**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ.**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Факультет: Информационных технологий

Кафедра: Информационная безопасность

Предмет: Проектная деятельность

Выполнила:

Валикова Анастасия Алекскандровна

Группа: 191-351

В данной работе рассматривается специальная публикация NIST 800-53 4 редакции «Контроль безопасности и приватности для федеральных информационных систем и организаций», в которой представлены способы организации работы предприятия с учетом современных способов организации безопасности, оценки мер и рисков в области информационной безопасности. NIST представляет собой наиболее полное обновление каталога средств контроля безопасности с момента его создания в 2005 году. Современные средства контроля безопасности и улучшения контроля были разработаны и интегрированы в фреймворк, в такие области как: мобильные и облачные вычисления; безопасность приложения; надежность и отказоустойчивость информационных систем. Данная публикация является частью серий специальных публикаций 800, в которой сообщается об исследованиях, руководящих принципах и информационно-пропагандистских усилиях [Лаборатории информационных технологий](https://en.wikipedia.org/wiki/Information_Technology_Laboratory) ( [ITL](https://www.nist.gov/itl) ) в области безопасности информационных систем, а также о деятельности ITL с промышленностью, правительством и академическими кругами. Также NIST 800-53 описывает шаги в структуре управления рисками, которые касаются выбора средств управления безопасностью для федеральных информационных систем в соответствии с требованиями безопасности [Федерального стандарта обработки информации](https://en.wikipedia.org/wiki/Federal_Information_Processing_Standard) (FIPS) 200. Это включает в себя выбор начального набора базовых уровней безопасности. средства контроля, основанные на анализе воздействия наихудшего случая FIPS 199, адаптируют базовые средства контроля безопасности и дополняют их на основе организационной оценки риска. Правила безопасности охватывают 18 областей, включая контроль доступа, реагирование на инциденты, непрерывность бизнеса и возможность восстановления после сбоев.

Публикация NIST 800-53 включает в себя:

* Расширенное и обновленное руководство по адаптации информационных систем
* Картографические таблицы для международного стандарта безопасности ISO/IEC 15408
* Дополнительные параметры назначения и выбора средств для контроля безопасности и конфиденциальности
* Таблицы мер безопасности, которые поддерживают разработку, оценку и эксплуатацию

NIST 800-53 содержит рекомендации по управлению рисками информационной безопасности на трех различных уровнях: организация, бизнес-процесс и уровень информационной системы. Система контроля, определенная в этом документе, рекомендована для использования организациями в целях удовлетворения требования обеспечения информационной безопасности как части хорошо организованной системы управления рисками, которая поддерживает организацию безопасности информационных программ.

Контроль безопасности – меры предосторожности для информационных систем или организаций, предназначенных для: защиты конфиденциальности, обеспечения целостности и доступности информации, обрабатываемой, хранящейся и передаваемой этими системами или организациями, удовлетворение набора определенных требований безопасности. Каждая организация должна отвечать на несколько основных вопросов, при рассмотрении организации безопасности информационной системы:

* Какие меры контроля безопасности необходимы для удовлетворения требований безопасности и адекватного снижения рисков, связанных с использованием информации информационных систем при выполнении организационных задач и бизнес-функций?
* Были ли внедрены меры контроля безопасности или уже существует план внедрения?
* Каков желаемый или требуемый уровень уверенности в том, что выбранные средства контроля безопасности будут или являются эффективными в применении?

Структура кибербезопасности NIST обеспечивает основу, опирающуюся на существующие стандарты, рекомендации и практики, для организаций частного сектора в США, чтобы лучше управлять [рисками кибербезопасности](https://www.upguard.com/blog/cybersecurity-risk) и снижать их.

NIST Cybersecurity Framework подойдет для обслуживания компаний с разным набором специалистов по информационным системам и информационной безопасности:

* Лица, имеющие обязанности по управлению информационными системами, безопасностью и контролю;
* Лица, ответственные за разработку информационных систем;
* Лица, отвечающие за внедрение информационной безопасности и оперативные обязанности в компании;
* Лица, ответственные за оценку и мониторинг информационной безопасности;
* Коммерческие компании, производящие продукты информационной системы, связанные с информационной безопасностью или предоставляющие услуги в сфере безопасности;

Организации используют Публикацию 199 FIPS для категоризации своих информационных систем. Категоризация безопасности осуществляется в рамках всей организации с вовлечением руководящего персонала, включая уполномоченных лиц, начальников, сотрудников информационных служб, старших сотрудников службы безопасности, владельцев информации или ее распорядителей. Информация категорируется по первым двум «Ярусам». Первый ярус – организационный уровень, второй – уровень бизнес-процесса. В соответствие с FIPS 200, организации используют результаты категоризации безопасности от первого и второго ярусов до обозначение организационных информационных систем третьего яруса – уровень информационной системы. Для каждой организационной информационной системы уровня 3 рекомендованы базовые меры безопасности, что является «отправной точкой» для процесса настройки системы контроля безопасности.

В NIST рассмотрен трехуровневый подход к формированию модели управления рисками. На каждом из уровней происходит оценка рисков, реагирование на риски и мониторинг рисков. Выбор и уточнение средств безопасности для информационной системы осуществляется в рамках общеорганизационной программы для управления рисками – то есть рисками для организационных мероприятий, физических лиц, других организаций и государств, связанных с функционированием информационных систем. Риск-ориентированные подходы к выбору и спецификации средств контроля безопасности, учитывают эффективность, действенность и ограничения, обусловленные применимыми федеральными законами, указами, директивами, политиками, нормативными актами, стандартами и руководящими принципами. Для управления рисками организации и эффективного решения возникших проблем, используется трехуровневый подход, учитывающий риске на организационном, бизнес и информационной системы. Процесс управления рисками осуществляется на трех уровнях с общей целью постоянного совершенствования системы управления рисками.

