Приложение 1
к приказу МКОУ «СОШ №14»
от 19.05.2017 года № 90

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МКОУ «СОШ №14»

а. Эдельбай 2017 г.

СОДЕРЖАНИЕ

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

АИС	Автоматизированная информационная система
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	База данных
ВТСС	Вспомогательные технические средства и системы
ВЧВС	Виртуальная частная вычислительная сеть
ЕСКД	Единая система конструкторской документации
ЕСПД	Единая система программной документации
ЕСТД	Единая система технологической документации
ЗИ	Защита информации
ЗП	Защищаемое помещение
ИБ	Информационная безопасность
ИТКС	Информационно-телекоммуникационная система
КЗ	Контролируемая зона
КСЗИ	Комплексная система защиты информации
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОБИ (ОИБ)	Обеспечение безопасности информации
ОТСС	Основные технические средства и системы
ПО	Программное обеспечение
ПС	Программные средства
РД	Руководящий документ
СЗИ НСД	Система защиты информации от НСД
СКЗИ	Средство криптографической защиты информации
СПД	Система передачи данных
СПО	Специальное программное обеспечение
СТК	Система телекоммуникаций;
СУБД	Система управления базами данных
ТП	Технический проект
ТТ	Технические требования
УЦ	Удостоверяющий центр
ФСБ России	Федеральная служба безопасности России
ФСТЭК России	Федеральная служба по техническому и экспертному контролю России
ЭЦП	Электронная цифровая подпись

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АУТЕНТИФИКАЦИЯ – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

АДМИНИСТРАТОР ЗАЩИТЫ - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ -состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

ВСПОМОГАТЕЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях

ДОСТУП К ИНФОРМАЦИИ - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

ЗАЩИТА ИНФОРМАЦИИ (ЗИ) - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА – деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

ЗАЩИЩАЕМЫЕ ПОМЕЩЕНИЯ – помещения, специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

ЗАЩИЩЕННОЕ СРЕДСТВО ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (ЗАЩИЩЕННАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА) – средство вычислительной техники (автоматизированная система), в которой реализован комплекс средств защиты.

ИНФОРМАЦИОННЫЕ РЕСУРСЫ – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах**)**

ИДЕНТИФИКАЦИЯ – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИДЕНТИФИКАТОР ДОСТУПА – уникальный признак субъекта или объекта доступа.

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ – совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

КОНТРОЛИРУЕМАЯ ЗОНА - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств.

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

НАРУШИТЕЛЬ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА – субъект доступа, осуществляющий несанкционированный доступ к информации.

ОБЪЕКТ ДОСТУПА – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ – содержание и порядок действий по обеспечению защиты информации

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации

ПАРОЛЬ – идентификатор субъекта доступа, который является его (субъекта) секретом.

СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА – совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах

САНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ – доступ к информации, не нарушающий правила разграничения доступа.

СЕРТИФИКАТ ЗАЩИТЫ – документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

СРЕДСТВО ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА – программное, техническое или программно-техническое средство,

предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ – реализующие алгоритмы криптографического преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи.

СУБЪЕКТ ДОСТУПА – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ – устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение Концепции

Настоящая Концепция определяет систему взглядов на проблему обеспечения комплексной безопасности информации и устанавливает порядок организации и правила обеспечения информационной безопасности в муниципальном казенном общеобразовательном учреждении «Средняя общеобразовательная школа №14» аула Эдельбай Благодарненского муниципального района Ставропольского края (далее - Учреждение), распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками Учреждения, требования по информационной безопасности к информационным средствам, применяемым в Учреждения. Документ представляет собой методологическую основу для разработки и реализации комплексных целевых программ обеспечения защиты информации на объектах информатизации Учреждения.

1.2. Сфера применения Концепции

Требования настоящей Концепции обязательны для всех структурных подразделений Учреждения и распространяются на:

- автоматизированные системы Учреждения;
- средства телекоммуникаций;
- помещения;
- сотрудников Учреждения.

Внутренние документы Учреждения, затрагивающие вопросы, рассматриваемые в данном документе, должны разрабатываться с учетом положений Концепции и не противоречить им.

1.3. Правовая основа Концепции

Правовую основу Концепции составляют:

- Конституция Российской Федерации;
- Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ;
- Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ;
- Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 26.07.2006 № 149-ФЗ;
- Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 Пр-1895;
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Гостехкомиссия России, 2002г.
- Федеральный закон «О персональных данных» от 27.07.06 № 152-ФЗ (в ред. от 27.07.2011);

– ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью" (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст)

– другие законодательные акты, руководящие и нормативно-методические документы Российской Федерации в области обеспечения информационной безопасности.

1.4. Цели и задачи обеспечения безопасности информации

Главная цель обеспечения безопасности информации, циркулирующей в Учреждения, - реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы Учреждения.

Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в Учреждения;
- предотвращение нарушений прав личности клиентов на сохранение конфиденциальности информации, циркулирующей в ИТКС Учреждения;
- предотвращение несанкционированных действий по блокированию информации;

Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Учреждения, нарушению нормального функционирования и развития ИТКС Учреждения;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
- создание условий для максимально возможного возмещения и локализации наносимого интересам Учреждения ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;

- разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности подразделений Учреждения по обеспечению защиты информации;
- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
- создание и применение защищенных информационных объектов и АИС, центров обработки защищаемой информации;
- развитие и совершенствование защищенного юридически значимого электронного документооборота.
- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности
- создание механизмов управления системой информационной безопасности;

2. ОБЪЕКТЫ ЗАЩИТЫ

2.1. Объектами защиты Учреждения являются:

- информационные ресурсы;
- средства и системы обработки информации;
- средства и системы защиты информации, в т.ч. криптографической защиты информации;
- помещения или объекты, предназначенные для ведения закрытых переговоров.

2.2. Информационные ресурсы Учреждения

Под информационными ресурсами в Учреждения понимаются совокупности сведений в электронном и бумажном виде (база данных, электронная библиотека, реестр, кадастр, фонд, архив и другие виды информационных массивов), поддерживаемые программно-техническими средствами автоматизированной информационной системы. Информационные ресурсы представляют собой хранилища данных, из которого путем специализированной обработки пользователю предоставляется информация на электронных или бумажных носителях, в том числе в виде отдельных фрагментов баз данных, отчетов и справок.

Технологической основой формирования информационных ресурсов является программно-техническая среда автоматизированных информационных систем, используемых в Учреждения

Используемые в информационных системах Учреждения технологии взаимодействия при обработке информационных ресурсов включают:

- электронную почту (протоколы SMTP и IMAP);
- электронный обмен файлами (протокол FTP);
- обмен файлами на магнитных носителях в формате XML;
- Web-доступ к ресурсам сети (протоколы HTTP/HTTPS/HTML);
- технологию терминального доступа для взаимодействия с удаленными пользователя (протокол RDP);

Основным источником информации для наполнения первичных баз данных ИТКС являются документы и сообщения, поступающие от структурных подразделений Учреждения и внешних организаций.

