FIPS PUB 199

ПУБЛИКАЦИЯ СТАНДАРТОВ ОБРАБОТКИ ФЕДЕРАЛЬНОЙ ИНФОРМАЦИИ

Стандарты для Категорирования Безопасности Федеральной Информации и Информационных Систем

Отдел Федеральной Компьютерной безопасности
Лаборатория Информационных технологий
Национальный институт стандартов и технологий

Гейтерсбург, Мэриленд 20899-8930

Декабрь 2003

Американское Министерство торговли

Дональд Л. Эванс, Министр

Администрация Технологий
Филип Дж. Бонд, Заместитель министра по Технологиям

Национальный институт стандартов и технологий

Арден Л. Беман, младший, Директор

ПРЕДИСЛОВИЕ

Серия Публикации стандартов обработки федеральной информации Национального института стандартов и технологий (NIST) является официальной серией публикаций, касающихся стандартов и руководств, принятых и провозглашенных в соответствии с положениями Раздела 5131 из Парламентской реформы управления информационными технологиями 1996 (Общественный закон 104-106) и закона об управлении безопасностью Федеральной информации 2002 (Общественный закон 107-347). Они определяют Министру торговли и NIST важные обязанности по улучшению использования и управления компьютерными и связанными телекоммуникационными системами в Федеральном правительстве. NIST, через его Лабораторию Информационных технологий, обеспечивает лидерство, техническое руководство и координацию правительственных усилий в разработке стандартов и руководств в этих областях.

Комментарии относительно Публикаций стандартов обработки федеральной информации приветствуются и должны адресоваться Директору, Лаборатории Информационной технологии, Национальному институту стандартов и технологий, 100 Проезд Бюро, Остановка 8900, Гейтерсбург, Мэриленд 20899-8900.

- Сьюзен Зевин, Исполняющий обязанности директора

Лаборатория информационных технологий

ПОЛНОМОЧИЯ

Публикации Стандартов обработки федеральной информации (FIPS PUBS) выпущены Национальным институтом стандартов и технологий (NIST) после санкционирования Министром торговли в соответствии с Разделом 5131 из Парламентской реформы управления информационными технологиями 1996 (Общественный закон 104-106) и законом об управлении безопасностью Федеральной информации 2002 (Общественный закон 107-347).

ОГЛАВЛЕНИЕ

1 НАЗНАЧЕНИЕ

Закон об Электронном правительстве 2002 (Общественный закон 107-347), принятый сто седьмым Конгрессом и утвержденный Президентом в декабре 2002, определил важность информационной безопасности по отношению к интересам экономической и национальной безопасности Соединенных Штатов. Заголовок III закона об Электронном правительстве, названного Закон об Управлении Безопасностью Федеральной Информации 2002 (FISMA), определил задачи для NIST с обязанностями по стандартам и руководствам, включая разработку:

- Стандартов, которые будут использоваться всеми Федеральными агентствами, чтобы категорировать всю информацию и информационные системы, принадлежащие или сопровождаемые непосредственно или от имени каждого агентства, основываясь на целях обеспечения соответствующих уровней информационной безопасности согласно масштабу уровней риска;
- Руководств, определяющих типы информации и информационных систем, которые должны быть включены в каждую категорию; и
- Минимальных требований информационной безопасности (т.е. управленческих, эксплуатационных и технических мер), для информации и информационных систем в каждой такой категории.

Публикация 199 FIPS адресуется первой указанной задаче - разработке стандартов для категорирования информации и информационных систем. Стандарты категорирования безопасности информации и информационных систем обеспечивают общие основы и понимание для определения безопасности, что для Федерального правительства способствует: (i) эффективному управлению и надзору за программами информационной безопасности, включая координацию усилий по информационной безопасности всюду по гражданскому сектору, национальной безопасности, подготовке к чрезвычайным ситуациям, безопасности отечества и обеспечению общественного правопорядка; и (ii) подготовке непротиворечивых отчетов для Министерства управления и бюджета (OMB) и Конгресса по соответствию и эффективности политик информационной безопасности, процедур и методов. Последующие стандарты NIST и руководства будут адресоваться второй и третьей указанным задачам.

