УТВЕРЖДАЮ
Главный врач учреждения здравоохранения
«Брестский областной диспансер спортивной медицины»

С.В.Евдолюк

___.03.2022 г.

РУКОВОДСТВО ПО СИСТЕМЕ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ISO/IEK 27001

Редакция № 1

г. Брест
2022 г.

СОДЕРЖАНИЕ

Введение

Любой вид деятельности человека можно представить как процесс, в результате которого появляется продукт, материальный или интеллектуальный, имеющий определенную ценность, то есть стоимость. Информация является одной из разновидностей таких ценностей, стоимость ее может оказаться настолько высокой, что ее потеря или утечка, даже частичная, способна поставить под вопрос само существование любого учреждения. Поэтому защита информации с каждым днем приобретает все большее значение, практически во всех более или менее крупных учреждениях существуют свои подразделения информационной безопасности.

На рынке информационной безопасности растет спектр предложений по обеспечению информационной безопасности. Как правильно сориентироваться в этом потоке предлагаемых продуктов? Как выбрать оптимальный по финансовым затратам вариант и учесть все потребности нашего учреждения? Какие критерии отбора применить? Ведь информационная безопасность любого учреждения здравоохранения сама по себе ни интеллектуальных, ни материальных ценностей не производит, в ее необходимости и важности уже ни у кого нет сомнений, и на расходах на эту службу редко экономят.

Что необходимо сделать, чтобы затраты и уровень информационной безопасности учреждения здравоохранения были в оптимальном соотношении — этим вопросам посвящена данная публикация.

Мероприятия по обеспечению информационной безопасности (ИБ), как известно, не приносят доходов, с их помощью можно лишь уменьшить ущерб от возможных инцидентов. Поэтому очень важно, чтобы затраты на создание и поддержание ИБ на должном уровне были соразмерны ценности активов организации, связанных с ее информационной системой (ИС). Соразмерность может быть обеспечена категорированием информации и информационной системы, а также выбором регуляторов безопасности на основе результатов категорирования.

Категорирование информации и информационных систем

Присвоение категорий безопасности информации и информационным системам производится на основе оценки ущерба, который может быть нанесен нарушениями безопасности. Подобные инциденты могут помешать учреждению в выполнении возложенной на нее миссии, скомпрометировать активы, поставить компанию в положение нарушителя действующего законодательства, создать угрозу повседневной деятельности, подвергнуть опасности персонал. Категории безопасности используются совместно с данными об уязвимостях и угрозах в процессе анализа рисков, которым подвержена организация.

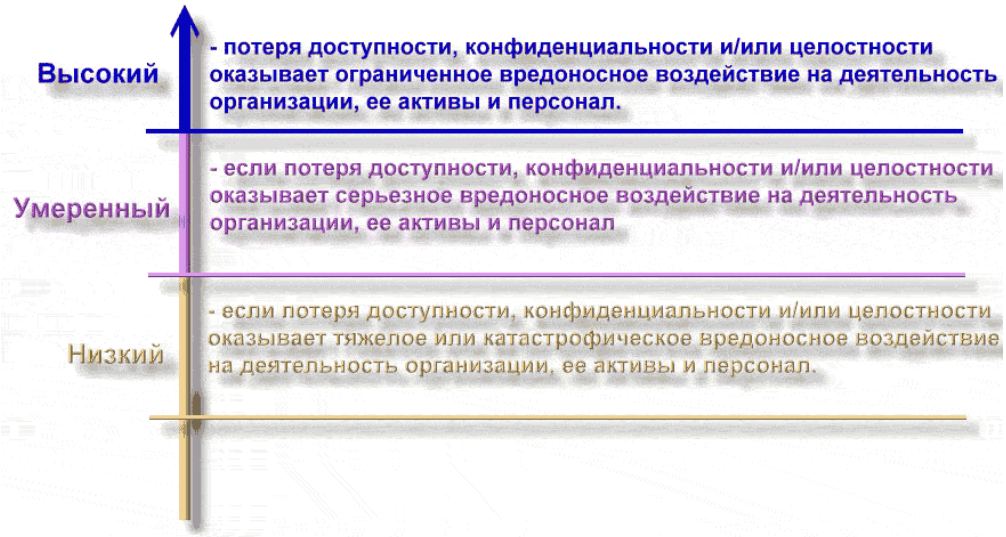
Существуют три основных аспекта ИБ:

- доступность;
- конфиденциальность;
- целостность.

Вообще говоря, нарушения ИБ могут затрагивать лишь часть этих аспектов, равно как и регуляторы безопасности могут быть специфичны для отдельных аспектов. Поэтому целесообразно оценивать возможный ущерб отдельно для нарушений доступности, конфиденциальности и целостности, а при необходимости можно получить интегральную оценку.

Размер ущерба удобно оценивать по трехуровневой шкале как **низкий, умеренный или высокий** (Рис. 1)

Рисунок 1. Шкала оценки ущерба при нарушении информационной безопасности



Потенциальный ущерб для учреждения оценивается как низкий, если потеря доступности, конфиденциальности и/или целостности оказывает ограниченное вредоносное воздействие на деятельность организации, ее активы и персонал. Ограниченность вредоносного воздействия означает, что:

- учреждение остается способной выполнять возложенную на нее миссию, но эффективность основных функций оказывается заметно сниженной;
- активам учреждения наносится незначительный ущерб;
- учреждение несет незначительные финансовые потери;
- персоналу наносится незначительный вред.

Потенциальный ущерб для учреждения оценивается как **умеренный**, если потеря доступности, конфиденциальности и/или целостности оказывает серьезное вредоносное воздействие на деятельность организации, ее активы и персонал. Серьезность вредоносного воздействия означает, что:

- учреждение остается способной выполнять возложенную на нее миссию, но эффективность основных функций оказывается существенно сниженной;
- активам учреждения причиняется значительный ущерб;
- учреждение несет значительные финансовые потери;
- персоналу наносится значительный вред, не создающий угрозы жизни или здоровью.

Потенциальный ущерб для учреждения оценивается как **высокий**, если потеря доступности, конфиденциальности и/или целостности оказывает тяжелое или катастрофически вредоносное воздействие на деятельность организации, ее активы и персонал, то есть:

- учреждение теряет способность выполнять все или некоторые из своих основных функций;
- активам учреждения причиняется крупный ущерб;
- учреждение несет крупные финансовые потери;
- персоналу наносится тяжелый или катастрофический вред, создающий возможную угрозу жизни или здоровью.

Категорировать необходимо и пользовательскую, и системную информацию, представленную как в электронной форме, так и в виде "твердой" копии.

Открытая информация может не иметь категории конфиденциальности. Например, сведения, содержащиеся на общедоступном web-сервере учреждения, не имеют категории конфиденциальности, а их доступность и целостность оцениваются как умеренные.

При категорировании информационной системы принимаются во внимание категории хранимой, обрабатываемой и передаваемой средствами ИС информации, а также ценность активов самой ИС, т.е. берется максимум категорий по всем видам информации и активов. Для получения интегральной оценки следует взять максимум категорий по основным аспектам информационной безопасности.

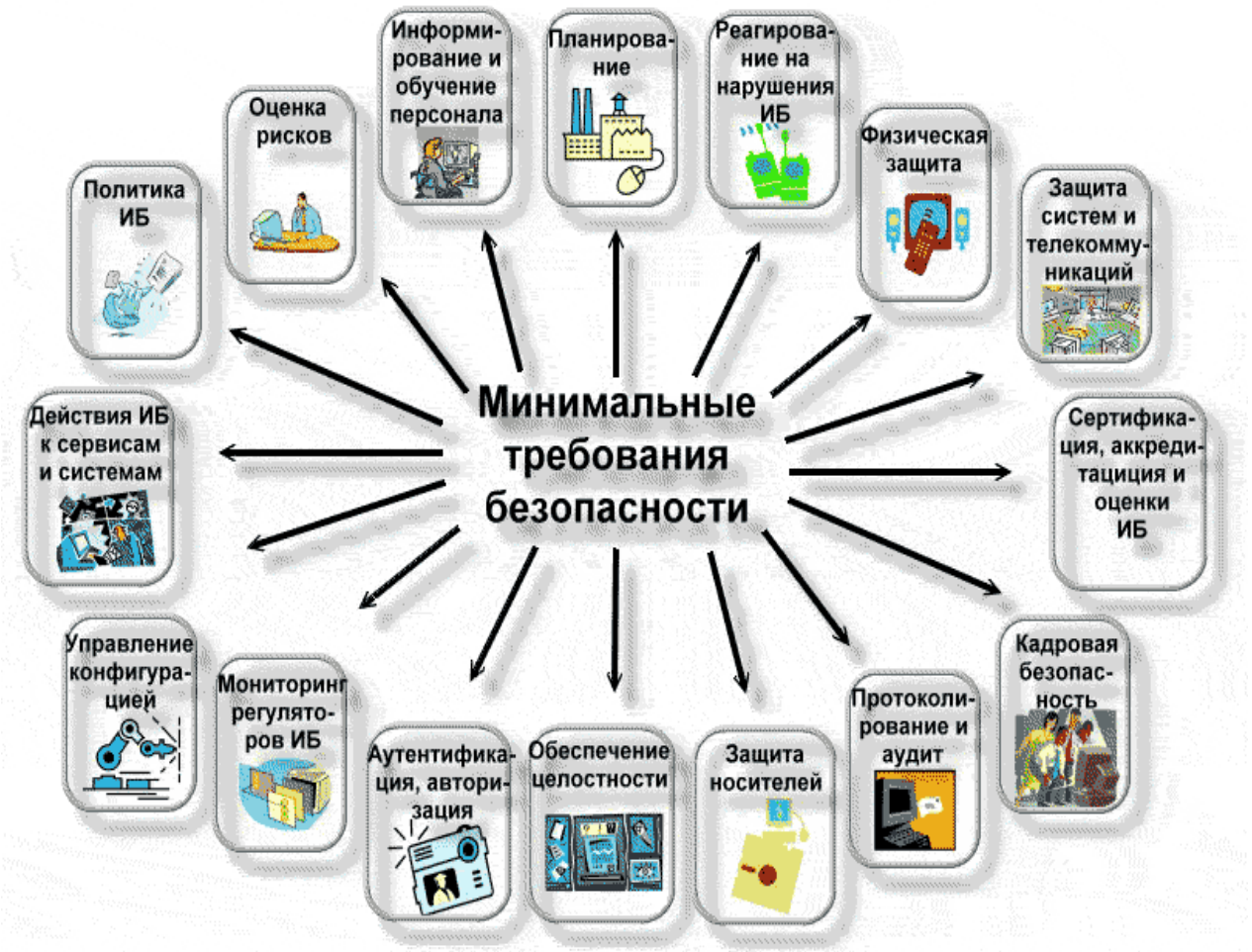
Минимальные (базовые) требования безопасности

Минимальные (базовые) требования безопасности формулируются в общем виде, без учета категории, присвоенной ИС. Они задают базовый уровень информационной безопасности, им должны удовлетворять все информационные системы. Результаты категорирования важны при выборе регуляторов безопасности, обеспечивающих выполнение требований, сформулированных на основе анализа рисков (Рис. 2).

Рисунок 2. Уровни информационной безопасности

Минимальные требования безопасности (Рис. 3) охватывают административный, процедурный и программно-технический уровни ИБ и формулируются следующим образом.

Рисунок 3. Базовые требования безопасности к информации и ИС.