Информационное и функциональное взаимодействие узлов ИТКС Учреждения осуществляется на основе интегрированных (логически единых) баз данных, обеспечивающих должностных лиц структурных подразделений Учреждения требуемой информацией.

Обмен информацией осуществляется:

- внутри узлов - по локальным вычислительным сетям - программными и техническими средствами ЛВС в соответствии с транспортными протоколами обмена информацией между абонентами;
- между узлами ИТКС Учреждения и информационными системами внешних организаций и ведомств - по каналам связи (или на магнитных

носителях) в соответствии с соглашениями и протоколами по обмену информацией.

Вся информация, хранимая, обрабатываемая или передаваемая в рамках подразделений Учреждения с использованием информационной системы, классифицирована по степени важности и критичности на следующие категории.

Конфиденциальная информация

К конфиденциальной относится информация, составляющая коммерческую тайну, информация о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющая идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях, а также любая другая закрытая информация, являющаяся собственностью Учреждения. При обработке этой информации необходимо соблюдать требования “Специальных требований и рекомендаций по защите информации с ограниченным доступом, обрабатываемой техническими средствами (СТР-К)” Государственной технической комиссии при Президенте РФ, положения Федерального закона «О персональных данных», а также прочих нормативных правовых актов, регламентирующих работу с конфиденциальной информацией.

При хранении, передаче и обработке данной информации необходимо обеспечить максимальный уровень её защиты.

Служебная информация

К служебной информации могут быть отнесены любые сведения, относящиеся к деятельности подразделений Учреждения, несанкционированное распространение которых может привести к отрицательным экономическим, этическим или иным последствиям для Учреждения. Хранение, обработка и передача такой информации должна осуществляться в соответствии с требованиями настоящего документа.

Рабочая информация

Рабочая информация включает в себя сведения, имеющие отношение к внутренней деятельности подразделений Учреждения и не относящиеся к конфиденциальной или служебной информации. При хранении, передаче и обработке такой информации необходимо обеспечить максимальный уровень её целостности и аутентичности в соответствии с положениями настоящего документа.

Прочие виды информации

Для прочих видов информации порядок хранения, передачи и обработки с использованием автоматизированных систем не регламентируется.

2.3. Средства и системы обработки информации

Средства и системы обработки информации Учреждения представляют собой совокупность программного обеспечения и технических средств обработки и передачи информации, а также систему телекоммуникаций (СТК).

Техническое обеспечение (ТО) включает следующие компоненты:

- серверные комплексы (платформы);
- рабочие станции пользователей;
- технические средства ввода/вывода информации:
- сканеры;
- принтеры.
- средства хранения и архивирования данных;
- активное и пассивное оборудование локальной вычислительной сети (ЛВС);
- средства бесперебойного питания.

Система телекоммуникаций (СТК), поддерживает информационный обмен между внутренними абонентами и информационными системами Учреждения, а также информационную связь с внешними абонентами. В системной архитектуре СТК выделены следующие функциональные подсистемы:

- Транспортная подсистема;
- Ведомственная телефонная сеть;
- Подсистема удаленного доступа к информационным ресурсам;
- Подсистема электронной почты;
- Подсистема сервисов глобальной сети Интернет;
- Подсистема управления, мониторинга и обслуживания СТК.

В состав **программного обеспечения** информационных систем входят:

- общесистемное программное обеспечение;
- специальное (прикладное) программное обеспечение.

Общесистемное программное обеспечение включает в себя:

- серверные и клиентские операционные системы;
- СУБД;
- пакеты офисных программ;
- антивирусные программы;
- пакеты программ для групповой работы
- терминальные серверные и клиентские программы
- средства электронной почты;
- средства управления информационной безопасностью;
- средства управления и администрирования системой;

Специальное программное обеспечение (СПО) является совокупностью аналитических и логических методов и алгоритмов, программ их реализации, отражающих специфику автоматизируемых процессов и предназначенных для обеспечения деятельности должностных лиц Учреждения.

2.4. Средства обеспечения

Под средствами обеспечения Учреждения понимаются вспомогательные инженерно-технические системы, не участвующие в обработке информации, содержащей конфиденциальные сведения. В общем виде к этим системам относятся:

– системы электропитания и заземления объектов;

– системы связи (ведомственной, междугородней, городской, внутренней), не предназначенной для закрытых переговоров;

– системы пожарной и охранной сигнализации;

– электронные системы контроля и управления доступом на территорию и в помещения;

– системы громкоговорящей связи и оповещения;

– системы кондиционирования, отопления и воздухоснабжения.

2.5. Объекты, предназначенные для ведения закрытых переговоров

В качестве объектов, предназначенных для ведения закрытых переговоров, необходимо рассматривать следующие помещения центрального аппарата и территориальных органов Учреждения:

– кабинеты руководящего состава, используемые для обсуждения конфиденциальной информации;

– помещения для проведения совещаний и переговоров по конфиденциальным вопросам (комнаты переговоров, конференцзалы);

– другие помещения, в том числе и технические, в которых может обсуждаться конфиденциальная информация.

3. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В УЧРЕЖДЕНИИ

3.1. Основные факторы, воздействующие на информационную безопасность Учреждения

Основными факторами, воздействующими на информационную безопасность Учреждения, являются:

– Природный фактор. Совокупность угроз природного характера, являющихся следствием воздействия естественной непреодолимой силы (стихии) – землетрясения, наводнения, метеорологические катаклизмы и т.п., приводящие к устойчивому нарушению функционирования информационных и телекоммуникационных ресурсов, вплоть до их утраты или физического уничтожения. Вероятность определяется спецификой территории, на которой дислоцируется защищаемый объект – многолетними метеорологическими наблюдениями, геотектоническими данными и др.

– Техногенный фактор. Совокупность угроз искусственного характера, вызванных результатами человеческой деятельности (цивилизации) – пожары, взрывы, затопления, радиационные и химические заражения, энергетические аварии, разрешение коммуникаций, в том числе – в результате террористических актов, диверсий, массовый беспорядков и ведения боевых действий.

– Системный фактор. Возникновение угрозы целостности информации и (или) функционированию информационно-телекоммуникационных средств, систем и сетей в результате ошибок в их проектировании и разработке или возникновения внутрисистемных сбоев (фатальных ошибок) при их эксплуатации, в том числе – из-за несовершенства или конфликтов программного обеспечения или неисправности оборудования.

– Человеческий фактор. Возникновение угрозы безопасности информации в результате отсутствия профессиональных навыков, недостаточной подготовки, халатности, ненадлежащего исполнения обязанностей или злого умысла персонала, эксплуатирующего информационно-телекоммуникационные средства, системы и сети, разработчиков программного обеспечения и пользователей, имеющих допуск к информации на законном основании. Нарушение правил эксплуатации ЭВМ, их систем и сетей лицами, ответственными за эту работу.