2 ПРИМЕНИМОСТЬ

Эти стандарты должны примениться к: (i) всей информации в пределах Федерального правительства кроме той информации, которая была определена в соответствии с Правительственным распоряжением 12958, уточненным Правительственным распоряжением 13292, или любым предшествующим порядком, или законом об Атомной энергии 1954 с уточнениями, как требующая защиты против несанкционированного раскрытия и маркирована, чтобы указать на её классифицированный статус; и (ii) всем Федеральным информационным системам кроме тех информационных систем, которые определяются, как системы национальной безопасности, как определено в Разделе 3542 (b)(2) 44 кодекса Соединенных Штатов. Должностные лица агентства должны использовать категорирование безопасности, описанное в Публикации FIPS 199, всякий раз, когда есть федеральное требование, чтобы обеспечить такое категорирование информации или информационных систем. Дополнительные показатели безопасности могут разрабатываться и использоваться по усмотрению агентства. Правительства штатов, локальные и племенные правительства, так же как и организации частного сектора, включенные в критическую инфраструктуру Соединенных Штатов, могут рассматривать использование этих стандартов при необходимости. Эти стандарты являются вступающими в силу после санкционирования Министром торговли.

3 КАТЕГОРИРОВАНИЕ ИНФОРМАЦИИ И ИНФОРМАЦИОННЫХ СИСТЕМ

Эта публикация устанавливает категории безопасности и для информации[1] и для информационных систем. Категории безопасности основаны на потенциальном воздействии на организацию в результате реализации некоторых событий, которые подвергают опасности информацию и информационные системы, необходимые организации, чтобы выполнять установленную ей задачу, защищать её активы, выполнять её юридическую ответственность, сопровождать её ежедневные функции и защищать людей. Категории безопасности должны использоваться в сочетании с информацией об уязвимостях и угрозах в оценке риска к организации.

Цели безопасности

FISMA определяет три цели безопасности для информации и информационных систем:

КОНФИДЕНЦИАЛЬНОСТЬ

“Сохранение авторизованных ограничений на доступ и раскрытие информации, включая средства по защите неприкосновенности частной жизни и конфиденциальной информации …” [44 U.S.C. США, Секция 3542]

Потеря *конфиденциальности* - несанкционированное разглашение информации.

ЦЕЛОСТНОСТЬ

“Принятие мер против несанкционированной модификации или разрушения информации, включая гарантирование неотказуемости от информации и её аутентичности …” [44 U.S.C. США, Секция 3542]

Потеря *целостности* - несанкционированная модификация или разрушение информации.

ДОСТУПНОСТЬ

“Гарантирование своевременного и надежного доступа к и использования информации …” [44 U.S.C. США, Секция 3542]

Потеря *доступности* - прекращение доступа к или использования информации или информационной системы.

Потенциальное воздействие на организации и людей

Публикация FIPS 199 определяет три уровня *потенциального воздействия* на организации или людей, являющегося нарушением безопасности (то есть, потерей конфиденциальности, целостности, или доступности). Эти определения должны применяться в соответствии с контекстом каждой организации и общего национального интереса.

Потенциальное воздействие **НИЗКО** если -

- потеря конфиденциальности, целостности или доступности, как ожидается, будет иметь **ограниченное** отрицательное воздействие на деятельность организации, активы организации или людей.[2]

ПОЯСНЕНИЕ: Ограниченное отрицательное воздействие означает, что, например, потеря конфиденциальности, целостности или доступности могла бы: (i) вызывать ухудшение в способности

[1] Информация категорируется согласно ее *информационному типу*. Тип информации - конкретная категория информации (например, приватная, медицинская, частная, финансовая, следственная, чувствительная для подрядчика, управления безопасностью) определенная организацией или, в некоторых случаях, согласно конкретному закону, Правительственному распоряжению, директиве, политике или регулированию.

[2] Отрицательные воздействия на людей могут включать, но не ограничены, потерей приватности, на которую люди наделены правом в соответствии с законом.

выполнять предназначение до степени и продолжительности, что организация в состоянии выполнить свои основные функции, но эффективность функций заметно уменьшена; (ii) результат в незначительном ущербе к активам организации; (iii) иметь результат в незначительных финансовых убытках; или (iv) иметь результат в незначительном вреде людям.

Потенциальное воздействие **УМЕРЕННО** если -

- потеря конфиденциальности, целостности или доступности, как ожидается, будет иметь **серьезное** отрицательное воздействие на деятельность организации, активы организации или людей.