1-ий уровень. Уровень информационных систем: Выделение существующих информационных систем, т.е. разделение всех машин организации по функционалу, например, компьютера бухгалтеров, почтовые сервера и тд. Для каждой из определенных систем будут характерны определенные угрозы, уязвимости и тд в зависимости от их функционала.

2-ой уровень. Уровень процессов: Оценивание возможных рисков и их последствий на информационную систему

3-ий уровень. Уровень организации: Оценивание возможного ущерба репутации компании, возможных санкций регуляторов, штрафы за невыполнение договорных обязательств и тд

В результате оценки информационных рисков мы должны получить знания о том, что случится на каждом уровне, при возникновении каких-то проблем в информационных системах на одном из описанных выше уровней. Существует две системы управления информационными риска по NIST:

* Мониторинг: 3-ий уровень: Логирование событий в ИС. Изучение потенциально опасных записей. 2-ой уровень: Измерение эффективности процессов, обеспечиваемых ИС. 1-ый уровень: Мониторинг эффективности организации.
* Реагирование: 3-ий уровень: Локализация, восстановление и поиск причины возникновения какой-либо проблемы для предотвращения ее возникновения в будущем. 2-ой уровень: Поиск неэффективных процессов. 1-ый уровень: Проверка на неэффективность задействованных процессов.

Элементы управления безопасностью, описанные в этой публикации, имеют четко определенную организацию и структуру. Для удобства использования в процессе выбора и спецификации средств контроля безопасности, элементы управления организованы в восемнадцать семейств. Каждое семейство содержит элементы управления безопасностью, относящиеся к общей теме безопасности данного семейства. Двухсимвольный идентификатор однозначно идентифицирует семейства элементов управления безопасностью, например PS (Personnel Security). Контроль безопасности может включать аспекты политики, надзора, действий отдельных лиц или автоматизированных механизмов, реализуемых информационными системами/устройствами. В таблице перечислены семейства элементов управления безопасностью, связанные с ними идентификаторы семейств и адаптации на русском языке.

|  |  |  |
| --- | --- | --- |
| ABBR | Control family | Адаптация |
| AT | Awareness and Training | Осведомленность и обучение |
| AU | Audit and Accountability | Аудит и отчётность |
| CA | Security Assessment and Authorization | Авторизация и оценка безопасности |
| CM | Configuration Management | Управление конфигурацией |
| CP | Contingency Planning | Планирование непрерывности бизнеса |
| IA | Identification and Authentication | Идентификация и аутентификация |
| IR | Incident Response | Реагирование на инциденты |
| MA | Maintenance | Техническое обслуживание |
| MP | Media Protection | Защита носителей информации |
| PE | Physical and Environmental Protection | Защита от стихийных и физических воздействий |
| PL | Planning | Планирование |
| PS | Personnel Security | Безопасность персонала |
| RA | Risk Assessment | Оценка рисков |
| SA | System and Services Acquisition | Приобретение систем и сервисов |
| SC | System and Communications Protection | Защита систем и коммуникаций |
| SI | System and Information Integrity | Целостность систем и информации |
| PM | Program Management | Управление программой ИБ |

Сами модели зрелости ИБ делятся на четыре уровня:

* 0-ой уровень: полное отсутствие определенного процесса по анализу и оценке рисков информационной безопасности, то есть в спектре рисков организации не рассматриваются риски информационной безопасности.
* 1-ый уровень: Документировано зафиксированное свидетельство осознания руководством существования проблем обеспечения информационной безопасности. Составлен перечень уязвимостей и возможное использование уязвимостей угрозами. При этом процесс анализа и оценки не стандартизирован. База по инцидентам информационной безопасности не обновляется
* 2-ой уровень: Процесс оценки рисков задокументирован и стандартизирован, доводится до заинтересованного персонала через специализированное обучение базовым принципам безопасности, оценки и анализа информационной безопасности. Методология в оценки рисков может гарантировать, своевременное выявление рисков информационной безопасности, поскольку результаты деятельности в рамках процесса по оценке и анализу соответствуют современным политикам, стандартам и процедурам.
* 3-ий уровень: Стратегия оценки рисков информационной безопасности активно совершенствуется, ориентируясь на последние достижения в области безопасности.

В заключение можно подчеркнуть, что NIST был разработан с учетом различных источников и обоснован современным набором средств контроля безопасности систем. Источниками являлись документации из таких сфера как безопасность со стороны оборонного, аудиторского, финансового, медицинского, промышленно-технологического контроля и разведывательных сообществ, определенных национальными и интернациональными стандартами организации. Основная цель специальной публикации NIST 800-53 – обеспечение контроля безопасности через набор необходимых средств, которые удовлетворяют требуемым критериям безопасности, использующихся в организации и согласованные с другими стандартами информационной безопасности или дополняют их. Каталог средств безопасности в специальной публикации 800-53 может быть эффективно использован для защиты информации и информационных систем от традиционных и продвинутых постоянных угроз в различных эксплуатационных технических сценариях. Элементы управления могут быть применены для демонстрации соответствия различным государственным, организационным или институциональным требованиям безопасности. Организации должны нести ответственность за выбор соответствующих мер безопасности для реализации средств контроля, а также демонстрировать эффективность выбранных средств контроля с учетом установленных требований безопасности. Благодаря внесенным мерам безопасности, разработка методов оценки значительно упрощается.