– Криминальный фактор. Целенаправленное внешнее воздействие на информационные ресурсы и информационно-телекоммуникационные средства, системы и сети («атаки», вторжения) с целью уничтожения, блокирования или копирования информации, разработка и внедрение вредоносных программ (вирусов, симуляторов, «троянских» программ, клавиатурных перехватчиков и др.) внедрение специальных технических средств для негласного получения информации.

3.2. Угрозы безопасности информации и их источники

Информация, обрабатываемая в ИТКС Учреждения, дает потенциальную возможность для проявления угроз безопасности, вызванных действиями, процессами или явлениями, приводящими к нанесению ущерба Учреждения. Предусматривается два типа угроз безопасности:

– связанные с утечкой информации (разглашение, утечка, несанкционированный доступ);

– связанные с несанкционированным воздействием на информацию и ее носители (искажение, уничтожение, копирование, блокирование, утрата, сбой функционирования носителя информации, сбои и ошибки техники, ошибки пользователей, природные явления, другие случайные воздействия).

Основными источниками угроз безопасности информации являются:

– Стихийные: Стихийные бедствия, катаклизмы;

– Техногенные: аварии, сбои и отказы оборудования (технических средств);

– Ошибки проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программного обеспечения и т. п.);

– Антропогенные: Ошибки эксплуатации;

– Антропогенные: Преднамеренные действия нарушителей и злоумышленников.

3.3. Классификация способов реализации угроз информационной безопасности

Угрозы информационной безопасности по отношению к защищаемым объектам могут быть разделены на:

– угрозы, связанные с применением технических средств;

– угрозы, связанные с использованием программного обеспечения;

– угрозы, связанные с нарушением технологического процесса обмена данными;

– угрозы, связанные с использованием сетей передачи данных.

3.3.1. Пути реализации непреднамеренных субъективных угроз безопасности информации

Пользователи, операторы, системные администраторы и сотрудники, обслуживающие информационные системы Учреждения, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и процедур.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности (действия,

совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) следующие:

– Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств: отключению оборудования или изменению режимов работы устройств и программ; разрушению информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и т.п.)

– Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.)

– Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.)

– Непреднамеренное заражение компьютера вирусами

– Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или ЭЦП, идентификационных карточек, пропусков и т.п.)

– Игнорирование организационных ограничений (установленных правил) при работе в системе

– Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом подразделения безопасности

– Ввод ошибочных данных

3.3.2. Пути реализации преднамеренных субъективных угроз безопасности информации

Основные возможные пути умышленной дезорганизации работы, вывода информационных систем Учреждения из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.) могут быть следующими:

– Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.), отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, линий связи и т.п.)

– Хищение носителей информации (распечаток, магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ), хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.)

– Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.

– Использование чужих прав по доступу к ресурсам АС путем незаконного получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы программными закладками и т.д.).

– Несанкционированное использование АРМ пользователей, имеющих уникальные физические характеристики, такие как имя рабочей станции в сети, физический адрес, адрес в системе связи и другие.

– Несанкционированная модификация программного обеспечения – внедрение программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации или дезорганизации функционирования АС

– Перехват данных, передаваемых по каналам связи, и их анализ с целью получения сведений, в том числе ограниченного распространения и выяснения протоколов обмена, правил вхождения в связь и авторизации пользователей и последующих попыток их имитации для проникновения в систему

– Вмешательство в процесс функционирования АС сетей общего пользования с целью несанкционированной модификации данных, доступа к сведениям ограниченного распространения, дезорганизации работы подсистем АС и т.п.

3.3.3. Пути реализации непреднамеренных техногенных угроз безопасности информации

– закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;

– аварии в системах электропитания;

– аварии в системах отопления и водоснабжения в непосредственной близости к техническим средствам обработки информации;

– нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи);

– неумышленное повреждение внешних кабельных систем связи строительными организациями, физическими лицами и т.п. в результате проведения несогласованных работ в местах прокладки кабелей связи;

– возникновение пожаров в непосредственной близости к техническим средствам обработки информации в результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил противопожарной безопасности.

3.3.4. Пути реализации непреднамеренных стихийных угроз безопасности информации

– Разрушение зданий, отдельных помещений, в которых установлены технические средства обработки информации, хранилища данных в результате стихийных бедствий (наводнений, землетрясений, ураганов) в районе размещения объекта информатизации Учреждения

– воздействие атмосферного электричества на технические средства обработки информации и системы обеспечения (электропитание, охранная, пожарная сигнализация и т.п.)

– возникновение стихийных очагов пожаров (лесные пожары) в непосредственной близости от объекта информатизации Учреждения

3.4. Классификация нарушителей информационной безопасности Учреждения

При анализе угроз информационной безопасности используется модель нарушителя по признаку принадлежности к Учреждения. В соответствии с этой моделью все нарушители делятся на две основные группы: внутренние и внешние.

Под внутренними нарушителями подразумеваются все сотрудники Учреждения, имеющие санкционированный доступ на территорию Учреждения или к ресурсам АС. Под внешними нарушителями подразумеваются все остальные лица.

Внутренним нарушителем может быть лицо из следующих категорий сотрудников:

– пользователи информационных ресурсов;

– обслуживающий персонал (системные администраторы, администраторы АС, администраторы баз данных, инженеры);

– сотрудники-программисты, сопровождающие системное, общее и прикладное программное обеспечение;

– другие сотрудники подразделений Учреждения, имеющие санкционированный доступ в здания, где расположено оборудование передачи и обработки информации АС Учреждения.

Предполагается, что несанкционированный доступ на объекты Учреждения посторонних лиц исключается организационными мерами (охрана территории, организация пропускного режима).

Внешние нарушители информационной безопасности:

– лица, самостоятельно осуществляющие создание методов и средств реализации атак, а также самостоятельно реализующие атаки, совершающие

свои действия с целью нанесения ущерба Учреждения (съем информации, искажение информации, разрушение системного или прикладного ПО);

Потенциальные нарушители делятся на три группы:

1 группа - субъекты, не имеющие доступ в пределы контролируемой зоны Учреждения.

2 группа - субъекты, не имеющие доступ к работе со штатными средствами АС Учреждения, но имеющие доступ в помещения, где они размещаются.

3 группа – субъекты, имеющие доступ к работе со штатными средствами АС Учреждения.

Квалификация потенциального нарушителя.

А – не является специалистом в области вычислительной техники.

В – самый низкий уровень возможностей – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции при обработке информации.

С – возможности создания и запуска собственных программ с новыми функциями по обработке информации.

Д – возможность управления функционированием автоматизированной системы, т.е. воздействием на базовое программное обеспечение системы, на конфигурацию ее оборудования.

Е – включает весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств автоматизированной системы, вплоть до включения в состав АС собственных технических средств с новыми функциями по обработке информации.

Наряду с классификацией, приведенной выше, нарушителей информационной безопасности можно разделить на следующие виды - неосторожные (халатные), манипулируемые, саботажники, нелояльные и мотивируемые извне.