- Учреждение должно разработать, документировать и обнародовать официальную политику безопасности и формальные процедуры, направленные на выполнение приведенных ниже требований, и обеспечить эффективную реализацию политики и процедур.
- В учреждении необходимо периодически производить оценку рисков, включая оценку угроз миссии, функционированию, имиджу и репутации учреждения, ее активам и персоналу. Эти угрозы являются следствием эксплуатации ИС и осуществляемых при этом обработки, хранения и передачи данных.
- Применительно к закупке систем и сервисов в учреждении необходимо:
  - выделить достаточный объем ресурсов для адекватной защиты ИС;
  - при разработке систем учитывать требования ИБ;
  - ограничивать использование и установку программного обеспечения;
  - обеспечить выделение внешними поставщиками услуг достаточных ресурсов для защиты информации, приложений и/или сервисов.

- В области сертификации, аккредитации и оценки безопасности в учреждении следует проводить:
    - постоянный мониторинг регуляторов безопасности, чтобы иметь доверие к их эффективности;
    - периодическую оценку регуляторов безопасности, применяемых в ИС, чтобы контролировать их эффективность;
    - разработку и претворение в жизнь плана действий по устранению недостатков и уменьшению или устранению уязвимостей в ИС;
    - авторизацию введения в эксплуатацию ИС и установление соединений с другими информационными системами.

- В области кадровой безопасности необходимо:
    - обеспечить надежность (доверенность) должностных лиц, занимающих ответственные посты, а также соответствие этих лиц предъявляемым к данным должностям требованиям безопасности;
    - обеспечить защиту информации и информационной системы при проведении дисциплинарных акций, таких как увольнение или перемещение сотрудников;
    - применять соответствующие официальные санкции к нарушителям политики и процедур безопасности.

- Учреждение должно обеспечить информирование и обучение сотрудников:
    - чтобы руководители и пользователи ИС знали о рисках, связанных с их деятельностью, и о соответствующих законах, нормативных актах, руководящих документах, стандартах, инструкциях и т.п.;
    - чтобы персонал имел должную практическую подготовку для выполнения обязанностей, связанных с информационной безопасностью.

- В области планирования необходимо разработать, документировать, периодически изменять и реализовать планы обеспечения безопасности ИС, описывающие регуляторы безопасности (имеющиеся и планируемые) и правила поведения персонала, имеющего доступ к ИС.
- С целью планирования бесперебойной работы в учреждении следует установить, поддерживать и эффективно реализовать планы реагирования на аварийные ситуации, резервного копирования, восстановления после аварий, чтобы обеспечить доступность критичных информационных ресурсов и непрерывность функционирования в аварийных ситуациях.

- В плане реагирования на нарушения информационной безопасности учреждение должно:
    - создать действующую структуру для реагирования на инциденты, имея в виду адекватные подготовительные мероприятия, выявление, анализ и локализацию нарушений, восстановление после инцидентов и обслуживание обращений пользователей;
    - обеспечить прослеживание, документирование и сообщение об инцидентах соответствующим должностным лицам организации и уполномоченным органам.

- С целью физической защиты учреждение должно:
    - предоставлять физический доступ к ИС, оборудованию, в производственные помещения только авторизованному персоналу;
    - физически защищать оборудование и поддерживающую инфраструктуру ИС;
    - обеспечить должные технические условия для функционирования ИС;
    - защищать ИС от угроз со стороны окружающей среды;
    - обеспечить контроль условий, в которых функционирует ИС;
    - обеспечить управление доступом, предоставив доступ к активам ИС только авторизованным пользователям, процессам, действующим от имени этих пользователей, а также устройствам (включая другие ИС) для выполнения разрешенных пользователям транзакций и функций.

- Для обеспечения протоколирования и аудита необходимо:
    - создавать, защищать и поддерживать регистрационные журналы, позволяющие отслеживать, анализировать, расследовать и готовить отчеты о незаконной, несанкционированной или ненадлежащей активности;
    - обеспечить прослеживаемость действий в ИС с точностью до пользователя (подотчетность пользователей).

- В плане управления конфигурацией в учреждении следует:
    - установить и поддерживать базовые конфигурации;
    - иметь опись (карту) ИС, актуализируемую с учетом жизненного цикла, в которую входят аппаратура, программное обеспечение и документация;
    - установить и обеспечить практическое применение настроек для конфигурирования средств безопасности в продуктах, входящих в ИС.
- В области идентификации и аутентификации необходимо обеспечить идентификацию и аутентификацию пользователей ИС, процессов, действующих от имени

пользователей, а также устройств как необходимое условие предоставления доступа к ИС.

Кроме того, необходимо:

- Применительно к сопровождению:
  - осуществлять периодическое и своевременное обслуживание ИС;
  - обеспечить эффективные регуляторы для средств, методов, механизмов и персонала, осуществляющих сопровождение.

- Для защиты носителей:
  - защищать носители данных как цифровые, так и бумажные;
  - предоставлять доступ к данным на носителях только авторизованным пользователям;
  - санировать или уничтожать носители перед выводом из эксплуатации или перед передачей для повторного использования.

- С целью защиты систем и коммуникаций:
  - отслеживать, контролировать и защищать коммуникации (то есть передаваемые и принимаемые данные) на внешних и ключевых внутренних границах ИС;
  - применять архитектурные и аппаратно-программные подходы, повышающие действующий уровень информационной безопасности ИС.

- Для обеспечения целостности систем и данных:
  - своевременно идентифицировать дефекты ИС и данных, докладывать о них и исправлять;
  - защищать ИС от вредоносного программного обеспечения;
  - отслеживать сигналы о нарушениях безопасности и сообщения о новых угрозах для информационной системы и должным образом реагировать на них.

Выбор базового набора регуляторов безопасности с целью выполнения требований безопасности

Необходимым условием выполнения требований безопасности являются выбор и реализация соответствующих регуляторов безопасности, то есть выработка и применение экономически оправданных контрмер и средств защиты. Регуляторы безопасности подразделяются на административные, процедурные и программно-технические и служат для обеспечения доступности, конфиденциальности и целостности информационной системы и обрабатываемых, хранимых и передаваемых ею данных.

Выбор регуляторов безопасности осуществляется на основе результатов категорирования данных и информационной системы. Кроме того, следует учесть, какие регуляторы безопасности уже реализованы и для каких имеются конкретные планы реализации, а также требуемую степень доверия к эффективности действующих регуляторов.

Адекватный выбор регуляторов безопасности можно упростить, если производить его из предопределенных базовых наборов, ассоциированных с требуемым уровнем ИБ. Применяя трехуровневую шкалу, используют три базовых набора, соответственно, для минимального (низкого, базового), умеренного и высокого уровня информационной безопасности.

Регуляторы безопасности для минимального уровня ИБ

На минимальном уровне информационной безопасности целесообразно применять следующие **административные регуляторы безопасности**.

Рисунок 4. Регуляторы безопасности по уровням ИБ

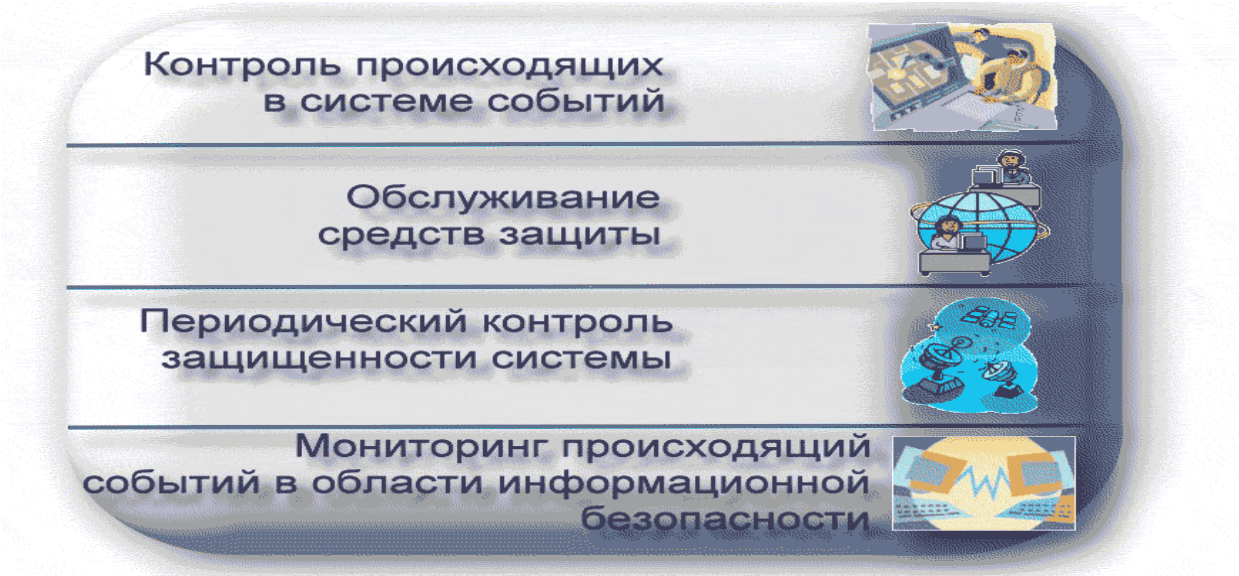
- **Оценка рисков: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменение:
  - официальной документированной политики оценки рисков, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
  - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов оценки рисков.
- **Оценка рисков: категорирование по требованиям безопасности.** Категорирование данных и информационной системы, документирование результатов, включая обоснование установленных категорий; документ заверяется руководством.
- **Оценка рисков: проведение.** Оценка рисков и возможного ущерба от несанкционированного доступа, использования, раскрытия, нарушения работы, модификации и/или разрушения данных и/или информационной системы, включая ресурсы, управляемые внешними организациями.
- **Оценка рисков: пересмотр результатов.** Пересмотр результатов оценки рисков проводится либо с заданной частотой, либо после существенных изменений в ИС или поддерживающей инфраструктуре, либо после иных событий, способных заметно повлиять на уровень безопасности ИС или ее статус аккредитации.
- **Планирование безопасности: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменения:
  - официальной документированной политики планирования безопасности, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
  - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов планирования безопасности.
- **Планирование безопасности: план безопасности ИС.** Разработка и реализация для информационной системы плана, в котором описаны требования безопасности для ИС и имеющиеся и планируемые регуляторы безопасности, служащие для выполнения этих требований; документ заверяется руководством.
- **Планирование безопасности: изменение плана безопасности ИС.** С заданной частотой пересматривается план безопасности ИС. В него вносятся изменения, отражающие изменения в компании и в ее информационной системе либо проблемы, выявленные при реализации плана или при оценке регуляторов безопасности.
- **Планирование безопасности: правила поведения.** В организации устанавливается и доводится до сведения пользователей ИС набор правил, описывающих обязанности и ожидаемое поведение по отношению к использованию информации и информационной системы. Прежде чем получить доступ к ИС и ее информационным ресурсам, пользователи подписывают подтверждение того, что они прочитали, поняли и согласны выполнять предписанные правила поведения.