**Многофункциональное управление рисками.**

Выбор и спецификация мер безопасности для информационных систем выполняется как часть общеорганизационной программы информационной безопасности для управления рисками, то есть риск для организационных операций и активов, частных лиц, других производств, связанных с работой информационных систем. Риск-ориентированные подходы к контролю безопасности при выборе и спецификации учитываются эффективность, действенность и ограничения, связанные с применимыми федеральными законами, постановлениями, директивами, политиками, постановлениями и стандартами руководства. Чтобы интегрировать процесс управления рисками во всей организации и более эффективно решать миссии/бизнес-концепт, используется трехуровневый подход, учитывающий риски:

* Организационного уровня;
* Уровень миссии/бизнес-процесса;
* Уровень информационной системы;

Процесс управления рисками осуществляется на трех уровнях с общей целью непрерывного улучшения деятельности организации, связанной с рисками и эффективного межуровневого и внутриуровневого общения между заинтересованными сторонами, имеющими общую заинтересованность в успехе бизнеса организации.

Подробнее об уровнях подхода:

* Первый уровень: обеспечивает приоритезацию бизнес-функции, в свою очередь, способствует реализации инвестиционных стратегий и решений о финансировании – продвижение рентабельной и эффективной информации о технологических решениях, соответствующих стратегическим целям, задачам организации и показателям эффективности.
* Второй уровень: определение миссии/бизнес-процессов, необходимых для поддержания организации, определение категории безопасности информационных систем, необходимые для выполнения миссии/бизнес-процессов, включение требований информационной безопасности в миссии/бизнес-процессов, создание архитектуры предприятия для облегчения распределения средств управления безопасностью для информационных систем организации и их среды. Структура управления рисками (RMF). В данной публикации основное внимание уделяется миссии/бизнес-процессам, где процесс выбора мер безопасности выполняется в контексте трех уровней организационного риска иерархии управления.

RMF решает проблемы безопасности организации, связанные с проектированием, разработкой, внедрением, эксплуатацией и утилизации информационных систем и сред, в которых эти системы работают. RMF состоит из шести шагов:

* 1 Шаг: классификация информационных систем на основе воздействия Публикации 199 FIPS;
* 2 Шаг: выбор применимого базового плана управления безопасностью на основе результатов безопасности категоризации и применения рекомендаций по адаптации;
* Шаг 3: внедрение мер безопасности и задокументированный дизайн, разработка и детализация средств управления;
* Шаг 4: оценка мер безопасности и определение степени их реализации;
* Шаг 5: авторизация работы информационной системы на основе определения риска для организации;
* Шаг 6: отслеживание мер безопасности в информационной системе и среде работы на постоянной основе для определения эффективности контроля, изменений в системе/ среде соблюдения законодательства, указов, директив, политик, постановлений и стандартов.

Организации обязаны надлежащим образом снижать риски, возникающие в результате использования информации и информационных систем при выполнении миссий и деловых функций. Существенной проблемой для организации является определение наиболее экономически эффективных и выгодных решений, соответствующих набору мер безопасности, которые в случае их осуществления, позволили бы уменьшить риски при соблюдении требований безопасности, определенных соответствующими федеральными законами, указами, положениями, политиками, директивами или стандартами, например, FISMA, OMG Circular A-130, HSPD-12, FIPS Publication 200. В наше время не существует единого правильного набора средств контроля безопасности, который бы учитывал все проблемы безопасности организации во всех случаях. Выбор наиболее подходящего набора средств контроля безопасности для конкретной ситуации или информационной системы в целях предотвращения возникновения рисков является важной задачей, требующей фундаментального понимания организационной миссии/бизнес-процесса, которое будет поддерживать информационные системы, а также условия функционирования среды, в которой находятся эти системы. При таком представлении, организации могут продемонстрировать, как наиболее эффективно обеспечить конфиденциальность, целостность и доступность организационной информации и информационных систем так, чтобы поддержать потребности миссии/бизнеса, демонстрируя при этом должную осторожность. Выбор, внедрение и поддержание соответствующего набора средств контроля безопасности для адекватной защиты информационных систем, используемых организациями, требует тесного сотрудничества с владельцами используемых систем в целях понимания текущих изменений миссий/бизнес-процессов, условий эксплуатации и использования систем.

Для оказания помощи организациям в надлежащем выборе средств контроля безопасности информационных систем вводится понятие базовых средств контроля. Базовые средства контроля являются отправной точкой для процесса выбора средств контроля безопасности, описанного в настоящем документе, и выбираются на основе категории безопасности и связанного с ней уровня воздействия информационных систем, определенных публикацией FIPS 199 и FIPS 200. Приложение-D приводит перечень базовых показателей контроля безопасности соответствующим информационным системам с низким, умеренным и высоким воздействием, использующим выделенную отметку, определенную публикацией FIPS 200 раздела 3.1, обеспечивающую начальный набор средств контроля безопасности для каждого уровня воздействия. Приложение-F представляет полный каталог средств контроля безопасности информационных систем и организаций, упорядоченных по семействам контроля. Также в нем содержится дополнительная информация о том, как использовать категории безопасности публикации FIPS 199 и уровни воздействия системы публикации FIPS 200 при применении руководства по адаптации к базовым мерам контроля безопасности для достижения адекватного снижения рисков. Описанного в этих публикациях руководство по адаптации помогает организациям настроить базовые уровни контроля безопасности, выбранные с использованием результатов организационных оценок рисков. Базовый уровень действия включает: идентификацию и определение общих элементов управления; применение соображений об аналитическом исследовании среды; выбор компенсирующих мер; присвоение конкретных значений безопасности контроля параметров; дополнительные меры безопасности или меры по усовершенствованию контроля; содержание дополнительной информации для осуществления контроля.

Обозначения контроля безопасности.