3.5. Обобщенная модель угроз безопасности информации Учреждения

Угроза информационной безопасности	**Источник угроз**	**Способы реализации угроз**
I. Получение информации	1. Антропогенный	а) Разглашение, передача или утрата атрибутов разграничения доступа
		б) Внедрение агентов в число персонала системы
		в) Хищение носителей информации
		г) Незаконное получение паролей и других реквизитов разграничения доступа
		д) Несанкционированная модификация программного обеспечения
		е) Перехват данных, передаваемых по каналам связи

Угроза информационной безопасности	Источник угроз	Способы реализации угроз
		ж) Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
II. Анализ характеристик информации	1. Антропогенный	а) Хищение носителей информации хищение производственных отходов
		б) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
		в) Несанкционированная модификация программного обеспечения
		г) Перехват данных, передаваемых по каналам связи, и их анализ
III. Изменение (искажение, подмена) информации	1. Антропогенный	а) Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.)
		б) Непреднамеренное заражение компьютера вирусами
		в) Ввод ошибочных данных
		г) Вмешательство в процесс функционирования АС сетей общего пользования с целью несанкционированной модификации данных
	2. Техногенный	а) аварии в системах электропитания
		б) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования
IV. Нарушение информации	1. Антропогенный	а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств
		б) Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.)
		в) Непреднамеренное заражение компьютера вирусами

Угроза информационной безопасности	Источник угроз	Способы реализации угроз
		г) Игнорирование организационных ограничений (установленных правил) при работе в системе
		д) Ввод ошибочных данных
	2. Техногенный	а) аварии в системах электропитания
		б) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования
V. Нарушение работоспособности систем	1. Антропогенный	а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств
		б) Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы
	2. Техногенный	а) закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;
		б) аварии в системах электропитания;
		в) аварии в системах отопления и водоснабжения в непосредственной близости к техническим средствам обработки информации;
		г) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования;
		д) неумышленное повреждения внешних кабельных систем связи строительными организациями, физическими лицами и т.п. в результате проведения несогласованных работ в местах прокладки кабелей связи;
		е) возникновение пожаров в непосредственной близости к техническим средствам обработки информации в результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил противопожарной безопасности.
	3. Стихийный	а) Разрушение зданий, отдельных помещений
		б) воздействие атмосферного электричества
		в) возникновение стихийных очагов пожаров

Наложение угроз безопасности информации на модель ИТКС Учреждения (Рис.1) позволяет в первом приближении оценить их опасность

и методом исключения определить наиболее актуальные для конкретного объекта защиты. Кроме того, можно оценить объемы необходимых работ и выбрать магистральное направление по обеспечению безопасности информации.

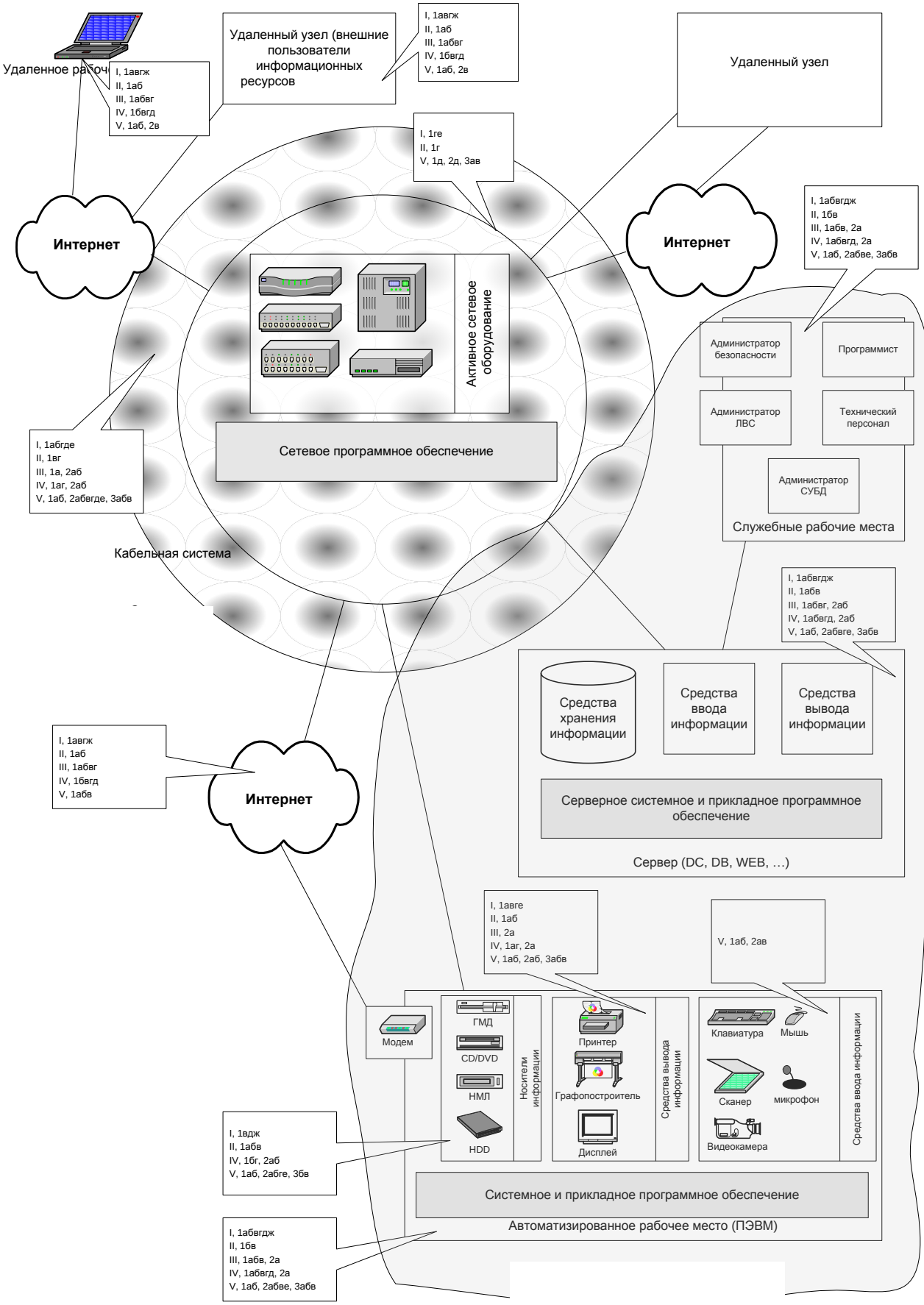
Удаленное рабоч
I, 1авгж
II, 1аб
III, 1абвг
IV, 1бвгд
V, 1аб, 2в
Удаленный узел (внешние пользователи информационных ресурсов
I, 1авгж
II, 1аб
III, 1абвг
IV, 1бвгд
V, 1аб, 2в
Удаленный узел
I, 1ге
II, 1г
V, 1д, 2д, 3ав
Интернет
Интернет
I, 1абвгдж
II, 1бв
III, 1абв, 2а
IV, 1абвгд, 2а
V, 1аб, 2абве, 3абв
Активное сетевое оборудование
Сетевое программное обеспечение
I, 1абгде
II, 1вг
III, 1а, 2аб
IV, 1аг, 2аб
V, 1аб, 2абвгде, 3абв
Кабельная система
Администратор безопасности
Программист
Администратор ЛВС
Технический персонал
Администратор СУБД
Служебные рабочие места
I, 1абвгдж
II, 1абв
III, 1абвг, 2аб
IV, 1абвгд, 2аб
V, 1аб, 2абвге, 3абв
Средства хранения информации
Средства ввода информации
Средства вывода информации
Серверное системное и прикладное программное обеспечение
Сервер (DC, DB, WEB, …)
I, 1авгж
II, 1аб
III, 1абвг
IV, 1бвгд
V, 1абв
Интернет
I, 1авге
II, 1аб
III, 2а
IV, 1аг, 2а
V, 1аб, 2аб, 3абв
V, 1аб, 2ав
Модем
ГМД
CD/DVD
НМЛ
HDD
Носители информации
Принтер
Графопостроитель
Дисплей
Средства вывода информации
Клавиатура
Мышь
Сканер
микрофон
Видеокамера
Средства ввода информации
I, 1вдж
II, 1абв
IV, 1бг, 2аб
V, 1аб, 2абге, 3бв
Системное и прикладное программное обеспечение
Автоматизированное рабочее место (ПЭВМ)
I, 1абвгдж
II, 1бв
III, 1абв, 2а
IV, 1абвгд, 2а
V, 1аб, 2абве, 3абв