- **Планирование безопасности: оценка приватности.** В учреждении проводится оценка выполнения в ИС требований приватности.
- **Закупка систем и сервисов: политика и процедуры.** Разрабатываются, распространяются, периодически пересматриваются и изменяются:
    - официальная документированная политика закупки систем и сервисов, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
    - формальные документированные процедуры, способствующие проведению в жизнь политики и ассоциированных регуляторов закупки систем и сервисов.
- **Закупка систем и сервисов: выделение ресурсов.** Определение, документирование и выделение ресурсов, необходимых для адекватной защиты информационной системы в компании, являются частью процессов капитального планирования и управления инвестициями.
- **Закупка систем и сервисов: поддержка жизненного цикла.** Учреждение управляет информационной системой, применяя методологию поддержки жизненного цикла с учетом аспектов информационной безопасности.
- **Закупка систем и сервисов: закупки.** В контракты на закупку включаются требования и/или спецификации безопасности, основанные на результатах оценки рисков.
- **Закупка систем и сервисов: документация.** Необходимо обеспечить наличие, защиту и распределение авторизованным должностным лицам учреждения адекватной документации на информационную систему и ее составные части.
- **Закупка систем и сервисов: ограничения на использование программного обеспечения.** Учреждение обеспечивает выполнение существующих ограничений на использование программного обеспечения.
- **Закупка систем и сервисов: программное обеспечение, устанавливаемое пользователями.** Необходимо проводить в жизнь явно сформулированные правила, касающиеся загрузки и установки пользователями программного обеспечения.
- **Закупка систем и сервисов: аутсорсинг информационных сервисов.** Необходимо следить, чтобы внешние организации, предоставляющие информационные сервисы, применяли адекватные регуляторы безопасности, соответствующие действующему законодательству и условиям контракта, а также отслеживать адекватность регуляторов безопасности.
- **Сертификация, аккредитация и оценка безопасности: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменения:
    - официальной документированной политики оценки безопасности, сертификации и аккредитации, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;

- формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов оценки безопасности, сертификации и аккредитации.

- **Сертификация, аккредитация и оценка безопасности: соединения с другими ИС.** Авторизация учреждением всех соединений своей информационной системы с другими ИС, находящимися вне границ аккредитации, и постоянное отслеживание/контроль этих соединений; подписание уполномоченными должностными лицами соглашения об установлении соединений между системами.
- **Сертификация, аккредитация и оценка безопасности: сертификация по требованиям безопасности.** Учреждение проводит оценку применяемых в ИС регуляторов безопасности, чтобы проверить, насколько корректно они реализованы, функционируют в соответствии со спецификациями и дают ожидаемые результаты с точки зрения выполнения предъявляемых к ИС требований информационной безопасности.
- **Сертификация, аккредитация и оценка безопасности: календарный план мероприятий.** В учреждении разрабатывается и с заданной частотой изменяется календарный план мероприятий. В нем описаны запланированные, реализованные и оцененные корректирующие действия, направленные на устранение всех недостатков, выявленных в процессе оценки регуляторов безопасности, и на уменьшение или устранение известных уязвимостей ИС.
- **Сертификация, аккредитация и оценка безопасности: аккредитация.** Учреждение явным образом санкционирует (осуществляет аккредитацию) ввод информационной системы в эксплуатацию и с заданной частотой, но не реже, чем раз в три года, проводит повторную аккредитацию.
- **Сертификация, аккредитация и оценка безопасности: постоянный мониторинг.** Постоянный мониторинг регуляторов безопасности в ИС.

Рисунок 5. Поддержание необходимого уровня безопасности



На минимальном уровне информационной безопасности рекомендуется применение следующих **процедурных регуляторов безопасности.**

- **Кадровая безопасность: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменение:
  - официальной документированной политики кадровой безопасности, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
  - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов кадровой безопасности.
- **Кадровая безопасность: категорирование должностей.** С каждой должностью ассоциируется определенный уровень риска и устанавливаются критерии отбора кандидатов на эти должности. Целесообразно с заданной частотой пересматривать установленные уровни риска.
- **Кадровая безопасность: отбор персонала.** Прежде чем предоставить доступ к информации и информационной системе, проводится проверка лиц, нуждающихся в подобном доступе.
- **Кадровая безопасность: увольнение.** Увольняемый сотрудник лишается доступа к ИС, с ним проводят заключительную беседу, проверяют сдачу всего казенного имущества, в том числе ключей, идентификационных карт, пропусков, и убеждаются, что соответствующие должностные лица имеют доступ к официальным данным, созданным увольняемым сотрудником и хранящимся в информационной системе.
- **Кадровая безопасность: перемещение персонала.** При переходе сотрудника на другую должность учреждение пересматривает предоставленные ему права доступа к ИС и ее ресурсам, и осуществляет соответствующие действия, такие как изготовление новых ключей, идентификационных карт, пропусков, закрытие старых и заведение новых системных счетов, а также смена прав доступа.
- **Кадровая безопасность: соглашения о доступе.** Прежде чем предоставить доступ к информации и информационной системе сотруднику, нуждающемуся в подобном доступе, составляются соответствующие соглашения (например, о неразглашении информации, о надлежащем использовании ИС), а также правила поведения, компания обеспечивает подписание этих соглашений сторонами и с заданной частотой пересматривает их.
- **Кадровая безопасность: требования безопасности к сотрудникам сторонних организаций.** Учреждение устанавливает требования безопасности, в том числе роли и обязанности, к сотрудникам сторонних организаций (сервисных служб, подрядчиков, разработчиков, поставщиков информационных услуг и услуг управления системами и сетями) и отслеживает обеспечение сторонними организациями адекватного уровня информационной безопасности.

- **Кадровая безопасность: санкции.** В учреждении применяется формализованный процесс наказания сотрудников, нарушивших установленные политику и процедуры безопасности.
- **Физическая защита: политика и процедуры.** Разрабатываются, распространяются, периодически пересматриваются и изменяются:
    - официальная документированная политика физической защиты, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
    - формальные документированные процедуры, способствующие проведению в жизнь политики и ассоциированных регуляторов физической защиты.
- **Физическая защита: авторизация физического доступа.** В учреждении составляются и поддерживаются в актуальном состоянии списки сотрудников, имеющих доступ в помещения, в которых расположены компоненты информационной системы (кроме помещений, официально считающихся общедоступными), выпускаются соответствующие удостоверения (бэйджи, идентификационные карты, интеллектуальные карты); соответствующие должностные лица с заданной частотой пересматривают и утверждают списки и удостоверения.
- **Физическая защита: управление физическим доступом.** Необходимо контролировать точки физического доступа, в том числе официально определенные точки входа/выхода, в помещения, в которых расположены компоненты информационной системы (кроме помещений, официально считающихся общедоступными). Следует проверять предоставленные сотрудникам права, прежде чем разрешить им доступ. Кроме того, контролируется доступ в помещения, официально считающиеся общедоступными, в соответствии с проведенной оценкой рисков.
- **Физическая защита: мониторинг физического доступа.** Отслеживается физический доступ к системе с целью выявления и реагирования на нарушения.
- **Физическая защита: контроль посетителей.** Физический доступ к информационной системе контролируется аутентификацией посетителей перед разрешением войти в помещения, где расположены компоненты ИС (кроме помещений, официально считающихся общедоступными).
- **Физическая защита: протоколирование доступа.** В учреждении поддерживаются журналы посещений помещений (кроме тех, что официально считаются общедоступными), где фиксируются:
    - фамилия, имя посетителя и название организации;
    - подпись посетителя;
    - представленные документы (форму идентификации);
    - дата и время доступа (входа и выхода);
    - цель посещения;

  - фамилия, имя посещаемого лица и его организационная принадлежность; соответствующие должностные лица с заданной частотой просматривают журналы посещений.
- **Физическая защита: аварийное освещение.** В учреждении необходимо применять и поддерживать автоматические системы аварийного освещения, которые включаются при перебоях электропитания и покрывают аварийные выходы и пути эвакуации.
- **Физическая защита: противопожарная защита.** Применяются и поддерживаются устройства/системы пожаротушения и обнаружения возгораний.
- **Физическая защита: средства контроля температуры и влажности.** Отслеживаются и поддерживаются в допустимых пределах температура и влажность в помещениях, содержащих компоненты ИС.
- **Физическая защита: защита от затопления.** Необходимо защищать ИС от затопления и протечек, возникающих из-за повреждения водопровода или в силу иных причин, обеспечивая доступность и исправность кранов, перекрывающих воду, и информируя соответствующих должностных лиц о расположении этих кранов.
- **Физическая защита: доставка и вывоз.** В учреждении контролируются доставка и вывоз компонентов информационной системы (аппаратное и программное обеспечения) и поддерживается информация о месте нахождения этих компонентов.
- **Планирование бесперебойной работы: политика и процедуры.** Разрабатываются, распространяются, периодически пересматриваются и изменяются:
  - официальная документированная политика планирования бесперебойной работы, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
  - формальные документированные процедуры, способствующие проведению в жизнь политики и ассоциированных регуляторов планирования бесперебойной работы.
- **Планирование бесперебойной работы: план обеспечения бесперебойной работы.** Разрабатывается и реализуется план обеспечения бесперебойной работы информационной системы, в котором описываются роли, обязанности ответственных должностных лиц, указываются их контактные координаты. Кроме того, в плане прописываются действия, выполняемые при восстановлении ИС после повреждений и аварий. Соответствующие должностные лица пересматривают и утверждают этот план и доводят его до сведения сотрудников, ответственных за бесперебойную работу.
- **Планирование бесперебойной работы: изменение плана обеспечения бесперебойной работы.** С заданной частотой, но не реже одного раза в год, в организации пересматривается план обеспечения бесперебойной работы информационной системы, чтобы отразить изменения в структуре ИС или организации и/или устранить проблемы, выявленные при реализации, выполнении и/или тестировании плана.

- **Планирование бесперебойной работы: резервное копирование.** С заданной частотой проводится резервное копирование содержащихся в информационной системе пользовательских и системных данных (включая данные о состоянии ИС), резервные копии хранятся в местах, защищенных должным образом.
- **Планирование бесперебойной работы: восстановление информационной системы.** В учреждении применяются механизмы и поддерживающие процедуры, позволяющие восстановить информационную систему после повреждений или аварий.
- **Управление конфигурацией: политика и процедуры.** Разрабатываются, распространяются, периодически пересматриваются и изменяются:
    - официальная документированная политика управления конфигурацией, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
    - формальные документированные процедуры, способствующие проведению в жизнь политики и ассоциированных регуляторов управления конфигурацией.
- **Управление конфигурацией: базовая конфигурация и опись компонентов информационной системы.** В учреждении разрабатываются, документируются и поддерживаются актуальная базовая конфигурация информационной системы, опись компонентов ИС и соответствующие данные об их владельцах.
- **Управление конфигурацией: настройки.** В учреждении:
    - утверждаются обязательные настройки для продуктов информационных технологий, применяемых в ИС;
    - устанавливаются настройки безопасности продуктов информационных технологий в наиболее ограничительный режим, совместимый с эксплуатационными требованиями;
    - документируются настройки;
    - обеспечиваются должные настройки всех компонентов информационной системы.
    - Сопровождение: политика и процедуры. Разрабатываются, распространяются, периодически пересматриваются и изменяются:
    - официальная документированная политика сопровождения, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
    - формальные документированные процедуры, способствующие проведению в жизнь политики и ассоциированных регуляторов сопровождения.
- **Сопровождение: периодическое сопровождение.** Планирование, осуществление и документирование повседневного, профилактического и регулярного сопровождения компонентов информационной системы в соответствии со спецификациями изготовителя или поставщика и/или организационными требованиями.

