХ | S | |
| AC-4 (13) | РАЗЛОЖЕНИЕ НА РЕЛЕВАНТНЫЕ ДЛЯ ПОЛИТИКИ ПОДКОМПОНЕНТЫ. | S | |
| AC-4 (14) | ОГРАНИЧЕНИЯ ФИЛЬТРА ПОЛИТИКИ БЕЗОПАСНОСТИ ИЛИ ПРИВАТНОСТИ | S | |
| AC-4 (15) | ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННОЙ ИНФОРМАЦИИ | S | |
| AC-4 (16) | ПЕРЕДАЧА ИНФОРМАЦИИ ПО ВЗАИМОСВЯЗАННЫМ СИСТЕМАМ | W: Включено в состав AC-4. | |
| AC-4 (17) | ОБЛАСТИ АУТЕНТИФИКАЦИИ | S | |
| AC-4 (18) | ПРИВЯЗКА АТРИБУТОВ БЕЗОПАСНОСТИ | W: Включено в состав AC-16. | |
| AC-4 (19) | ПОДТВЕРЖДЕНИЕ СООТВЕТСТВИЯ МЕТАДАННЫХ | S | |
| AC-4 (20) | ОДОБРЕННЫЕ РЕШЕНИЯ | O | |
| AC-4 (21) | ФИЗИЧЕСКОЕ ИЛИ ЛОГИЧЕСКОЕ РАЗДЕЛЕНИЕ ИНФОРМАЦИОННЫХ ПОТОКОВ. | O/S | |
| AC-4 (22) | ТОЛЬКО ДОСТУП | S | |
| AC-4 (23) | МОДИФИКАЦИЯ НЕРАЗГЛАШАЕМОЙ ИНФОРМАЦИИ. | O/S | |
| AC-4 (24) | ВНУТРЕННИЙ НОРМАЛИЗОВАННЫЙ ФОРМАТ. | S | |
| AC-4 (25) | ОЧИСТКА ДАННЫХ | S | |
| AC-4 (26) | ДЕЙСТВИЯ ПО ФИЛЬТРАЦИИ АУДИТА | O/S | |
| AC-4 (27) | РЕЗЕРВНЫЕ/НЕЗАВИСИМЫЕ МЕХАНИЗМЫ ФИЛЬТРАЦИИ | S | |
| AC-4 (28) | КОНВЕЙЕРЫ ЛИНЕЙНЫХ ФИЛЬТРОВ | S | |
| AC-4 (29) | МЕХАНИЗМЫ ОРКЕСТРОВКИ ФИЛЬТРОВ. | O/S | |
| AC-4 (30) | МЕХАНИЗМЫ ФИЛЬТРАЦИИ С ИСПОЛЬЗОВАНИЕМ НЕСКОЛЬКИХ ПРОЦЕССОВ. | S | |
| AC-4 (31) | ПРЕДОТВРАЩЕНИЕ НЕУДАЧНОЙ ПЕРЕДАЧИ КОНТЕНТА | S | |
| AC-4 (32) | ТЕХНОЛОГИЧЕСКИЕ ТРЕБОВАНИЯ К ПЕРЕДАЧЕ ИНФОРМАЦИИ | S | |
| **AC-5** | **Разделение обязанностей** | O | |
| **AC-6** | **Наименьшее количество привилегии** | O | |
| AC-6 (1) | РАЗРЕШЕНИЕ ДОСТУПА К ФУНКЦИЯМ БЕЗОПАСНОСТИ | O | |
| AC-6 (2) | НЕПРИВИЛЕГИРОВАННЫЙ ДОСТУП ДЛЯ ФУНКЦИЙ, НЕ ОТНОСЯЩИХСЯ К БЕЗОПАСНОСТИ. | O | |
| AC-6 (3) | СЕТЕВОЙ ДОСТУП К ПРИВИЛЕГИРОВАННЫМ КОМАНДАМ. | O | |
| AC-6 (4) | ОТДЕЛЬНЫЕ ОБЛАСТИ ОБРАБОТКИ. | O/S | |
| AC-6 (5) | ПРИВИЛЕГИРОВАННЫЕ УЧЕТНЫЕ ЗАПИСИ | O | |
| AC-6 (6) | ПРИВИЛЕГИРОВАННЫЙ ДОСТУП НЕОРГАНИЗАЦИОННЫХ ПОЛЬЗОВАТЕЛЕЙ | O | |
| AC-6 (7) | ПЕРЕСМОТР ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЯ | O | |
| AC-6 (8) | УРОВНИ ПРИВИЛЕГИЙ ДЛЯ ВЫПОЛНЕНИЯ КОДА. | S | |
| AC-6 (9) | РЕГИСТРАЦИЯ ИСПОЛЬЗОВАНИЯ ПРИВИЛЕГИРОВАННЫХ ФУНКЦИЙ | S | |
| AC-6 (10) | ЗАПРЕЩЕНИЕ НЕПРИВИЛЕГИРОВАННЫМ ПОЛЬЗОВАТЕЛЯМ ВЫПОЛНЯТЬ ПРИВИЛЕГИРОВАННЫЕ ФУНКЦИИ. | S | |
| **AC-7** | **Неудачные попытки входа в систему** | S | |
| AC-7 (1) | АВТОМАТИЧЕСКАЯ БЛОКИРОВКА УЧЕТНОЙ ЗАПИСИ | W: Включено в состав AC-7. | |
| AC-7 (2) | ОЧИСТКА ИЛИ СТИРАНИЕ МОБИЛЬНЫХ УСТРОЙСТВ | S | |
| AC-7 (3) | ОГРАНИЧЕНИЕ БИОМЕТРИЧЕСКИХ ПОПЫТОК | O | |
| AC-7 (4) | ИСПОЛЬЗОВАНИЕ АЛЬТЕРНАТИВНОГО ФАКТОРА АУТЕНТИФИКАЦИИ. | O/S | |
| **AC-8** | **Уведомление об использовании системы** | O/S | |
| **AC-9** | **Предыдущее уведомление о входе в систему** | S | |
| AC-9 (1) | НЕУДАЧНЫЕ ВХОДЫ В СИСТЕМУ | S | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| AC-9 (2) | УСПЕШНЫЙ И НЕУДАЧНЫЙ ВХОД | S | |
| AC-9 (3) | УВЕДОМЛЕНИЕ ОБ ИЗМЕНЕНИЯХ В УЧЕТНОЙ ЗАПИСИ | S | |
| AC-9 (4) | ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ДЛЯ ВХОДА В СИСТЕМУ | S | |
| **AC-10** | **Управление параллельными сеансами** | S | |
| **AC-11** | **Электронный замок** | S | |
| AC-11 (1) | ДИСПЛЕИ СО СКРЫТИЕМ ЭКРАНА | S | |
| **AC-12** | **Завершение сессии** | S | |
| AC-12 (1) | ВЫХОДЫ ИЗ СИСТЕМЫ ПО ИНИЦИАТИВЕ ПОЛЬЗОВАТЕЛЯ | O/S | |
| AC-12 (2) | СООБЩЕНИЕ О ЗАВЕРШЕНИИ | S | |
| AC-12 (3) | ПРЕДУПРЕЖДЕНИЕ О ТАЙМ-АУТЕ | S | |
| AC-13 | **Меры надзора и проверки доступа** | W: Включено в AC-2 и AU-6. | |
| **AC-14** | **Разрешенные действия без идентификации или аутентификации** | O | |
| AC-14 (1) | НЕОБХОДИМОЕ ИСПОЛЬЗОВАНИЕ | W: Включено в состав AC-14. | |
| AC-15 | **Автоматизированное маркирование** | W: Включено в состав MP-3. | |
| **AC-16** | **Атрибуты безопасности и приватности** | O | |
| AC-16 (1) | ДИНАМИЧЕСКАЯ АССОЦИАЦИЯ АТРИБУТОВ | S | |
| AC-16 (2) | ИЗМЕНЕНИЕ ЗНАЧЕНИЯ АТРИБУТА УПОЛНОМОЧЕННЫМИ ЛИЦАМИ | S | |
| AC-16 (3) | ПОДДЕРЖКА АССОЦИАЦИИ АТРИБУТОВ В СИСТЕМЕ | S | |
| AC-16 (4) | АССОЦИАЦИЯ АТРИБУТОВ УПОЛНОМОЧЕННЫМИ ЛИЦАМИ | S | |
| AC-16 (5) | ОТОБРАЖЕНИЕ АТРИБУТОВ ВЫВОДИМЫХ ОБЪЕКТОВ | S | |
| AC-16 (6) | ПОДДЕРЖКА АССОЦИАЦИИ АТРИБУТОВ. | O | |
| AC-16 (7) | ПОСЛЕДОВАТЕЛЬНАЯ ИНТЕРПРЕТАЦИЯ АТРИБУТОВ | O | |
| AC-16 (8) | МЕТОДЫ И ТЕХНОЛОГИИ АССОЦИАЦИИ | S | |
| AC-16 (9) | ПЕРЕНАЗНАЧЕНИЕ АТРИБУТОВ - МЕХАНИЗМЫ РЕГРЕЙДИНГА | O | |
| AC-16 (10) | НАСТРОЙКА АТРИБУТОВ АВТОРИЗОВАННЫМИ ЛИЦАМИ | O | |
| **AC-17** | **Удаленный доступ** | O | |
| AC-17 (1) | КОНТРОЛЬ И УПРАВЛЕНИЕ | O/S | |
| AC-17 (2) | ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ И ЦЕЛОСТНОСТИ С ИСПОЛЬЗОВАНИЕМ ШИФРОВАНИЯ | S | |
| AC-17 (3) | УПРАВЛЕНИЕ ТОЧКАМИ КОНТРОЛЯ ДОСТУПА | S | |
| AC-17 (4) | ПРИВИЛЕГИРОВАННЫЕ КОМАНДЫ И ДОСТУП | O | |
| AC-17 (5) | МОНИТОРИНГ НЕСАНКЦИОНИРОВАННЫХ ПОДКЛЮЧЕНИЙ | W: Включено в состав SI-4. | |
| AC-17 (6) | ЗАЩИТА ИНФОРМАЦИИ О МЕХАНИЗМАХ | O | |
| AC-17 (7) | ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА ДОСТУПА К ФУНКЦИЯМ БЕЗОПАСНОСТИ | W: Включено в AC-3 (10). | |
| AC-17 (8) | ОТКЛЮЧЕНИЕ НЕБЕЗОПАСНЫХ СЕТЕВЫХ ПРОТОКОЛОВ. | W: Включено в УК -7 | |
| AC-17 (9) | ОТКЛЮЧЕНИЕ ИЛИ ЗАПРЕТ ДОСТУПА | O | |
| AC-17 (10) | АУТЕНТИФИКАЦИЯ УДАЛЕННЫХ КОМАНД. | S | |
| **AC-18** | **Беспроводной доступ** | O | |
| AC-18 (1) | АУТЕНТИФИКАЦИЯ И ШИФРОВАНИЕ | S | |
| AC-18 (2) | МОНИТОРИНГ НЕАВТОРИЗОВАННЫХ СОЕДИНЕНИЙ | W: Включено в состав SI-4. | |
| AC-18 (3) | ОТКЛЮЧЕНИЕ БЕСПРОВОДНЫХ СЕТЕЙ | O/S | |
| AC-18 (4) | ОГРАНИЧЕНИЕ КОНФИГУРИРОВАНИЯ ПОЛЬЗОВАТЕЛЯМИ | O | |
| AC-18 (5) | АНТЕННЫ И УРОВНИ МОЩНОСТИ ПЕРЕДАЧИ. | O | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **AC-19** | **Контроль доступа для мобильных устройств** | O | |
| AC-19 (1) | ИСПОЛЬЗОВАНИЕ ЗАПИСЫВАЕМЫХ И ПЕРЕНОСНЫХ ЗАПОМИНАЮЩИХ УСТРОЙСТВ. | W: Включено в состав MP-7. | |
| AC-19 (2) | ИСПОЛЬЗОВАНИЕ ЛИЧНЫХ ПОРТАТИВНЫХ ЗАПОМИНАЮЩИХ УСТРОЙСТВ. | W: Включено в состав MP-7. | |
| AC-19 (3) | ИСПОЛЬЗОВАНИЕ ПОРТАТИВНЫХ ЗАПОМИНАЮЩИХ УСТРОЙСТВ БЕЗ ИДЕНТИФИЦИРУЕМОГО ВЛАДЕЛЬЦА | W: Включено в состав MP-7. | |
| AC-19 (4) | ОГРАНИЧЕНИЯ В ОТНОШЕНИИ КЛАССИФИЦИРОВАННОЙ ИНФОРМАЦИИ | O | |
| AC-19 (5) | ПОЛНОЕ ШИФРОВАНИЕ НА БАЗЕ УСТРОЙСТВА ИЛИ КОНТЕЙНЕРА | O | |
| **AC-20** | **Использование внешних систем** | O | |
| AC-20 (1) | ОГРАНИЧЕНИЯ НА РАЗРЕШЕННОЕ ИСПОЛЬЗОВАНИЕ | O | |
| AC-20 (2) | ПОРТАТИВНЫЕ ЗАПОМИНАЮЩИЕ УСТРОЙСТВА - ОГРАНИЧЕНИЕ ИСПОЛЬЗОВАНИЯ | O | |
| AC-20 (3) | СИСТЕМЫ НЕ ПРИНАДЛЕЖАЩИЕ ОРГАНИЗАЦИИ - ОГРАНИЧЕННИЕ ИСПОЛЬЗОВАНИЯ | O | |
| AC-20 (4) | СЕТЕВЫЕ УСТРОЙСТВА ХРАНЕНИЯ ДАННЫХ - ЗАПРЕЩЕНИЕ ИСПОЛЬЗОВАНИЯ | O | |
| AC-20 (5) | ПОРТАТИВНЫЕ ЗАПОМИНАЮЩИЕ УСТРОЙСТВА - ЗАПРЕЩЕНИЕ ИСПОЛЬЗОВАНИЯ | O | |
| **AC-21** | **Совместное использование информаци** | O | |
| AC-21 (1) | АВТОМАТИЗИРОВАННАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ | S | |
| AC-21 (2) | ПОИСК И ИЗВЛЕЧЕНИЕ ИНФОРМАЦИИ | S | |
| **AC-22** | **Общедоступный контент** | O | |
| **AC-23** | **Защита интеллектуального анализа данных** | O | |
| **AC-24** | **Решения по контролю доступа** | O | |
| AC-24 (1) | ПЕРЕДАЧА ИНФОРМАЦИИ САНКЦИОНИРОВАНИЯ ДОСТУПА. | S | |
| AC-24 (2) | ОТСУТСТВИЕ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ИЛИ ПРОЦЕССА | S | |
| **AC-25** | **Диспетчер доступа** | S | √ |

## ТАБЛИЦА C-2: ОСВЕДОМЛЕННОСТЬ И ПРОФЕССИОНАЛЬНАЯ ПОДГОТОВКА

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **AT- 1** | **Политика и процедуры** | O | √ |
| **AT- 2** | **Обучение и освоение** | O | √ |
| AT- 2 (1) | ПРАКТИЧЕСКИЕ УПРАЖНЕНИЯ | O | √ |
| AT- 2 (2) | УГРОЗА ПОСВЯЩЕННОГО ЛИЦА | O | √ |
| AT- 2 (3) | СОЦИАЛЬНАЯ ТЕХНИКА И МИНИРОВАНИЕ | O | √ |
| AT- 2 (4) | ПОДОЗРИТЕЛЬНЫЕ СВЯЗИ И АНОМАЛЬНОЕ ПОВЕДЕНИЕ СИСТЕМЫ | O | √ |
| AT- 2 (5) | РАСШИРЕННАЯ ДОЛГОВРЕМЕННАЯ УГРОЗА | O | √ |
| AT- 2 (6) | СРЕДА КИБЕРУГРОЗ | O | √ |
| **AT- 3** | **Ролевое обучение** | O | √ |
| AT- 3 (1) | КОНТРОЛЬ ЗА СОСТОЯНИЕМ ОКРУЖАЮЩЕЙ СРЕДЫ | O | √ |
| AT- 3 (2) | ФИЗИЧЕСКИЕ МЕРЫ БЕЗОПАСНОСТИ | O | √ |
| AT- 3 (3) | ПРАКТИЧЕСКИЕ УПРАЖНЕНИЯ | O | √ |
| AT- 3 (4) | ПОДОЗРИТЕЛЬНЫЕ связи И АНОМАЛЬНОЕ ПОВЕДЕНИЕ СИСТЕМЫ | W: Включено в AT-2 (4). | |
| AT- 3 (5) | ОБРАБОТКА ПЕРСОНАЛЬНОЙ ИДЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ | O | √ |
| **AT- 4** | **Записи по обучению** | O | √ |
| AT- 5 | **Контакты с группами безопасности и ассоциациями** | W: Включено в PM -15 | |
| **AT- 6** | **Обратная связь по обучению** | O | √ |