Рисунок 1

4. ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ

4.1. Организационно-штатная структура подразделений отвечающих за обеспечение информационной безопасности Учреждения

Общее руководство системой информационной безопасности и принятие всех решений по вопросам ее функционирования осуществляет Руководитель Учреждения.

Руководство и контроль за выполнением мероприятий по защите информации в подразделениях Учреждения осуществляют их руководители.

4.2. Порядок разработки и эксплуатации системы обеспечения информационной безопасности Учреждения

Жизненный цикл системы обеспечения информационной безопасности Учреждения включает этап развертывания и этапы постоянного функционирования и совершенствования.

К моменту начала развертывания системы информационной безопасности должны быть уточнены и утверждены Руководством права и обязанности участников работ по защите информации в соответствии с данной Концепцией. Должен быть разработан и утвержден план-график развертывания системы информационной безопасности Учреждения.

Основные этапы развертывания системы должны включать в себя последовательное проведение следующих мероприятий:

- Издание Приказа по Учреждения об организации системы информационной безопасности.
- Разработка и уточнение функций различных подразделений и структур, распределение прав и обязанностей подразделений в системе информационной безопасности Учреждения.
- Назначение администратора безопасности.
- Уточнение состава администраторов сетей, БД и систем.
- Подготовка к информационному обследованию в подразделениях.
- Информационное обследование подразделений Учреждения.
- Определение перечня угроз, модели нарушителя, требований к системе информационной безопасности;
- Разработка (доработка) нормативно-методической базы системы обеспечения информационной безопасности;
- Ввод системы обеспечения информационной безопасности в действие;
- Категорирование информационных ресурсов Учреждения;
- Аттестация объектов информатизации Учреждения по требованиям безопасности информации.
- Поддержка системы обеспечения информационной безопасности в работоспособном и актуальном состоянии.

4.3. Организация системы комплексного мониторинга и контроля состояния информационной безопасности Учреждения

Контроль и комплексный мониторинг состояния системы информационной безопасности Учреждения выполняется с целью обеспечения надежности и устойчивости системы информационной безопасности, обеспечения доверия к ней и гарантий выполнения требований по ИБ.

Задачи контроля и комплексного мониторинга состояния информационной безопасности:

– определение критериев для оценки безопасности существующих и создаваемых систем в рамках информационно-телекоммуникационной системы Учреждения;

– определение соответствия или несоответствие создаваемых и существующих систем этим критериям;

– формулировка обоснованных предложений по совершенствованию существующих методов и систем обеспечения защищенности, безопасности и достоверности информации в тех случаях, когда они не удовлетворяют имеющимся критериям.

Для осуществления контроля выполнения требований должна быть организована система отчетности о выполнении требований по безопасности. Отчетность должна вестись ответственным за ИБ соответствующего рабочего места, процесса, системы или организационной структуры. С заданной периодичностью отчетность должна отправляться руководству. На основании этих данных руководство сможет реально оценивать ситуацию с состоянием безопасности во всех подразделениях Учреждения.

Основные операции по учету и контролю выполнения требований должны быть автоматизированы.

Обязанности по контролю распределяются между исполнительными органами системы информационной безопасности следующим образом:

– администраторы систем, СУБД, сетей контролируют текущее состояние информационной безопасности в системах, СУБД, сетях;

– сотрудники подразделения контролируют текущее состояние информационной безопасности на своих рабочих местах.

Мероприятия для организации системы комплексного мониторинга и контроля состояния информационной безопасности

Должна быть организована система непрерывного контроля за состояние системы информационной безопасности следующим образом:

– определение перечня подразделений, рабочих мест, систем, процессов, по которым должен проводиться контроль выполнения требований.

– определение списка требований, для каждой структурной единицы.

– организация сбора отчетности о выполнении требований по ИБ.

– обработка и анализ собранных форм отчетности выводами о выполнении требований;

– периодический пересмотр системы требований

– контроль полноты и непротиворечивости системы требований.

Решение всех перечисленных задач должно быть автоматизировано путем использования необходимых программных средств контроля выполнения требований.

Помимо ежедневного контроля должны выполняться периодические проверки организации и состояния информационной безопасности, в том числе:

Проверки организации и состояния информационной безопасности проводятся в подразделениях и в ИТКС Учреждения и могут быть:

- плановыми;
- внезапными;
- по фактам нарушения информационной безопасности.

Плановые проверки проводятся в соответствии с годовым Планом проверок, утверждается руководителем Учреждения и рассылается во все подразделения. В ходе плановых проверок должна полностью проверяться вся организация системы информационной безопасности подразделения.

Проверки по фактам нарушения информационной безопасности проводятся после того, как нарушение устранено. Проверка проводится с целью выявление причин и предпосылок нарушения и выработка мер по предупреждению подобных нарушений в дальнейшем. Проверка проводится в обязательном порядке по каждому факту нарушения независимо от его последствий.

Результаты всех проверок оформляются в виде актами с необходимыми в каждом конкретном случае приложениями.

Администраторы систем, СУБД и сетей контролируют состояние информационной безопасности на подведомственных участках. С этой целью они:

- контролируют правильность выполнения сотрудниками действий по доступу к объектам информационной системы;
- анализируют состояние информационной системы с целью выявлений попыток несанкционированного доступа и использования информационных средств и информации;
- контролируют правильность использования имеющихся коллективных и индивидуальных средств информационной защиты.