- **Сопровождение: удаленное сопровождение.** Учреждение санкционирует, контролирует и отслеживает удаленно осуществляемую деятельность по сопровождению и диагностике.
- **Сопровождение: персонал сопровождения.** Необходимо поддерживать список лиц, авторизованных для осуществления сопровождения информационной системы. Только авторизованный персонал осуществляет сопровождение ИС.
- **Целостность систем и данных: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменение:
    - официальной документированной политики целостности систем и данных, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
    - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов целостности систем и данных.
- **Целостность систем и данных: устранение дефектов.** Идентификация дефектов информационной системы, информирование о них и исправление.
- **Целостность систем и данных: защита от вредоносного программного обеспечения.** В учреждении реализуется в информационной системе защита от вредоносного программного обеспечения, включая возможность автоматических обновлений.
- **Целостность систем и данных: сигналы о нарушениях безопасности и сообщения о новых угрозах.** Необходимо регулярно отслеживать сигналы о нарушениях безопасности и сообщения о новых угрозах для ИС, доводить их до сведения соответствующих должностных лиц и должным образом реагировать на них.
- **Защита носителей: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменение:
    - официальной документированной политики защиты носителей, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
    - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов защиты носителей.
- **Защита носителей: доступ к носителям.** Необходимо обеспечить, чтобы только авторизованные пользователи имели доступ к информации в печатной форме или на цифровых носителях, изъятых из информационной системы.
- **Защита носителей: санация и вывод из эксплуатации.** Учреждение:
    - санирует носители (как бумажные, так и цифровые) перед выводом из эксплуатации или передачей для повторного использования;
    - прослеживает, документирует и верифицирует деятельность по санации носителей;

- периодически тестирует санирующее оборудование и процедуры, чтобы убедиться в корректности их функционирования.

- **Реагирование на нарушения информационной безопасности: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменения:
  - официальной документированной политики реагирования на нарушения информационной безопасности, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
  - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов реагирования на нарушения информационной безопасности.
- **Реагирование на нарушения информационной безопасности: реагирование.** В учреждении формируются структуры для реагирования на нарушения информационной безопасности (группа реагирования), включая подготовку, выявление и анализ, локализацию, ликвидацию воздействия и восстановление после нарушений.
- **Реагирование на нарушения информационной безопасности: доклады о нарушениях.** Необходимо своевременно доводить информацию о нарушениях ИБ до сведения уполномоченных должностных лиц.
- **Реагирование на нарушения информационной безопасности: помощь.** Формирование структуры для выдачи рекомендаций и оказания помощи пользователям ИС при реагировании на нарушения ИБ и докладах о них; эта структура является неотъемлемой составной частью группы реагирования.
- **Информирование и обучение: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменения:
  - официальной документированной политики информирования и обучения сотрудников, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
  - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов информирования и обучения сотрудников.
- **Информирование и обучение: информирование о проблемах ИБ.** Следует обеспечить, чтобы до всех пользователей, включая руководителей, доводилась основная информация по проблематике ИБ, прежде чем этим пользователям будет предоставлен доступ к ИС; подобное информирование должно продолжаться и дальше с заданной частотой, но не реже, чем раз в год.
- **Информирование и обучение: обучение по проблематике ИБ.** Необходимо определить должностных лиц, играющих важную роль и имеющих ответственные обязанности по обеспечению информационной безопасности ИС, документировать эти роли и обязанности и обеспечить соответствующее обучение указанных лиц,

прежде чем предоставить им доступ к ИС. Подобное обучение должно продолжаться и дальше с заданной частотой.

- **Информирование и обучение: документирование обучения по проблематике ИБ.** В учреждении документируется и отслеживается ход обучения каждого сотрудника по проблематике ИБ, включая вводный курс и курсы, специфичные для ИС.
- **Информирование и обучение: контакты с группами и ассоциациями информационной безопасности.** Целесообразно установить и поддерживать контакты с группами, форумами и ассоциациями, специализирующимися в области информационной безопасности, чтобы быть в курсе современного состояния ИБ, передовых рекомендуемых защитных средств, методов и технологий.

На минимальном уровне информационной безопасности рекомендуется применение следующих **программно-технических регуляторов безопасности**.

- **Идентификация и аутентификация: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменения:
  - официальной документированной политики идентификации и аутентификации, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
  - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов идентификации и аутентификации.
- **Идентификация и аутентификация: идентификация и аутентификация пользователей.** Информационная система однозначно идентифицирует и аутентифицирует пользователей (или процессы, действующие от имени пользователей).
- **Идентификация и аутентификация: управление идентификаторами.** Учреждение управляет идентификаторами пользователей посредством:
  - уникальной идентификации каждого пользователя;
  - верификации идентификатора каждого пользователя;
  - получения официальной санкции от уполномоченных должностных лиц на выпуск идентификатора пользователя;
  - обеспечения выпуска идентификатора для нужного пользователя;
  - прекращения действия идентификатора пользователя после заданного периода отсутствия активности;
  - архивирования идентификаторов пользователей.
- **Идентификация и аутентификация: управление аутентификаторами.** Учреждение управляет аутентификаторами в информационной системе (токенами, сертификатами в инфраструктуре открытых ключей, биометрическими данными, паролями, ключевыми картами и т.п.) посредством:
  - определения начального содержимого аутентификаторов;

- регламентацией административных процедур начального распространения аутентификаторов, замещения утерянных, скомпрометированных или поврежденных аутентификаторов, а также отзыва аутентификаторов;
- изменения подразумеваемых аутентификаторов после установки информационной системы.

- **Идентификация и аутентификация: отклик аутентификаторов.** Информационная система скрывает эхо-отображение аутентификационной информации в процессе аутентификации, чтобы защитить эту информацию от возможного использования неавторизованными лицами.
- **Идентификация и аутентификация: аутентификация по отношению к криптографическим модулям.** Для аутентификации по отношению к криптографическим модулям информационная система применяет методы, удовлетворяющие требованиям стандартов на подобные модули.
- **Управление доступом: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменения:
  - официальной документированной политики управления доступом, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
  - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов управления доступом.
- **Управление доступом: управление счетами.** Учреждение управляет счетами в информационной системе, включая их создание, активацию, модификацию, пересмотр (с заданной частотой), отключение и удаление.
- **Управление доступом: проведение в жизнь.** Информационная система проводит в жизнь присвоенные привилегии для управления доступом к системе в соответствии с применимой политикой.
- **Управление доступом: неудачные попытки входа.** Информационная система проводит в жизнь заданное ограничение на число последовательных неудачных попыток доступа со стороны пользователя в течение заданного промежутка времени, автоматически запирая счет или задерживая по заданному алгоритму выдачу приглашения на вход на заданное время при превышении максимально допустимого числа неудачных попыток.
- **Управление доступом: предупреждение об использовании системы.** Информационная система отображает официально одобренное предупреждающее сообщение об использовании системы, прежде чем предоставить доступ к ней, информируя потенциальных пользователей:
  - об организационной принадлежности системы;
  - о возможном мониторинге, протоколировании и аудите использования системы;
  - о запрете и возможном наказании за несанкционированное использование системы;

- о согласии пользователя на мониторинг и протоколирование в случае использования системы; предупреждающее сообщение содержит соответствующие положения политики безопасности и остается на экране, пока пользователь не предпримет явных действий для входа в ИС.

- **Управление доступом: надзор и просмотр.** Учреждение надзирает и проверяет действия пользователей в отношении проведения в жизнь и использования имеющихся в ИС регуляторов доступа.
- **Управление доступом: действия, разрешенные без идентификации и аутентификации**. Определение конкретных действий пользователей, которые могут быть выполнены в информационной системе без идентификации и аутентификации.
- **Управление доступом: удаленный доступ.** Документирование, отслеживание и контроль всех видов удаленного доступа к ИС (например, через модемные входы или через Интернет), включая удаленный доступ для выполнения привилегированных действий; соответствующие должностные лица санкционируют применение каждого вида удаленного доступа и авторизуют для его применения только тех пользователей, которым он необходим.
- **Управление доступом: ограничения на беспроводной доступ.** Учреждение:
  - устанавливает ограничения на использование и руководит реализацией беспроводных технологий;
  - документирует, отслеживает и контролирует беспроводной доступ к ИС; соответствующие должностные лица санкционируют применение беспроводных технологий.
- **Управление доступом: персональные информационные системы.** Ограничение применения персональных информационных систем для производственных нужд, включая обработку, хранение и передачу производственной информации.
- **Протоколирование и аудит: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменения:
  - официальной документированной политики протоколирования и аудита, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
  - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов протоколирования и аудита.
- **Протоколирование и аудит: протоколируемые события.** Информационная система генерирует регистрационные записи для заданных событий.
- **Протоколирование и аудит: содержимое регистрационных записей.** Информационная система сохраняет в регистрационных записях достаточно информации, чтобы установить, какое событие произошло, что послужило источником события, каким оказался исход события.
- **Протоколирование и аудит: ресурсы для хранения регистрационной информации.** Необходимо выделять достаточный объем ресурсов для хранения

регистрационной информации и конфигурировать протоколирование так, чтобы не допустить исчерпания этих ресурсов.

- **Протоколирование и аудит: обработка регистрационной информации.** В случае сбоя протоколирования или исчерпания ресурсов хранения регистрационной информации информационная система предупреждает соответствующих должностных лиц и предпринимает заданные дополнительные действия.
- **Протоколирование и аудит: защита регистрационной информации.** Информационная система защищает регистрационную информацию и средства протоколирования/аудита от несанкционированного доступа, модификации и удаления.
- **Протоколирование и аудит: сохранение регистрационной информации.** Следует сохранять регистрационную информацию в течение заданного времени, чтобы обеспечить поддержку расследований ранее произошедших нарушений информационной безопасности и выполнение требований действующего законодательства и организационных требований сохранения информации.
- **Защита систем и коммуникаций: политика и процедуры.** Разработка, распространение, периодический пересмотр и изменение:
    - официальной документированной политики защиты систем и коммуникаций, в которой представлены цель, охват, роли, обязанности, поддержка руководства, координация среди организационных структур и соответствие действующему законодательству;
    - формальных документированных процедур, способствующих проведению в жизнь политики и ассоциированных регуляторов защиты систем и коммуникаций.
- **Защита систем и коммуникаций: защита от атак на доступность.** Информационная система защищает от атак на доступность заданных видов или ограничивает их воздействие.
- **Защита систем и коммуникаций: защита границ.** Информационная система отслеживает и контролирует коммуникации на своих внешних и ключевых внутренних границах ИС.
- **Защита систем и коммуникаций: применение узаконенной криптографии.** Если в информационной системе применяются криптографические средства, они должны удовлетворять требованиям действующего законодательства, технических регламентов, стандартов, руководящих и нормативных документов, отраслевых и организационных стандартов.
- **Защита систем и коммуникаций: защита общедоступных систем.** Информационная система обеспечивает целостность данных и приложений для общедоступных систем.

Дополнительные и усиленные регуляторы безопасности для умеренного уровня ИБ

Для умеренного уровня информационной безопасности целесообразно применение следующих дополнительных и усиленных (по сравнению с минимальным уровнем) регуляторов безопасности.