Согласно Приложению-F, существует три различных типа обозначения, связанных с элементами контроля безопасности, определяющие: сферу применимости контроля; общий характер контроля; ответственность за разработку, внедрение, оценку и санкционирование контроля. Эти обозначения включают общие, системные и гибридные элементы управления. Общие элементы управления – элементы управления безопасностью, реализация которых приводит к наследованию одной или несколькими организационными информационными системами. Контроль защищенности наследуемых информационных систем или компонентов информационной системы, когда эти системы или компоненты получают защиту от контрольных функций при этом контроль развит, реализован, оценен, авторизирован и находится под наблюдением лиц, отвечающих за систему или ее компоненты, то есть внутренние или внешние сущности организаций, где размещены эти системы или компоненты. Возможности безопасности, предоставляемые общими элементами управления могут быть унаследованы от многих источников, включая, например организации, организационные миссии/бизнес-направления, сайты, анклавы, операционные среды или другие информационные системы. Многие средства контроля, необходимые для защиты организационных информационных систем, например обучение по вопросам безопасности, планы реагирования на инциденты, физический доступ и тд, являются кандидатами на статус общего контроля. Кроме того, существуют различные основанные на технологии общие средства контроля, например публичная ключевая инфраструктура PKI, безопасные стандарты конфигурации для клиентов/сервисов, доступ системы управления, защита границ. Благодаря централизированному управлению и документированию разработки, внедрения, оценки, авторизации и мониторинга общих средств контроля затраты на обеспечение безопасности могут быть авторизированы в различных информационных системах.

Организации возлагают ответственность за общие средства контроля на соответствующих должностных лиц организации и координирует разработку, внедрение, оценку, санкционирование и мониторинг контроля. Определение общих средств контроля. Определение общих средств контроля наиболее эффективно осуществляется в рамках всей организации при активном участии главных сотрудников по вопросам информации, старших сотрудников по вопросам информационной безопасности, руководителя по рискам, уполномоченных должностных лиц, владельцев информации/управляющих владельцев информационных систем, других должностных лиц и сотрудников службы безопасности, необходимые для адекватного снижения рисков, возникающих в результате использования этих систем. Каждый общий контроль, определенный организацией, рассматривается на предмет применимости к каждой конкретной организационной информационной системе, как правило, владельцами информационных систем и уполномоченных должностными лицами. Ключевые заинтересованные стороны сотрудничают в целях определения возможности эффективного использования общих средств контроля на уровне миссии/бизнес-процесса. Когда общие средства контроля защищают несколько организационных информационных систем с различными уровнями воздействия, средства контроля реализуются в отношении самого высокого уровня воздействия среди систем. Если общие средства управления реализуются на самом высоком уровне воздействия информационных систем, где владельцы систем должны учитывать эту ситуацию в своих оценках риска и принимать соответствующие меры по снижению риска, например добавлять средства контроля безопасности или улучшения контроля, изменяя присвоенные значения параметров контроля безопасности, внедряя компенсирующие средства контроля или изменяя определенные аспекты миссии/бизнес-процессов. Внедрение общих мер контроля, которые являются менее эффективными или которые обеспечивают недостаточный потенциал безопасности для информационных систем с более высокой отдачей, может оказать значительное негативное воздействие на организационные задачи или бизнес-функции.

Выбор базовых уровней контроля безопасности.

При подготовке к выбору и определению соответствующих средств контроля безопасности для организационных информационных систем и их соответствующих сред функционирования организации сначала определяют критичность и чувствительность информации, подлежащей обработке, хранению или передаче этими системами. Этот процесс, известный как категоризация безопасности, описанный в FIPS 199. Стандарт категоризации безопасности основан на простой и устоявшейся концепции - определение потенциального негативного воздействия на организационные информационные системы. Результаты классификации безопасности помогают направлять и информировать выбор соответствующих средств контроля безопасности для адекватной защиты этих информационных систем. Средства контроля безопасности, выбранные для информационных систем соизмеримы с потенциальным негативным воздействием на организации или страну в случае потери конфиденциальности, целостности или доступности. Публикация FIPS 199требует от организации классифицировать системы на малозатратные, умеренные или высокоэффективные для заявления целей безопасности конфиденциальности, целостности и доступности. NIST 800-60 является руководством для типов отражения информации и систем информационной безопасности. Категории содержат рекомендации по присвоению категорий безопасности информационным системам. Обобщенным форматом выражения категории безопасности информации системы является:

SC информационная система = {(конфиденциальность, воздействие), (целостность, воздействие), (доступность, воздействие)}

Поскольку потенциальные значения воздействия на конфиденциальность, целостность и доступность не всегда могут быть одинаковыми для конкретной информационной системы, концепция высокой отметки (введенная в FIPS Публикация 199) используется и в публикации 200 FIPS для определения уровня воздействия информационной системы с явной целью выбора применимого базового уровня контроля безопасности для одного из трех базовых уровней, указанных в Приложении-D.

Базовые показатели контроля безопасности, приведенные в приложении-D, учитывают потребности в области безопасности широкого и разнообразного круга заинтересованных сторон (включая отдельных пользователей и организации). Некоторые предположения, лежащие в основе исходных данных приложения-D, включают, например: условия организации информационных систем управления; сведения о характере операций, осуществляемых организацией; функциональность работающей информационной системы; виды угроз, с которыми сталкиваются организации, организация бизнес-процессов и информационные системы; тип информации, обрабатываемый, хранящейся или передаваемый информационными системами. Формулирование базовых допущений является ключевым элементом начального этапа формирования рисков процесса управления рисками, описанного в специальной публикации NIST 800-39. Некоторые из предположений, лежащих в основе исходных условий в приложении D, это:

* Расположение информационных систем на физических объектах;
* Пользовательские данные в организационных информационных системах относительно устойчивы;
* Информационные системы являются многопользовательскими;
* Некоторые пользовательские данные информационных систем не могут быть переданы другим пользователям, имеющим авторизированный доступ к тем же системам;
* Информационные системы существуют в сетевых средах;
* Информационные системы носят универсальный характер;
* Организации имеют необходимую структуру, ресурсы и инфраструктуру для реализации управления

Если одно или несколько из этих предположений не выполняется, то некоторые меры контроля безопасности, назначенные первоначальными базовыми показателями в приложении-D, могут быть неприменимы—ситуация, которую можно легко решить, применив руководство по адаптации. И наоборот, существуют также некоторые возможные ситуации, которые конкретно не рассматриваются в исходных условиях. К ним относятся:

* Внутри организации существуют внутренние угрозы;
* Секретные данные/информация обрабатываются, хранятся или передаются информационными системами;
* Расширенные постоянные угрозы (APTs) существуют в организации;
* Отдельные данные/информация требуют специальной защиты на основе федерального законодательства, директив, нормативных актов или политик;
* Информационные системы должны взаимодействовать с другими системами в различных областях безопасности.