ПОЯСНЕНИЕ: Серьезное отрицательное воздействие означает, что, например, потеря конфиденциальности, целостности или доступности могла бы: (i) вызывать существенное ухудшение в способности выполнять предназначение до степени и продолжительности, что организация в состоянии выполнить свои основные функции, но эффективность функций значительно уменьшена; (ii) иметь результат в существенном ущербе активам организации; (iii) иметь результат в существенных финансовых убытках; или (iv) иметь результат в существенном вреде людям, который не включает потерю жизни или серьезные опасные для жизни повреждения.

Потенциальное воздействие **ВЫСОКО** если -

- потеря конфиденциальности, целостности, или доступности, как ожидается, будет иметь **тяжелое или катастрофическое** отрицательное воздействие на деятельность организации, активы организации или людей.

ПОЯСНЕНИЕ: Тяжелое или катастрофическое отрицательное воздействие означает, что, например, потеря конфиденциальности, целостности, или доступности могла бы: (i) вызывать тяжелое ухудшение или потерю способности выполнять предназначение до степени и продолжительности, при которой организация не в состоянии выполнить одну или более ее основных функций; (ii) иметь результат в крупном ущербе активам организации; (iii) иметь результат в крупных финансовых убытках; или (iv) иметь результат в тяжелом или катастрофическом вреде людям, включающим потерю жизни или серьезные опасные для жизни повреждения.

Категорирование безопасности, применяемое к типам информации

Категория безопасности типа информации может быть связана и с пользовательской информацией и с системной информацией[3] и может быть применимой к информации или в электронной или в неэлектронной форме. Она может также использоваться как входные данные в рассмотрении соответствующей категории безопасности информационной системы (см. описание категорий безопасности для информационных систем ниже). Установление соответствующей категории безопасности типа информации по существу требует определения потенциального воздействия для каждой цели безопасности, связанной с определенным типом информации.

Обобщенный формат для того, чтобы определить категорию безопасности, SC, типа информации:

SC$_{\text{тип информации}}$ = {(**конфиденциальность**, *воздействие*), (**целостность**, *воздействие*), (**доступность**, *воздействие*)},

где приемлемые значения для потенциального воздействия НИЗКО, УМЕРЕННО, ВЫСОКО или НЕ ПРИМЕНИМО[4]

ПРИМЕР 1: Организация, управляющая *публичной информацией* на её веб-сервере, решает, что отсутствует потенциальное воздействие от потери конфиденциальности (то есть, требования

[3] Системная информация (например, сетевые таблицы маршрутизации, файлы пароля и информация управления криптографическим ключом) должна быть защищена на уровне, соразмерном с самой критической или чувствительной пользовательской информацией, обрабатываемой, хранимой или передаваемой информационной системой, чтобы гарантировать конфиденциальность, целостность и доступность.

[4] Потенциальное значение воздействия *НЕ ПРИМЕНИМО* применяется только к цели безопасности конфиденциальность.

конфиденциальности не применимы), умеренное потенциальное воздействие от потери целостности и умеренное потенциальное воздействие от потери доступности. Результирующая категория безопасности, SC, этого типа информации выражены как:

SCобщественная информация = {(**конфиденциальность**, NA), (**целостность**, УМЕРЕННО), (**доступность**, УМЕРЕННО)}.

ПРИМЕР 2: Организация обеспечения правопорядка, управляющая чрезвычайно чувствительной *следственной информацией*, решает, что потенциальное воздействие от потери конфиденциальности высоко, потенциальное воздействие от потери целостности умеренно и потенциальное воздействие от потери доступности умеренно. Результирующая категория безопасности, SC, этого типа информации выражены как:

SCследственная информация={(**конфиденциальность**, ВЫСОКО), (**целостность**, УМЕРЕННО), (**доступность**, УМЕРЕННО)}

ПРИМЕР 3: Финансовая организация, управляющая стандартной *административной информацией* (информация не связанная с приватностью), решает, что потенциальное воздействие от потери конфиденциальности низко, потенциальное воздействие от потери целостности низко, и потенциальное воздействие от потери доступности низко. Результирующая категория безопасности, SC, этого типа информации выражены как:

SCадминистративная информация = {(**конфиденциальность**, НИЗКО), (**целостность**, НИЗКО), (**доступность**, НИЗКО)}.