- **Оценка рисков: сканирование уязвимостей.** С заданной частотой или после появления сведений о новых критичных для ИС уязвимостях необходимо сканировать уязвимости в информационной системе.
- **Планирование безопасности: планирование деятельности, связанной с безопасностью.** Обеспечение должного планирования и координации деятельности, связанной с безопасностью и затрагивающей информационную систему, с целью минимизации отрицательного воздействия на работу и активы организации (в том числе на ее миссию, функции, имидж и репутацию).
- **Закупка систем и сервисов: документация.** Необходимо включать в общий пакет документов документацию от изготовителя/поставщика (при наличии таковой), описывающую функциональные свойства регуляторов безопасности, задействованных в информационной системе, достаточно детальную для того, чтобы сделать возможным анализ и тестирование регуляторов.
- **Закупка систем и сервисов: принципы проектирования информационной безопасности.** Проектирование и реализация информационной системы проводится с применением принципов проектирования информационной безопасности.
- **Закупка систем и сервисов: тестирование безопасности разработчиком.** Разработчик информационной системы формирует план тестирования и оценки безопасности, реализует его и документирует результаты; последние могут быть использованы для поддержки сертификации по требованиям безопасности и аккредитации поставленной ИС.
- **Сертификация, аккредитация и оценка безопасности: оценка безопасности.** С заданной частотой, но не реже, чем раз в год, целесообразно осуществлять оценку регуляторов безопасности в информационной системе, чтобы определить, насколько они корректно реализованы, функционируют в соответствии со спецификациями и дают ожидаемые результаты с точки зрения выполнения предъявляемых к ИС требований информационной безопасности.
- **Сертификация, аккредитация и оценка безопасности: сертификация по требованиям безопасности.** Оценка регуляторов безопасности в информационной системе для целей сертификации по требованиям безопасности осуществляется независимой сертифицирующей организацией.
- **Физическая защита: контроль доступа к устройствам отображения информации.** Контроль физического доступа к устройствам отображения информации с целью защиты последней от просмотра неавторизованными лицами.
- **Физическая защита: мониторинг физического доступа.** В режиме реального времени отслеживаются поступающие сигналы о вторжениях и данные со следящих устройств.
- **Физическая защита: контроль посетителей.** Обеспечение сопровождения посетителей и, если нужно, мониторинга их активности.

- **Физическая защита: электрическое оборудование и проводка.** Защита электрического оборудования и проводки для информационной системы от повреждений и разрушений.
- **Физическая защита: аварийное отключение.** Для определенных помещений, в которых концентрируются ресурсы информационной системы (центры обработки данных, серверные комнаты, машинные залы для мэйнфреймов и т.п.), следует обеспечить возможность отключения электропитания к любому отказавшему (например, из-за короткого замыкания) или оказавшемуся под угрозой (например, из-за разрыва водопровода) компоненту ИС, не подвергая при этом персонал опасности, сопряженной с доступом к оборудованию.
- **Физическая защита: аварийное электропитание.** Обеспечение краткосрочных источников бесперебойного питания, чтобы дать возможность аккуратно выключить информационную систему в случае нарушения основного электропитания.
- **Физическая защита: противопожарная защита.** Необходимо применять и поддерживать устройства/системы пожаротушения и обнаружения возгораний, автоматически срабатывающие в случае пожара.
- **Физическая защита: запасная производственная площадка**. Сотрудники организации на запасной производственной площадке применяют соответствующие регуляторы безопасности для ИС.
- **Физическая защита: расположение компонентов информационной системы.** Следует располагать компоненты информационной системы на отведенных площадях так, чтобы минимизировать потенциальный ущерб от физических рисков и угроз со стороны окружающей среды, а также возможность несанкционированного доступа.
- **Планирование бесперебойной работы: план обеспечения бесперебойной работы.** Организация координирует разработку плана обеспечения бесперебойной работы со структурами, ответственными за родственные планы (например, планы восстановления после аварий, реагирования на нарушения безопасности и т.п.).
- **Планирование бесперебойной работы: обучение.** В компании организуется обучение сотрудников их ролям и обязанностям по обеспечению бесперебойной работы информационной системы, а также с заданной частотой, но не реже, чем раз в год, проводятся тренировки для поддержания практических навыков.
- **Планирование бесперебойной работы: тестирование плана обеспечения бесперебойной работы.** С заданной частотой, но не реже, чем раз в год, в организации тестируется план обеспечения бесперебойной работы информационной системы. Для этого применяются заданные тесты и тренировочные процедуры, чтобы определить эффективность плана и готовность организации к его выполнению. Соответствующие должностные лица проверяют результаты тестирования плана и инициируют корректирующие действия. Организация координирует тестирование плана обеспечения бесперебойной работы со структурами, ответственными за родственные планы (например, планы восстановления после аварий, реагирования на нарушения безопасности и т.п.).

- **Планирование бесперебойной работы: запасные места хранения.** Необходимо определить запасное место хранения и заключить необходимые соглашения, чтобы сделать возможным хранение там резервных копий данных информационной системы; запасное место хранения территориально должно быть удалено от основного, чтобы не подвергать его тем же опасностям.
- **Планирование бесперебойной работы: запасные места обработки данных.** Определяется запасное место обработки данных, и инициируются необходимые соглашения, чтобы сделать возможным возобновление выполнения информационной системой критически важных производственных функций в течение заданного промежутка времени, если основные средства обработки данных оказываются недоступными. Запасное место обработки данных территориально удалено от основного и, следовательно, не подвержено тем же опасностям. Определяются потенциальные проблемы с доступом к запасному месту обработки данных в случае широкомасштабных аварий или стихийных бедствий, намечаются явные действия по смягчению выявленных проблем. Соглашение о запасном месте обработки данных содержит обязательства приоритетного обслуживания в соответствии с требованиями организации к доступности.
- **Планирование бесперебойной работы: телекоммуникационные услуги.** Определяются основной и запасной источники телекоммуникационных услуг, поддерживающих информационную систему. Инициируются необходимые соглашения, чтобы сделать возможным возобновление выполнения информационной системой критически важных производственных функций в течение заданного промежутка времени, если основной источник телекоммуникационных услуг оказывается недоступным. Соглашения об основном и запасном источниках телекоммуникационных услуг содержат обязательства приоритетного обслуживания в соответствии с требованиями организации к доступности. Запасной источник телекоммуникационных услуг не разделяет единую точку отказа с основным источником.
- **Планирование бесперебойной работы: резервное копирование.** С заданной частотой в организации тестируются резервные копии, чтобы убедиться в надежности носителей и целостности данных.
- **Управление конфигурацией: базовая конфигурация и опись компонентов информационной системы.** При установке новых компонентов изменяются базовая конфигурация информационной системы и опись компонентов ИС.
- **Управление конфигурацией: контроль изменений конфигурации.** Документируются и контролируются изменения в информационной системе; соответствующие должностные лица санкционируют изменения ИС в соответствии с принятыми в организации политикой и процедурами.
- **Управление конфигурацией: мониторинг изменений конфигурации**. Необходимо отслеживать изменения в информационной системе и осуществлять анализ их воздействия на безопасность, чтобы определить эффект изменений.

- **Управление конфигурацией: ограничение доступа для изменений.** Организация проводит в жизнь физические и логические ограничения доступа, связанного с изменениями в информационной системе, и генерирует, сохраняет и пересматривает записи, отражающие все подобные изменения.
- **Управление конфигурацией: минимизация функциональности.** Следует конфигурировать информационную систему так, чтобы обеспечить только необходимые возможности, и явным образом запретить и/или ограничить использование определенных функций, портов, протоколов и/или сервисов.
- **Сопровождение: периодическое сопровождение.** Поддерживается регистрационный журнал сопровождения информационной системы, в котором фиксируются:
    - дата и время обслуживания;
    - фамилия и имя лица, производившего обслуживание;
    - фамилия и имя сопровождающего, если это необходимо;
    - описание произведенных действий по обслуживанию ИС;
    - список удаленного или перемещенного оборудования (с идентификационными номерами).
- **Сопровождение: средства сопровождения.** Организация санкционирует, контролирует и отслеживает применение средств сопровождения информационной системы и постоянно поддерживает эти средства.
- **Сопровождение: своевременное обслуживание.** Организация получает обслуживание и запчасти для заданных ключевых компонентов информационной системы в течение заданного промежутка времени.
- **Целостность систем и данных: защита от вредоносного программного обеспечения.** Централизованное управление механизмами защиты от вредоносного программного обеспечения.
- **Целостность систем и данных: средства и методы мониторинга информационной системы.** Применение средств и методов мониторинга событий в информационной системе, выявление атак и идентификация несанкционированного использования ИС.
- **Целостность систем и данных: защита от спама.** В информационной системе реализуется защита от спама.
- **Целостность систем и данных: ограничения на ввод данных.** Организация предоставляет право на ввод данных в информационную систему только авторизованным лицам.
- **Целостность систем и данных: точность, полнота, достоверность и аутентичность данных**. Информационная система проверяет данные на точность, полноту, достоверность и аутентичность.
- **Целостность систем и данных: обработка ошибок.** Информационная система явным образом выявляет и обрабатывает ошибочные ситуации.
- **Целостность систем и данных: обработка и сохранение выходных данных.** Выходные данные информационной системы обрабатываются и сохраняются в соответствии с принятыми в организации политикой и эксплуатационными требованиями.

- **Защита носителей: метки носителей.** Съемные носители данных и выходные данные ИС снабжаются внешними метками, содержащими ограничения на распространение и обработку этих данных; заданные типы носителей или аппаратных компонентов освобождаются от меток, поскольку остаются в пределах контролируемой зоны.
- **Защита носителей: хранение носителей**. Следует организовать физический контроль и безопасное хранение носителей данных, бумажных и цифровых, основываясь на максимальной категории, присвоенной данным, записанным на носителе.
- **Защита носителей: транспортировка носителей.** Контроль носителей данных, бумажных и цифровых, и ограничение отправки, получения, транспортировки и доставки носителей авторизованным лицам.
- **Реагирование на нарушения информационной безопасности: обучение.** Компания обучает сотрудников их ролям и обязанностям, связанным с реагированием на нарушения информационной безопасности ИС, и с заданной частотой, но не реже, чем раз в год, проводит тренировки для поддержания практических навыков.
- **Реагирование на нарушения информационной безопасности: тестирование.** С заданной частотой, но не реже, чем раз в год, тестируются средства реагирования на нарушения информационной безопасности ИС, при этом используются заданные тесты и тренировочные процедуры, чтобы определить эффективность реагирования. Результаты документируются.
- **Реагирование на нарушения информационной безопасности: реагирование.** Для поддержки процесса реагирования на нарушения информационной безопасности применяются автоматические механизмы.
- **Реагирование на нарушения информационной безопасности: мониторинг.** Необходимо постоянно прослеживать и документировать нарушения информационной безопасности ИС.
- **Реагирование на нарушения информационной безопасности: доклады о нарушениях.** Применение автоматических механизмов для содействия докладам о нарушениях информационной безопасности.
- **Реагирование на нарушения информационной безопасности: помощь.** Применение автоматических механизмов, чтобы повысить доступность информации и поддержки, ассоциированной с реагированием на нарушения информационной безопасности.
- **Идентификация и аутентификация: идентификация и аутентификация устройств.** Информационная система идентифицирует и аутентифицирует определенные устройства, прежде чем установить с ними соединение.
- **Управление доступом: управление счетами.** Применение автоматических механизмов для поддержки управления счетами в информационной системе; информационная система автоматически терминирует временные и аварийные счета по истечении заданного для каждого типа счетов промежутка времени;

информационная система автоматически отключает неактивные счета по истечении заданного промежутка времени.