В случае выявления каких-либо отклонений или нарушений в системе информационной безопасности администраторы безопасности принимают меры к их устранению самостоятельно, или через руководителя соответствующего подразделения. Ответственность за принятие этих мер и сообщение о происшедшем руководителю несет администратор.

Сотрудники подразделения анализируют состояние своих рабочих мест с целью выявления попыток несанкционированного доступа и использования

информационных средств и информации. В случае выявления таких попыток сотрудник сообщает об этом администратору безопасности организации и руководителю структурного подразделения.

Для эффективного контроля состояния информационной безопасности необходимо провести обучение сотрудников подразделений Учреждения с целью повышения уровня их осведомленности в вопросах информационной безопасности.

Для организации контроля и комплексного мониторинга системы информационной безопасности необходимо разработать и внедрить следующие организационно-распорядительные и нормативно-технические документы:

– Регламент расследования инцидентов информационной безопасности;

– Должностные инструкции администраторов систем, СУБД, сетей (в том числе разделы, касающиеся организации контроля и мониторинга информационной безопасности);

– Памятка сотрудника Учреждения по информационной безопасности;

5. МЕРОПРИЯТИЯ ПО РЕШЕНИЮ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ

5.1. Организационно-режимные мероприятия

Выполнение организационно-режимных мероприятий при обеспечении информационной безопасности предполагает:

– категорирование объектов информатизации Учреждения в соответствии с руководящими нормативно-методическими документами по защите информации РФ;

– разграничение допуска к информационным ресурсам ограниченного распространения;

– разграничения допуска к программно-аппаратным ресурсам ИТКС Учреждения;

– ведение учета ознакомления сотрудников с информацией ограниченного распространения;

– включение в функциональные обязанности сотрудников обязательства о неразглашении и сохранении сведений ограниченного распространения;

– организация уничтожения информационных отходов (бумажных, магнитных и т.д.);

– ведение учета отчуждаемых носителей информации;

– организация и осуществление периодического контроля за обеспечением информационной безопасности;

– организация учета СКЗИ, ключей шифрования и подписи, их хранения, эксплуатации и уничтожения.

В соответствии с вышеуказанными задачами необходимо разработать или актуализировать комплект следующих организационно-распорядительных документов:

– методика категорирования объектов информатизации Учреждения;

– перечень критичных информационных ресурсов Учреждения;

– регламент предоставления доступа к информационным и программно-аппаратным ресурсам Учреждения;

– должностные обязанности сотрудников Учреждения по обеспечению информационной безопасности.

5.2. Мероприятия по физической защите объектов и средств информатизации Учреждения

Обеспечение физической безопасности всей информационно-телекоммуникационной системы Учреждения и отдельных ее элементов является одной из основных задач, решаемых подсистемой защиты информации. Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных

нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита направлена на обеспечение безопасности:

- периметра информационной системы (защита контролируемой зоны);
- периметра отдельных объектов системы (выделенных территорий, зданий, помещений);
- носителей информации, оборудования и каналов передачи данных, хранящих, обрабатывающих и передающих информацию в открытом виде (магнитных и бумажных носителей информации, экранов мониторов, серверов и рабочих станций, открытых каналов связи и т.п.);
- ключевых элементов криптографических и парольных систем;

Основными направлениями физической защиты Учреждения являются:

- контроль физического доступа к оборудованию, на контролируемую территорию и в помещения;
- обеспечение безопасности кабельной системы;
- обеспечение безопасности при утилизации отработавшего оборудования и носителей информации;
- обеспечение безопасности рабочих мест.

Контроль физического доступа к оборудованию, на контролируемую территорию и в помещения

На территории Учреждения и территориальных подразделений следует установить надлежащий контроль доступа в помещения. Правила доступа на территорию должны регламентироваться соответствующим положением (инструкцией).

Для разграничения доступа в помещения, где располагается серверное оборудование и другие критически важные объекты ИТКС Учреждения, целесообразно использовать системы физической защиты. Необходимо соблюдать следующие правила доступа в помещения:

- Во всех подразделениях Учреждения необходимо исключить несанкционированное нахождение посторонних лиц, дата и время их входа и выхода должны регистрироваться.
- Посетители должны носить на одежде хорошо различимые идентификационные карточки;
- Необходимо немедленно изъять права доступа в защищенные области (территорию, помещения) у увольняющихся сотрудников.

Кроме того, для предотвращения утечки информации и противодействия потенциальным нарушителям необходимо соблюдать следующие правила:

- Эксплуатация АРМ и серверов должна осуществляться в

помещениях, оборудованных надежными замками, средствами сигнализации, исключающими возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающими физическую сохранность находящихся в помещении защищаемых ресурсов (АРМ, документов, реквизитов доступа и т.п.).

- Размещение и установка АРМ и серверов должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней доступ.
- Уборка помещений, в которых обрабатывается или хранится конфиденциальная или служебная информация, должна производиться в присутствии ответственного, за которым закреплены технические средства (данные), или дежурного по подразделению с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.
- В помещениях во время обработки и отображения на АРМ информации ограниченного распространения должен присутствовать только персонал, допущенный к работе с данной информацией. Запрещается прием посетителей в помещениях, когда осуществляется обработка защищаемой информации.
- Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами и металлическими шкафами. Помещения должны быть обеспечены средствами уничтожения документов.
- Вспомогательное оборудование (например, копировальные аппараты, факс-машины) должно быть так размещено, чтобы уменьшить риск НСД к защищенным областям или компрометации конфиденциальной информации.
- Физические барьеры должны по необходимости простираться от пола до потолка, чтобы предотвратить несанкционированный доступ в помещение.
- Запрещается без надобности предоставлять посторонним лицам информацию о происходящем в защищенных областях (территории, помещениях).
- Для обеспечения должного уровня безопасности и для предотвращения вредоносных действий запрещается работать в одиночку (без надлежащего контроля) с критически важными компонентами информационной системы.
- В нерабочее время защищенные области (территория, помещения) должны быть физически недоступны (закрыты на замки) и периодически проверяться охраной.
- Персоналу, осуществляющему техническое обслуживание серверов, должен быть предоставлен доступ в защищенные области (территорию, помещения) только в случае необходимости и после получения разрешения. По необходимости доступ такого персонала (особенно к конфиденциальным данным) следует ограничить, а их действия

следует отслеживать.

- Запрещается использование фотографической, звукозаписывающей и видео аппаратуры в защищенных областях, за исключением санкционированных случаев.
- По окончании рабочего дня помещения с установленными защищенными АРМ должны сдаваться под охрану с включением сигнализации.
-

Обеспечение безопасности кабельной системы ИТКС Учреждения

Защита кабельной системы ИТКС направлена на снижение вероятности несанкционированного доступа к информации путем гальванического подключения к информационным кабелям или снятия информации через побочные электромагнитные излучения и наводки на другие кабели, а также на обеспечение защиты кабельного оборудования от электромагнитных помех.