Если какое-либо из вышеприведенных предположений применимо, то для обеспечения адекватной защиты, вероятно, потребуется дополнительный контроль безопасности из приложения-F—ситуация, которая также может быть эффективно решена путем применения руководства по адаптации и результаты организационных оценок риска.

После выбора применимого базового уровня контроля безопасности из приложения-D организации инициируют процесс адаптации для соответствующего изменения и более тесного согласования средств контроля с конкретными условиями внутри организации (т. е. условиями, связанными с задачами организации/бизнес- функциями, информационными системами или средой функционирования). Процесс включает в себя:

* Применение соображений определения области применения к оставшимся базовым средствам контроля безопасности;
* Выбор компенсирующих средств контроля безопасности по необходимости;
* Назначение параметров, определяемых организацией параметрам контроля безопасности с помощью явных операторов назначения и выбора;
* Дополнение базовых показателей новыми средствами контроля безопасности и улучшения контроля по необходимости;
* Предоставление дополнительной технической информации для реализации контроля по необходимости;

Организации могут иногда находить и применять компенсирующие меры безопасности, используемые организациями вместо конкретных средств контроля на низких, умеренных и высоких базовых уровнях, описанных в приложении-D, которые обеспечивают эквивалентную или сопоставимую защиту организационных информационных систем и информации, обрабатываемой, хранящейся или передаваемой этими системами. Для обеспечения эквивалентной защиты конкретной ценной бумаги может потребоваться более одного компенсирующего элемента управления в приложении-F. Например, организации с существенно ограниченным персоналом может компенсировать разделение обязанностей – контроль безопасности за счет усиления аудита, отчетности и контроль кадровой безопасности. Это может произойти, например, когда организация оказывается не в состоянии эффективно осуществлять конкретные меры безопасности в базовых показателях или когда в силу специфики информационных систем или сред эксплуатации, органы управления в исходных условиях оказываются не рентабельными для получения необходимого снижения рисков. Компенсирующие средства контроля обычно выбираются после применения соображений в области применения по руководству в адаптации применимого базового уровня контроля безопасности. Компенсационный контроля может применять организациями при:

* Организации выбирают компенсационные меры контроля из приложения-F, если соответствующие компенсационные меры контроля отсутствуют, организации принимают соответствующие компенсационные меры из других источников. Организации должны сделать все возможное, чтобы выбрать компенсирующие элементы управления из каталога контроля безопасности в приложении-F. Определяемые организацией компенсационные средства контроля используются только в тех случаях, когда организация определяет, что каталог средств контроля безопасности не содержит подходящих компенсационных средств контроля;
* Организации предоставляют подтверждающее обоснование того, как компенсационные средства контроля обеспечивают эквивалентные возможности безопасности для информационных систем и почему базовые средства контроля безопасности не могут быть использованы;
* Организации оценивают и принимают риск, связанный с внедрением компенсационного контроля в организационные информационные системы.

Назначение значений параметров контроля безопасности.

Элементы управления безопасностью и улучшение управления, содержащие встроенные параметры, дают организациям гибкость в определении частей элементов управления и улучшение поддержки конкретных организационных требований. После первоначального применения соображений в определенной области и выбора компенсирующих средств контроля организации, рассматривают средства контроля для инструкции назначения/ выбора и определяют соответствующие заданные организацией значения для идентификации параметров. Значения параметров могут быть установлены применимыми федеральными законами, указами, директивами, нормативными актами, политиками или стандартами. Как только организации определят значения параметров для контроля безопасности и улучшения управления, назначения и выборки становятся частью элементов управления и улучшения. Инструкция CNSS 1253 предусматривает назначения минимальных значений для определяемых организацией переменных, применимых к средам национальной безопасности. Организации могут выбрать указанные значения параметров контроля безопасности перед выбором компенсирующих элементов управления, поскольку спецификация параметров завершает определение контроля и может повлиять на требования к компенсирующему контролю. Сотрудничество в разработке значений параметров также может принести значительную выгоду. Для организаций, которые часто сотрудничают друг с другом, может оказаться полезной разработка взаимноприемлимого набора единообразных значений параметров контроля безопасности. Это может помочь организациям в достижении большей степени взаимности при зависимости от информационных систем или услуг, предлагаемых другими организациями.

Окончательно определение набора средств контроля безопасности, необходимых для обеспечения адекватной безопасности организационных информационных систем и сред, в которых эти системы функционируют, являются функции оценки риска и того, что требуется для достаточного снижения рисков для организационных операций и активов отдельных лиц, других организаций и стран. Соображения относительно потенциальных взаимодействий на национальном уровне и воздействий на друге организации при классификации организационных информационных систем, основанных на Патриотическом акте США и президентских директивах по национальной безопасности. Во многих случаях дополнительные меры безопасности или управления улучшениями потребуются для решения конкретных угроз и уязвимостей в организациях, представительствах/ бизнес-процессах, системах для удовлетворения требованиям действующих федеральных законов, указов, директив, политик, стандартов или правил оценки рисков в процессе выбора средств контроля безопасности. Это предоставляет важную информацию для определения необходимости и достаточности мер контроля безопасности и улучшения контроля в первоначальных исходных условиях. Организациям рекомендуется максимально использовать приложение-F для обозначения процесса дополнения первоначальных исходных условий дополнительными мерами контроля безопасности или улучшения контроля. Средства контроля безопасности и улучшения контроля, выбранные в дополнение к базовым показателям, распределяются между соответствующими компонентами информационной системы таким же образом, как и контрольные ассигнования, осуществляемые организациями в первоначальных базовых показателях.