- **Управление доступом: проведение в жизнь.** Информационная система обеспечивает, чтобы доступ к функциям безопасности (реализованным аппаратно и/или программно) и к защитным данным предоставлялся только авторизованным лицам (например, администраторам безопасности).
- **Управление доступом: проведение в жизнь управления информационными потоками.** Информационная система проводит в жизнь присвоенные привилегии для управления информационными потоками в системе и между взаимосвязанными системами в соответствии с принятой политикой безопасности.
- **Управление доступом: разделение обязанностей.** Информационная система проводит в жизнь разделение обязанностей посредством присвоения привилегий доступа.
- **Управление доступом: минимизация привилегий.** Информационная система проводит в жизнь наиболее ограничительный набор прав/привилегий доступа, необходимых пользователям (или процессам, действующим от имени этих пользователей) для выполнения их задач.
- **Управление доступом: блокирование сеансов.** Информационная система предотвращает дальнейший доступ к ИС посредством блокирования сеанса до тех пор, пока пользователь не восстановит доступ, применяя соответствующие процедуры идентификации и аутентификации.
- **Управление доступом: терминирование сеансов.** Информационная система автоматически терминирует сеанс по истечении заданного периода неактивности.
- **Управление доступом: действия, разрешенные без идентификации и аутентификации.** Организация разрешает выполнение действий без идентификации и аутентификации, только если они необходимы для достижения ключевых целей организации.
- **Управление доступом: удаленный доступ.** Применение автоматических механизмов, чтобы облегчить мониторинг и контроль методов удаленного доступа, шифрование — для защиты конфиденциальности сеансов удаленного доступа. Необходимо контролировать весь удаленный доступ в управляемой точке контроля доступа.
- **Управление доступом: ограничения на беспроводной доступ.** Применение аутентификации и шифрования для защиты беспроводного доступа к информационной системе.
- **Управление доступом: мобильные устройства.** Организация:
    - устанавливает ограничения на применение и разрабатывает руководства по использованию мобильных устройств;
    - документирует, отслеживает и контролирует доступ посредством подобных устройств к ИС; соответствующие должностные лица санкционируют использование мобильных устройств; применяются съемные жесткие диски

или криптография для защиты данных, располагающихся в мобильных устройствах.

- **Протоколирование и аудит: содержимое регистрационных записей.** Информационная система обеспечивает возможность включения в регистрационные записи дополнительной, более детальной информации для протоколируемых событий, идентифицируемых по типу, месту или субъекту.
- **Протоколирование и аудит: мониторинг, анализ и отчет о регистрационной информации.** Необходимо регулярно изучать/анализировать регистрационную информацию с целью выявления ненадлежащей или нетипичной активности, расследовать случаи подозрительной активности или предполагаемых нарушений, докладывать о результатах соответствующим должностным лицам и предпринимать необходимые действия.
- **Протоколирование и аудит: редукция регистрационной информации и генерация отчетов.** Информационная система предоставляет возможности редукции регистрационной информации и генерации отчетов.
- **Протоколирование и аудит: метки времени.** Информационная система предоставляет метки времени для использования при генерации регистрационных записей.
- **Защита систем и коммуникаций: разделение приложений.** Информационная система разделяет пользовательскую функциональность (включая сервисы пользовательского интерфейса) от функциональности управления ИС.
- **Защита систем и коммуникаций: остаточная информация.** Информационная система предотвращает несанкционированную и ненамеренную передачу информации через разделяемые системные ресурсы.
- **Защита систем и коммуникаций: защита границ.** Целесообразно физически размещать общедоступные компоненты информационной системы (например, общедоступные web-серверы) в отдельных подсетях с отдельными физическими сетевыми интерфейсами, предотвратить публичный доступ во внутреннюю сеть, за исключением должным образом контролируемого доступа.
- **Защита систем и коммуникаций: целостность передаваемых данных.** Информационная система защищает целостность передаваемых данных.
- **Защита систем и коммуникаций: конфиденциальность передаваемых данных.** Информационная система защищает конфиденциальность передаваемых данных.
- **Защита систем и коммуникаций: разрыв сетевых соединений.** Информационная система терминирует сетевое соединение в конце сеанса или по истечении заданного периода неактивности.
- **Защита систем и коммуникаций: выработка криптографических ключей и управление ими.** Информационная система применяет автоматические механизмы и вспомогательные процедуры или ручные процедуры для выработки криптографических ключей и управления ключами.
- **Защита систем и коммуникаций: коллективные приложения.** Информационная система запрещает удаленную активацию механизмов коллективных приложений

(например, видео- или аудиоконференций) и предоставляет явные свидетельства их использования локальным пользователям (например, индикацию использования видеокамер или микрофонов).

- **Защита систем и коммуникаций: сертификаты инфраструктуры открытых ключей.** Организация разрабатывает и реализует политику для сертификатов и спецификацию сертификационной практики для выпуска сертификатов открытых ключей, используемых в информационной системе.
- **Защита систем и коммуникаций: мобильный код.** Организация:
  - устанавливает ограничения на применение и разрабатывает руководства по использованию технологий мобильного кода, исходя из возможности нанесения ущерба информационной системе при злоумышленном применении этих технологий;
  - документирует, отслеживает и контролирует использование мобильного кода в информационной системе; соответствующие должностные лица санкционируют использование мобильного кода.
- **Защита систем и коммуникаций: протокол VoIP.** Организация:
  - устанавливает ограничения на применение и разрабатывает руководства по использованию технологий VoIP, исходя из возможности нанесения ущерба информационной системе при злоумышленном применении этих технологий;
  - документирует, отслеживает и контролирует использование VoIP в информационной системе; соответствующие должностные лица санкционируют использование VoIP.
- **Защита систем и коммуникаций: сервис безопасного поиска имен (уполномоченные источники).** Информационные системы (уполномоченные серверы доменных имен), предоставляющие внешним пользователям сервис поиска имен для доступа к информационным ресурсам организации через Интернет, обеспечивают атрибуты для аутентификации источника данных и контроля целостности данных, чтобы дать пользователям возможность получить гарантии аутентичности и целостности сообщений при получении данных в рамках сетевых транзакций.

Дополнительные и усиленные регуляторы безопасности для высокого уровня ИБ

Для высокого уровня информационной безопасности рекомендуется применение следующих дополнительных и усиленных (по сравнению с умеренным уровнем) регуляторов безопасности.

- **Оценка рисков: сканирование уязвимостей.** Средства сканирования уязвимостей включают возможность оперативного изменения списка сканируемых уязвимостей информационной системы.

  С заданной частотой или после появления сведений о новых критичных для ИС уязвимостях организация изменяет список сканируемых уязвимостей информационной системы.

- **Закупка систем и сервисов: документация.** Следует включить в общий пакет документов документацию от изготовителя/поставщика (при наличии таковой), описывающую детали проектирования и реализации регуляторов безопасности, задействованных в информационной системе, со степенью подробности, достаточной для того, чтобы сделать возможным анализ и тестирование регуляторов (включая функциональные интерфейсы между компонентами регуляторов).
- **Закупка систем и сервисов: управление конфигурацией разработчиком.** Разработчик информационной системы создает и реализует план управления конфигурацией, контролирующий изменения системы в процессе разработки, прослеживающий дефекты безопасности, требующий авторизации изменений, и предоставляет документацию плана и его реализации.
- **Физическая защита: контроль доступа к каналам передачи данных.** Контролируется физический доступ к линиям распространения и передачи данных, принадлежащим ИС и расположенным в пределах охраняемых границ, чтобы предотвратить неумышленное повреждение, прослушивание, модификацию в процессе передачи, разрыв или физическое искажение линий.
- **Физическая защита: мониторинг физического доступа.** Применяются автоматические механизмы, чтобы обеспечить выявление потенциальных вторжений и инициирование реакции на них.
- **Физическая защита: протоколирование доступа.** Применяются автоматические механизмы, чтобы облегчить поддержку и просмотр регистрационных журналов.
- **Физическая защита: аварийное электропитание.** Необходимо обеспечить долгосрочные альтернативные источники электропитания для информационной системы, способные поддерживать минимальные требуемые эксплуатационные возможности в случае долговременного выхода из строя первичного источника электропитания.
- **Физическая защита: противопожарная защита.** Применяются и поддерживаются устройства/системы пожаротушения и обнаружения возгораний, автоматически извещающие о своей активации организацию и аварийные службы.
- **Физическая защита: защита от затопления.** Автоматические механизмы применяются, чтобы автоматически перекрыть воду в случае ее интенсивной утечки.
- **Планирование бесперебойной работы: обучение.** Моделирование событий включается в учебные курсы, чтобы способствовать эффективному реагированию сотрудников на возможные кризисные ситуации.

- **Планирование бесперебойной работы: тестирование плана обеспечения бесперебойной работы.** План обеспечения бесперебойной работы тестируется на запасной производственной площадке, чтобы ознакомить сотрудников с имеющимися возможностями и ресурсами и оценить способность площадки поддерживать непрерывность функционирования.
- **Планирование бесперебойной работы: запасные места хранения.** Запасное место хранения конфигурируется так, чтобы облегчить своевременные и эффективные восстановительные действия; определяются потенциальные проблемы с доступом к запасному месту хранения в случае широкомасштабных аварий или стихийных бедствий и намечаются явные действия по смягчению выявленных проблем.
- **Планирование бесперебойной работы: запасные места обработки данных.** Запасное место обработки данных полностью конфигурируется для поддержания минимальных требуемых эксплуатационных возможностей и готовности к использованию в качестве производственной площадки.
- **Планирование бесперебойной работы: телекоммуникационные услуги.** Запасной источник телекоммуникационных услуг должен быть в достаточной степени удален территориально от основного, чтобы не подвергаться тем же опасностям; основной и запасной источники телекоммуникационных услуг имеют адекватные планы обеспечения бесперебойной работы.
- **Планирование бесперебойной работы: резервное копирование.** Для восстановления функций информационной системы выборочно используются резервные копии как часть тестирования плана обеспечения бесперебойной работы. Резервные копии операционной системы и другого критичного для ИС программного обеспечения хранятся в отдельном месте или в огнеупорном контейнере, расположенном отдельно от эксплуатационного ПО.

Планирование бесперебойной работы: восстановление информационной системы. Организация включает полное восстановление информационной

- **Планирование бесперебойной работы: телекоммуникационные услуги.** Определяются основной и запасной источники телекоммуникационных услуг, поддерживающих информационную систему. Инициируются необходимые соглашения, чтобы сделать возможным возобновление выполнения информационной системой критически важных производственных функций в течение заданного промежутка времени, если основной источник телекоммуникационных услуг оказывается недоступным. Соглашения об основном и запасном источниках телекоммуникационных услуг содержат обязательства приоритетного обслуживания в соответствии с требованиями организации к доступности. Запасной источник телекоммуникационных услуг не разделяет единую точку отказа с основным источником.
- **Планирование бесперебойной работы: резервное копирование.** С заданной частотой в организации тестируются резервные копии, чтобы убедиться в надежности носителей и целостности данных.

- **Управление конфигурацией: базовая конфигурация и опись компонентов информационной системы.** При установке новых компонентов изменяются базовая конфигурация информационной системы и опись компонентов ИС.
- **Управление конфигурацией: контроль изменений конфигурации.** Документируются и контролируются изменения в информационной системе; соответствующие должностные лица санкционируют изменения ИС в соответствии с принятыми в организации политикой и процедурами.
- **Управление конфигурацией: мониторинг изменений конфигурации**. Необходимо отслеживать изменения в информационной системе и осуществлять анализ их воздействия на безопасность, чтобы определить эффект изменений.
- **Управление конфигурацией: ограничение доступа для изменений.** Организация проводит в жизнь физические и логические ограничения доступа, связанного с изменениями в информационной системе, и генерирует, сохраняет и пересматривает записи, отражающие все подобные изменения.
- **Управление конфигурацией: минимизация функциональности.** Следует конфигурировать информационную систему так, чтобы обеспечить только необходимые возможности, и явным образом запретить и/или ограничить использование определенных функций, портов, протоколов и/или сервисов.
- **Сопровождение: периодическое сопровождение.** Поддерживается регистрационный журнал сопровождения информационной системы, в котором фиксируются:
    - дата и время обслуживания;
    - фамилия и имя лица, производившего обслуживание;
    - фамилия и имя сопровождающего, если это необходимо;
    - описание произведенных действий по обслуживанию ИС;
    - список удаленного или перемещенного оборудования (с идентификационными номерами).
- **Сопровождение: средства сопровождения.** Организация санкционирует, контролирует и отслеживает применение средств сопровождения информационной системы и постоянно поддерживает эти средства.
- **Сопровождение: своевременное обслуживание.** Организация получает обслуживание и запчасти для заданных ключевых компонентов информационной системы в течение заданного промежутка времени.
- **Целостность систем и данных: защита от вредоносного программного обеспечения.** Централизованное управление механизмами защиты от вредоносного программного обеспечения.
- **Целостность систем и данных: средства и методы мониторинга информационной системы.** Применение средств и методов мониторинга событий в информационной системе, выявление атак и идентификация несанкционированного использования ИС.
- **Целостность систем и данных: защита от спама.** В информационной системе реализуется защита от спама.