## ТАБЛИЦА C-3: СИСТЕМА АУДИТА И ПОДОТЧЕТНОСТИ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **AU-1** | **Политика и процедуры** | O | √ |
| **AU-2** | **Регистрация событий** | O | |
| AU-2 (1) | КОМПИЛЯЦИЯ ЗАПИСЕЙ АУДИТА ИЗ РАЗЛИЧНЫХ ИСТОЧНИКОВ | W: Включено в состав AU-12. | |
| AU-2 (2) | ВЫБОР СОБЫТИЙ АУДИТА ПО КОМПОНЕНТАМ | W: Включено в состав AU-12. | |
| AU-2 (3) | ПЕРЕСМОТРЫ И ОБНОВЛЕНИЯ | W: Включено в состав AU-2. | |
| AU-2 (4) | ПРИВИЛЕГИРОВАННЫЕ ФУНКЦИИ | W: Включено в AC-6 (9). | |
| **AU-3** | **Содержание записей аудита** | S | |
| AU-3 (1) | ДОПОЛНИТЕЛЬНЫЙ АУДИТ ИНФОРМАЦИЯ | S | |
| AU-3 (2) | ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ПЛАНИРУЕМЫМ СОДЕРЖАНИЕМ ЗАПИСЕЙ АУДИТА | W: Включено в состав PL-9. | |
| AU-3 (3) | ОГРАНИЧЕНИЕ ЭЛЕМЕНТОВ ПЕРСОНАЛЬНОЙ ИДЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ | O | |
| **AU-4** | **Возможность хранилища журналов аудита** | O/S | |
| AU-4 (1) | ПЕРЕНОС В АЛЬТЕРНАТИВНОЕ ХРАНИЛИЩЕ | O/S | |
| **AU-5** | **Реагирование на сбои в процессе ведения журнала аудита** | S | |
| AU-5 (1) | ПРЕДУПРЕЖДЕНИЕ О ВОЗМОЖНОСТZ[ ХРАНИЛИЩА | S | |
| AU-5 (2) | ОПОВЕЩЕНИЯ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ | S | |
| AU-5 (3) | НАСТРАИВАЕМЫЕ ПОРОГОВЫЕ ЗНАЧЕНИЯ ОБЪЕМА ТРАФИКА. | S | |
| AU-5 (4) | ОСТАНОВ ПРИ ОТКАЗЕ | S | |
| AU-5 (5) | ВОЗМОЖНОСТЬ ВЕДЕНИЯ АЛЬТЕРНАТИВНОГО ЖУРНАЛА АУДИТА. | O | |
| **AU-6** | **Пересмотр, анализ и отчетность записей аудита** | O | √ |
| AU-6 (1) | АВТОМАТИЗИРОВАННАЯ ИНТЕГРАЦИЯ ПРОЦЕССОВ | O | √ |
| AU-6 (2) | АВТОМАТИЧЕСКJТ ОПОВЕЩЕНИТ О БЕЗОПАСНОСТИ | W: Включено в состав SI-4. | |
| AU-6 (3) | КОРРЕЛИРОВКА РЕПОЗИТОРИЯ ЗАПИСЕЙ АУДИТА | O | √ |
| AU-6 (4) | ЦЕНТРАЛИЗОВАННЫЙ ПЕРЕСМОТР И АНАЛИЗ | S | √ |
| AU-6 (5) | КОМПЛЕКСНЫЙ АНАЛИЗ ЗАПИСЕЙ АУДИТА | O | √ |
| AU-6 (6) | КОРРЕЛЯЦИЯ С ФИЗИЧЕСКИМ МОНИТОРИНГОМ | O | √ |
| AU-6 (7) | РАЗРЕШЕННЫЕ ДЕЙСТВИЯ | O | √ |
| AU-6 (8) | ПОЛНОТЕКСТОВЫЙ АНАЛИЗ ПРИВИЛЕГИРОВАННЫХ КОМАНД. | O | √ |
| AU-6 (9) | КОРРЕЛЯЦИЯ С ИНФОРМАЦИЕЙ ИЗ НЕТЕХНИЧЕСКИХ ИСТОЧНИКОВ. | O | √ |
| AU-6 (10) | КОРРЕКТИРОВКА УРОВНЯ АУДИТА | W: Включено в состав AU-6. | |
| **AU-7** | **Сокращение количества записей аудита и создание отчетов** | S | √ |
| AU-7 (1) | АВТОМАТИЧЕСКАЯ ОБРАБОТКА | S | √ |
| AU-7 (2) | АВТОМАТИЧЕСКАЯ СОРТИРОВКА И ПОИСК | W: Включено в AU-7 (1). | |
| **AU-8** | **Отметки времени** | S | |
| AU-8 (1) | СИНХРОНИЗАЦИЯ С АВТОРИТЕТНЫМ ИСТОЧНИКОМ ВРЕМЕНИ. | W: Перенесен в SC -45 (1 | |
| AU-8 (2) | ВТОРИЧНЫЙ АВТОРИТЕТНЫЙ ИСТОЧНИК ВРЕМЕНИ | W: Перенесен в SC -45 (2 | |
| **AU-9** | **Защита информаци аудита** | S | |
| AU-9 (1) | АППАРАТНЫЕ ОДНОЗАПИСЫВАЕМЫЕ НОСИТЕЛИ ИНФОРМАЦИИ. | S | |
| AU-9 (2) | ХРАНЕНИЕ НА ОТДЕЛЬНЫХ ФИЗИЧЕСКИХ СИСТЕМАХ ИЛИ КОМПОНЕНТАХ | S | |
| AU-9 (3) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | S | |
| AU-9 (4) | ДОСТУП ПОДМНОЖЕСТВА ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ. | O | |
| AU-9 (5) | ДВОЙНОЕ САНКЦИОНИРОВАНИЕ | O/S | |
| AU-9 (6) | ДОСТУП ТОЛЬКО ДЛЯ ЧТЕНИЯ | O/S | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| AU-9 (7) | ХРАНЕНИЕ В КОМПОНЕНТАХ С РАЗЛИЧНЫМИ ОПЕРАЦИОННЫМИ СИСТЕМАМИ. | O | |
| **AU-10** | **Неотказуемость** | S | √ |
| AU-10 (1) | АССОЦИАЦИЯ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ | S | √ |
| AU-10 (2) | ПОДТВЕРЖДЕНИЕ ПРИВЯЗКИ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ ИСТОЧНИКА ИНФОРМАЦИИ | S | √ |
| AU-10 (3) | ЦЕПОЧКА ХРАНЕНИЯ | O/S | √ |
| AU-10 (4) | ПОДТВЕРЖДЕНИЕ ПРИВЯЗКИ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ ОБОЗРЕВАТЕЛЯ ИНФОРМАЦИИ | S | √ |
| AU-10 (5) | ЦИФРОВЫЕ ПОДПИСИ | W: Включено в состав SI-7. | |
| **AU-11** | **Хранение записей аудита** | O | |
| AU-11 (1) | ВОЗМОЖНОСТЬ ДОЛГОСРОЧНОГО ПОИСКА | O | √ |
| **AU-12** | **Генерация записей аудита** | S | |
| AU-12 (1) | ОБЩЕСИСТЕМНЫЙ И КОРРЕЛИРОВАННЫЙ ПО ВРЕМЕНИ ЖУРНАЛ АУДИТА | S | |
| AU-12 (2) | СТАНДАРТИЗИРОВАННЫЕ ФОРМАТЫ | S | |
| AU-12 (3) | ИЗМЕНЕНИЯ, ВНОСИМЫЕ УПОЛНОМОЧЕННЫМИ ЛИЦАМИ | S | |
| AU-12 (4) | ПРОВЕРКА ПАРАМЕТРОВ ЗАПРОСОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНО ИДЕНТИФИЦИРУЕМУЮ ИНФОРМАЦИЮ | S | |
| **AU-13** | **Мониторинг раскрытия информации** | O | √ |
| AU-13 (1) | ИСПОЛЬЗОВАНИЕ АВТОМАТИЗИРОВАННЫХ ИНСТРУМЕНТОВ. | O/S | √ |
| AU-13 (2) | ОБЗОР КОНТРОЛИРУЕМЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ | O | √ |
| AU-13 (3) | НЕСАНКЦИОНИРОВАННОЕ КОПИРОВАНИЕ ИНФОРМАЦИИ | O/S | √ |
| **AU-14** | **Аудит сессий** | S | √ |
| AU-14 (1) | ЗАПУСК СИСТЕМЫ | S | √ |
| AU-14 (2) | СБОР И ЗАПИСЬ СОДЕРЖАНИЯ | W: Включено в состав AU-14. | |
| AU-14 (3) | УДАЛЕННЫЙ ПРОСМОТР И ПРОСЛУШИВАНИЕ | S | √ |
| **AU-15** | **Возможность ведения альтернативного журнала аудита** | W: Переехал в AU-5 (5). | |
| **AU-16** | **Ведение журнала аудита между организациями** | O | |
| AU-16 (1) | СОХРАНЕНИЕ ИДЕНТИЧНОСТИ | O | |
| AU-16 (2) | ОБМЕН ИНФОРМАЦИЕЙ АУДИТА | O | |
| AU-16 (3) | РАЗОБЩЕННОСТЬ | O | |

## ТАБЛИЦА C-4: СЕМЕЙСТВО ОЦЕНКИ, САНКЦИОНИРОВАНИЯ И МОНИТОРИНГА

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **CA-1** | **Политика и процедуры** | O | √ |
| **CA-2** | **Оценка мер** | O | √ |
| CA-2 (1) | НЕЗАВИСИМЫЕ ОЦЕНЩИКИ | O | √ |
| CA-2 (2) | СПЕЦИАЛИЗИРОВАННЫЕ ОЦЕНКИ | O | √ |
| CA-2 (3) | ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ВНЕШНИХ ОРГАНИЗАЦИЙ | O | √ |
| **CA-3** | **Обмен информацией** | O | √ |
| CA-3 (1) | НЕКЛАССИФИЦИРОВАННЫЕ СОЕДИНЕНИЯ СИСТЕМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ | W: Перенесены в SC -7 (25 | |
| CA-3 (2) | КЛАССИФИЦИРОВАННЫЕ СОЕДИНЕНИЯ СИСТЕМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ | W: Перенесен в SC -7 (26 | |
| CA-3 (3) | НЕКЛАССИФИЦИРОВАННЫЕ ПОДКЛЮЧЕНИЯ СИСТЕМ НЕ ОТНОСЯЩИХСЯ К НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ | W: Перенесены в SC -7 (27 | |
| CA-3 (4) | ПОДКЛЮЧЕНИЯ К СЕТЯМ ОБЩЕГО ПОЛЬЗОВАНИЯ | W: Перенесены в SC -7 (28 | |
| CA-3 (5) | ОГРАНИЧЕНИЯ НА ПОДКЛЮЧЕНИЕ ВНЕШНИХ СИСТЕМ | W: Включено в SC -7 (5 | |
| CA-3 (6) | САНКЦИОНИРОВАНИЕ ПЕРЕДАЧИ | O/S | √ |
| CA-3 (7) | ПЕРЕХОДНЫЙ ОБМЕН ИНФОРМАЦИЕЙ | O/S | √ |
| **CA-4** | **Сертификация безопасности** | W: Включено в CA -2 | |
| **CA-5** | **План действий и вехи** | O | √ |
| CA-5 (1) | ПОДДЕРЖКА АВТОМАТИЗАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ТОЧНОСТИ И СТОИМОСТИ | O | √ |
| **CA-6** | **Санкционирование** | O | √ |
| CA-6 (1) | СОВМЕСТНОЕ САНКЦИОНИРОВАНИЕ – ВНУТРИ ОРГАНИЗАЦИИ | O | √ |
| CA-6 (2) | СОВМЕСТНОЕ САНКЦИОНИРОВАНИЕ – МЕЖДУ ОРГАНИЗАЦИЯМИ | O | √ |
| **CA-7** | **Непрерывный мониторинг** | O | √ |
| CA-7 (1) | НЕЗАВИСИМАЯ ОЦЕНКА | O | √ |
| CA-7 (2) | ТИПЫ ОЦЕНОК | W: Включено в CA -2 | |
| CA-7 (3) | АНАЛИЗ ТЕНДЕНЦИЙ | O | √ |
| CA-7 (4) | МОНИТОРИНГ РИСКА | O/S | √ |
| CA-7 (5) | АНАЛИЗ СОГЛАСОВАННОСТИ | O | √ |
| CA-7 (6) | АВТОМАТИЗИРОВАННАЯ ПОДДЕРЖКА МОНИТОРИНГА | O/S | √ |
| **CA-8** | **Тестирование проникновения** | O | √ |
| CA-8 (1) | НЕЗАВИСИМЫЙ АГЕНТ ИЛИ КОМАНДА ПО ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ | O | √ |
| CA-8 (2) | УЧЕНИЯ КРАСНЫХ БРИГАД | O | √ |
| CA-8 (3) | ВОЗМОЖНОСТИ ТЕСТИРОВАНИЯ ПРОНИКНОВЕНИЯ | O | √ |
| **CA-9** | **Внутренние подключения к системе** | O | √ |
| CA-9 (1) | ПРОВЕРКИ СООТВЕТСТВИЯ | O/S | √ |

## ТАБЛИЦА C-5: СЕМЕЙСТВО УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **CM 1** | **Политика и процедуры** | O | √ |
| **CM 2** | **Базовая конфигурация** | O | √ |
| CM 2 (1) | ОБЗОРЫ И ОБНОВЛЕНИЯ | W: Включено в CM -2 | |
| CM 2 (2) | ПОДДЕРЖКА АВТОМАТИЗАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ТОЧНОСТИ И СТОИМОСТИ | O | √ |
| CM 2 (3) | СОХРАНЕНИЕ ПРЕДЫДУЩИХ КОНФИГУРАЦИЙ | O | √ |
| CM 2 (4) | НЕСАНКЦИОНИРОВАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ | W: Включено в CM -7 | |
| CM 2 (5) | САНКЦИОНИРОВАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ | W: Включено в CM -7 | |
| CM 2 (6) | СРЕДЫ РАЗРАБОТКИ И ТЕСТИРОВАНИЯ | O | √ |
| CM 2 (7) | КОНФИГУРИРОВАНИЕ СИСТЕМ И КОМПОНЕНТОВ ДЛЯ ОБЛАСТЕЙ ПОВЫШЕННОГО РИСКА | O | √ |
| **CM 3** | **Контроль изменений конфигурации** | O | √ |
| CM 3 (1) | АВТОМАТИЗИРОВАННОЕ ДОКУМЕНТИРОВАНИЕ, УВЕДОМЛЕНИЕ И ЗАПРЕТ ИЗМЕНЕНИЙ | O | √ |
| CM 3 (2) | ТЕСТИРОВАНИЕ, ПОДТВЕРЖДЕНИЕ СООТВЕТСТВИЯ И ДОКУМЕНТИРОВАНИЕ ИЗМЕНЕНИЙ | O | √ |
| CM 3 (3) | АВТОМАТИЗИРОВАННАЯ РЕАЛИЗАЦИЯ ИЗМЕНЕНИЙ | O | |
| CM 3 (4) | ПРЕДСТАВЛЕНИЕ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ | O | |
| CM 3 (5) | АВТОМАТИЗИРОВАННОЕ РЕАГИРОВАНИЕ БЕЗОПАСНОСТИ | S | |
| CM 3 (6) | УПРАВЛЕНИЕ КРИПТОГРАФИЕЙ | O | |
| CM 3 (7) | СМОТРЕНИЕ ИЗМЕНЕНИЙ В СИСТЕМЕ | O | |
| CM 3 (8) | ПРЕДОТВРАЩЕНИЕ ИЛИ ОГРАНИЧЕНИЕ ИЗМЕНЕНИЙ КОНФИГУРАЦИИ | S | |
| **CM 4** | **Анализ воздействий** | O | √ |
| CM 4 (1) | ОТДЕЛЬНЫЕ ИСПЫТАТЕЛЬНЫЕ СРЕДЫ | O | √ |
| CM 4 (2) | ПРОВЕРКА МЕР | O | √ |
| **CM 5** | **Ограничения доступа для изменения** | O | |
| CM 5 (1) | АВТОМАТИЗИРОВАННОЕ ОСУЩЕСТВЛЕНИЕ ДОСТУПА И ЗАПИСИ АУДИТА | S | |
| CM 5 (2) | РАССМОТРЕНИЕ ИЗМЕНЕНИЙ В СИСТЕМЕ | W: Включено в CM -3 (7 | |
| CM 5 (3) | ПОДПИСАННЫЕ КОМПОНЕНТЫ | W: Перенесены в CM -14 | |
| CM 5 (4) | ДВОЙНОЕ САНКЦИОНИРОВАНИЕ | O/S | |
| CM 5 (5) | ОГРАНИЧЕНИЕ ПРИВИЛЕГИЙ ДЛЯ ПРОИЗВОДСТВА И ЭКСПЛУАТАЦИИ. | O | |
| CM 5 (6) | ОГРАНИЧЕНИЕ ПРИВИЛЕГИЮ БИБЛИОТЕК | O/S | |
| CM 5 (7) | АВТОМАТИЧЕСКАЯ РЕАЛИЗАЦИЯ БЕЗОПАСНОСТИ МЕР ЗАЩИТЫ | W: Включено в состав SI-7. | |
| **CM 6** | **Установки конфигурации** | O/S | |
| CM 6 (1) | АВТОМАТИЗИРОВАННОЕ УПРАВЛЕНИЕ, ПРИМЕНЕНИЕ И ПРОВЕРКА | O | |
| CM 6 (2) | РЕАГИРОВАНИЕ НА НЕСАНКЦИОНИРОВАННЫЕ ИЗМЕНЕНИЯ | O | |
| CM 6 (3) | ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННЫХ ИЗМЕНЕНИЙ | W: Включено в состав SI-7. | |
| CM 6 (4) | ДЕМОНСТРАЦИЯ СООТВЕТСТВИЯ | W: Включено в CM -4 | |
| **CM 7** | **Минимальная функциональность** | O/S | |
| CM 7 (1) | ПЕРИОДИЧЕСКИОЕ РАССМОТРЕНИЕ | O/S | |
| CM 7 (2) | ПРЕДОТВРАЩЕНИЕ ВЫПОЛНЕНИЯ ПРОГРАММ | S | |
| CM 7 (3) | СОБЛЮДЕНИЕ ПРАВИЛ РЕГИСТРАЦИИ | O | |
| CM 7 (4) | НЕСАНКЦИОНИРОВАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ - ЗАПРЕТ ЗА ИСКЛЮЧЕНИЕМ | O/S | |
| CM 7 (5) | АВТОРИЗОВАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ - РАЗРЕШЕНИЕ ЗА ИСКЛЮЧЕНИЕМ | O/S | |
| CM 7 (6) | ЗАМКНУТЫЕ СРЕДЫ С ОГРАНИЧЕННЫМИ ПРИВИЛЕГИЯМИ | O | √ |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| CM 7 (7) | ВЫПОЛНЕНИЕ КОДА В ЗАЩИЩЕННЫХ СРЕДАХ | O/S | √ |
| CM 7 (8) | БИНАРНЫЙ ИЛИ МАШИННЫЙ ИСПОЛНЯЕМЫЙ КОД. | O/S | √ |
| CM 7 (9) | ЗАПРЕТ НА ИСПОЛЬЗОВАНИЕ НЕСАНКЦИОНИРОВАННЫХ АППАРАТНЫХ СРЕДСТВ | O/S | √ |
| **CM 8** | **Инвентаризация компонентов системы** | O | √ |
| CM 8 (1) | ОБНОВЛЕНИЕ ПРИ УСТАНОВКЕ И УДАЛЕНИИ | O | √ |
| CM 8 (2) | АВТОМАТИЗИРОВАННАЯ ПОДДЕРЖКА | O | √ |
| CM 8 (3) | АВТОМАТИЗИРОВАННОЕ ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННЫХ КОМПОНЕНТОВ | O | √ |
| CM 8 (4) | ИНФОРМАЦИЯ О ПОДОТЧЕТНОСТИ | O | √ |
| CM 8 (5) | ОТСУТСТВИЕ ДУБЛИРУЮЩЕГО УЧЕТА КОМПОНЕНТОВ | W: Включено в CM -8 | |
| CM 8 (6) | ОЦЕНЕННЫЕ КОНФИГУРАЦИИ И УТВЕРЖДЕННЫЕ ОТКЛОНЕНИЯ | O | √ |
| CM 8 (7) | ЦЕНТРАЛИЗОВАННОЕ ХРАНИЛИЩЕ | O | √ |
| CM 8 (8) | АВТОМАТИЗИРОВАННОЕ ПРОСЛЕЖИВАНИЕ МЕСТОПОЛОЖЕНИЯ | O | √ |
| CM 8 (9) | НАЗНАЧЕНИЕ КОМПОНЕНТОВ СИСТЕМАМ | O | √ |
| **CM 9** | **План управления конфигурацией** | O | |
| CM 9 (1) | РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ | O | |
| **CM 10** | **Ограничения на использование программного обеспечения** | O | |
| CM 10 (1) | ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ | O | |
| **CM 11** | **Установленное пользователями программное обеспечение** | O | |
| CM 11 (1) | ОПОВЕЩЕНИЯ О НЕСАНКЦИОНИРОВАННЫХ УСТАНОВКАХ | W: Включено в CM -8 (3 | |
| CM 11 (2) | УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ПРИВИЛЕГИРОВАННЫМ СТАТУСОМ | S | |
| CM 11 (3) | АВТОМАТИЗИРОВАННОЕ ОСУЩЕСТВЛЕНИЕ И МОНИТОРИНГ | S | √ |
| **CM 12** | **Информационное местоположение** | O | √ |
| CM 12 (1) | АВТОМАТИЗИРОВАННЫЕ ИНСТРУМЕНТЫ ДЛЯ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ИНФОРМАЦИИ | O | √ |
| **CM 13** | **Сопоставление действий с данными** | O | |
| **CM 14** | **Подписанные компоненты** | O/S | √ |