Ситуации, требующие потенциального базового дополнительных средств.

Организации могут быть подчинены условиям, которые с точки зрения оперативной, экологической или угрозы оправдывают выбор и внедрение дополнительных (дополнительных) средств контроля для обеспечения надлежащей защиты организационных миссий/бизнес-функций и информационных систем, поддерживающих эти миссии/функции. Примеры условий и дополнительных средств контроля, которые могут потребоваться:

* Расширенная постоянная угроза. Исходные условия контроля безопасности не предполагают, что текущая среда угроз—это та, в которой противники достигли значительного плацдарма и присутствия в организациях и организационных информационных системах, то есть организации имеют дело с продвинутой постоянной угрозой (APT). Противники продолжают атаковать организационные информационные системы и инфраструктуру информационных технологий и добиваются успеха в некоторых аспектах таких атак.
* Кросс-доменные службы. Базовые уровни контроля безопасности не предполагают, что информационные системы должны работать через несколько доменов безопасности. Базовые линии предполагают плоское представление информационных потоков. Для решения кросс-доменных служб и операций, некоторые улучшения контроля безопасности могут быть рассмотрены для обеспечения адекватной защиты информации при передаче между информационными системами с различными политиками безопасности.
* Мобильность. Использование мобильных устройств может привести к необходимости дополнительных средств контроля безопасности и улучшения контроля по выбранным первоначальным исходным условиям. Например, возможность удаленной очистки могут быть выбраны для устранения угрозы кражи или потери мобильным устройств.
* Секретность информации. В некоторым сферах секретная и конфиденциальная информационная может находиться в национальных системах безопасности без того, чтобы все пользователя имели необходимые решения на доступ ко всей этой информации. В таких случаях требуются дополнительные меры безопасности, чтобы гарантировать, что информация строго разделена и не будет доступна неавторизированным пользователям. Например, когда секретная информация обрабатывается, хранится или передается в информационных системах, совместно принадлежащая нескольким организациям, может потребовать более строгий контроль за обслуживающим персоналом.

Повышение информационной безопасности без изменения выбора управления.

Такая ситуация может возникнуть, в случае, если организации не могут применять достаточные меры контроля безопасности в своих информационных системах для адекватного снижения или смягчения рисков. Поэтому необходимы альтернативные стратегии для предотвращения негативного воздействия на организационные миссии/бизнес-функции, возникающие в результате агрессивного использования информационных технологий. Ограничения на типы используемых технологий и способы использования информационных систем обеспечивают альтернативный метод снижения рисков, который может использоваться в сочетании с дополнительными средствами контроля безопасности или вместо них. Ограничения на использование информационных систем и конкретных информационных технологий могут быть в некоторых ситуациях единственными практическими или разумными действиями, которые могут предпринять организации для того, чтобы иметь возможность выполнять возложенные на них задачи. Примеры использования ограничения включают в себя:

* Ограничение информации, которую информационные системы могут обрабатывать, хранить или передавать, или способа автоматизации организационных задач/бизнес-функций;
* Запрещение внешнего доступа к организационной информации путем удаления отдельных компонентов информационной системы из сетей;
* Запрещение информации средней или высокой степени воздействия на компоненты организационной информационной системы, к которой имеет доступ общественность, если только не будет сделано явное определение риска, разрешающее такой доступ.

Базовые показатели контроля безопасности.

Приложение-D содержит базовые показатели контроля безопасности, которые представляют собой отправную точку при определении средств контроля безопасности для информационных систем с низким, умеренным и высоким уровнем воздействия. Полное описание всех средств контроля безопасности приводится в приложениях F и G. Три базовых уровня контроля безопасности имеют иерархический характер в отношении средств контроля безопасности, используемых в этих базовых уровнях. Иерархический характер распространяется на требования к безопасности каждого элемента управления c низкой, умеренной и высокой степени влияния в том, что требования управления на определенном уровне воздействия удовлетворяет более сильному набор безопасности требования к этому контролю выше, чем к следующему более низкому уровню воздействия того же самого контроля.

Уверенность и надежность меры доверия к информационным системам

Обеспечение безопасности является важнейшим аспектом в определении надежности информационных система. Гарантия – это мера уверенности в том, что функции, методы, политики, процедуры, механизмы и архитектура безопасности организационных информационных систем точно обеспечивают соблюдение установленных политик безопасности. Целями положения-E являются:

* Поощрение организаций к включению требований обеспечения в закупки информационных систем, компонентов системы и услуг;
* Поощрение разработчиков аппаратного, программного и микропрограммного обеспечения к использованию методов разработки, приводящих к созданию более надежных продуктов и систем информационных технологий;
* Поощрение организаций к выявлению, отбору и использованию продуктов информационных технологий, созданных с соответствующим уровнем надежности систем и технических методов обеспечения безопасности в процессе жизненного цикла разработки систем;
* Снижение рисков информационной безопасности за счет внедрения более надежных информационных технологий и продуктов в рамках критических информационных систем или компонентов систем;
* Поощрение разработчиков и организаций к получению на постоянной основе подтверждающих доказательств для поддержания надежности информационных систем.