- **Целостность систем и данных: ограничения на ввод данных.** Организация предоставляет право на ввод данных в информационную систему только авторизованным лицам.
- **Целостность систем и данных: точность, полнота, достоверность и аутентичность данных**. Информационная система проверяет данные на точность, полноту, достоверность и аутентичность.
- **Целостность систем и данных: обработка ошибок.** Информационная система явным образом выявляет и обрабатывает ошибочные ситуации.
- **Целостность систем и данных: обработка и сохранение выходных данных.** Выходные данные информационной системы обрабатываются и сохраняются в соответствии с принятыми в организации политикой и эксплуатационными требованиями.
- **Защита носителей: метки носителей.** Съемные носители данных и выходные данные ИС снабжаются внешними метками, содержащими ограничения на распространение и обработку этих данных; заданные типы носителей или аппаратных компонентов освобождаются от меток, поскольку остаются в пределах контролируемой зоны.
- **Защита носителей: хранение носителей**. Следует организовать физический контроль и безопасное хранение носителей данных, бумажных и цифровых, основываясь на максимальной категории, присвоенной данным, записанным на носителе.
- **Защита носителей: транспортировка носителей.** Контроль носителей данных, бумажных и цифровых, и ограничение отправки, получения, транспортировки и доставки носителей авторизованным лицам.
- **Реагирование на нарушения информационной безопасности: обучение.** Компания обучает сотрудников их ролям и обязанностям, связанным с реагированием на нарушения информационной безопасности ИС, и с заданной частотой, но не реже, чем раз в год, проводит тренировки для поддержания практических навыков.
- **Реагирование на нарушения информационной безопасности: тестирование.** С заданной частотой, но не реже, чем раз в год, тестируются средства реагирования на нарушения информационной безопасности ИС, при этом используются заданные тесты и тренировочные процедуры, чтобы определить эффективность реагирования. Результаты документируются.
- **Реагирование на нарушения информационной безопасности: реагирование.** Для поддержки процесса реагирования на нарушения информационной безопасности применяются автоматические механизмы.
- **Реагирование на нарушения информационной безопасности: мониторинг.** Необходимо постоянно прослеживать и документировать нарушения информационной безопасности ИС.
- **Реагирование на нарушения информационной безопасности: доклады о нарушениях.** Применение автоматических механизмов для содействия докладам о нарушениях информационной безопасности.

- **Реагирование на нарушения информационной безопасности: помощь.** Применение автоматических механизмов, чтобы повысить доступность информации и поддержки, ассоциированной с реагированием на нарушения информационной безопасности.
- **Идентификация и аутентификация: идентификация и аутентификация устройств.** Информационная система идентифицирует и аутентифицирует определенные устройства, прежде чем установить с ними соединение.
- **Управление доступом: управление счетами.** Применение автоматических механизмов для поддержки управления счетами в информационной системе; информационная система автоматически терминирует временные и аварийные счета по истечении заданного для каждого типа счетов промежутка времени; информационная система автоматически отключает неактивные счета по истечении заданного промежутка времени.
- **Управление доступом: проведение в жизнь.** Информационная система обеспечивает, чтобы доступ к функциям безопасности (реализованным аппаратно и/или программно) и к защитным данным предоставлялся только авторизованным лицам (например, администраторам безопасности).
- **Управление доступом: проведение в жизнь управления информационными потоками.** Информационная система проводит в жизнь присвоенные привилегии для управления информационными потоками в системе и между взаимосвязанными системами в соответствии с принятой политикой безопасности.
- **Управление доступом: разделение обязанностей.** Информационная система проводит в жизнь разделение обязанностей посредством присвоения привилегий доступа.
- **Управление доступом: минимизация привилегий.** Информационная система проводит в жизнь наиболее ограничительный набор прав/привилегий доступа, необходимых пользователям (или процессам, действующим от имени этих пользователей) для выполнения их задач.
- **Управление доступом: блокирование сеансов.** Информационная система предотвращает дальнейший доступ к ИС посредством блокирования сеанса до тех пор, пока пользователь не восстановит доступ, применяя соответствующие процедуры идентификации и аутентификации.
- **Управление доступом: терминирование сеансов.** Информационная система автоматически терминирует сеанс по истечении заданного периода неактивности.
- **Управление доступом: действия, разрешенные без идентификации и аутентификации.** Организация разрешает выполнение действий без идентификации и аутентификации, только если они необходимы для достижения ключевых целей организации.
- **Управление доступом: удаленный доступ.** Применение автоматических механизмов, чтобы облегчить мониторинг и контроль методов удаленного доступа, шифрование — для защиты конфиденциальности сеансов удаленного доступа.

Необходимо контролировать весь удаленный доступ в управляемой точке контроля доступа.

- **Управление доступом: ограничения на беспроводной доступ.** Применение аутентификации и шифрования для защиты беспроводного доступа к информационной системе.
- **Управление доступом: мобильные устройства.** Организация:
  - устанавливает ограничения на применение и разрабатывает руководства по использованию мобильных устройств;
  - документирует, отслеживает и контролирует доступ посредством подобных устройств к ИС; соответствующие должностные лица санкционируют использование мобильных устройств; применяются съемные жесткие диски или криптография для защиты данных, располагающихся в мобильных устройствах.
- **Протоколирование и аудит: содержимое регистрационных записей.** Информационная система обеспечивает возможность включения в регистрационные записи дополнительной, более детальной информации для протоколируемых событий, идентифицируемых по типу, месту или субъекту.
- **Протоколирование и аудит: мониторинг, анализ и отчет о регистрационной информации.** Необходимо регулярно изучать/анализировать регистрационную информацию с целью выявления ненадлежащей или нетипичной активности, расследовать случаи подозрительной активности или предполагаемых нарушений, докладывать о результатах соответствующим должностным лицам и предпринимать необходимые действия.
- **Протоколирование и аудит: редукция регистрационной информации и генерация отчетов.** Информационная система предоставляет возможности редукции регистрационной информации и генерации отчетов.
- **Протоколирование и аудит: метки времени.** Информационная система предоставляет метки времени для использования при генерации регистрационных записей.
- **Защита систем и коммуникаций: разделение приложений.** Информационная система разделяет пользовательскую функциональность (включая сервисы пользовательского интерфейса) от функциональности управления ИС.
- **Защита систем и коммуникаций: остаточная информация.** Информационная система предотвращает несанкционированную и ненамеренную передачу информации через разделяемые системные ресурсы.
- **Защита систем и коммуникаций: защита границ.** Целесообразно физически размещать общедоступные компоненты информационной системы (например, общедоступные web-серверы) в отдельных подсетях с отдельными физическими сетевыми интерфейсами, предотвратить публичный доступ во внутреннюю сеть, за исключением должным образом контролируемого доступа.
- **Защита систем и коммуникаций: целостность передаваемых данных.** Информационная система защищает целостность передаваемых данных.

- **Защита систем и коммуникаций: конфиденциальность передаваемых данных.** Информационная система защищает конфиденциальность передаваемых данных.
- **Защита систем и коммуникаций: разрыв сетевых соединений.** Информационная система терминирует сетевое соединение в конце сеанса или по истечении заданного периода неактивности.
- **Защита систем и коммуникаций: выработка криптографических ключей и управление ими.** Информационная система применяет автоматические механизмы и вспомогательные процедуры или ручные процедуры для выработки криптографических ключей и управления ключами.
- **Защита систем и коммуникаций: коллективные приложения.** Информационная система запрещает удаленную активацию механизмов коллективных приложений (например, видео- или аудиоконференций) и предоставляет явные свидетельства их использования локальным пользователям (например, индикацию использования видеокамер или микрофонов).
- **Защита систем и коммуникаций: сертификаты инфраструктуры открытых ключей.** Организация разрабатывает и реализует политику для сертификатов и спецификацию сертификационной практики для выпуска сертификатов открытых ключей, используемых в информационной системе.
- **Защита систем и коммуникаций: мобильный код.** Организация:
  - устанавливает ограничения на применение и разрабатывает руководства по использованию технологий мобильного кода, исходя из возможности нанесения ущерба информационной системе при злоумышленном применении этих технологий;
  - документирует, отслеживает и контролирует использование мобильного кода в информационной системе; соответствующие должностные лица санкционируют использование мобильного кода.
- **Защита систем и коммуникаций: протокол VoIP.** Организация:
  - устанавливает ограничения на применение и разрабатывает руководства по использованию технологий VoIP, исходя из возможности нанесения ущерба информационной системе при злоумышленном применении этих технологий;
  - документирует, отслеживает и контролирует использование VoIP в информационной системе; соответствующие должностные лица санкционируют использование VoIP.
- **Защита систем и коммуникаций: сервис безопасного поиска имен (уполномоченные источники).** Информационные системы (уполномоченные серверы доменных имен), предоставляющие внешним пользователям сервис поиска имен для доступа к информационным ресурсам организации через Интернет, обеспечивают атрибуты для аутентификации источника данных и контроля целостности данных, чтобы дать пользователям возможность получить гарантии аутентичности и целостности сообщений при получении данных в рамках сетевых транзакций.

Дополнительные и усиленные регуляторы безопасности для высокого уровня ИБ

Для высокого уровня информационной безопасности рекомендуется применение следующих дополнительных и усиленных (по сравнению с умеренным уровнем) регуляторов безопасности.

- **Оценка рисков: сканирование уязвимостей.** Средства сканирования уязвимостей включают возможность оперативного изменения списка сканируемых уязвимостей информационной системы.

  С заданной частотой или после появления сведений о новых критичных для ИС уязвимостях организация изменяет список сканируемых уязвимостей информационной системы.

- **Закупка систем и сервисов: документация.** Следует включить в общий пакет документов документацию от изготовителя/поставщика (при наличии таковой), описывающую детали проектирования и реализации регуляторов безопасности, задействованных в информационной системе, со степенью подробности, достаточной для того, чтобы сделать возможным анализ и тестирование регуляторов (включая функциональные интерфейсы между компонентами регуляторов).
- **Закупка систем и сервисов: управление конфигурацией разработчиком.** Разработчик информационной системы создает и реализует план управления конфигурацией, контролирующий изменения системы в процессе разработки, прослеживающий дефекты безопасности, требующий авторизации изменений, и предоставляет документацию плана и его реализации.
- **Физическая защита: контроль доступа к каналам передачи данных.** Контролируется физический доступ к линиям распространения и передачи данных, принадлежащим ИС и расположенным в пределах охраняемых границ, чтобы предотвратить неумышленное повреждение, прослушивание, модификацию в процессе передачи, разрыв или физическое искажение линий.
- **Физическая защита: мониторинг физического доступа.** Применяются автоматические механизмы, чтобы обеспечить выявление потенциальных вторжений и инициирование реакции на них.
- **Физическая защита: протоколирование доступа.** Применяются автоматические механизмы, чтобы облегчить поддержку и просмотр регистрационных журналов.
- **Физическая защита: аварийное электропитание.** Необходимо обеспечить долгосрочные альтернативные источники электропитания для информационной системы, способные поддерживать минимальные требуемые эксплуатационные возможности в случае долговременного выхода из строя первичного источника электропитания.