## ТАБЛИЦА C-6: ПЛАНИРОВАНИЕ НА СЛУЧАЙ НЕПРЕДВИДЕННЫХ ОБСТОЯТЕЛЬСТВ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **CP-1** | **Политика и процедуры** | O | √ |
| **CP-2** | **Резервный план** | O | |
| CP-2 (1) | КООРДИНАЦИЯ С СООТВЕТСТВУЮЩИМИ ПЛАНАМИ | O | |
| CP-2 (2) | ПЛАНИРОВАНИЕ ВОЗМОЖНОСТЕЙ | O | |
| CP-2 (3) | ВОЗОБНОВЛЕНИЕ ФУНКЦИЙПРЕДНАЗНАЧЕНИЯ И ДЕЯТЕЛЬНОСТИ | O | |
| CP-2 (4) | ВОЗОБНОВЛЕНИЕ ВСЕХ ФУНКЦИЙПРЕДНАЗНАЧЕНИЯ И ДЕЯТЕЛЬНОСТИ | W: Включено в CP-2 (3). | |
| CP-2 (5) | ПРОДОЛЖЕНИЕ ВЫПОЛНЕНИЯ ФУНКЦИЙ ПРЕДНАЗНАЧЕНИЯ И ДЕЯТЕЛЬНОСТИ | O | |
| CP-2 (6) | АЛЬТЕРНАТИВНЫЕ ОБЪЕКТЫ ОБРАБОТКИ И ХРАНЕНИЯ ИНФОРМАТИЗАЦИИ | O | |
| CP-2 (7) | КООРДИНАЦИЯ С ВНЕШНИМИ ПОСТАВЩИКАМИ СЕРВИСОВ | O | |
| CP-2 (8) | ОПРЕДЕЛЕНИЕ КРИТИЧЕСКИ ВАЖНЫХ АКТИВОВ | O | |
| **CP-3** | **Обучение действиям в непредвиденных обстоятельствах** | O | √ |
| CP-3 (1) | МОДЕЛИРУЕМЫЕ СОБЫТИЯ | O | √ |
| CP-3 (2) | МЕХАНИЗМЫ, ИСПОЛЬЗУЕМЫЕ В СРЕДАХ ОБУЧЕНИЯ | O | √ |
| **CP-4** | **Тестирование плана на случай непредвиденных обстоятельств** | O | √ |
| CP-4 (1) | КООРДИНАЦИЯ С СООТВЕТСТВУЮЩИМИ ПЛАНАМИ | O | √ |
| CP-4 (2) | АЛЬТЕРНАТИВНЫЙ ОБЪЕКТ ОБРАБОТКИ ИНФОРМАЦИИ | O | √ |
| CP-4 (3) | АВТОМАТИЗИРОВАННОЕ ТЕСТИРОВАНИЕ | O | √ |
| CP-4 (4) | ПОЛНОЕ ВОССТАНОВЛЕНИЕ И ВОССОЗДАНИЕ | O | √ |
| CP-4 (5) | САМОПРОВЕРКА | O/S | √ |
| CP-5 | **Обновление плана на случай непредвиденных обстоятельств** | W: Включено в состав CP-2. | |
| **CP-6** | **Альтернативный объект хранения информации** | O | |
| CP-6 (1) | РАЗДЕЛЕНИЕ С ОСНОВНЫМ ОБЪЕКТОМ | O | |
| CP-6 (2) | ЦЕЛИ ВРЕМЕНИ ВОССТАНОВЛЕНИЯ И ТОЧКИ ВОССТАНОВЛЕНИЯ | O | |
| CP-6 (3) | ДОСТУПНОСТЬ | O | |
| **CP-7** | **Альтернативный объект обработки информации** | O | |
| CP-7 (1) | РАЗДЕЛЕНИЕ С ОСНОВНЫМ ОБЪЕКТОМ | O | |
| CP-7 (2) | ДОСТУПНОСТЬ | O | |
| CP-7 (3) | ПРИОРИТЕТ ОБСЛУЖИВАНИЯ | O | |
| CP-7 (4) | ПОДГОТОВКА К ИСПОЛЬЗОВАНИЮ | O | |
| CP-7 (5) | ЭКВИВАЛЕНТНЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ | W: Включено в состав CP-7. | |
| CP-7 (6) | НЕВОЗМОЖНОСТЬ ВОЗВРАТА НА ОСНОВНОЙ ОБЪЕКТ | O | |
| **CP-8** | **Телекоммуникационные сервисы** | O | |
| CP-8 (1) | ПОЛОЖЕНИЯ О ПРИОРИТЕТТ СЕРВИСОВ | O | |
| CP-8 (2) | ОДИНОЧНЫЕ ТОЧКИ ОТКАЗА | O | |
| CP-8 (3) | РАЗДЕЛЕНИЕ ОСНОВНЫХ И АЛЬТЕРНАТИВНЫХ ПОСТАВЩИКОВ | O | |
| CP-8 (4) | ПЛАН НА СЛУЧАЙ НЕПРЕДВИДЕННЫХ ОБСТОЯТЕЛЬСТВ ДЛЯ ПОСТАВЩИКА | O | |
| CP-8 (5) | ТЕСТИРОВАНИЕ АЛЬТЕРНАТИВНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕРВИСОВ | O | |
| **CP-9** | **Системы резервного копирования** | O | |
| CP-9 (1) | ИСПЫТАНИЯ НА НАДЕЖНОСТЬ И ЦЕЛОСТНОСТЬ | O | |
| CP-9 (2) | ПРОВЕРКА ВОССТАНОВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ВЫБОРКИ | O | |
| CP-9 (3) | ОТДЕЛЬНАЯ СИСТЕМА ХРАНЕНИЯ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИИ | O | |
| CP-9 (4) | ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ИЗМЕНЕНИЯ | W: Включено в состав CP-9. | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| CP-9 (5) | ПЕРЕНОС НА АЛЬТЕРНАТИВНЫЙ ОБЪЕКТ ХРАНЕНИЯ ИНФОРМАЦИИ | O | |
| CP-9 (6) | ВТОРИЧНАЯ СИСТЕМА РЕЗЕРВИРОВАНИЯ | O | |
| CP-9 (7) | ДВОЙНОЕ РАЗРЕШЕНИЕ НА УДАЛЕНИЕ ИЛИ УНИЧТОЖЕНИЕ | O | |
| CP-9 (8) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | O | |
| **CP-10** | **Восстановление и рекофигурирование системы** | O | |
| CP-10 (1) | ТЕСТИРОВАНИЕ ПЛАНА НА СЛУЧАЙ НЕПРЕДВИДЕННЫХ ОБСТОЯТЕЛЬСТВ | W: Включено в состав CP-4. | |
| CP-10 (2) | ВОССТАНОВЛЕНИЕ ТРАНЗАКЦИЙ | O | |
| CP-10 (3) | КОМПЕНСИРУЮЩИЕ МЕРЫ БЕЗОПАСНОСТИ | W: Адресовано посредством | |
| CP-10 (4) | ВОССТАНОВЛЕНИЕ В ТЕЧЕНИЕ ПЕРИОДА ВРЕМЕНИ | O | |
| CP-10 (5) | СПОСОБНОСТЬ ВОССТАНОВЛЕНИЯ ПОСЛЕ ОТКАЗА | W: Включено в состав SI-13. | |
| CP-10 (6) | КОМПОНЕНТНАЯ ЗАЩИТА | O | |
| **CP-11** | **Альтернативные протоколы взаимодействия** | O | |
| **CP-12** | **Безопасный способ** | S | √ |
| **CP-13** | **Альтернативные механизмы обеспечения безопасности** | O/S | |

## ТАБЛИЦА C-7: СЕМЕЙСТВО ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **IA-1** | **Политика и процедуры** | O | √ |
| **IA-2** | **Идентификация и аутентификация (пользователи организации)** | O/S | |
| IA-2 (1) | МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ ПРИВИЛЕГИРОВАННЫХ УЧЕТНЫХ ЗАПИСЕЙ. | S | |
| IA-2 (2) | МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ НЕПРИВИЛЕГИРОВАННЫХ УЧЕТНЫХ ЗАПИСЕЙ. | S | |
| IA-2 (3) | ЛОКАЛЬНЫЙ ДОСТУП К ПРИВИЛЕГИРОВАННЫМ УЧЕТНЫМ ЗАПИСЯМ | W: Включено в IA -2 (1 | |
| IA-2 (4) | ЛОКАЛЬНЫЙ ДОСТУП К НЕПРИВИЛЕГИРОВАННЫМ УЧЕТНЫМ ЗАПИСЯМ. | W: Включено в IA -2 (2 | |
| IA-2 (5) | ИНДИВИДУАЛЬНАЯ АУТЕНТИФИКАЦИЯ С ГРУППОВОЙ АУТЕНТИФИКАЦИЕЙ | O/S | |
| IA-2 (6) | ДОСТУП К УЧЕТНЫМ ЗАПИСЯМ - ОТДЕЛЬНОЕ УСТРОЙСТВО. | S | |
| IA-2 (7) | СЕТЕВОЙ ДОСТУП К НЕПРИВИЛЕГИРОВАННЫМ УЧЕТНЫМ ЗАПИСЯМ - ОТДЕЛЬНОЕ УСТРОЙСТВО. | W: Включено в IA -2 (6 | |
| IA-2 (8) | ДОСТУП К УЧЕТНЫМ ЗАПИСЯМ - УСТОЙЧИВОСТЬ К ПОДМЕНЕ | S | |
| IA-2 (9) | СЕТЕВОЙ ДОСТУП К НЕПРИВИЛЕГИРОВАННЫМ УЧЕТНЫМ ЗАПИСЯМ - УСТОЙЧИВОСТЬ К ПОДМЕНЕ. | W: Включено в IA -2 (8 | |
| IA-2 (10) | ОТДЕЛЬНЫЙ ВХОД В СИСТЕМУ | S | |
| IA-2 (11) | УДАЛЕННЫЙ ДОСТУП - ОТДЕЛЬНОЕ УСТРОЙСТВО. | W: Включено в IA -2 (6 | |
| IA-2 (12) | ПРИНЯТИЕ УЧЁТНЫХ ДАННЫХ PIV | S | |
| IA-2 (13) | ВНЕПОЛОСНАЯ АУТЕНТИФИКАЦИЯ | S | |
| **IA-3** | **Идентификация и аутентификация устройств** | S | |
| IA-3 (1) | КРИПТОГРАФИЧЕСКАЯ ДВУНАПРАВЛЕННАЯ АУТЕНТИФИКАЦИЯ. | S | |
| IA-3 (2) | КРИПТОГРАФИЧЕСКАЯ ДВУНАПРАВЛЕННАЯ СЕТЕВАЯ АУТЕНТИФИКАЦИЯ. | W: Включено в IA -3 (1 | |
| IA-3 (3) | ДИНАМИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ АДРЕСОВ | O | |
| IA-3 (4) | АТТЕСТАЦИЯ УСТРОЙСТВА | O | |
| **IA-4** | **Управление идентификацией** | O | |
| IA-4 (1) | ЗАПРЕЩЕНИЕ ИСПОЛЬЗОВАНИЯ ИДЕНТИФИКАТОРОВ УЧЕТНЫХ ЗАПИСЕЙ В КАЧЕСТВЕ ОТКРЫТЫХ ИДЕНТИФИКАТОРОВ | O | |
| IA-4 (2) | САНКЦИОНИРОВАНИЕ СУПЕРВИЗОРА | W: Включено в IA -12 (1 | |
| IA-4 (3) | МНОЖЕСТВЕННЫЕ ФОРМЫ СЕРТИФИКАЦИИ | W: Включено в IA -12 (2 | |
| IA-4 (4) | ОПРЕДЕЛЕНИЕ СТАТУСА ПОЛЬЗОВАТЕЛЯ | O | |
| IA-4 (5) | ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ | S | |
| IA-4 (6) | УПРАВЛЕНИЕ МЕЖДУ ОРГАНИЗАЦИЯМИ | O | |
| IA-4 (7) | ОЧНАЯ РЕГИСТРАЦИЯ | W: Включено в IA -12 (4 | |
| IA-4 (8) | ПАРНЫЕ ПСЕВДОНИМНЫЕ ИДЕНТИФИКАТОРЫ. | O | |
| IA-4 (9) | ПОДДЕРЖКА И ЗАЩИТА АТРИБУТОВ | O/S | |
| **IA-5** | **Управление утентификацией** | O/S | |
| IA-5 (1) | АУТЕНТИФИКАЦИЯ ОСНОВАННАЯ НА ПАРОЛЕ | O/S | |
| IA-5 (2) | АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ОТКРЫТОГО КЛЮЧА. | S | |
| IA-5 (3) | ОЧНАЯ РЕГИСТРАЦИЯ ИЛИ РЕГИСТРАЦИЯ У ДОВЕРЕННЫХ ВНЕШНИХ ЛИЦ | W: Включено в IA -12 (4 | |
| IA-5 (4) | АВТОМАТИЗИРОВАННАЯ ПОДДЕРЖКА ОПРЕДЕЛЕНИЯ СТОЙКОСТИ ПАРОЛЯ | W: Включено в IA -5 (1 | |
| IA-5 (5) | ИЗМЕНЕНИЕ АУТЕНТИФИКАТОРОВ ПЕРЕД ДОСТАВКОЙ | O | |
| IA-5 (6) | ЗАЩИТА АУТЕНТИФИКАТОРОВ | O | |
| IA-5 (7) | ОТСУТСТВИЕ ВСТРОЕННЫХ НЕЗАШИФРОВАННЫХ СТАТИЧЕСКИХ АУТЕНТИФИКАТОРОВ | O | |
| IA-5 (8) | НЕСКОЛЬКО СИСТЕМНЫХ УЧЕТНЫХ ЗАПИСЕЙ | O | |
| IA-5 (9) | ФЕДЕРАТИВНОЕ УПРАВЛЕНИЕ УЧЁТНЫМИ ДАННЫМИ | O | |
| IA-5 (10) | ДИНАМИЧЕСКАЯ ПРИВЯЗКА УЧЁТНЫХ ДАННЫХ | S | |
| IA-5 (11) | АППАРАТНАЯ АУТЕНТИФИКАЦИЯ НА ОСНОВЕ МАРКЕРОВ. | W: Включено в IA -2 (1) и IA -2 | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| IA-5 (12) | ПРОИЗВОДИТЕЛЬНОСТЬ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ | S | |
| IA-5 (13) | СРОК ДЕЙСТВИЯ КЭШИРОВАННЫХ АУТЕНТИФИКАТОРОВ | S | |
| IA-5 (14) | УПРАВЛЕНИЕ СОДЕРЖИМЫМ ХРАНИЛИЩ ДОВЕРИЯ PKI | O | |
| IA-5 (15) | ПРОДУКТЫ И СЕРВИСЫ, ОДОБРЕННЫЕ GSA | O | |
| IA-5 (16) | ВЫДАЧА АУТЕНТИФИКАТОРА ОЧНАЯ ИЛИ ДОВЕРЕННОЙ ВНЕШНЕЙ СТОРОНОЙ | O | |
| IA-5 (17) | ОБНАРУЖЕНИЕ АТАКИ ПРЕДСТАВЛЕНИЯ ДЛЯ БИОМЕТРИЧЕСКИХ АУТЕНТИФИКАТОРОВ | S | |
| IA-5 (18) | МЕНЕДЖЕРЫ ПАРОЛЕЙ | S | |
| **IA-6** | **Обратная связь при аутентификации** | S | |
| **IA-7** | **Аутентификация криптографическим модулем** | S | |
| **IA-8** | **Идентификация и аутентификация (пользователи не из организации)** | S | |
| IA-8 (1) | ПРИНЯТИЕ УЧЁТНЫХ ДАННЫХ PIV ОТ ДРУГИХ АГЕНТСТВ | S | |
| IA-8 (2) | ПРИНЯТИЕ ВНЕШНИХ АУТЕНТИФИКАТОРОВ | S | |
| IA-8 (3) | ИСПОЛЬЗОВАНИЕ ПРОДУКТОВ, ОДОБРЕННЫХ FICAM | W: Включено в IA -8 (2 | |
| IA-8 (4) | ИСПОЛЬЗОВАНИЕ УСТАНОВЛЕННЫХ ПРОФИЛЕЙ | S | |
| IA-8 (5) | ПРИНЯТИЕ УЧЁТНЫХ ДАННЫХ PIV-I | S | |
| IA-8 (6) | ДИССОЦИАТИВНОСТЬ | O | |
| **IA-9** | **Сервисы идентификации и аутентификации** | O/S | |
| IA-9 (1) | ОБМЕН ИНФОРМАЦИЕЙ | W: Включено в IA -9 | |
| IA-9 (2) | ПЕРЕДАЧА РЕШЕНИЙ | W: Включено в IA -9 | |
| **IA-10** | **Адаптивная аутентификация** | O | |
| **IA-11** | **Переаутентификация** | O/S | |
| **IA-12** | **Подтверждение личности** | O | |
| IA-12 (1) | СУПЕРВИЗОР АВТОРИЗАЦИИ | O | |
| IA-12 (2) | ИДЕНТИФИКАЦИОННЫЕ ДАННЫЕ | O | |
| IA-12 (3) | ПРОВЕРКА И ПОДТВЕРЖДЕНИЕ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ | O | |
| IA-12 (4) | ОЧНАЯ ПРОВЕРКА И ПОДТВЕРЖДЕНИЕ | O | |
| IA-12 (5) | ПОДТВЕРЖДЕНИЕ АДРЕСА | O | |
| IA-12 (6) | ПРИЯТИЕ ИДЕНТИФИКАЦИООНЫХ ДАННЫХ, ПОДТВЕРЖДЕННЫХ ВНЕШНИМИ ИСТОЧНИКАМИ | O | |