Минимальные требования к безопасности Федеральной информации и информационных систем определены в публикации FIPS 200.Эти требования могут быть удовлетворены путем выбора, адаптации, внедрения и получения подтверждающих доказательств для контроля безопасности в низких, умеренных или высоких базовых уровнях в приложении-D. Инструкция CNSS 1253 обеспечивает базовые уровни контроля безопасности для национальных систем безопасности. Таким образом, меры контроля, связанные с обеспечением безопасности в исходных условиях, установленных для сообщества национальной безопасности, если они будут определены таким образом, могут отличаться от таковых элементы управления. Исходные условия также включают меры контроля, связанные с обеспечением минимальных требований к обеспечению, которые обычно применяются к федеральной информации и информационным системам. Трудно определить, обеспечивает ли данный базовый уровень контроля безопасности по приложению-D гарантии, необходимые для всех информационных технологий, пользователей, платформ и организаций. Например, в то время как использование формальных методов может быть уместным в междоменном продукте, различные методы обеспечения безопасности могут быть уместны для сложных облачных систем управления или веб-серверов, предоставляющих информацию о готовности к чрезвычайным ситуациям из Министерства внутренних дел Безопасность. Тем не менее, существующие исходные условия имеют аспекты обеспечения, которые отражают минимальные гарантии, ожидающие, какими будут общими для всех технологий, пользователи платформ и организаций. Однако, учитывая нынешнее пространство угроз и растущий риск для организационных операций и активов, отдельных лиц, других организаций и нации, создаваемый APT, организации могут принять решение о внедрении дополнительных гарантий, связанных с дополнительными средствами контроля, выбранными на основе рекомендаций по адаптации. Организации также могут рассмотреть возможность разработки высоконадежных накладок для критически важных миссий/бизнес-функций, специализированных условий эксплуатации и/или информационных технологий. Когда контроль, связанный с обеспечением гарантий, не может быть удовлетворен, организации могут предложить компенсирующий контроль или взять на себя более высокую степень контроля, риска в отношении фактического достигнутого потенциала безопасности.

В общем случае контроль, связанный с обеспечением безопасности, - это контроль, который: определяет процессы, процедуры, методы или методологии проектирования и разработки информационных систем и компонентов системы; обеспечивает поддержку оперативных процессов, включая совершенствование качества систем/компонентов/процессов; представляет доказательства безопасности по развитию или оперативной деятельности; определяет контроля безопасности, эффективности или риска (например, аудита, испытаний, оценка, анализ, оценка, верификация, валидация, мониторинг); позволяет совершенствование навыков персонала, знания и понимания (например, по вопросам безопасности/подготовки, реагирования на инциденты обучения, учебных действий в чрезвычайных ситуациях). Средства контроля безопасности могут быть обозначены как средства контроля, связанные с обеспечением безопасности, даже если они обладают некоторыми функциональными характеристиками или свойствами. Различие между функциональностью и обеспечением менее важно при описании средств контроля в базовых системах, прежде всего потому, что средства контроля безопасности в трех базовых системах после применения процесса адаптации становятся частью планов обеспечения безопасности для информационных систем и организаций. Организации предупреждаются о необходимости тщательного изучения мер контроля, связанных с обеспечением гарантий, в исходных условиях в процессе адаптации, включая разработку накладок, чтобы помочь обеспечить непреднамеренное устранение мер контроля, которые обеспечивают меры доверия к функциям безопасности, необходимым для защиты миссии/бизнеса. Однако это различие становится более важным, когда организации используют возможность выбора дополнительных средств контроля безопасности для повышения уровня уверенности (или степень уверенности) в функциональности безопасности и возможностях безопасности.

**Минимальные требования к обеспечению безопасности в системах с низким уровнем воздействия. Требования к обеспечению:**

Организация, исходя из своих требований безопасности, политики безопасности и необходимых возможностей безопасности, рассчитывает на: ограниченную силу функциональных возможностей безопасности; ограниченную степень уверенности, подкрепленную глубиной и охватом соответствующих доказательств безопасности, в том, что функциональные возможности безопасности являются полными, последовательными и правильными.

Функциональность безопасности и обеспечение безопасности для систем с низким уровнем воздействия достигаются внедрение средств контроля безопасности на основе адаптированного низкого базового уровня в приложении D. Требования к обеспечению безопасности для систем с низким уровнем воздействия (включая компоненты информационных технологий, входящие в состав этих систем) согласуются с теми, которые легко достижимы с немодифицированными коммерческими готовыми продуктами и услугами (COTS). Из-за ограниченной функциональности, ожидаемой для систем с низким уровнем воздействия, глубина / охват производимых доказательств безопасности NIST Special Publication 800-53A предоставляет дополнительную информацию о глубине и охвате в области контроля безопасности оценки минимальна. Данные о глубине / охвате дополнительно дополняются результатами оценок контроля безопасности и постоянного мониторинга организационных информационных систем и сред, в которых эти системы функционируют.

**Минимальные требования к обеспечению безопасности в системах со средним уровнем воздействия. Требования к обеспечению:**

Организация, исходя из своих требований безопасности, политики безопасности и необходимых возможностей безопасности, ожидает: умеренного уровня функциональности безопасности; умеренной степени уверенности, подкрепленной глубиной и охватом соответствующих доказательств безопасности, в том, что функциональность безопасности является полной, последовательной и правильной.

Функциональность безопасности и обеспечение безопасности для систем с умеренным воздействием достигаются за счет осуществление контроля безопасности. Требования к умеренным системам добавить в ожидания за низкого уровня надежности посредством: включение безопасности функциональность при большей прочности механизма и возможностей, чем прочность механизма и возможность достичь в низкой отдачей системами; требование, возможно, какого-то особенного развития; установление более безопасных параметров конфигурации; требование некоторой дополнительной оценки реализованных возможностей. Из-за умеренной силы функциональности, ожидаемой для систем с умеренным воздействием, глубина/охват производимых доказательств безопасности 100 является более существенной, чем минимальные доказательства, производимые для систем с низким воздействием, но все же в диапазоне того, что может быть предоставлено производителями, поставщиками и реселлерами COTS. оценка контроля безопасности и постоянный мониторинг организационных информационных систем и сред функционирования. Для других функций, помимо технологических, акцент делается на умеренной степени уверенности в полноте, правильности и последовательности процедурных и / или оперативных функций безопасности.