Кабели электропитания и сетевые кабели для передачи данных необходимо защищать от вскрытия для целей перехвата информации и повреждения. Для уменьшения такого риска в помещениях организации предлагается реализовать следующие защитные меры:

- Кабели электропитания и линии связи, идущие к информационным системам, должны быть проведены под землей (по возможности) или защищены надлежащим образом с помощью других средств.
- Необходимо рассмотреть меры по защите сетевых кабелей от их несанкционированного вскрытия для целей перехвата данных и от повреждения, например, воспользовавшись экранами или проложив эти линии так, чтобы они не проходили через общедоступные места.
- С целью снижения влияния электромагнитных помех, силовые и коммуникационные кабели должны быть разнесены в пространстве.
- Для исключительно уязвимых или критически важных систем следует рассмотреть необходимость принятия дополнительных мер, таких, как:
- шифрование данных;
- установка бронированных экранов и использование запираемых помещений;
- использование других маршрутов или сред передачи данных.

Надежная утилизация отработавшего оборудования и носителей информации

Оборудование, подлежащее выводу из эксплуатации, и использованные носители информации могут содержать остаточную информацию ограниченного доступа. Регламентация порядка и процедур их утилизации позволяет перекрыть каналы несанкционированного доступа к этой информации:

- устройства хранения информации, содержащие ценную

информацию, при выведении из эксплуатации должны быть физически уничтожены, либо должно быть проведено гарантированное стирание с них остаточной информации;

- все оборудование, включая носители информации, перед передачей другому владельцу или списанием должно быть проверено на отсутствие важной информации или лицензионного программного обеспечения;
- дальнейшая судьба поврежденных устройств хранения, содержащих важную информацию, (уничтожение или ремонт) определяется на основе заключения экспертной комиссии.

Безопасность рабочего места сотрудников Учреждения

Рабочие места сотрудников Учреждения - наиболее многочисленная категория объектов ИТКС, через которые возможен несанкционированный доступ к информации. Действия сотрудников сложно контролировать, поэтому в системе защиты информации необходимо предусмотреть автоматизированные механизмы контроля доступа к терминалам, мониторинга за действиями пользователей и сигнализации при обнаружении попыток несанкционированного доступа, а также установлен жесткий регламент доступа к рабочим местам с помощью организационных мер.

Безопасность рабочих мест сотрудников Учреждения предусматривает:

- документы на всех видах носителей и технические средства обработки информации, должны храниться (размещаться) в помещениях, исключающих несанкционированный доступ к ним;
- исключение несанкционированного доступа к информации, хранящейся на различного рода носителях;
- персональные компьютеры, терминалы и принтеры должны защищаться блокираторами клавиатуры, паролями или другими методами на время отсутствия пользователя;
- должны быть приняты надежные меры, исключающие несанкционированное использование копировальной техники;
- распечатки, содержащие информацию ограниченного доступа должны изыматься из печатающего устройства немедленно Необходимо устанавливать печатающие устройства для печати конфиденциальных документов в помещениях, где работают сотрудники, ответственные за их учет, хранение и выдачу исполнителям.

5.3. Мероприятия по обеспечению катастрофоустойчивости информационно-телекоммуникационной системы Учреждения

Обеспечение катастрофоустойчивости необходимо для сохранения устойчивости и стабильности функционирования Учреждения и ее информационно-телекоммуникационной системы в различных условиях неблагоприятного воздействия внешних и внутренних факторов техногенного и/или природного характера.

Для обеспечения катастрофоустойчивости необходимо выполнить работы, направленных на минимизацию возможных потерь Учреждения в условиях активного воздействия внутренней и внешней среды.

Основные мероприятия по обеспечению катастрофоустойчивости информационно-телекоммуникационной системы Учреждения

– идентификация и анализ неблагоприятных воздействий на информационно-телекоммуникационную систему Учреждения, разработка стратегий управления рисками, связанными с применением информационно-телекоммуникационной системы

– определение требований Учреждения к непрерывности функционирования информационно-телекоммуникационной системы;

– определение стратегий восстановления информационных и других технических систем в случае возникновения отказов и сбоев;

– разработка и документирование плана обеспечения катастрофоустойчивости информационно-телекоммуникационной системы Учреждения;

– внедрение необходимых изменений в техническом, организационном и информационном обеспечении Учреждения согласно разработанному плану обеспечения катастрофоустойчивости информационно-телекоммуникационной системы Учреждения;

– поддержка плана обеспечения катастрофоустойчивости информационно-телекоммуникационной системы Учреждения в актуальном состоянии (включая тестирование плана, обучение персонала, техническая поддержка используемого программного и аппаратного обеспечения, периодическое обновление плана)

Важнейшим качеством ИТКС и, в частности, центров обработки данных (ЦОД) Учреждения является способность обеспечивать требуемый уровень отказоустойчивости. Возможно применения следующих технических мероприятий для обеспечения отказоустойчивости:

- Следует внедрять технологии резервирования хранилищ данных.
- Серверное и другое критическое оборудование следует размещать таким образом, чтобы свести к минимуму излишний доступ в рабочие помещения.
- Оборудование необходимо защищать от сбоев в системе электропитании и других неполадок в электрической сети. Источник питания должен соответствовать спецификациям производителя оборудования.
- Следует рассмотреть необходимость использования резервного источника питания. Для оборудования, поддерживающего критически важные производственные сервисы, рекомендуется установить источник бесперебойного питания. План действий в чрезвычайных ситуациях должен включать меры, которые необходимо принять по окончании срока годности источников бесперебойного питания. Оборудование, работающее с источниками бесперебойного питания, необходимо регулярно тестировать в

соответствии с рекомендациями изготовителя.

- Следует рассмотреть возможность изоляции областей, требующих специальной защиты, для понижения необходимого уровня общей защиты.

Для создания системы обеспечения катастрофоустойчивости необходимо разработать следующие организационно-распорядительные и нормативно-технические документы:

– Политика резервного копирования и восстановления данных

– План обеспечения непрерывной работы и восстановления работоспособности подсистем АС

–

5.4. Мероприятия по решению задач защиты информации от несанкционированного доступа в информационно-телекоммуникационных системах Учреждения

Основные мероприятия по защите информации от несанкционированного доступа в ИТКС должны предусматривать следующее:

- Применение сертифицированных аппаратно-программных средств защиты информации от НСД.
- Механизмы защиты от НСД должны осуществлять защиту системы от возможности посторонних лиц осуществлять работу в системе (механизмы идентификации и аутентификации), а также получать НСД к информационным ресурсам системы (механизмы разграничения доступа в соответствии с полномочиями субъекта). При реализации этих механизмов защиты должна использоваться совокупность организационных, программных (пароли, матрицы доступа и др.), аппаратно-программных и технических методов защиты.
- Защита системы от НСД должна обеспечиваться на всех технологических этапах передачи, обработки и хранения информации и при всех режимах работы системы, в том числе при проведении ремонтных и регламентных работ. При этом реализованные в системе средства защиты от НСД не должны ухудшать основные функциональные характеристики системы.
- Защита системы от НСД с помощью программных, программно-аппаратных и технических методов должна обеспечивать:
  - защиту технических средств обработки информации;
  - защиту баз данных;
  - защиту системы управления.
- Защита от НСД должна строиться на основе системы разграничения доступа (СРД) пользователей к системе и ее информационным ресурсам. Основными функциями СРД должны являться:
  - реализация правил разграничения доступа (ПРД) пользователей и их процессов к информационным ресурсам;
  - реализация ПРД пользователей к устройствам создания

твердых копий;

- изоляция программ процесса, выполняемого в интересах пользователя, от других пользователей системы;
- реализация правил обмена данных между пользователями системы, построенных по сетевым принципам.