- **Физическая защита: противопожарная защита.** Применяются и поддерживаются устройства/системы пожаротушения и обнаружения возгораний, автоматически извещающие о своей активации организацию и аварийные службы.
- **Физическая защита: защита от затопления.** Автоматические механизмы применяются, чтобы автоматически перекрыть воду в случае ее интенсивной утечки.
- **Планирование бесперебойной работы: обучение.** Моделирование событий включается в учебные курсы, чтобы способствовать эффективному реагированию сотрудников на возможные кризисные ситуации.
- **Планирование бесперебойной работы: тестирование плана обеспечения бесперебойной работы.** План обеспечения бесперебойной работы тестируется на запасной производственной площадке, чтобы ознакомить сотрудников с имеющимися возможностями и ресурсами и оценить способность площадки поддерживать непрерывность функционирования.
- **Планирование бесперебойной работы: запасные места хранения.** Запасное место хранения конфигурируется так, чтобы облегчить своевременные и эффективные восстановительные действия; определяются потенциальные проблемы с доступом к запасному месту хранения в случае широкомасштабных аварий или стихийных бедствий и намечаются явные действия по смягчению выявленных проблем.
- **Планирование бесперебойной работы: запасные места обработки данных.** Запасное место обработки данных полностью конфигурируется для поддержания минимальных требуемых эксплуатационных возможностей и готовности к использованию в качестве производственной площадки.
- **Планирование бесперебойной работы: телекоммуникационные услуги.** Запасной источник телекоммуникационных услуг должен быть в достаточной степени удален территориально от основного, чтобы не подвергаться тем же опасностям; основной и запасной источники телекоммуникационных услуг имеют адекватные планы обеспечения бесперебойной работы.
- **Планирование бесперебойной работы: резервное копирование.** Для восстановления функций информационной системы выборочно используются резервные копии как часть тестирования плана обеспечения бесперебойной работы. Резервные копии операционной системы и другого критичного для ИС программного обеспечения хранятся в отдельном месте или в огнеупорном контейнере, расположенном отдельно от эксплуатационного ПО.
- **Планирование бесперебойной работы: восстановление информационной системы.** Организация включает полное восстановление информационной системы как часть тестирования плана обеспечения бесперебойной работы.
- **Управление конфигурацией: базовая конфигурация и опись компонентов информационной системы.** Применяются автоматические механизмы, чтобы поддерживать актуальную, полную, точную и легко доступную базовую конфигурацию информационной системы и опись компонентов ИС.
- **Управление конфигурацией: контроль изменений конфигурации.** Автоматические механизмы применяются, чтобы:

- документировать предлагаемые изменения информационной системы;
- извещать соответствующих должностных лиц;
- привлекать внимание к не полученным своевременно утверждающим визам;
- откладывать изменения до получения необходимых утверждающих виз;
- документировать произведенные изменения информационной системы.

- **Управление конфигурацией: ограничение доступа для изменений.** Чтобы проводить в жизнь ограничения доступа и поддерживать протоколирование ограничивающих действий, применяются автоматические механизмы.
- **Управление конфигурацией: настройки.** Автоматические механизмы применяются для централизованного управления, применения и верифицирования настроек.
- **Управление конфигурацией: минимизация функциональности.** С заданной частотой пересматривается информационная система, чтобы идентифицировать и ликвидировать функции, порты, протоколы и иные сервисы, не являющиеся необходимыми.
- **Сопровождение: периодическое сопровождение.** Применяются автоматические механизмы, чтобы обеспечить планирование и проведение периодического сопровождения в соответствии с установленными требованиями, а также актуальность, точность, полноту и доступность регистрационных записей о необходимых и произведенных действиях по сопровождению.
- **Сопровождение: средства сопровождения.** Необходимо досматривать все средства сопровождения (например, диагностическое и тестовое оборудования), вносимые на территорию организации обслуживающим персоналом, на предмет видимых ненадлежащих модификаций. Следует проверять все носители, содержащие диагностические тестовые программы (например, программное обеспечение, используемое для сопровождения и диагностики систем), на предмет наличия вредоносного ПО, прежде чем носители будут применены в информационной системе. Проверке подвергается все оборудование, применяемое в целях сопровождения и способное сохранять информацию, чтобы удостовериться, что в оборудовании не записана принадлежащая организации информация или что оно должным образом санировано перед повторным использованием. Если оборудование не может быть санировано, оно остается на территории организации или уничтожается, за исключением случаев, явно санкционированных соответствующими должностными лицами.
- **Сопровождение: удаленное сопровождение.** Протоколируются все сеансы удаленного сопровождения, а соответствующие должностные лица просматривают регистрационный журнал удаленных сеансов. Установка и использование каналов удаленной диагностики отражаются в плане безопасности информационной системы. Сервисы удаленной диагностики или сопровождения допустимы только в том случае, если обслуживающая организация поддерживает в своей ИС по крайней мере тот же уровень безопасности, что и обслуживаемая.

- **Целостность систем и данных: защита от вредоносного программного обеспечения.** Информационная система автоматически изменяет механизмы защиты от вредоносного программного обеспечения.
- **Целостность систем и данных: верификация функциональности безопасности.** Информационная система в рамках технических возможностей, при старте или перезапуске системы, по команде уполномоченного пользователя и/или периодически с заданной частотой верифицирует корректность работы функций безопасности и извещает системного администратора и/или выключает или перезапускает систему в случае выявления каких-либо аномалий.
- **Целостность систем и данных: целостность программного обеспечения и данных.** Информационная система выявляет и защищает от несанкционированного изменения программного обеспечения и данных.
- **Целостность систем и данных: защита от спама.** Организация централизованно управляет механизмами защиты от спама.
- **Защита носителей: доступ к носителям.** Применяются либо посты охраны, либо автоматические механизмы для управления доступом к местам хранения носителей, обеспечения защиты от несанкционированного доступа, а также регистрации попыток доступа и доступа предоставленного.
- **Реагирование на нарушения информационной безопасности: обучение.** В учебные курсы включается моделирование событий, чтобы способствовать эффективному реагированию сотрудников на возможные кризисные ситуации.
- **Реагирование на нарушения информационной безопасности: тестирование.** Для более тщательного и эффективного тестирования возможностей реагирования применяются автоматические механизмы.
- **Реагирование на нарушения информационной безопасности: мониторинг.** Автоматические механизмы применяются, чтобы способствовать прослеживанию нарушений безопасности, а также сбору и анализу информации о нарушениях.
- **Идентификация и аутентификация: идентификация и аутентификация пользователей.** Информационная система применяет многофакторную аутентификацию.
- **Управление доступом: управление счетами.** Применяются автоматические механизмы, чтобы обеспечить протоколирование и, при необходимости, уведомление соответствующих лиц о создании, модификации, отключении и терминировании счетов.
- **Управление доступом: управление параллельными сеансами.** Информационная система ограничивает число параллельных сеансов для одного пользователя.
- **Управление доступом: надзор и просмотр**. Автоматические механизмы применяются, чтобы облегчить просмотр пользовательской активности.
- **Управление доступом: автоматическая маркировка.** Информационная система маркирует выходные данные, используя стандартные соглашения об именовании, чтобы идентифицировать все специальные инструкции по распространению, обработке и распределению данных.

- **Протоколирование и аудит: содержимое регистрационных записей.** Информационная система обеспечивает возможность централизованного управления содержимым регистрационных записей, генерируемых отдельными компонентами ИС.
- **Протоколирование и аудит: обработка регистрационной информации.** Информационная система обеспечивает выдачу предупреждающего сообщения, когда доля занятого пространства, отведенного для хранения регистрационной информации, достигает заданного значения.
- **Протоколирование и аудит: мониторинг, анализ и отчет о регистрационной информации.** Применение автоматических механизмов, чтобы интегрировать мониторинг, анализ и отчет о регистрационной информации в общий процесс выявления и реагирования на подозрительную активность.
- **Протоколирование и аудит: редукция регистрационной информации и генерация отчетов.** Информационная система предоставляет возможность автоматической обработки регистрационной информации о требующих внимания событиях, основываясь на заданных критериях выбора.
- **Защита систем и коммуникаций: изоляция функций безопасности.** Информационная система изолирует функции безопасности от прочих функций.
- **Защита систем и коммуникаций: целостность передаваемых данных.** Применение криптографических механизмов для обеспечения распознавания изменений в данных в процессе передачи, если данные не защищены альтернативными физическими мерами (например, защитной системой распределения).
- **Защита систем и коммуникаций: конфиденциальность передаваемых данных.** Применение криптографических механизмов для предотвращения несанкционированного раскрытия информации в процессе передачи, если она не защищена альтернативными физическими мерами (например, защитной системой распределения).
- **Защита систем и коммуникаций: сервис безопасного поиска имен (разрешение имен).** Информационные системы (уполномоченные серверы доменных имен), предоставляющие внутренним пользователям сервис поиска имен для доступа к информационным ресурсам, обеспечивают механизмы для аутентификации источника данных и контроля целостности данных, а также осуществляют эти действия по запросу клиентских систем.

Минимальные требования доверия для регуляторов безопасности

Минимальные требования доверия для регуляторов безопасности предъявляются к определенным процессам и действиям. Специалисты, разрабатывающие и реализующие регуляторы, определяют и применяют (выполняют) эти процессы и действия для повышения степени уверенности в том, что регуляторы реализованы корректно, функционируют в соответствии со спецификациями и дают ожидаемые результаты с точки зрения выполнения предъявляемых к ИС требований информационной безопасности.

На минимальном уровне информационной безопасности необходимо, чтобы регуляторы безопасности были задействованы и удовлетворяли явно заданным в их определении функциональным требованиям.

На умеренном уровне информационной безопасности дополнительно должны выполняться следующие условия. Специалисты, разрабатывающие (реализующие) регуляторы, предоставляют описание их функциональных свойств, достаточно детальное, чтобы было возможно выполнять анализ и тестирование регуляторов. Как неотъемлемая составная часть регуляторов разработчиками документируются и предоставляются распределение обязанностей и конкретные действия, благодаря которым после завершения разработки (реализации) регуляторы должны удовлетворять предъявляемым к ним функциональным требованиям. Технология, по которой разрабатываются регуляторы, должна поддерживать высокую степень уверенности в их полноте, непротиворечивости и корректности.

Рисунок 6. Обеспечение информационной безопасности. Процессный подход.

На высоком уровне информационной безопасности, кроме всего вышеуказанного, необходимо предоставить описание проекта и реализации регуляторов, включая функциональные интерфейсы между их компонентами. От разработчиков требуются свидетельства того, что после завершения разработки (реализации) выполнение предъявляемых к регуляторам требований будет непрерывным и непротиворечивым в масштабах всей информационной системы, и будет поддерживаться возможность повышения эффективности регуляторов.

Заключение

Обеспечение информационной безопасности — сложный, многоаспектный процесс, требующий принятия множества решений, анализа множества факторов и требований, порой противоречивых. Наличие категорий и минимальных требований безопасности, а также предопределенного каталога регуляторов безопасности, способно служить базой для системного подхода к обеспечению ИБ, подхода, требующего разумных трудовых и материальных затрат и способного дать практически приемлемые результаты для большинства организаций.