## ТАБЛИЦА C-8: СЕМЕЙСТВО РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **IR-1** | **Политика и процедуры** | O | √ |
| **IR-2** | **Обучение реагированию на инциденты** | O | √ |
| IR-2 (1) | МОДЕЛИРУЕМЫЕ СОБЫТИЯ | O | √ |
| IR-2 (2) | АВТОМАТИЗИРОВАННЫЕ УЧЕБНЫЕ СРЕДЫ | O | √ |
| IR-2 (3) | ОБЗОР | O | √ |
| **IR-3** | **Тестирование реакции на инциденты** | O | √ |
| IR-3 (1) | АВТОМАТИЗИРОВАННОЕ ТЕСТИРОВАНИЕ | O | √ |
| IR-3 (2) | КООРДИНАЦИЯ С СООТВЕТСТВУЮЩИМИ ПЛАНАМИ | O | √ |
| IR-3 (3) | НЕПРЕРЫВНОЕ СОВЕРШЕНСТВОВАНИЕ | O | √ |
| **IR-4** | **Обработка инцидентов** | O | |
| IR-4 (1) | АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ОБРАБОТКИ ИНЦИДЕНТОВ | O | |
| IR-4 (2) | ДИНАМИЧЕСКАЯ РЕКОНФИГУРАЦИЯ | O | |
| IR-4 (3) | НЕПРЕРЫВНОСТЬ ДЕЯТЕЛЬНОСТИ | O | |
| IR-4 (4) | КОРРЕЛЯЦИЯ ИНФОРМАЦИИ | O | |
| IR-4 (5) | АВТОМАТИЧЕСКОЕ ОТКЛЮЧЕНИЕ СИСТЕМЫ | O/S | |
| IR-4 (6) | УГРОЗЫ ПОСВЯЩЕННОГО ЛИЦА | O | |
| IR-4 (7) | ИНСАЙДЕРСКИЕ УГРОЗЫ - КООРДИНАЦИЯ ВНУТРИ ОРГАНИЗАЦИИ | O | |
| IR-4 (8) | СВЯЗЬ С ВНЕШНИМИ ОРГАНИЗАЦИЯМИ | O | |
| IR-4 (9) | ВОЗМОЖНОСТЬ ДИНАМИЧЕСКОГО ОТВЕТА | O | |
| IR-4 (10) | КООРДИНАЦИЯ ЦЕПОЧКИ ПОСТАВОК | O | |
| IR-4 (11) | ОБЪЕДИНЕННАЯ ГРУППА РЕАКЦИИ НА ИНЦИДЕНТЫ | O | |
| IR-4 (12) | ВРЕДОНОСНЫЙ КОД И КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ | O | |
| IR-4 (13) | АНАЛИЗ ПОВЕДЕНИЯ | O | |
| IR-4 (14) | ЦЕНТР ОПЕРАЦИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ | O/S | |
| IR-4 (15) | СВЯЗИ С ОБЩЕСТВЕННОСТЬЮ И ВОССТАНОВЛЕНИЕ РЕПУТАЦИИ | O | |
| **IR-5** | **Мониторинг инцидентов** | O | √ |
| IR-5 (1) | АВТОМАТИЗИРОВАННОЕ ОТСЛЕЖИВАНИЕ, СБОР И АНАЛИЗ ДАННЫХ | O | √ |
| **IR-6** | **Отчетность об инцидентах** | O | |
| IR-6 (1) | АВТОМАТИЗИРОВАННАЯ ОТЧЕТНОСТЬ | O | |
| IR-6 (2) | УЯЗВИМОСТИ, СВЯЗАННЫЕ С ИНЦИДЕНТАМИ | O | |
| IR-6 (3) | КООРДИНАЦИЯ ЦЕПОЧКИ ПОСТАВОК | O | |
| **IR-7** | **Помощь в реагировании на инциденты** | O | |
| IR-7 (1) | АВТОМАТИЗИРОВАННАЯ ПОДДЕРЖКА ОБЕСПЕЧЕНИЯ И ПОДДЕРЖАНИЯ ДОСТУПНОСТИ ИНФОРМАЦИИ | O | |
| IR-7 (2) | КООРДИНАЦИЯ С ВНЕШНИМИ ПОСТАВЩИКАМИ | O | |
| **IR-8** | **План реагирования на инциденты** | O | |
| IR-8 (1) | ОБЗОРЫ | O | |
| **IR-9** | **Реагирование на утечку информации** | O | |
| IR-9 (1) | ОТВЕТСТВЕННЫЙ ПЕРСОНАЛ | W: Включено в состав IR-9. | |
| IR-9 (2) | ОБУЧЕНИЕ | O | |
| IR-9 (3) | ДЕЙСТВИЯ ПОСЛЕ УТЕЧКИ | O | |
| IR-9 (4) | ВОЗДЕЙСТВИЕ НА НЕАВТОРИЗОВАННЫЙ ПЕРСОНАЛ | O | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| IR-10 | Объединённая группа анализа информационной безопасности | Ш: Перенесено в IR-4 (11). | |

## ТАБЛИЦА C-9: СЕМЕЙСТВО ПОДДЕРЖКИ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **MA 1** | **Политика и процедуры** | O | √ |
| **MA 2** | **Контролируемая поддержка** | O | |
| MA 2 (1) | СОДЕРЖАНИЕ ОТЧЁТА | W: Включено в состав MA-2. | |
| MA 2 (2) | АВТОМАТИЗИРОВАННЫЕ РАБОТЫ ПО ПОДДЕРЖКЕ | O | |
| **MA 3** | **Инструменты поддержки** | O | |
| MA 3 (1) | ИНСПЕКЦИЯ ИНСТРУМЕНТОВ | O | |
| MA 3 (2) | ИНСПЕКЦИЯ НОСИТЕЛТQ ИНФОРМАЦИИ | O | |
| MA 3 (3) | ПРЕДОТВРАЩЕНИЕ НЕСАНКЦИОНИРОВАННОГО ДЕМОНТАЖА | O | |
| MA 3 (4) | ОГРАНИЧЕННОЕ НА ИСПОЛЬЗОВАНИЕ ИНСТРУМЕНТОВ | O/S | |
| MA 3 (5) | ВЫПОЛНЕНИЕ С ПРИВИЛЕГИЯМИ | O/S | |
| MA 3 (6) | ОБНОВЛЕНИЯ И ИСПРАВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ | O/S | |
| **MA 4** | **Нелокальная поддержка** | O | |
| MA 4 (1) | РЕГИСТРАЦИЯ И ПЕРЕСМОТР | O | |
| MA 4 (2) | ДОКУМЕНТ НЕЛОКАЛЬНОЙ ПОДДЕРЖКИ | W: Включено в MA-1 и MA-4. | |
| MA 4 (3) | СОПОСТАВИМАЯ БЕЗОПАСНОСТЬ И САНАЦИЯ | O | |
| MA 4 (4) | АУТЕНТИФИКАЦИЯ И РАЗДЕЛЕНИЕ СЕССИЙ ПОДДЕРЖКИ | O | |
| MA 4 (5) | ОДОБРЕНИЯ И УВЕДОМЛЕНИЯ | O | |
| MA 4 (6) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | O/S | |
| MA 4 (7) | ПРЕКРАЩЕНИЕ ПРОВЕРКИ | S | |
| **MA 5** | **Персонал поддержки** | O | |
| MA 5 (1) | ЛИЦА, НЕ ИМЕЮЩИЕ НАДЛЕЖАЩЕГО ДОСТУПА | O | |
| MA 5 (2) | ДОПУСК КРАБОТЕ С КЛАССИФИЦИРОВАННЫМИ СИСТЕМАМИ | O | |
| MA 5 (3) | ТРЕБОВАНИЯ К ГРАЖДАНСТВУ ДЛЯ КЛАССИФИЦИРОВАННЫХ СИСТЕМ | O | |
| MA 5 (4) | ИНОСТРАННЫЕ ПОДДАННЫЕ | O | |
| MA 5 (5) | НЕСИСТЕМНАЯ ПОДДЕРЖКА | O | |
| **MA 6** | **Своевременная поддержка** | O | |
| MA 6 (1) | ПРЕВЕНТИВНАЯ ПОДДЕРЖКА | O | |
| MA 6 (2) | ПРОГНОЗИРУЮЩАЯ ПОДДЕРЖКА | O | |
| MA 6 (3) | АВТОМАТИЗИРОВАННАЯ ПОДДЕРЖКА ПРОГНОСТИЧЕСКОГО ОБСЛУЖИВАНИЯ | O | |
| **MA 7** | **Обектовая поддержка** | O | |

## ТАБЛИЦА C-10: СЕМЕЙСТВО ЗАЩИТЫ НОСИТЕЛЕЙ ИНФОРМАЦИИ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **MP 1** | **Политика и процедуры** | O | √ |
| **MP 2** | **Доступ к носителяv информации** | O | |
| MP 2 (1) | АВТОМАТИЗИРОВАННЫЙ ОГРАНИЧЕННЫЙ ДОСТУП | W: Включено в MP-4 (2). | |
| MP 2 (2) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | W: Включено в SC -28 (1). | |
| **MP 3** | **Маркирование носителей информации** | O | |
| **MP 4** | **Хранение носителей информации** | O | |
| MP 4 (1) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | W: Включено в SC -28 (1). | |
| MP 4 (2) | АВТОМАТИЗИРОВАННЫЙ ОГРАНИЧЕННЫЙ ДОСТУП | O | |
| **MP 5** | **Транспортировка носителя информации** | O | |
| MP 5 (1) | ЗАЩИТА ЗА ПРЕДЕЛАМИ КОНТРОЛИРУЕМЫХ ЗОН | W: Включено в состав MP-5. | |
| MP 5 (2) | ДОКУМЕНТРОВАНИЕ О РАБОТ | W: Включено в состав MP-5. | |
| MP 5 (3) | ОХРАННИКИ | O | |
| MP 5 (4) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | W: Включено в SC -28 (1). | |
| **MP 6** | **Очистка носителей информации** | O | |
| MP 6 (1) | РАССМОТРЕНИЕ, УТВЕРЖДЕНИЕ, ОТСЛЕЖИВАНИЕ, ДОКУМЕНТИРОВАНИЕ И ПРОВЕРКА | O | |
| MP 6 (2) | ТЕСТИРОВАНИЕ ОБОРУДОВАНИЯ | O | |
| MP 6 (3) | НЕРАЗРУШАЮЩИЕ ТЕХНОЛОГИИ | O | |
| MP 6 (4) | КОНТРОЛИРУЕМАЯ НЕКЛАССИФИЦИРОВАННАЯ ИНФОРМАЦИЯ | W: Включено в состав MP-6. | |
| MP 6 (5) | СЕКРЕТНЫЕ ДАННЫЕ | W: Включено в состав MP-6. | |
| MP 6 (6) | РАЗРУШЕНИЕ НОСИТЕЛЕЙ ИНФОРМАЦИИ | W: Включено в состав MP-6. | |
| MP 6 (7) | ДВОЙНОЕ САНКЦИОНИРОВАНИЕ | O | |
| MP 6 (8) | ДИСТАНЦИОННАЯ ОЧИСТКА ИЛИ СТИРАНИЕ ИНФОРМАЦИИ. | O | |
| **MP 7** | **Использование носителей информации** | O | |
| MP 7 (1) | ЗАПРЕЩЕНИЕ ИСПОЛЬЗОВАНИЯ БЕЗ ВЛАДЕЛЬЦА | W: Включено в состав MP-7. | |
| MP 7 (2) | ЗАПРЕЩЕНИЕ ИСПОЛЬЗОВАНИЯ УСТОЙЧИВЫХ К САНИРОВАНИЮ НОСИТЕЛЕЙ ИНФОРМАЦИИ | O | |
| **MP 8** | **Понижение статуса носителя информации** | O | |
| MP 8 (1) | ДОКУМЕНТАЦИЯ ПО ПРОЦЕССУ | O | |
| MP 8 (2) | ТЕСТИРОВАНИЕ ОБОРУДОВАНИЯ | O | |
| MP 8 (3) | КОНТРОЛИРУЕМАЯ НЕКЛАССИФИЦИРОВАННАЯ ИНФОРМАЦИЯ | O | |
| MP 8 (4) | СЕКРЕТНЫЕ ДАННЫЕ | O | |

## ТАБЛИЦА C-11: СЕМЕЙСТВО ФИЗИЧЕСКОЙ ЗАЩИТЫ И ЗАЩИТЫ СРЕДЫ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **PE-1** | **Политика и процедуры** | O | √ |
| **PE-2** | **Разрешение физического доступа** | O | |
| PE-2 (1) | ДОСТУП ПО ДОЛЖНОСТИ И РОЛИ | O | |
| PE-2 (2) | ДВЕ ФОРМЫ ИДЕНТИФИКАЦИИ | O | |
| PE-2 (3) | ОГРАНИЧЕНИЕ ДОСТУПА БЕЗ СОПРОВОЖДЕНИЯ | O | |
| **PE-3** | **Контроль физического доступа** | O | |
| PE-3 (1) | СИСТЕМНЫЙ ДОСТУП | O | |
| PE-3 (2) | ВОЗМОЖНОСТИ И СИСТЕМЫ | O | |
| PE-3 (3) | НЕПРЕРЫВНАЯ ОХРАНА | O | |
| PE-3 (4) | ЗАПИРАЕМЫЕ ПОМЕЩЕНИЯ | O | |
| PE-3 (5) | ЗАЩИТА ОТ ВСКРЫТИЯ | O | |
| PE-3 (6) | ТЕСТИРОВАНИЕ ОБЪЕКТОВ НА ПРОНИКНОВЕНИЕ | W: Включено в CA -8 | |
| PE-3 (7) | ФИЗИЧЕСКИЕ БАРЬЕРЫ | O | |
| PE-3 (8) | КОНТРОЛЯ ДОСТУПА В ВЕСТИБЮЛИ | O | |
| **PE-4** | **Контроль доступа при переносе** | O | |
| **PE-5** | **Контроль доступа к устройствам вывода** | O | |
| PE-5 (1) | ДОСТУП К ВЫВОДУ УПОЛНОМОЧЕННЫХ ЛИЦ | W: Включено в состав PE-5. | |
| PE-5 (2) | СВЯЗЬ С ИДЕНТИФИКАЦИОННЫМИ ДАННЫМИ ИНДИВИДУУМОВ | S | |
| PE-5 (3) | МАРКИРОВКА УСТРОЙСТВ ВЫВОДА | W: Включено в состав PE-22. | |
| **PE-6** | **Мониторинг физического доступа** | O | √ |
| PE-6 (1) | ОБОРУДОВАНИЕ ДЛЯ СИГНАЛИЗАЦИИ И НАБЛЮДЕНИЯ ВТОРЖЕНИЯ | O | √ |
| PE-6 (2) | АВТОМАТИЧЕСКОЕ РАСПОЗНАВАНИЕ ВТОРЖЕНИЙ И РЕАГИРОВАНИЕ НА НИХ | O | √ |
| PE-6 (3) | ВИДЕОНАБЛЮДЕНИЕ | O | √ |
| PE-6 (4) | КОНТРОЛЬ ФИЗИЧЕСКОГО ДОСТУПА К СИСТЕМАМ | O | √ |
| **PE-7** | **Контроль посетителей** | W: Включено в PE-2 и PE-3. | |
| **PE-8** | **Записи о доступе посетителей** | O | √ |
| PE-8 (1) | АВТОМАТИЗИРОВАННАЯ ПОДДЕРЖКА И ПЕРЕСМОТР ЗАПИСЕЙ | O | |
| PE-8 (2) | ЗАПИСИ ФИЗИЧЕСКОГО ДОСТУПА | W: Включено в состав PE-2. | |
| PE-8 (3) | ОГРАНИЧЕНИЕ ЭЛЕМЕНТОВ ПЕРСОНАЛЬНОЙ ИДЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ | O | |
| **PE-9** | **Силовое оборудование и кабели** | O | |
| PE-9 (1) | РЕЗЕРВИРОВАНИЕ КАБЕЛЕЙ | O | |
| PE-9 (2) | МЕРЫ АВТОМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ НАПРЯЖЕНИЯ | O | |
| **PE-10** | **Аварийное отключение** | O | |
| PE-10 (1) | СЛУЧАЙНОЕ И НЕСАНКЦИОНИРОВАННОЕ ВКЛЮЧЕНИЕ | W: Включено в состав PE-10. | |
| **PE-11** | **Аварийные источники питания** | O | |
| PE-11 (1) | АЛЬТЕРНАТИВНЫЙ ИСТОЧНИК ПИТАНИЯ - МИНИМАЛЬНЫЕ ЭКСПЛУАТАЦИОННЫЕ ВОЗМОЖНОСТИ | O | |
| PE-11 (2) | АЛЬТЕРНАТИВНЫЙ ИСТОЧНИК ЭНЕРГИИ - АВТОНОМНЫЙ | O | |
| **PE-12** | **Аварийное освещение** | O | |
| PE-12 (1) | ОСНОВНОЕ ПРЕДНАЗНАЧЕНИЕ И ЗАДАЧИ | O | |
| **PE-13** | **Противопожарная защита** | O | |
| PE-13 (1) | СИСТЕМЫ ОБНАРУЖЕНИЯ - АВТОМАТИЧЕСКОЕ ВКЛЮЧЕНИЕ И ОПОВЕЩЕНИЕ | O | |
| PE-13 (2) | СИСТЕМЫ ПОДАВЛЕНИЯ - АВТОМАТИЧЕСКОЕ ВКЛЮЧЕНИЕ И ОПОВЕЩЕНИЕ | O | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| PE-13 (3) | АВТОМАТИЧЕСКОЕ ПОЖАРОТУШЕНИЕ | W: Включено в PE-13 (2). | |
| PE-13 (4) | ПРОВЕРКИ | O | |
| **PE-14** | **Контроль за состоянием среды** | O | |
| PE-14 (1) | АВТОМАТИЧЕСКИЙ КОНТРОЛЬ | O | |
| PE-14 (2) | МОНИТОРИНГ С ПОМОЩЬЮ АВАРИЙНЫХ СИГНАЛОВ И УВЕДОМЛЕНИЙ | O | |
| **PE-15** | **Защита от повреждения водой** | O | |
| PE-15 (1) | АВТОМАТИЗОВАННАЯ ПОДДЕРЖКА | O | |
| **PE-16** | **Поставка и ликвидация** | O | |
| **PE-17** | **Альтернативный рабочий объект информатизации** | O | |
| **PE-18** | **Расположение компонентов системы** | O | |
| PE-18 (1) | ВОЗМОЖНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ | w: Перенесено в PE-23. | |
| **PE-19** | **Утечка информации** | O | |
| PE-19 (1) | НАЦИОНАЛЬНАЯ ПОЛИТИКА И ПРОЦЕДУРЫ В ОБЛАСТИ УТЕЧКИ | O | |
| **PE-20** | **Мониторинг и прослеживание активов** | O | |
| **PE-21** | **Защита от электромагнитных импульсов** | O | |
| **PE-22** | **Маркирование компонентов** | O | |
| **PE-23** | **Возможности местоположения** | O | |