Категорирование безопасности, применяемое к информационным системам

Определение категории безопасности информационной системы требует немного большее анализа и должно учитывать категории безопасности всех типов информации, используемых в информационной системе. Для информационной системы потенциальные значения воздействия, присвоенные соответствующим целям безопасности (конфиденциальность, целостность, доступность), должны быть самыми высокими значениями (то есть, наивысший уровень) из числа тех категорий безопасности, которые были определены для каждого типа информации, используемого в информационной системе.[5]

Обобщенный формат для того, чтобы определить категорию безопасности, SC, информационной системы:

SCинформационная система={(**конфиденциальность**, *воздействие*), (**целостность**, *воздействие*), (**доступность**, *воздействие*)},

где приемлемые значения для потенциального воздействия НИЗКО, УМЕРЕННО или ВЫСОКО.

Следует отметить, что значение *не применимо* не может быть присвоено какой-либо цели безопасности в контексте установления категории безопасности для информационной системы. Это учитывает то, что есть наименьшее минимальное потенциальное воздействие (то есть, наименьший уровень), связанное с потерей конфиденциальности, целостности, и доступности для информационной системы как следствие фундаментального требования, чтобы защитить функции обработки на уровне системы и информацию, критическую по отношению к деятельности информационной системы.

[5] Информационные системы включают программы и информацию. Программы, выполняемые в информационной системе (то есть, системные процессы) облегчают обработку, хранение и передачу информации и необходимы для организации, чтобы осуществить ее существенные связанные с предназначением функции и деятельность. Функции, реализуемые системными процессами, также требуют защиты и могли бы быть также субъектами категорирования безопасности. Однако, в интересах упрощения, предполагается, что категорирование безопасности всех типов информации, связанных с информационной системой, обеспечивает соответствующий *худший случай* потенциала воздействия для всей информационной системы, таким образом, устраняя потребность рассматривать системные процессы в категорировании безопасности информационной системы.

ПРИМЕР 4:. Информационная система, используемая для больших приобретений в подрядной организации, содержит и чувствительную контрактную информацию переговорной фазы и стандартную административную информацию. Руководство подрядной организации решает что: (i) для чувствительной контрактной информации, потенциальное воздействие от потери конфиденциальности умеренно, потенциальное воздействие для потери целостности умеренно и потенциальное воздействие от потери доступности низко; и (ii) для стандартной административной информации (информации не связанной с приватностью), потенциальное воздействие от потери конфиденциальности низко, потенциальное воздействие от потери целостности низко и потенциальное воздействие от потери доступности низко. Результирующие категории безопасности, SC, этих типов информации выражены как:

$\mathbf{SC}_{\text{информация контракта}}$ = {(**конфиденциальность**, УМЕРЕННО), (**целостность**, УМЕРЕННО), (**доступность**, НИЗКО)}, и

$\mathbf{SC}_{\text{административная информация}}$ = {(**конфиденциальность**, НИЗКО), (**целостность**, НИЗКО), (**доступность**, НИЗКО)}.

Результирующая категория безопасности информационной системы выраженная как:

$\mathbf{SC}_{\text{система приобретения}}$ = {(**конфиденциальность**, УМЕРЕННО), (**целостность**, УМЕРЕННО), (**доступность**, НИЗКО)},

представляет наивысшие значение или максимальные значения потенциального воздействия по каждой цели безопасности для типов информации, используемых в системе приобретения.

ПРИМЕР 5:. Электростанция содержит SCADA систему (диспетчерское управление и сбор данных), контролирующую распределение электроэнергии для большой военной установки. Система SCADA содержит и данные датчиков в реальном времени и стандартную административную информацию. Руководство электростанции решает что: (i) для данных датчиков, получаемых системой SCADA, отсутствует потенциальное воздействие от потери конфиденциальности, высокое потенциальное воздействие от потери целостности и высокое потенциальное воздействие от потери доступности; и (ii) для административной информации, обрабатываемой системой, есть низкое потенциальное воздействие от потери конфиденциальности, низкое потенциальное воздействие от потери целостности, и низкое потенциальное воздействие от потери доступности. Результирующие категории безопасности, SC, этих типов информации выражены как:

$SC_{\text{данные датчика}}$ = {(**конфиденциальность**, NA), (**целостность**, ВЫСОКО), (**доступность**, ВЫСОКО)}, и

$SC_{\text{административная информация}}$ = {(**конфиденциальность**, НИЗКО), (**целостность**, НИЗКО), (**доступность**, НИЗКО)}.