**Минимальные требования к обеспечению безопасности в системах с высоким уровнем воздействия. Требования к обеспечению:**

Организация, исходя из своих требований безопасности, политики безопасности и необходимых возможностей безопасности, ожидает: высокая степени надежности функций безопасности; высокая степень уверенности, подкрепленная глубиной и охватом соответствующих доказательств безопасности, в том, что функции безопасности являются полными, последовательными и правильными.

Функциональность безопасности и обеспечение безопасности для высокоэффективных систем достигаются осуществлением контроля безопасности с учетом высокого исходного уровня в приложении-D. Обеспечение требований для высокоэффективных систем добавляются в ожидания на умеренном уровне по гарантии: включение более высокого класса возможностей безопасности, что в результате применения общепринятых передовых коммерческих практик, развиваются для уменьшения цены изъяна. Из-за высокой прочности функциональности, ожидаемой для систем с высокой степенью воздействия, глубина/охват полученных доказательств безопасности является более всеобъемлющим, чем доказательства, полученные для систем с умеренной степенью воздействия. Хотя доказательства все еще могут быть в пределах того, что может быть предоставлено производителями, поставщиками и реселлерами COTS, также может потребоваться большая уверенность со стороны независимых поставщиков оценки. Доказательства глубины/охвата дополняются результатами дополнительных оценок контроля безопасности и постоянным мониторингом организационных информационных систем / сред функционирования. Помимо технологических функций, существует высокая степень уверенности в полноте, правильности и последовательности процедурных и / или оперативных функций безопасности.

**Атрибуты безопасности организации:**

* предоставляет средства для связывания, имеющих определенные организацией значения атрибутов безопасности, с информацией, находящейся в хранилище, в процессе обработки и/или при передаче;
* обеспечивает создание и сохранение ассоциаций атрибутов безопасности с информацией;
* устанавливает разрешения, определяемые организацией атрибуты безопасности для информационных систем, определяемых организацией;
* определяет разрешенные определения организации, значения или диапазоны для каждого из установленных атрибутов безопасности.

Информация, представленная внутри информационных систем с использованием абстракций, известных как структуры данных. Внутренние структуры данных могут представлять различные типы сущностей, как активных, так и пассивных. Активные сущности, также известные как субъекты, обычно связаны с отдельными лицами, устройствами или процессами, действующими от имени отдельных лиц. Пассивные сущности, также известные как объекты, они обычно связаны со структурами данных, такими как записи, буферы, таблицы, файлы, межпроцессные каналы и коммуникационные порты. Атрибуты безопасности, форма метаданных, представляют собой абстракции, дающие основные свойства или характеристики активных и пассивных сущностей в отношении защиты информации. Эти атрибуты могут быть связаны с активными сущностями (т. е. субъектами), которые могут передавать или получать информацию, вызывать поток информации между объектами или изменять состояние информационной системы. Эти атрибуты также могут быть связаны с пассивными сущностями (т. е. объектами), которые содержат или получают информацию. Связь атрибутов безопасности с субъектами и объектами называется привязкой и обычно включает в себя установку значения атрибута и типа атрибута. Атрибуты безопасности при привязке к данным / информации включают принудительное исполнение политики информационной безопасности для контроля доступа и управления информационными потоками, либо через организационные процессы, либо через функции или механизмы информационной системы. Содержание или присвоенные значения атрибутов безопасности могут непосредственно влиять на способность отдельных лиц получать доступ к организационной информации.

Организации могут определять типы атрибутов, необходимых для выбранных информационных систем для поддержки миссий/бизнес-функций. Потенциально существует широкий диапазон значений, которые могут быть присвоены любому заданному атрибуту безопасности. Маркировка выпуска может включать, например, только США, НАТО или NOFORN (не распространяется на иностранных граждан). Указывая допустимые диапазоны и значения атрибутов, организации могут гарантировать, что значения атрибутов безопасности являются значимыми и релевантными. Термин маркировка безопасности относится к ассоциации атрибутов безопасности с субъектами и объектами представлены внутренними структурами данных внутри организационных информационных систем, что позволяет обеспечить применение политик информационной безопасности на основе информационных систем. Метки безопасности включают, например, разрешения на доступ, защиту жизненного цикла данных (т. е. шифрование и истечение срока действия данных), гражданство, принадлежность к подрядчику и классификацию информации в соответствии с юридическими требованиями и требованиями соответствия. Термин маркировка безопасности относится к ассоциации атрибутов безопасности с объектами в удобочитаемой для человека форме, позволяющей обеспечить соблюдение требований безопасности на основе организационных процессов. Базовый элемент управления AC-16 представляет собой требование к пользовательской ассоциации атрибутов (маркировке). Усовершенствования AC-16 представляют собой дополнительные требования, включая Ассоциацию атрибутов на основе информационной системы (маркировку). Типы атрибутов включают, например, уровень классификации для объектов и уровень разрешения (авторизации доступа) для субъектов.

Список сокращений:

ИС - информационная система.

ИБ – информационная безопасность.

FIPS publication – публикация федеральных стандартов обработки информации.

NIST – национальный стандарт стандартов и технологий.

COTS - коммерческая готовая продукция.

APT – развитая устойчивая угроза.

CNSS – комитет по системам национальной безопасности.

FISMA – федеральный закон об управлении информационной безопасностью.

PS – безопасность персонала.

ISO – международная организация по стандартизации.

IEC – международная комиссия по электротехнике.

ITL – информационно-технологическая лаборатория.