## ТАБЛИЦА C-12: СЕМЕЙСТВО ПЛАНИРОВАНИЯ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **PL- 1** | **Политика и процедуры** | O | √ |
| **PL- 2** | **Планы безопасности и приватности системы** | O | √ |
| PL- 2 (1) | КОНЦЕПЦИЯ ПРИМЕНЕНИЯ | W: Включено в состав PL-7. | |
| PL- 2 (2) | ФУНКЦИОНАЛЬНАЯ АРХИТЕКТУРА | W: Включено в состав PL-8. | |
| PL- 2 (3) | ПЛАНИРОВАНИЕ И КООРДИНАЦИЯ С ДРУГИМИ СУЩНОСТЯМИ ОРГАНИЗАЦИИ | W: Включено в состав PL-2. | |
| **PL- 3** | **Обновление плана безопасности системы** | W: Включено в состав PL-2. | |
| **PL- 4** | **Правила поведения** | O | √ |
| PL- 4 (1) | ОГРАНИЧЕНИЯ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНЫХ МЕДИА И ВНЕШНИХ САЙТОВ/ПРИЛОЖЕНИЙ | O | √ |
| **PL- 5** | **Оценка влияния на приватность** | W: Включено в RA -8 | |
| **PL- 6** | **Планирование работ, связанных с безопасностью** | W: Включено в состав PL-2. | |
| **PL- 7** | **Концепция применения** | O | |
| **PL- 8** | **Архитектуры безопасности и приватности** | O | √ |
| PL- 8 (1) | ГЛУБОКАЯ ЗАЩИТА | O | √ |
| PL- 8 (2) | РАЗНООБРАЗИЕ ПОСТАВЩИОВ | O | √ |
| **PL- 9** | **Центральное управление** | O | √ |
| **PL- 10** | **Базовый выбор** | O | |
| **PL- 11** | **Базовая адаптация** | O | |

## ТАБЛИЦА C-13: СЕМЕЙСТВО УПРАВЛЕНИЯ ПРОГРАММАМИ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| PM-1 | **План программы информационной безопасности** | o | |
| PM-2 | **Роль лидера программы информационной безопасности** | o | |
| PM-3 | **Ресурсы по информационной безопасности и приватности** | o | |
| PM-4 | **Процесс планирования действий и вех** | o | |
| PM-5 | **Инвентаризация систем** | o | |
| PM-5 (1) | ИНВЕНТАРИЗАЦИЯ ПЕРСОНАЛЬНОЙ ИДЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ | o | |
| PM-6 | **Показатели эффективности** | o | √ |
| PM-7 | **Архитектура предприятия** | o | |
| PM-7 (1) | РАЗГРУЗКА | o | |
| PM-8 | **План критической инфраструктуры** | o | |
| PM-9 | **Стратегия управления рисками** | o | √ |
| PM-10 | **Процесс санкционирования** | o | √ |
| PM-11 | **Определение предназначения и деятельности** | o | |
| PM-12 | **Программа защиты от инсайдерских угроз** | o | √ |
| PM-13 | **Сотрудники безопасности и приватности** | o | |
| PM-14 | **Тестирование, обучение имониторинг** | o | √ |
| PM-15 | **Группы и ассоциации безопасности и приватности** | o | |
| PM-16 | **Программа освоения по угрозам** | o | √ |
| PM-16 (1) | АВТОМАТИЗИРОВАННЫЕ СРЕДСТВА ОБМЕНА РАЗВЕДКОЙ ОБ УГРОЗАХ. | o | √ |
| PM-17 | **Защита неклассифицированной информации о внешних** | o | √ |
| PM-18 | **План программы приватности** | o | |
| PM-19 | **Роль лидера программы приватности** | o | |
| PM-20 | **Распространение информации о программе приватности** | o | |
| PM-20 (1) | ПОЛИТИКИ ПРИВАТНОСТИ НА ВЕБСАЙТАХ, В ПРИЛОЖЕНИЯХ И ЦИФРОВЫХ СЕРВИСАХ | o | √ |
| PM-21 | **Учет раскрытия информации** | o | |
| PM-22 | **Управление персональной идентификационной информацией** | o | √ |
| PM-23 | **Орган управления данными** | o | √ |
| PM-24 | **Совет по целостности данных** | o | √ |
| PM-25 | **Минимизация персональной идентификационной информации, используемой при тестировании, обучении и** | o | |
| PM-26 | **Управление жалобами** | o | |
| PM-27 | **Сообщения приватности** | o | |
| PM-28 | **Определение рисков** | o | √ |
| PM-29 | **Руководящие роли в программе управления рисками** | o | |
| PM-30 | **Стратегия управления рисками в логистической цепочке** | o | √ |
| PM-30 (1) | ПОСТАВЩИКИ КРИТИЧЕСКИХ ИЛИ ВАЖНЫХ ДЛЯ ПРЕДНАЗНАЧЕНИЯ ЭЛЕМЕНТОВ | o | √ |
| PM-31 | **Стратегия непрерывного мониторинга** | o | |
| PM-32 | **Намерения** | o | √ |

## ТАБЛИЦА C-14: СЕМЕЙСТВО БЕЗОПАСНОСТИ ПЕРСОНАЛА

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **PS-1** | **Политика и процедуры** | O | √ |
| **PS-2** | **Назначение должностного риска** | O | |
| **PS-3** | **Подбор персонала** | O | |
| PS-3 (1) | КЛАССИФИЦИРОВАННАЯ ИНФОРМАЦИЯ | O | |
| PS-3 (2) | ФОРМАЛЬНАЯ ИДЕОЛОГИЧЕСКАЯ ОБРАБОТКА | O | |
| PS-3 (3) | ИНФОРМАЦИЯ, ТРЕБУЮЩАЯ СПЕЦИАЛЬНЫХ МЕР ЗАЩИТЫ | O | |
| PS-3 (4) | ТРЕБОВАНИЯ ГРАЖДАНСТВА | O | |
| **PS-4** | **Увольнение персонала** | O | |
| PS-4 (1) | ТРЕБОВАНИЯ ПОСТЗАНЯТОСТИ | O | |
| PS-4 (2) | АВТОМАТИЗИРОВАННЫЕ ДЕЙСТВИЯ | O | |
| **PS-5** | **Перемещение персонала** | O | |
| **PS-6** | **Соглашения о допуске** | O | √ |
| PS-6 (1) | ИНФОРМАЦИЯ, ТРЕБУЮЩАЯ СПЕЦИАЛЬНОЙ ЗАЩИТЫ | W: Включено в PS -3 | |
| PS-6 (2) | КЛАССИФИЦИРОВАННАЯ ИНФОРМАЦИЯ, ТРЕБУЮЩАЯ СПЕЦИАЛЬНОЙ ЗАЩИТЫ | O | √ |
| PS-6 (3) | ТРЕБОВАНИЯ ПОСТЗАНЯТОСТИ | O | √ |
| **PS-7** | **Безопасность внешнего персонала** | O | √ |
| **PS-8** | **Санкционтрование персонала** | O | |
| **PS-9** | **Описание должности** | O | |

## ТАБЛИЦА C-15: СЕМЕЙСТВО ОБРАБОТКИ И ПРОЗРАЧНОСТИ ПЕРСОНАЛЬНОЙ ИДЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **PT-1** | **Политика и процедуры** | O | √ |
| **PT-2** | **Полномочия на обработку персональной идентификационной информации** | O | √ |
| PT-2 (1) | МАРКИРОВКА ДАННЫХ | S | √ |
| PT-2 (2) | АВТОМАТИЗАЦИЯ | O | √ |
| **PT-3** | **Персональная идентификационная информация Обработка** | O | |
| PT-3 (1) | МАРКИРОВКА ДАННЫХ | S | √ |
| PT-3 (2) | АВТОМАТИЗАЦИЯ | O | √ |
| **PT-4** | **Согласие** | O | |
| PT-4 (1) | СПЕЦИАЛИЗИРОВАННОЕ СОГЛАСИЕ | O | |
| PT-4 (2) | СВОЕВРЕМЕННОЕ СОГЛАСИЕ | O | |
| PT-4 (3) | АННУЛИРОВАНИЕ | O | |
| **PT-5** | **Политика конфиденциальности** | O | |
| PT-5 (1) | СВОЕВРЕМЕННОЕ УВЕДОМЛЕНИЕ | O | |
| PT-5 (2) | ОПИСАНИЯ АКТА О ПРИВАТНОСТИ | O | |
| **PT-6** | **Система уведомления о записях** | O | |
| PT-6 (1) | ОБЫЧНОЕ ИСПОЛЬЗОВАНИЕ | O | |
| PT-6 (2) | ПРАВИЛА ОСВОБОЖДЕНИЯ | O | |
| **PT-7** | **Конкретные категории персональной идентификационной информации** | O | |
| PT-7 (1) | НОМЕРА СОЦИАЛЬНОГО СТРАХОВАНИЯ | O | |
| PT-7 (2) | ПЕРВАЯ ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ | O | |
| **PT-8** | **Требования к соответствию компьютеров** | O | |

## ТАБЛИЦА C-16: СИСТЕМА ОЦЕНКИ РИСКОВ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **RA-1** | **Политика и процедуры** | O | √ |
| **RA-2** | **Классификация безопасности** | O | |
| RA-2 (1) | НАЗНАЧЕНИЕ ПРИОРИТЕТОВ УРОВНЕЙ ВОЗДЕЙСТВИЯ | O | |
| **RA-3** | **Оценка риска** | O | √ |
| RA-3 (1) | ОЦЕНКА РИСКОВ В ЦЕПОЧКЕ ПОСТАВОК | O | √ |
| RA-3 (2) | ИСПОЛЬЗОВАНИЕ ВСЕХ ИСТОЧНИКОВ РАЗВЕДКИ | O | √ |
| RA-3 (3) | ДИНАМИЧЕСКАЯ ПОДГОТОВКА ОБ УГРОЗАХ | O | √ |
| RA-3 (4) | ПРОГНОЗНАЯ КИБЕР-АНАЛИТИКА. | O | √ |
| **RA-4** | **Обновление оценки рисков** | W: Включено в RA -3 | |
| **RA-5** | **Мониторинг и сканирование уязвимостей** | O | √ |
| RA-5 (1) | ВОЗМОЖНОСТИ ОБНОВЛЕНИЯ ИНСТРУМЕНТОВ | W: Включено в RA -5 | |
| RA-5 (2) | ОБНОВЛЕНИЕ УЯЗВИМОСТЕЙ ДЛЯ СКАНИРОВАНИЯ | O | √ |
| RA-5 (3) | ШИРИНА И ГЛУБИНА ОХВАТА | O | √ |
| RA-5 (4) | ПОДДАЮЩАЯСЯ ОБНАРУЖЕНИЮ ИНФОРМАЦИЯ | O | √ |
| RA-5 (5) | ПРИВИЛЕГИРОВАННЫЙ ДОСТУП | O | √ |
| RA-5 (6) | АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ ТРЕНДОВ | O | √ |
| RA-5 (7) | АВТОМАТИЗИРОВАННОЕ ОБНАРУЖЕНИЕ И ОПОВЕЩЕНИЕ О НЕСАНКЦИОНИРОВАННЫХ КОМПОНЕНТАХ | W: Включено в УК -8 | |
| RA-5 (8) | ПРОСМОТР ИСТОРИЧЕСКИХ ЖУРНАЛОВ РЕГИСТРАЦИИ АУДИТА | O | √ |
| RA-5 (9) | ИСПЫТАНИЯ НА ПРОНИКНОВЕНИЕ И АНАЛИЗ | W: Включено в CA -8 | |
| RA-5 (10) | КОРРЕЛИРОВАИЕ ИНФОРМАЦИИ СКАНИРОВАНИЯ | O | √ |
| RA-5 (11) | ПРОГРАММА ПУБЛИЧНОГО РАСКРЫТИЯ ИНФОРМАЦИИ | O | √ |
| **RA-6** | **Обследование мер по борьбе с техническим наблюдением** | O | √ |
| **RA-7** | **Реагирование на риски** | O | √ |
| **RA-8** | **Оценки влияния на приватность** | O | √ |
| **RA-9** | **Анализ критичности** | O | |
| **RA-10** | **Охота на угрозы** | O/S | √ |