Результирующая категория безопасности информационной системы первоначально выраженная как:

$SC_{\text{система SCADA}}$ = {(**конфиденциальность**, НИЗКО), (**целостность**, ВЫСОКО), (**доступность**, ВЫСОКО)},

представляет наивысшие значение или максимальные значения потенциального воздействия по каждой цели безопасности для типов информации, используемых в системе SCADA. Руководство электростанции хочет увеличить потенциальное воздействие от потери конфиденциальности от низко до умеренно, что более реалистично представляет потенциальное воздействие на информационную систему если будет нарушение защиты вследствие несанкционированное раскрытие информации на уровне системы или функций обработки. Заключительная категория безопасности информационной системы выражена как:

$SC_{\text{система SCADA}}$ = {(**конфиденциальность**, УМЕРЕННО), (**целостность**, ВЫСОКО), (**доступность**, ВЫСОКО)}.

Таблица 1 суммирует определения потенциальных воздействий для каждой цели безопасности - конфиденциальности, целостности и доступности.

	ПОТЕНЦИАЛЬНОЕ ВОЗДЕЙСТВИЕ		
Цель безопасности	**НИЗКО**	**УМЕРЕННО**	**ВЫСОКО**
Конфиденциальность "Сохранение авторизованных ограничений на доступ и раскрытие информации, включая средства по защите неприкосновенности частной жизни и конфиденциальной информации …" [44 U.S.C. США, Секция 3542]	Несанкционированное разглашение информации, как ожидается, будет иметь **ограниченное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированное разглашение информации, как ожидается, будет иметь **серьезное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированное разглашение информации, как ожидается, будет иметь **тяжелое или катастрофическое** отрицательное воздействие на деятельность организации, активы организации или людей.
Целостность "Принятие мер против несанкционированной модификации или разрушения информации, включая гарантирование неотказуемости от информации и её аутентичности …" [44 U.S.C. США, Секция 3542]	Несанкционированная модификация или разрушение информации, как ожидается, будет иметь **ограниченное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированная модификация или разрушение информации, как ожидается, будет иметь **серьезное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированная модификация или разрушение информации, как ожидается, будет иметь **тяжелое или катастрофическое** отрицательное воздействие на деятельность организации, активы организации или людей.
Доступность "Гарантирование своевременного и надежного доступа к и использования информации …" [44 U.S.C. США, Секция 3542]	Прекращение доступа к или использования информации или информационной системы, как ожидается, будет иметь **ограниченное** отрицательное воздействие на деятельность организации, активы организации или людей.	Прекращение доступа к или использования информации или информационной системы, как ожидается, будет иметь **серьезное** отрицательное воздействие на деятельность организации, активы организации или людей.	Прекращение доступа к или использования информации или информационной системы, как ожидается, будет иметь **тяжелое или катастрофическое** отрицательное воздействие на деятельность организации, активы организации или людей.

ТАБЛИЦА 1: ОПРЕДЕЛЕНИЯ ПОТЕНЦИАЛЬНЫХ ВОЗДЕЙСТВИЙ ДЛЯ ЦЕЛЕЙ БЕЗОПАСНОСТИ

ПРИЛОЖЕНИЕ А ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ДОСТУПНОСТЬ: Обеспечение своевременного и надежного доступа к и использования информации. [44 U.S.C. США, Секция 3542]

КОНФИДЕНЦИАЛЬНОСТЬ: Сохранение санкционированных ограничений на доступ к и раскрытие информации, включая средства по защите неприкосновенности частной жизни и конфиденциальной информации. [44 U.S.C. США, Секция 3542]

ИСПОЛНИТЕЛЬНОЕ АГЕНТСТВО: Исполнительный департамент, определенный в 5 U.S.C. США, Секция 101; военный департамент, определенный в 5 U.S.C. США, Секция 102; независимое учреждение как определено в 5 U.S.C. США, Секция 104 (1); и полностью находящаяся в собственности Правительства корпорация, полностью попадающая под действие 31 U.S.C. США, ГЛАВЫ 91. [41 U.S.C. США, Секция 403]

ФЕДЕРАЛЬНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА: Информационная система, которая используется или управляется исполнительным агентством, подрядчиком исполнительного агентства или другой организацией от имени исполнительного агентства. [40 U.S.C. США, Секция 11331]

ИНФОРМАЦИЯ: Частный случай типа информации.