## ТАБЛИЦА C-17: СЕМЕЙСТВО ПРИОБРЕТЕНИЯ СИСТЕМ И СЕРВИСОВ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **SA-1** | **Политика и процедуры** | O | √ |
| **SA-2** | **Распределение ресурсов** | O | √ |
| **SA-3** | **Жизненный цикл разработки системы** | O | √ |
| SA-3 (1) | УПРАВЛЕНИЕ ПРЕДПРОИЗВОДСТВЕННОЙ СРЕДОЙ | O | √ |
| SA-3 (2) | ИСПОЛЬЗОВАНИЕ ТЕКУЩИХ ИЛИ ОПЕРАТИВНЫХ ДАННЫХ | O | √ |
| SA-3 (3) | ОБНОВЛЕНИЕ ТЕХНОЛОГИЙ | O | √ |
| **SA-4** | **Процесс приобретения** | O | √ |
| SA-4 (1) | ФУНКЦИОНАЛЬНЫЕ СВОЙСТВА МЕР ОБЕСПЕЧЕНИЯ | O | √ |
| SA-4 (2) | ИНФОРМАЦИЯ О ПРОЕКТЕ И РЕАЛИЗАЦИИ СРЕДСТВ КОНТРОЛЯ | O | √ |
| SA-4 (3) | МЕТОДЫ, ТЕХНОЛОГИ И ПРАКТИКА РАЗРАБОТКИ | O | √ |
| SA-4 (4) | НАЗНАЧЕНИЕ КОМПОНЕНТОВ СИСТЕМАМ | W: Включено вУК -8 (9 | |
| SA-4 (5) | КОНФИГУРАЦИИ СИСТЕМ, КОМПОНЕНТОВ И СЕРВИСОВ | O | √ |
| SA-4 (6) | ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ДОВЕРЕННЫХ ПРОДУКТОВ | O | √ |
| SA-4 (7) | ПРОФИЛЬ ЗАЩИТЫ УТВЕРЖДЁННЫЕ NIAP | O | √ |
| SA-4 (8) | ПОСТОЯННЫЙ МОНИТОРИНГ ПЛАНА МЕР ОБЕСПЕЧЕНИЯ | O | √ |
| SA-4 (9) | ИСПОЛЬЗУЕМЫЕ ФУНКЦИИ, ПОРТЫ, ПРОТОКОЛЫ И СЕРВИСЫ | O | √ |
| SA-4 (10) | ИСПОЛЬЗОВАНИЕ УТВЕРЖДЕННЫХ ПРОДУКТОВ PIV | O | √ |
| SA-4 (11) | СИСТЕМА УЧЕТА | O | √ |
| SA-4 (12) | СОБСТВЕННОСТЬ ДАННЫХ | O | √ |
| **SA-5** | **Документация по системе** | O | √ |
| SA-5 (1) | ФУНКЦИОНАЛЬНЫЕ СВОЙСТВА МЕР БЕЗОПАСНОСТИ | W: Включено вSA-4 (1). | |
| SA-5 (2) | ВНЕШНИЕ СИСТЕМНЫЕ ИНТЕРФЕЙСЫ, ИМЕЮЩИЕ ОТНОШЕНИЕ К БЕЗОПАСНОСТИ | W: Включено вSA-4 (2). | |
| SA-5 (3) | ПРОЕКТ ВЫСОКОГО УРОВНЯ | W: Включено вSA-4 (2). | |
| SA-5 (4) | ПРОЕКТ НИЗКОГО УРОВНЯ | W: Включено вSA-4 (2). | |
| SA-5 (5) | ИСХОДНЫЙ КОД | W: Включено вSA-4 (2). | |
| **SA-6** | **Ограничения на использование программного обеспечения** | W: Включено в УК -10 иSI-7 | |
| **SA-7** | **Установленное пользователями программное обеспечение** | W: Включено в УК -11 иSI-7 | |
| **SA-8** | **Принципы техники безопасности и приватности** | O | √ |
| SA-8 (1) | ЧЕТКИЕ АБСТРАКЦИИ | O/S | √ |
| SA-8 (2) | НАИМЕНЕЕ ОБЩИЙ МЕХАНИЗМ | O/S | √ |
| SA-8 (3) | МОДУЛЬНОСТЬ И МНОГОСЛОЙНОСТЬ | O/S | √ |
| SA-8 (4) | ЧАСТИЧНО УПОРЯДОЧЕННЫЕ ЗАВИСИМОСТИ | O/S | √ |
| SA-8 (5) | ЭФФЕКТИВНО ОПОСРЕДОВАННЫЙ ДОСТУП | O/S | √ |
| SA-8 (6) | МИНИМИЗАЦИЯ РАСПРОСТРАНЕНИЯ | O/S | √ |
| SA-8 (7) | УМЕНЬШЕНИЕ СЛОЖНОСТИ | O/S | √ |
| SA-8 (8) | СПОСОБНОСТЬ К БЕЗОПАСНОМУ РАЗВИТИЮ | O/S | √ |
| SA-8 (9) | ДОВЕРЕННЫЕ КОМПОНЕНТЫ | O/S | √ |
| SA-8 (10) | ИЕРАРХИЧЕСКОЕ ДОВЕРИЕ | O/S | √ |
| SA-8 (11) | ПОРОГ ОБРАТНОЙ МОДИФИКАЦИИ | O/S | √ |
| SA-8 (12) | ИЕРАРХИЧЕСКАЯ ЗАЩИТА | O/S | √ |
| SA-8 (13) | МИНИМИЗАЦИЯ ЭЛЕМЕНОВЫ БЕЗОПАСНОСТИ | O/S | √ |
| SA-8 (14) | НАИМЕНЬШЕЕ КОЛИЧЕСТВО ПРИВИЛЕГИИ | O/S | √ |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| SA-8 (15) | ПРЕДОПРЕДЕЛЁННЫЕ РАЗРЕШЕНИЯ НА ДОСТУП | O/S | √ |
| SA-8 (16) | САМОДОСТАТОЧНАЯ ДОВЕРЕННОСТЬ | O/S | √ |
| SA-8 (17) | ЗАЩИЩЕННЫЙ РАСПРЕДЕЛЕННЫЙ СОСТАВ | O/S | √ |
| SA-8 (18) | НАДЕЖНЫЕ КАНАЛЫ СВЯЗИ | O/S | √ |
| SA-8 (19) | НЕПРЕРЫВНАЯ ЗАЩИТА | O/S | √ |
| SA-8 (20) | БЕЗОПАСНОЕ УПРАВЛЕНИЕ МЕТАДАННЫМИ | O/S | √ |
| SA-8 (21) | САМОАНАЛИЗ | O/S | √ |
| SA-8 (22) | ПОДОТЧЕТНОСТЬ И ПРОСЛЕЖИВАЕМОСТЬ | O/S | √ |
| SA-8 (23) | БЕЗОПАСНЫЕ ДЕФОЛТЫ | O/S | √ |
| SA-8 (24) | БЕЗОПАСНЫЙ ОТКАЗ И ВОССТАНОВЛЕНИЕ | O/S | √ |
| SA-8 (25) | ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ | O/S | √ |
| SA-8 (26) | ГАРАНТИЯ ИСПОЛНЕНИЯ | O/S | √ |
| SA-8 (27) | БЕЗОПАСНОСТЬ С ТОЧКИ ЗРЕНИЯ ЧЕЛОВЕКА | O/S | √ |
| SA-8 (28) | ПРИЕМЛЕМАЯ БЕЗОПАСНОСТЬ | O/S | √ |
| SA-8 (29) | ПОВТОРЯЕМЫЕ И ДОКУМЕНТИРОВАННЫЕ ПРОЦЕДУРЫ | O/S | √ |
| SA-8 (30) | ПРОЦЕДУРНАЯ СТРОГОСТЬ | O/S | √ |
| SA-8 (31) | МОДИФИКАЦИЯ ЗАЩИЩЕННОЙ СИСТЕМЫ. | O/S | √ |
| SA-8 (32) | ДОСТАТОЧНОСТЬ ДОКУМЕНТАЦИИ | O/S | √ |
| SA-8 (33) | МИНИМИЗАЦИЯ | O/S | √ |
| **SA-9** | **Внешние сервисы системы** | O | √ |
| SA-9 (1) | ОЦЕНКИ РИСКОВ И ОДОБРЕНИЯ | O | √ |
| SA-9 (2) | ИДЕНТИФИКАЦИЯ ФУНКЦИЙ, ПОРТОВ, ПРОТОКОЛОВ И СЕРВИСОВ | O | √ |
| SA-9 (3) | УСТАНОВЛЕНИЕ И ПОДДЕРЖАНИЕ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ С ПОСТАВЩИКАМИ | O | √ |
| SA-9 (4) | ПОСЛЕДОВАТЕЛЬНЫЕ ИНТЕРЕСЫ ПОТРЕБИТЕЛЕЙ И ПОСТАВЩИКОВ | O | √ |
| SA-9 (5) | МЕСТО ОБРАБОТКИ, ХРАНЕНИЯ И ОБСЛУЖИВАНИЯ | O | √ |
| SA-9 (6) | УПРАВЛЯЕМЫЕ ОРГАНИЗАЦИЕЙ КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ | O | √ |
| SA-9 (7) | ПРОВЕРКА ЦЕЛОСТНОСТИ ПОД КОНТРОЛЕМ ОРГАНИЗАЦИИ | O | √ |
| SA-9 (8) | МЕСТО ОБРАБОТКИ И ХРАНЕНИЯ - ЮРИСДИКЦИЯ США | O | √ |
| **SA-10** | **Управление конфигурацией разработчика** | O | √ |
| SA-10 (1) | ПРОВЕРКА ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ВСТРОЕННОГО ПО | O | √ |
| SA-10 (2) | АЛЬТЕРНАТИВНЫЕ ПРОЦЕССЫ УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ | O | √ |
| SA-10 (3) | ПРОВЕРКА ЦЕЛОСТНОСТИ АППАРАТНЫХ СРЕДСТВ | O | √ |
| SA-10 (4) | ДОВЕРЕННАЯ ГЕНЕРАЦИЯ | O | √ |
| SA-10 (5) | ЦЕЛОСТНОСТЬ ОТОБРАЖЕНИЯ ДЛЯ УПРАВЛЕНИЯ ВЕРСИЯМИ | O | √ |
| SA-10 (6) | ДОВЕРЕННОЕ РАСПРЕДЕЛЕНИЕ | O | √ |
| SA-10 (7) | ПРЕДСТАВЛЕНИЕ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ | O | √ |
| **SA-11** | **Тестирование и оценка разработчика** | O | √ |
| SA-11 (1) | АНАЛИЗ СТАТИЧЕСКОГО КОДА | O | √ |
| SA-11 (2) | МОДЕЛИРОВАНИЕ УГРОЗ И АНАЛИЗ УЯЗВИМОСТИ | O | √ |
| SA-11 (3) | НЕЗАВИСИМАЯ ПРОВЕРКА ПЛАНОВ ОЦЕНКИ И СВИДЕТЕЛЬСТВ | O | √ |
| SA-11 (4) | РУЧНЫЕ ПЕРЕСМОТРЫ КОДА | O | √ |
| SA-11 (5) | ТЕСТИРОВАНИЕ ПРОНИКНОВЕНИЯ | O | √ |
| SA-11 (6) | ПЕРЕСМОТРЫ ПОВЕРХНОСТИ АТАКИ | O | √ |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| SA-11 (7) | ПРОВЕРКА ОБЛАСТИ ИСПЫТАНИЙ И ОЦЕНКИ | O | √ |
| SA-11 (8) | ДИНАМИЧЕСКИЙ АНАЛИЗ КОДА | O | √ |
| SA-11 (9) | ИНТЕРАКТИВНОЕ ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ | O | √ |
| **SA-12** | **Защита логистической цепочки** | W: Перемещен в SR Family. | |
| SA-12 (1) | СТРАТЕГИИ, ИНСТРУМЕНТЫ И МЕТОДЫ ПРИОБРЕТЕНИЯ | Ж: Переехал в SR-5. | |
| SA-12 (2) | ПЕРЕСМОТРЫ ПОСТАВЩИКОВ | Ж: Переехал в SR-6. | |
| SA-12 (3) | НАДЕЖНАЯ ДОСТАВКА И ХРАНЕНИЕ | W: Включено в состав SR-3. | |
| SA-12 (4) | РАЗНООБРАЗИЕ ПОСТАВЩИКОВ | W: Перенесен в SR-3 (1). | |
| SA-12 (5) | ОГРАНИЧЕНИЕ ВРЕДА | W: Перенесен в SR-3 (2). | |
| SA-12 (6) | МИНИМИЗАЦИЯ ВРЕМЕНИ ЗАКУПОК | W: Включено в SR-5 (1). | |
| SA-12 (7) | ОЦЕНКИ ПЕРЕД ОТБОРОМ/ПРИЕМКОЙ/ОБНОВЛЕНИЕМ | W: Перенесен в SR-5 (2). | |
| SA-12 (8) | ИСПОЛЬЗОВАНИЕ ВСЕХ ИСТОЧНИКОВ РАЗВЕДКИ | W: Включено в RA -3 (2 | |
| SA-12 (9) | БЕЗОПАСНОСТЬ ДЕЯТЕЛЬНОСТИ | Ж: Переехал в SR-7. | |
| SA-12 (10) | ВАЛИДАЦИЯ КАК ПОДЛИННАЯ И НЕ ИЗМЕНЕННАЯ | W: Перенесен в SR-4 (3). | |
| SA-12 (11) | ИСПЫТАНИЯ НА ПРОНИКНОВЕНИЕ/АНАЛИЗ ЭЛЕМЕНТОВ, ПРОЦЕССОВ И СУБЪЕКТОВ | W: Перенесен в SR-6 (1). | |
| SA-12 (12) | СОГЛАШЕНИЯ МЕЖДУ ОРГАНИЗАЦИЯМИ | Ж: Переехал в SR-8. | |
| SA-12 (13) | КОМПОНЕНТЫ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ | W: Включено в MA-6 и RA -9 | |
| SA-12 (14) | ИДЕНТИФИКАЦИЯ И ОТСЛЕЖИВАЕМОСТЬ | W: Перенесены в SR-4 (1) и SR-4 (2 | |
| SA-12 (15) | ПРОЦЕССЫ УСТРАНЕНИЯ СЛАБЫХ МЕСТ ИЛИ НЕДОСТАТКОВ | W: Включено в состав SR-3. | |
| **SA-13** | **Доверенность** | W: Включено в состав SA-8. | |
| **SA-14** | **Анализ критичности** | W: Включено в RA -9 | |
| SA-14 (1) | КРИТИЧЕСКИ ВАЖНЫЕ КОМПОНЕНТЫ БЕЗ ЖИЗНЕСПОСОБНЫХ АЛЬТЕРНАТИВНЫХ ИСТОЧНИКОВ ПОСТАВОК | W: Включено в состав SA-20. | |
| **SA-15** | **Процесс разработки, стандарты и инструменты** | O | √ |
| SA-15 (1) | КАЧЕСТВЕННЫЕ МЕТРИКИ | O | √ |
| SA-15 (2) | ИНСТРУМЕНТЫ ПРОСЛЕЖИВАНИЯ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ | O | √ |
| SA-15 (3) | АНАЛИЗ КРИТИЧНОСТИ | O | √ |
| SA-15 (4) | МОДЕЛИРОВАНИЕ УГРОЗ И АНАЛИЗ УЯЗВИМОСТЕЙ | W: Включено в SA-11 (2). | |
| SA-15 (5) | УМЕНЬШЕНИЕ ПОВЕРХНОСТИ АТАКИ | O | √ |
| SA-15 (6) | НЕПРЕРЫВНОЕ СОВЕРШЕНСТВОВАНИЕ | O | √ |
| SA-15 (7) | АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ УЯЗВИМОСТИ | O | √ |
| SA-15 (8) | ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИИ ОБ УГРОЗАХ И УЯЗВИМОСТИ | O | √ |
| SA-15 (9) | ИСПОЛЬЗОВАНИЕ ОПЕРАТИВНЫХ ДАННЫХ | W: Включено в SA-3 (2). | |
| SA-15 (10) | ПЛАН РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ | O | √ |
| SA-15 (11) | АРХИВАЦИЯ СИСТЕМ ИЛИ КОМПОНЕНТОВ | O | √ |
| SA-15 (12) | МИНИМИЗАЦИЯ ПЕРСОНАЛЬНОЙ ИДЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ | O | √ |
| **SA-16** | **Предоставленное разработчиками обучение** | O | √ |
| **SA-17** | **Проект безопасности и приватности разработчика** | O | √ |
| SA-17 (1) | ФОРМАЛЬНАЯ МОДЕЛЬ ПОЛИТИКИ | O | √ |
| SA-17 (2) | КОМПОНЕНТЫ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ, | O | √ |
| SA-17 (3) | ФОРМАЛЬНОЕ СООТВЕТСТВИЕ | O | √ |
| SA-17 (4) | НЕФОРМАЛЬНОЕ СООТВЕТСТВИЕ | O | √ |
| SA-17 (5) | КОНЦЕПТУАЛЬНО ПРОСТОЙ ПРОЕКТ | O | √ |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| SA-17 (6) | СТРУКТУРА ДЛЯ ИСПЫТАНИЙ | O | √ |
| SA-17 (7) | СТРУКТУРА ДЛЯ НАИМЕНЬШИХ ПРИВИЛЕГИЙ | O | √ |
| SA-17 (8) | ГАРМОНИЧНОЕ СОЧЕТАНИЕ | O | √ |
| SA-17 (9) | РАЗНООБРАЗИЕ ПРОЕКТОВ | O | √ |
| **SA-18** | **Устойчивость и обнаружение изменений** | Ж: Переехал в SR-9. | |
| SA-18 (1) | МНОЖЕСТВО ФАЗ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ РАЗРАБОТКИ. | W: Перенесен в SR-9 (1). | |
| SA-18 (2) | ПРОВЕРКА СИСТЕМ ИЛИ КОМПОНЕНТОВ | Ж: Переехал в SR-10. | |
| **SA-19** | **Аутентификация компонентов** | Ж: Переехал в SR-11. | |
| SA-19 (1) | АНТИПОДДЕЛЬНОЕ ОБУЧЕНИЕ | W: Перенесен в SR-11 (1). | |
| SA-19 (2) | УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ ДЛЯ ОБСЛУЖИВАНИЯ И РЕМОНТА КОМПОНЕНТОВ | W: Перенесен в SR-11 (2). | |
| SA-19 (3) | ЛИКВИДАЦИЯ КОМПОНЕНТНОЕ | Ж: Переехал в SR-12. | |
| SA-19 (4) | АНТИПОДДЕЛЬНЫЙ ПРОСМОТР | W: Перенесен в SR-11 (3). | |
| **SA-20** | **Индивидуальная разработка критически важных компонентов** | O | √ |
| **SA-21** | **Подбор разработчиков** | O | √ |
| SA-21 (1) | ПОДТВЕРЖДЕНИЕ СООТВЕТСТВИЯ ПОДБОРА | W: Включено в состав SA-21. | |
| **SA-22** | **Неподдерживаемые компоненты системы** | O | √ |
| SA-22 (1) | АЛЬТЕРНАТИВНЫЕ ИСТОЧНИКИ ДАЛЬНЕЙШЕЙ ПОДДЕРЖКИ | W: Включено в состав SA-22. | |
| **SA-23** | **Специализация** | O | √ |

## ТАБЛИЦА C-18: СЕМЕЙСТВО ЗАЩИТЫ СИСТЕМЫ И КОММУНИКАЦИЙ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **SC-1** | **Политика и процедуры** | O | √ |
| **SC-2** | **Разделение функциональных возможностей системы и пользователя** | S | √ |
| SC-2 (1) | ИНТЕРФЕЙСЫ ДЛЯ НЕПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ. | S | √ |
| SC-2 (2) | РАЗДЕЛЯЕМОСТЬ | S | √ |
| **SC-3** | **Изоляция функций безопасности** | S | √ |
| SC-3 (1) | РАЗДЕЛЕНИЕ АППАРАТНЫХ СРЕДСТВ | S | √ |
| SC-3 (2) | ФУНКЦИИ УПРАВЛЕНИЯ ДОСТУПОМ И ПОТОКОМ | S | √ |
| SC-3 (3) | МИНИМИЗАЦИЯ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ, НЕ СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ | O/S | √ |
| SC-3 (4) | СВЯЗИ МОДУЛЕЙ И СВЯЗНОСТЬ | O/S | √ |
| SC-3 (5) | СЛОИСТЫЕ СТРУКТУРЫ | O/S | √ |
| **SC-4** | **Информация в общих системных ресурсах** | S | |
| SC-4 (1) | УРОВНИ БЕЗОПАСНОСТИ | W: Включено в SC -4 | |
| SC-4 (2) | МНОГОУРОВНЕВАЯ ИЛИ ПЕРИОДИЧЕСКАЯ ОБРАБОТКА | S | |
| **SC-5** | **Защита отказа в обслуживании** | S | |
| SC-5 (1) | ОГРАНИЧЕНИЕ ВОЗМОЖНОСТИ АТАКИ НА ДРУГИЕ СИСТЕМЫ | S | |
| SC-5 (2) | ВОЗМОЖНОСТЬ, ПРОПУСКНАЯ СПОСОБНОСТЬ И ИЗБЫТОЧНОСТЬ | S | |
| SC-5 (3) | ОБНАРУЖЕНИЕ И МОНИТОРИНГ | S | |
| **SC-6** | **Доступность ресурсов** | S | √ |
| **SC-7** | **Защита границ** | S | |
| SC-7 (1) | ФИЗИЧЕСКИ РАЗДЕЛЕННЫЕ ПОДСЕТИ | W: Включено в SC -7 | |
| SC-7 (2) | ОТКРЫТЫЙ ДОСТУП | W: Включено в SC -7 | |
| SC-7 (3) | ТОЧКИ ДОСТУПА | S | |
| SC-7 (4) | ВНЕШНИЕ ТЕЛЕКОММУНИКАЦИОННЫЕ СЕРВИСЫ | O | |
| SC-7 (5) | ЗАПРЕЩЕНИЕ ПО УМОЛЧАНИЮ - РАЗРЕШЕНИЕ ПО ИСКЛЮЧЕНИЮ | S | |
| SC-7 (6) | РЕАКЦИЯ НА ВЫЯВЛЕННЫЕ ОТКАЗЫ | W: Включено в SC -7 (18 | |
| SC-7 (7) | РАЗДЕЛЬНОЕ ТУННЕЛИРОВАНИЕ ДЛЯ УДАЛЕННЫХ УСТРОЙСТВ. | S | |
| SC-7 (8) | МАРШРУТИЗАЦИЯ ТРАФИКА НА АУТЕНТИФИЦИРОВАННЫЕ ПРОКСИ-СЕРВЕРЫ | S | |
| SC-7 (9) | ОГРАНИЧЕНИЕ ТРАФИКА ИСХОДЯЩИХ СООБЩЕНИЙ С УГРОЗАМИ | S | |
| SC-7 (10) | ПРЕДОТВРАЩЕНИЕ ЭКСФИЛЬТРАЦИИ | S | |
| SC-7 (11) | ОГРАНИЧЕНИЕ ВХОДЯЩЕГО ТРАФИКА СВЯЗИ | S | |
| SC-7 (12) | ЗАЩИТА ОСНОВНОГО ВЫЧИСЛИТЕЛЯ | S | |
| SC-7 (13) | ИЗОЛЯЦИЯ СРЕДСТВ, МЕХАНИЗМОВ И КОМПОНЕНТОВ ПОДДЕРЖКИ | S | |
| SC-7 (14) | ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ПОДКЛЮЧЕНИЯ | S | |
| SC-7 (15) | СЕТЕВОЙ ПРИВИЛЕГИРОВАННЫЙ ДОСТУП | S | |
| SC-7 (16) | ПРЕДОТВРАЩЕНИЕ ОБНАРУЖЕНИЯ КОМПОНЕНТОВ СИСТЕМЫ | S | |
| SC-7 (17) | АВТОМАТИЗИРОВАННОЕ ОСУЩЕСТВЛЕНИЕ ФОРМАТОВ ПРОТОКОЛОВ | S | |
| SC-7 (18) | ОТКАЗОУСТОЙЧИВОСТЬ | S | √ |
| SC-7 (19) | БЛОКИРОВАНИЕ СВЯЗИ С ХОСТАМИ, НАСТРОЕННЫМИ НЕ ОРГАНИЗАЦИЕЙ | S | |
| SC-7 (20) | ДИНАМИЧЕСКАЯ ИЗОЛЯЦИЯ И СЕГРЕГАЦИЯ | S | |
| SC-7 (21) | ИЗОЛЯЦИЯ КОМПОНЕНТОВ СИСТЕМЫ | O/S | √ |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| SC-7 (22) | ОТДЕЛЬНЫЕ ПОДСЕТИ ДЛЯ ПОДКЛЮЧЕНИЯ К РАЗЛИЧНЫМ ДОМЕНАМ | S | √ |
| SC-7 (23) | ОТКЛЮЧЕНИЕ ОБРАТНОЙ СВЯЗИ ОТПРАВИТЕЛЯ ПРИ ОТКАЗЕ ПОДТВЕРЖДЕНИЯ | S | |
| SC-7 (24) | ПЕРСОНАЛЬНАЯ ИДЕНТИФИКАЦИОННАЯ ИНФОРМАЦИЯ | O/S | |
| SC-7 (25) | НЕКЛАССИФИЦИРОВАННЫЕ СОЕДИНЕНИЯ СИСТЕМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ | O | |
| SC-7 (26) | ЗАСЕКРЕЧЕННЫЕ СОЕДИНЕНИЯ СИСТЕМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ | O | |
| SC-7 (27) | НЕКЛАССИФИЦИРОВАННЫЕ ПОДКЛЮЧЕНИЯ НЕНАЦИОНАЛЬНЫХ СИСТЕМ БЕЗОПАСНОСТИ | O | |
| SC-7 (28) | ПОДКЛЮЧЕНИЯ К СЕТЯМ ОБЩЕГО ПОЛЬЗОВАНИЯ | O | |
| SC-7 (29) | ОТДЕЛЬНЫЕ ПОДСЕТИ ДЛЯ ВЫДЕЛЕНИЯ ФУНКЦИЙ | S | |
| **SC-8** | **Конфиденциальность и целостность передачи** | S | |
| SC-8 (1) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | S | |
| SC-8 (2) | ОБРАБОТКА ДО И ПОСЛЕ ПЕРЕДАЧИ | S | |
| SC-8 (3) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ВНЕШНИХ СООБЩЕНИЙ. | S | |
| SC-8 (4) | СКРЫТИЕ ИЛИ РАНДОМИЗАЦИЯ СООБЩЕНИЙ | S | |
| SC-8 (5) | ЗАЩИЩЕННАЯ РАСПРЕДЕЛИТЕЛЬНАЯ СИСТЕМА | S | |
| SC-9 | **Конфиденциальность передачи** | W: Включено в SC -8 | |
| **SC-10** | **Сетевое разъединение** | S | |
| **SC-11** | **Доверенный путь** | S | √ |
| SC-11 (1) | НЕОПРОВЕРЖИМЫЙ ПУТЬ СВЯЗИ | S | √ |
| **SC-12** | **Создание криптографического ключа и управление им** | O/S | |
| SC-12 (1) | ДОСТУПНОСТЬ | O/S | |
| SC-12 (2) | СИММЕТРИЧНЫЕ КЛЮЧИ | O/S | |
| SC-12 (3) | АСИММЕТРИЧНЫЕ КЛЮЧИ | O/S | |
| SC-12 (4) | СЕРТИФИКАТЫ PKI | W: Включено в SC -12 (3 | |
| SC-12 (5) | СЕРТИФИКАТЫ PKI/АППАРАТНЫЕ МАРКЕРЫ | W: Включено в SC -12 (3 | |
| SC-12 (6) | ФИЗИЧЕСКОЕ УПРАВЛЕНИЕ КЛЮЧАМИ | O/S | |
| **SC-13** | **Криптографическая защита** | S | |
| SC-13 (1) | FIPS-УТВЕРЖДЕННАЯ КРИПТОГРАФИЯ | W: Включено в SC -13 | |
| SC-13 (2) | NSA ОДОБРЕННАЯ КРИПТОГРАФИЯ | W: Включено в SC -13 | |
| SC-13 (3) | ЛИЦА БЕЗ ОФИЦИАЛЬНЫХ ОДОБРЕНИЙ НА ДОСТУП | W: Включено в SC -13 | |
| SC-13 (4) | ЦИФРОВЫЕ ПОДПИСИ | W: Включено в SC -13 | |
| SC-14 | **Защиты общего доступа** | W: Включено в AC-2, AC-3, AC-5, SI- 3, SI-4, SI-5, SI-7 и SI-10. | |
| **SC-15** | **Устройства и приложения для совместной работы** | S | |
| SC-15 (1) | ФИЗИЧЕСКОЕ ИЛИ ЛОГИЧЕСКОЕ ОТКЛЮЧЕНИЕ | S | |
| SC-15 (2) | БЛОКИРОВАНИЕ ВХОДЯЩЕГО И ИСХОДЯЩЕГО ТРАФИКА СВЯЗИ | W: Включено в SC -7 | |
| SC-15 (3) | ОТКЛЮЧЕНИЕ И ДЕМОНТАЖ В БЕЗОПАСНЫХ ОБЛАСТЯХ | O | |
| SC-15 (4) | ЯВНОЕ УКАЗАНИЕ ТЕКУЩИХ УЧАСТНИКОВ | S | |
| **SC-16** | **Передача атрибутов безопасности и приватности** | S | |
| SC-16 (1) | ПРОВЕРКА ЦЕЛОСТНОСТИ | S | |
| SC-16 (2) | АНТИИМИТАЦИЯ МЕХАНИЗМОВ | S | |
| SC-16 (3) | КРИПТОГРАФИЧЕСКОЕ СВЯЗЫВАНИЕ | S | |
| **SC-17** | **Сертификаты инфраструктуры публичных ключей** | O/S | |
| **SC-18** | **Мобильный код** | O | |
| SC-18 (1) | ОПРЕДЕЛЕНИЕ НЕПРИЕМЛЕМОГО КОДА И ПРЕДПРИНЯТИЕ КОРРЕКТИРУЮЩИХ ДЕЙСТВИЙ | S | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| SC-18 (2) | ПРИОБРЕТЕНИЕ, РАЗРАБОТКА И ИСПОЛЬЗОВАНИЕ | O | |
| SC-18 (3) | ПРЕДОТВРАЩЕНИЕ ЗАГРУЗКИ И ВЫПОЛНЕНИЯ | S | |
| SC-18 (4) | ПРЕДОТВРАЩЕНИЕ АВТОМАТИЧЕСКОГО ВЫПОЛНЕНИЯ | S | |
| SC-18 (5) | РАЗРЕШЕНИЕ ВЫПОЛНЕНИЯ ТОЛЬКО В ЗАМКНУТЫХ СРЕДАХ | S | |
| **SC-19** | **Протокол передачи речи через Интернет** | W: Конкретный технологией; рассматривается как любая | |
| **SC-20** | **Служба безопасного разрешения имен и адресов (авторитетный источник)** | S | |
| SC-20 (1) | ДОЧЕРНИЕ ПОДПРОСТРАНСТВА | W: Включено в SC -20 | |
| SC-20 (2) | ПРОИСХОЖДЕНИЕ И ЦЕЛОСТНОСТЬ ДАННЫХ | S | |
| **SC-21** | **Служба безопасного разрешения имен/ адресов (Рекурсивный или кешированный преобразователь)** | S | |
| SC-21 (1) | ПРОИСХОЖДЕНИЕ И ЦЕЛОСТНОСТЬ ДАННЫХ | W: Включено в SC -21 | |
| **SC-22** | **Архитектура и выделение ресурсов для службы разрешения имен и адресов** | S | |
| **SC-23** | **Аутентичность сессии** | S | |
| SC-23 (1) | АННУЛИРОВАИЕ ИДЕНТИФИКАТОРОВ СЕАНСА ПРИ ВЫХОДЕ ИЗ СИСТЕМЫ | S | |
| SC-23 (2) | ИНИЦИИРУЕМЫЕ ПОЛЬЗОВАТЕЛЕМ ВЫХОДЫ ИЗ СИСТЕМЫ И МОНИТОРЫ СООБЩЕНИЙ. | W: Включено в AC-12 (1). | |
| SC-23 (3) | УНИКАЛЬНЫЕ СИСТЕМНЫЕ ИДЕНТИФИКАТОРЫ СЕАНСОВ. | S | |
| SC-23 (4) | УНИКАЛЬНЫЕ ИДЕНТИФИКАТОРЫ СЕАНСОВ С РАНДОМИЗАЦИЕЙ. | W: Включено в SC -23 (3 | |
| SC-23 (5) | ПОЛНОМОЧИЯ РАЗРЕШЁННЫЕ СЕРТИФИКАТОМ | S | |
| **SC-24** | **Сбой в известном месте** | S | √ |
| **SC-25** | **Тонкие узлы** | S | |
| **SC-26** | **Ложные цели** | S | |
| SC-26 (1) | ОБНАРУЖЕНИЕ ВРЕДОНОСНОГО КОДА. | W: Включено в SC -35 | |
| **SC-27** | **Независимые от платформы приложения** | S | |
| **SC-28** | **Защита информации в состоянии покоя** | S | |
| SC-28 (1) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | S | |
| SC-28 (2) | ОФЛАЙНОВОЕ ХРАНЕНИЕ | O | |
| SC-28 (3) | КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ | O/S | |
| **SC-29** | **Разнородность** | O | √ |
| SC-29 (1) | ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ | O | √ |
| **SC-30** | **Сокрытие и неправильное направление** | O | √ |
| SC-30 (1) | ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ | W: Включено в SC -29 (1 | |
| SC-30 (2) | ХАОТИЧНОСТЬ | O | √ |
| SC-30 (3) | ИЗМЕНЕНИЕ ПРОЦЕССОВ ОБРАБОТКИ И ХРАНЕНИЯ | O | √ |
| SC-30 (4) | ИНФОРМАЦИЯ, ВВОДЯЩАЯ В ЗАБЛУЖДЕНИЕ | O | √ |
| SC-30 (5) | СОКРЫТИЕ КОМПОНЕНТОВ СИСТЕМЫ | O | √ |
| **SC-31** | **Скрытый анализ каналов** | O | √ |
| SC-31 (1) | ТЕСТИРОВАНИЕ СКРЫТЫХ КАНАЛОВ НА ЭКСПЛУАТИРУЕМОСТЬ | O | √ |
| SC-31 (2) | МАКСИМАЛЬНАЯ ПРОПУСКНАЯ СПОСОБНОСТЬ | O | √ |
| SC-31 (3) | ИЗМЕРЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ В РАБОЧИХ СРЕДАХ | O | √ |
| **SC-32** | **Разделение систем** | O/S | √ |
| SC-32 (1) | ОТДЕЛЬНЫЕ ФИЗИЧЕСКИЕ ДОМЕНЫ ДЛЯ ПРИВИЛЕГИРОВАННЫХ ФУНКЦИЙ. | O/S | √ |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| SC-33 | **Целостность подготовки передачи** | W: Включено в SC -8 | |
| **SC-34** | **Неизменяемость исполняемых программ** | S | √ |
| SC-34 (1) | ХРАНЕНИЕ БЕЗ ВОЗМОЖНОСТИ ЗАПИСИ | O | √ |
| SC-34 (2) | ЗАЩИТА ЦЕЛОСТНОСТИ И НОСИТЕЛЬ ИНФОРМАЦИИ ТОЛЬКО ДЛЯ ЧТЕНИЯ | O | √ |
| SC-34 (3) | ЗАЩИТА, ОСНОВАННАЯ НА АППАРАТНЫХ СРЕДСТВАХ | Ш: Перенесен в SC -51 | |
| **SC-35** | **Идентификация внешнего вредоносного кода** | S | |
| **SC-36** | **Распределенная обработка и хранение** | O | √ |
| SC-36 (1) | ОПРОС ТЕХНОЛОГИЙ | O | √ |
| SC-36 (2) | СИНХРОНИЗАЦИЯ | O | √ |
| **SC-37** | **Внеполосные каналы** | O | √ |
| SC-37 (1) | ОБЕСПЕЧЕНИЕ ДОСТАВКИ И ПЕРЕДАЧИ | O | √ |
| **SC-38** | **Безопасность деятельности** | O | √ |
| **SC-39** | **Изоляция процесса** | S | √ |
| SC-39 (1) | РАЗДЕЛЕНИЕ АППАРАТНЫХ СРЕДСТВ | S | √ |
| SC-39 (2) | ОТДЕЛЬНЫЙ ДОМЕН ВЫПОЛНЕНИЯ ДЛЯ КАЖДОГО ПОТОКА. | S | √ |
| **SC-40** | **Защита беспроводной линии связи** | S | |
| SC-40 (1) | ЭЛЕКТРОМАГНИТНОЕ ВМЕШАТЕЛЬСТВО | S | |
| SC-40 (2) | СНИЖЕНИЕ ПОТЕНЦИАЛА ОБНАРУЖЕНИЯ | S | |
| SC-40 (3) | ИМИТАЦИОННЫЙ ИЛИ МАНИПУЛЯТИВНЫЙ КОММУНИКАЦИОННЫЙ ОБМАН | S | |
| SC-40 (4) | ИДЕНТИФИКАЦИЯ ПАРАМЕТРОВ СИГНАЛА | S | |
| **SC-41** | **Доступ к портам и устройствам ввода-вывода** | O/S | |
| **SC-42** | **Возможности датчиков и данные** | S | |
| SC-42 (1) | ОТЧЕТНОСТЬ УПОЛНОМОЧЕННЫМ ЛИЦАМ ИЛИ РОЛЯМ | O | |
| SC-42 (2) | САНКЦИОНИРОВАННОЕ ИСПОЛЬЗОВАНИЕ | O | |
| SC-42 (3) | ЗАПРЕЩЕНИЕ ИСПОЛЬЗОВАНИЯ УСТРОЙСТВ | W: Включено в SC -42 | |
| SC-42 (4) | УВЕДОМЛЕНИЕ О СБОРЕ | O | |
| SC-42 (5) | МИНИМИЗАЦИЯ КОЛЛЕКЦИИ | O | |
| **SC-43** | **Ограничения использования** | O/S | |
| **SC-44** | **Детонационные камеры** | S | |
| **SC-45** | **Синхронизация системного времени** | S | |
| SC-45 (1) | СИНХРОНИЗАЦИЯ С АВТОРИТЕТНЫМ ИСТОЧНИКОМ ВРЕМЕНИ | S | |
| SC-45 (2) | ВТОРИЧНЫЙ АВТОРИТЕТНЫЙ ИСТОЧНИК ВРЕМЕНИ | S | |
| **SC-46** | **Осуществление междоменных политик** | S | |
| **SC-47** | **Альтернативные пути связи** | O/S | |
| **SC-48** | **Перемещение датчика** | O/S | |
| SC-48 (1) | ДИНАМИЧЕСКОЕ ПЕРЕМЕЩЕНИЕ ДАТЧИКОВ ИЛИ ВОЗМОЖНОСТИ МОНИТОРИНГА | O/S | |
| **SC-49** | **Аппаратное разделение и осуществление политик** | O/S | √ |
| **SC-50** | **Принудительное разделение программного обеспечения и осуществление политик** | O/S | √ |
| **SC-51** | **Защита, основанная на аппаратных средствах** | O/S | √ |