ИНФОРМАЦИОННЫЕ РЕСУРСЫ: Информация и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии. [44 U.S.C. США, Секция. 3502]

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения, с целью обеспечить конфиденциальность, целостность и доступность. [44 U.S.C. США, Секция 3542]

ИНФОРМАЦИОННАЯ СИСТЕМА: Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или уничтожения информации. [44 U.S.C. США, Секция 3502]

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ: Любое оборудование или взаимосвязанная система или подсистема оборудования, которое используется в автоматизированном получении, хранении, манипулировании, управлении, перемещении, контроле, показе, переключении, обмене, передаче или приеме данных или информации исполнительным агентством. Для целей предыдущего предложения, оборудование используется исполнительным агентством, если оборудование используется исполнительным агентством непосредственно или используется подрядчиком в соответствии с контрактом с исполнительным агентством который: (i) требует использования такого оборудования; или (ii) требует использования, до существенной степени, такого оборудования в реализации сервиса или оснащении продукта. Термин информационная технология включает компьютеры, вспомогательное оборудование, программное обеспечение, встроенное микропрограммное обеспечение и подобные процедуры, сервисы (включая службу поддержки) и связанные ресурсы. [40 U.S.C. США, Секция 1401]

ТИП ИНФОРМАЦИИ: Конкретная категория информации (например, приватная, медицинская, имущественная, финансовая, следственная, чувствительная для подрядчика, управления безопасностью), определенная организацией или, в некоторых случаях, согласно конкретному закону, Правительственному распоряжению, директиве, политике или постановлению.

ЦЕЛОСТНОСТЬ: Принятие мер против несанкционированной модификации или разрушения информации, включая гарантирование неотказуемости от информации и её аутентичности … [44 U.S.C. США, Секция 3542]

СИСТЕМА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ: Любая информационная система (включая любую телекоммуникационную систему) используемая или управляемая агентством или подрядчиком агентства, или другой организации от имени агентства - (i) функция, деятельность или использование которой включает разведывательную деятельность; включает криптологические работы, связанные с национальной безопасностью; включает руководство и управление вооруженными силами; включает оборудование, которое является неотъемлемой частью оружия или системы оружия; или являются критическими по отношению к прямому выполнению военных задач или задач разведки (исключая систему, которая должна использоваться для стандартных административных и бизнес-приложений, например, платежей, финансов, логистики и приложений управления персоналом); или, (ii) постоянно защищена процедурами, установленными для информации, которая была специально определена критериями, установленными Правительственным распоряжением или законом конгресса, быть классифицированной в интересах национальной обороны или внешней политики. [44 U.S.C. США, Секция 3542]

КАТЕГОРИЯ БЕЗОПАСНОСТИ: Характеристика информации или информационной системы, основанная на оценке потенциального воздействия, которое имелось бы на деятельность организации, активы организации или людей от потери конфиденциальности, целостности или доступности такой информации или информационной системы.

МЕРЫ БЕЗОПАСНОСТИ: Управленческие, эксплуатационные и технические меры (то есть, меры защиты или контрмеры), предписанные для информационной системы, чтобы защитить конфиденциальность, целостность и доступность системы и ее информации.

ЦЕЛЬ БЕЗОПАСНОСТИ: Конфиденциальность, целостность или доступность.

ПРИЛОЖЕНИЯ В ССЫЛКИ

[1] Закон о неприкосновенности частной жизни 1974 (Общественный закон 93-579), сентябрь 1975.

[2] Закон о Сокращении документов 1995 (Общественный закон 104-13), май 1995.

[3] Циркуляр OMB A-130, Переходящий Меморандум #4, Управление Федеральными Информационными Ресурсами, ноябрь 2000.

[4] Парламентская реформа управления информационными технологиями 1996 (Общественный закон 104-106), август 1996.

[5] Закон об управлении безопасностью Федеральной информации 2002 (Общественный закон 107-347), декабрь 2002.