## ТАБЛИЦА C-19: СЕМЕЙСТВО ЦЕЛОСТНОСТИ СИСТЕМЫ И ИНФОРМАЦИИ

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **SI- 1** | **Политика и процедуры** | O | √ |
| **SI- 2** | **Устранение недостатков** | O | |
| SI- 2 (1) | ЦЕНТРАЛЬНОЕ УПРАВЛЕНИЕ | W: Включено в состав PL-9. | |
| SI- 2 (2) | СТАТУС АВТОМАТИЧЕСКОГО УСТРАНЕНИЯ НЕДОСТАТКОВ | O | |
| SI- 2 (3) | ВРЕМЯ УСТРАНЕНИЯ НЕДОСТАТКОВ И КОНТРОЛЬНЫЕ ПОКАЗАТЕЛИ ДЛЯ КОРРЕКТИРУЮЩИХ ДЕЙСТВИЙ | O | |
| SI- 2 (4) | АВТОМАТИЗИРОВАННЫЕ СРЕДСТВА УПРАВЛЕНИЯ ИСПРАВЛЕНИЯМИ | O/S | |
| SI- 2 (5) | АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ВСТРОЕННОГО ПО | O/S | |
| SI- 2 (6) | УДАЛЕНИЕ ПРЕДЫДУЩИХ ВЕРСИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ВСТРОЕННОГО ПО | O/S | |
| **SI- 3** | **Защита от вредоносного кода** | O/S | |
| SI- 3 (1) | ЦЕНТРАЛЬНОЕ УПРАВЛЕНИЕ | W: Включено в состав PL-9. | |
| SI- 3 (2) | АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ | W: Включено в состав SI-3. | |
| SI- 3 (3) | НЕПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ | W: Включено в AC-6 (10). | |
| SI- 3 (4) | ОБНОВЛЕНИЯ ТОЛЬКО ПРИВИЛЕГИРОВАННЫМИ ПОЛЬЗОВАТЕЛЯМИ | O/S | |
| SI- 3 (5) | ПОРТАТИВНЫЕ ЗАПОМИНАЮЩИЕ УСТРОЙСТВА. | W: Включено в состав MP-7. | |
| SI- 3 (6) | ИСПЫТАНИЯ И ВЕРИФИКАЦИЯ | O | |
| SI- 3 (7) | ОБНАРУЖЕНИЕ, ОСНОВАННОЕ НА НЕПОДПИСАНИИ | W: Включено в состав SI-3. | |
| SI- 3 (8) | ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННЫХ КОМАНД | S | |
| SI- 3 (9) | АУТЕНТИФИКАЦИЯ УДАЛЕННЫХ КОМАНД. | W: Переехал в AC-17 (10). | |
| SI- 3 (10) | АНАЛИЗ ВРЕДОНОСНОГО КОДА | O | |
| **SI- 4** | **Мониторинг систем** | O/S | √ |
| SI- 4 (1) | ОБЩЕСИСТЕМНАЯ СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ. | O/S | √ |
| SI- 4 (2) | АВТОМАТИЗИРОВАННЫЕ ИНСТРУМЕНТЫ И МЕХАНИЗМЫ АНАЛИЗА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ | S | √ |
| SI- 4 (3) | АВТОМАТИЗИРОВАННАЯ ИНТЕГРАЦИЯ ИНСТРУМЕНТОВ И МЕХАНИЗМОВ | S | √ |
| SI- 4 (4) | ВХОДЯЩИЙ И ИСХОДЯЩИЙ ТРАФИК СВЯЗИ | S | √ |
| SI- 4 (5) | ТРЕВОГИ? ГЕНЕРИРУЕМЫЕ СИСТЕМОЙ | S | √ |
| SI- 4 (6) | ОГРАНИЧЕНИЕ НЕПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ | W: Включено в AC-6 (10). | |
| SI- 4 (7) | АВТОМАТИЗИРОВАННЫЙ ОТВЕТ НА ПОДОЗРИТЕЛЬНЫЕ СОБЫТИЯ | S | √ |
| SI- 4 (8) | ЗАЩИТА ИНФОРМАЦИИ МОНИТОРИНГА | W: Включено в состав SI-4. | |
| SI- 4 (9) | ИСПЫТАНИЯ СРЕДСТВ И МЕХАНИЗМОВ МОНИТОРИНГА | O | √ |
| SI- 4 (10) | ВИДИМОСТЬ ЗАШИФРОВАННЫХ СООБЩЕНИЙ | O | √ |
| SI- 4 (11) | АНАЛИЗ АНОМАЛИЙ ТРАФИКА СВЯЗИ | O/S | √ |
| SI- 4 (12) | АВТОМАТИЧЕСКИ ГЕНЕРИРУЕМЫЕ ОРГАНИЗАЦИЕЙ ОПОВЕЩЕНИЯ | O/S | √ |
| SI- 4 (13) | АНАЛИЗ ТРАФИКА И ОБРАЗЦОВ СОБЫТИЙ | O/S | √ |
| SI- 4 (14) | БЕСПРОВОДНОЕ ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ | S | √ |
| SI- 4 (15) | БЕСПРОВОДНАЯ ПРОВОДНАЯ СВЯЗЬ | S | √ |
| SI- 4 (16) | КОРРЕЛИРОВАТЬ ИНФОРМАЦИЮ МОНИТОРИНГА | O/S | √ |
| SI- 4 (17) | КОМПЛЕКСНАЯ СИТУАЦИОННАЯ ПОДГОТОВКА | O | √ |
| SI- 4 (18) | АНАЛИЗ ТРАФИКА И СКРЫТАЯ ФИЛЬТРАЦИЯ | O/S | √ |
| SI- 4 (19) | РИСК ДЛЯ ФИЗИЧЕСКИХ ЛИЦ | O | √ |
| SI- 4 (20) | ПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ | S | √ |
| SI- 4 (21) | ИСПЫТАТЕЛЬНЫЕ СРОКИ | O | √ |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| SI- 4 (22) | НЕСАНКЦИОНИРОВАННЫЕ СЕТЕВЫЕ СЕРВИСЫ | S | √ |
| SI- 4 (23) | УСТРОЙСТВА ОСНОВНОГО ВЫЧИСЛИТЕЛЯ | O | √ |
| SI- 4 (24) | ПОКАЗАТЕЛИ КОМПРОМИССА | S | √ |
| SI- 4 (25) | ОПТИМИЗАЦИЯ АНАЛИЗА СЕТЕВОГО ТРАФИКА | S | √ |
| **SI- 5** | **Предупреждения о безопасности, рекомендации и директивы** | O | √ |
| SI- 5 (1) | АВТОМАТИЗИРОВАННЫЕ ОПОВЕЩЕНИЯ И РЕКОМЕНДАЦИИ | O | √ |
| **SI- 6** | **Проверка функций безопасности и приватности** | S | √ |
| SI- 6 (1) | УВЕДОМЛЕНИЕ О НЕУДАЧНЫХ ТЕСТАХ БЕЗОПАСНОСТИ | W: Включено в состав SI-6. | |
| SI- 6 (2) | ПОДДЕРЖКА АВТОМАТИЗАЦИИ РАСПРЕДЕЛЕННОГО ТЕСТИРОВАНИЯ | S | |
| SI- 6 (3) | ОТЧЕТ О РЕЗУЛЬТАТАХ ПРОВЕРКИ | O | |
| **SI- 7** | **Целостность программного обеспечения, встроенного ПО и информации** | O/S | √ |
| SI- 7 (1) | ПРОВЕРКИ ЦЕЛОСТНОСТИ | S | √ |
| SI- 7 (2) | АВТОМАТИЗИРОВАННЫЕ УВЕДОМЛЕНИЯ О НАРУШЕНИЯХ ЦЕЛОСТНОСТИ | S | √ |
| SI- 7 (3) | ИНСТРУМЕНТЫ ДЛЯ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ С ЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ | O | √ |
| SI- 7 (4) | УПАКОВКА, ЗФЩИЩЕННАЯ ОТ ВСКРЫТИЯ | W: Включено в состав SR-9. | |
| SI- 7 (5) | АВТОМАТИЗИРОВАННЫЙ ОТВЕТ НА НАРУШЕНИЯ ЦЕЛОСТНОСТИ | S | √ |
| SI- 7 (6) | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | S | √ |
| SI- 7 (7) | ИНТЕГРАЦИЯ ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ | O | √ |
| SI- 7 (8) | ВОЗМОЖНОСТЬ АУДИТА ЗНАЧИМЫХ СОБЫТИЙ | S | √ |
| SI- 7 (9) | ПРОВЕРКА ПРОЦЕССА ЗАГРУЗКИ | S | √ |
| SI- 7 (10) | ЗАЩИТА ЗАГРУЗОЧНОГО ВСТРОЕННОГО МИКРОПРОГРАММНОГО ОБЕСПЕЧЕНИЯ | S | √ |
| SI- 7 (11) | ЗАМКНУТЫЕ СРЕДЫ С ОГРАНИЧЕННЫМИ ПРИВИЛЕГИЯМИ | Ш: Перенесен в УК -7 (6 | |
| SI- 7 (12) | ПРОВЕРКА ЦЕЛОСТНОСТИ | O/S | √ |
| SI- 7 (13) | ВЫПОЛНЕНИЕ КОДА В ЗАЩИЩЕННЫХ СРЕДАХ | Ш: Перенесен в УК -7 (7 | |
| SI- 7 (14) | БИНАРНЫЙ ИЛИ МАШИННЫЙ ИСПОЛНЯЕМЫЙ КОД. | Ш: Перенесен в УК -7 (8 | |
| SI- 7 (15) | АУТЕНТИФИКАЦИЯ КОДА | S | √ |
| SI- 7 (16) | СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕССА БЕЗ КОНТРОЛЯ | O | √ |
| SI- 7 (17) | САМОЗАЩИТА ИСПОЛНЯЕМОГО ПРИЛОЖЕНИЯ. | O/S | √ |
| **SI- 8** | **Защита от спама** | O | |
| SI- 8 (1) | ЦЕНТРАЛЬНОЕ УПРАВЛЕНИЕ | W: Включено в состав PL-9. | |
| SI- 8 (2) | АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ | S | |
| SI- 8 (3) | ВОЗМОЖНОСТИ НЕПРЕРЫВНОГО ОБУЧЕНИЯ | S | |
| **SI- 9** | **Ограничения на ввод информации** | W: Включено в AC-2, AC-3, AC-5 и AC-6. | |
| **SI- 10** | **Подтверждение соответствия ввода информации** | S | √ |
| SI- 10 (1) | ВОЗМОЖНОСТЬ РУЧНОГО ПЕРЕОПРЕДЕЛЕНИЯ | O/S | √ |
| SI- 10 (2) | АНАЛИЗ И УСТРАНЕНИЕ ОШИБОК | O | √ |
| SI- 10 (3) | ПРЕДСКАЗУЕМОЕ ПОВЕДЕНИЕ | O/S | √ |
| SI- 10 (4) | ВЫБОР ВРЕМЕНИ ВЗАИМОДЕЙСТВИЙ | S | √ |
| SI- 10 (5) | ОГРАНИЧЕНИЕ ВВОДА НАДЕЖНЫХ ИСТОЧНИКОВ И УТВЕРЖДЕННЫХ ФОРМАТОВ | S | √ |
| SI- 10 (6) | ПРЕДОТВРАЩЕНИЕ ИНЪЕКЦИИ | S | √ |
| **SI- 11** | **Обработка ошибок** | S | |
| **SI- 12** | **Управление информацией и ее хранение** | O | |
| SI- 12 (1) | ОГРАНИЧЕНИЕ ЭЛЕМЕНТОВ ПЕРСОНАЛЬНОЙ ИДЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ | O | |

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| SI- 12 (2) | МИНИМИЗАЦИЯ ПЕРСОНАЛЬНОЙ ИДЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ В ТЕСТИРОВАНИИ, ОБУЧЕНИИ И ИССЛЕДОВАНИЯХ | O | |
| SI- 12 (3) | ЛИКВИДАЦИЯ ИНФОРМАЦИИ | O | |
| **SI- 13** | **Предсказуемое предотвращение отказов** | O | √ |
| SI- 13 (1) | ПЕРЕДАЧА ОТВЕТСТВЕННОСТИ ЗА КОМПОНЕНТЫ | O | √ |
| SI- 13 (2) | СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕССА БЕЗ КОНТРОЛЯ | W: Включено в SI-7(16). | |
| SI- 13 (3) | РУЧНАЯ ПЕРЕДАЧА МЕЖДУ КОМПОНЕНТАМИ | O | √ |
| SI- 13 (4) | УСТАНОВКА И ОПОВЕЩЕНИЕ О РЕЗЕРВНЫХ КОМПОНЕНТАХ | O/S | √ |
| SI- 13 (5) | ВОЗМОЖНОСТИ ОТКАЗОУСТОЙЧИВОСТИ | O | √ |
| **SI- 14** | **Непостоянство** | O | √ |
| SI- 14 (1) | ОБНОВЛЕНИЕ ИЗ НАДЕЖНЫХ ИСТОЧНИКОВ | O | √ |
| SI- 14 (2) | НЕСТОЙКАЯ ИНФОРМАЦИЯ | O | √ |
| SI- 14 (3) | НЕСТОЙКАЯ ВОЗМОЖНОСТЬ СОЕДИНЕНИЯ | O | √ |
| **SI- 15** | **Фильтрация выходной информации** | S | √ |
| **SI- 16** | **Защита памяти** | S | √ |
| **SI- 17** | **Предохранительные процедуры** | S | √ |
| **SI- 18** | **Операции по обеспечению качества персональной идентификационной информации** | O/S | |
| SI- 18 (1) | ПОДДЕРЖКА АВТОМАТИЗАЦИИ | O/S | |
| SI- 18 (2) | ТЭГИ ДАННЫХ | O/S | |
| SI- 18 (3) | КОЛЛЕКЦИЯ | O/S | |
| SI- 18 (4) | ОТДЕЛЬНЫЕ ЗАПРОСЫ | O/S | |
| SI- 18 (5) | УВЕДОМЛЕНИЕ ОБ ИСПРАВЛЕНИИ ИЛИ ИСКЛЮЧЕНИИ | O/S | |
| **SI- 19** | **Де-идентификация** | O/S | |
| SI- 19 (1) | КОЛЛЕКЦИЯ | O/S | |
| SI- 19 (2) | АРХИВИРОВАНИЕ | O/S | |
| SI- 19 (3) | ВЫПУСК | O/S | |
| SI- 19 (4) | УДАЛЕНИЕ, МАСКИРОВАНИЕ, ШИФРОВАНИЕ, ХЕШИРОВАНИЕ ИЛИ ЗАМЕНА ПРЯМЫХ ИДЕНТИФИКАТОРОВ | S | |
| SI- 19 (5) | КОНТРОЛЬ ЗА РАСКРЫТИЕМ СТАТИСТИЧЕСКИХ ДАННЫХ | O/S | |
| SI- 19 (6) | ОТЛИЧИТЕЛЬНАЯ ПРИВАТНОСТЬ | O/S | |
| SI- 19 (7) | ПРОВЕРЕННЫЕ АЛГОРИТМЫ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ | O | |
| SI- 19 (8) | МОТИВИРОВАННЫЙ ЗЛОУМЫШЛЕННИК | O/S | |
| **SI- 20** | **Заражение** | O/S | √ |
| **SI- 21** | **Обновление информации** | O/S | √ |
| **SI- 22** | **Разнообразие информации** | O/S | √ |
| **SI- 23** | **Фрагментация информации** | O/S | √ |

## ТАБЛИЦА C-20: СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ В ЦЕПОЧКЕ ПОСТАВОК

| НОМЕР МЕРЫ | НАЗВАНИЕ МЕРЫ<br>НАЗВАНИЕ РАСШИРЕНИЯ МЕРЫ | РЕАЛИЗАЦИЯ | ДОВЕРИЕ |
|---|---|---|---|
| **SR-1** | **Политика и процедуры** | O | √ |
| **SR-2** | **План управления рисками цепочки поставок** | O | √ |
| SR-2 (1) | СОЗДАНИЕ ГРУППЫ SCRM | O | √ |
| **SR-3** | **Меры обеспечения и процессы цепочки поставок** | O/S | √ |
| SR-3 (1) | РАЗНООБРАЗНАЯ БАЗА ПОСТАВОК | O | √ |
| SR-3 (2) | ОГРАНИЧЕНИЕ ВРЕДА | O | √ |
| SR-3 (3) | НИСХОДЯЩИЙ ПОТОК НА ПОДУРОВНЕ | O | √ |
| **SR-4** | **Происхождение** | O | √ |
| SR-4 (1) | ИДЕНТИЧНОСТЬ | O | √ |
| SR-4 (2) | СЛЕД И ТРАССИРОВКА | O | √ |
| SR-4 (3) | ВАЛИДАЦИЯ КАК ПОДЛИННАЯ И НЕ ИЗМЕНЕННАЯ | O | √ |
| SR-4 (4) | ЦЕЛОСТНОСТЬ ЦЕПОЧКИ ПОСТАВОК - РОДОСЛОВНАЯ | O | √ |
| **SR-5** | **Стратегии, инструменты и методы приобретения** | O | √ |
| SR-5 (1) | ДОСТАТОЧНЫЙ ЗАПАС | O | √ |
| SR-5 (2) | ОЦЕНКИ ПЕРЕД ВЫБОРОМ, ПРИЕМКОЙ, ИЗМЕНЕНИЕМ ИЛИ ОБНОВЛЕНИЕМ | O | √ |
| **SR-6** | **Оценки и пересмотры поставщиков** | O | √ |
| SR-6 (1) | ИСПЫТАНИЯ И АНАЛИЗ | O | √ |
| **SR-7** | **Безопасность операций цепочки поставок** | O | √ |
| **SR-8** | **Соглашения об уведомлении** | O | √ |
| **SR-9** | **Искажение и обнаружение изменений** | O | √ |
| SR-9 (1) | МНОЖЕСТВО СТАДИЙ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ РАЗРАБОТКИ | O | √ |
| **SR-10** | **Проверка систем или компонентов** | O | √ |
| **SR-11** | **Компонентная аутентичность** | O | √ |
| SR-11 (1) | АНТИПОДДЕЛЬНОЕ ОБУЧЕНИЕ | O | √ |
| SR-11 (2) | УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ ДЛЯ ОБСЛУЖИВАНИЯ И РЕМОНТА КОМПОНЕНТОВ | O | √ |
| SR-11 (3) | АНТИПОДДЕЛЬНЫЙ ПРОСМОТР | O | √ |
| **SR-12** | **Ликвидация компонентов** | O | √ |