- Обеспечивающие средства СРД должны выполнять следующие основные функции:
  - идентификацию и аутентификацию пользователей системы и поддержание привязки к их процессам, выполняемым в их интересах;
  - регистрацию действий пользователей и выполняемых в их интересах процессов, предоставление возможности исключения и включения новых пользователей и объектов доступа, а также изменение полномочий пользователей;
  - реакцию на попытки несанкционированного доступа (сигнализацию, блокировку и т.д.), восстановление механизмов защиты после НСД;
  - тестирование;
  - очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищенными данными;
  - учет выходных печатных и графических форм, а также твердых копий в системе;
  - контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.
- Практическая реализация СРД должна определяться с учетом конкретных особенностей системы и может включать в себя следующие способы и их сочетания:
  - распределенная система разграничения доступа и СРД, локализованная в аппаратно-программном комплексе системы;
  - СРД в рамках операционной системы, системы управления базами данных или прикладных программ;
  - СРД в средствах реализации сетевых протоколов взаимодействия или на уровне приложений;
  - Программная и (или) техническая реализация СРД;
  - Программная и (или) аппаратная реализация криптографических функций.

В рамках системы защиты от НСД необходимо внедрить комплексную систему защиты баз данных, содержащих критичную к нарушению безопасности информацию.

Для создания системы защиты информации от несанкционированного доступа в информационно-телекоммуникационных системах Учреждения необходимо разработать следующие организационно-распорядительные и нормативно-технические документы:

- Положение о разграничении прав доступа к информационным

ресурсам

- Должностные инструкции администраторов и сотрудников безопасности.

5.5. Мероприятия по обеспечению безопасного информационного взаимодействия Учреждения с организациями, министерствами и ведомствами

К основным мероприятиям по обеспечению безопасности сетевого информационного взаимодействия Учреждения с внешними потребителями, пользователями и источниками информации, относятся:

- Предотвращение возможности утечки конфиденциальной информации, обрабатываемой в ИТКС Учреждения, через внешнюю сеть.
- Обеспечение защиты ресурсов ИТКС со стороны внешней сети.

Так как ресурсы ИТКС (в частности – система «Галактика ERP»), предназначенные для доступа из внешней сети (по каналам связи сетей общего пользования), подвержены атакам из внешней открытой сети, то ведомственный (защищенный, содержащий конфиденциальную информацию) и внешний (открытый) трафики должны быть физически разделены – в ИТКС не должно быть вычислительных средств (рабочих станций, серверов, межсетевых экранов), концентрирующих на себе одновременно ведомственный и внешний трафик.

При организации сетевого взаимодействия следует использовать средства защиты:

- Выделенные средства межсетевого экранирования (или межсетевые экраны), устанавливаемые на стыке сетей, концентрирующие на себе межсетевой трафик;
- Механизмы контроля доступа к локальным и сетевым ресурсам, входящие в состав СЗИ НСД, устанавливаемой на рабочие станции и серверы ИТКС, решающие задачи фильтрации внутрисетевого трафика и доступа к локальным ресурсам;
- Антивирусные средства;
- Средства обнаружения компьютерных атак.

Указанными средствами должно обеспечиваться:

- разграничение доступа (по входящему и исходящему трафикам) по адресам (IP адресам) и сетевым протоколам к хостам внешней/внтуренней сети;
- трансляция адресов – во внешней сети должен быть “виден” только адрес криптомаршрутизатора, что позволяет скрывать структуру внутренней сети (адреса рабочих станций и серверов внутренней сети);
- защита от сетевых атак (вирусы, шпионские программы, атаки на отказ в обслуживании);
- аудит доступа к ресурсам внешней сети;
- аутентификация удаленных пользователей

Важнейшим условием обеспечения защищенного доступа к внешним ресурсам является реализация демилитаризованной зоны, с целью физической изоляции внутрисетевого и внешнего трафиков. Данное решение должно позволять взаимодействовать пользователям внешней сети только с серверами внешнего доступа, и делать недоступным для них доступ, прежде всего, к внутренним серверам, а также к рабочим станциям защищаемой корпоративной сети, даже при преодолении защиты, реализуемой средствами межсетевого экранирования.

5.6. Мероприятия по организации криптографической защиты информации

В целях защиты конфиденциальной информации в АИС Учреждения должны применяться средства криптографической защиты информации (СКЗИ).

К СКЗИ предъявляются следующие требования:

– СКЗИ должны допускать их встраивание в технологическую схему обработки электронных сообщений, обеспечивать взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;

– СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;

– СКЗИ должны быть реализованы на основе алгоритмов, соответствующих национальным стандартам Российской Федерации и (или) условиям договоров с контрагентами;

– СКЗИ должны иметь строгий регламент использования ключей, предполагающий контроль со стороны администратора безопасности за действиями пользователя на всех этапах работы с ключевой информацией (получение ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя);

– СКЗИ должны обеспечивать реализацию процедур сброса ключей в случаях отсутствия штатной активности пользователей в соответствии с регламентом использования ключей;

– СКЗИ не должны предъявлять требований к ЭВМ по специальной проверке на отсутствие закладных устройств, если иное не оговорено в технической документации на конкретное средство защиты;

– СКЗИ не должны требовать дополнительной защиты от утечки по побочным каналам электромагнитного излучения.

При применении СКЗИ в АИС должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для всех элементов АИС.

Информационная безопасность процессов изготовления ключевой информации документов СКЗИ должна обеспечиваться комплексом

технологических, организационных, технических и программных мер и средств защиты.

Регламент генерации, распределения, хранения и уничтожения, поэкземплярного учета криптографических ключей, а также периодические проверки выполнения пользователями требований по хранению и эксплуатации криптографических ключей определяется «Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» от 13 июня 2001 г. №152. Данная Инструкция определяет единый на территории Российской Федерации порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных СКЗИ (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Использование СКЗИ должно осуществляться в полном соответствии с конструкторской и эксплуатационной документацией, представляемой производителем СКЗИ. Внутренний порядок применения СКЗИ в Учреждения должен включать:

– порядок ввода в действие;
– порядок эксплуатации;
– порядок восстановления работоспособности в аварийных случаях;
– порядок внесения изменений;
– порядок снятия с эксплуатации;
– порядок управления ключевой системой;
– порядок обращения с носителями ключевой информации.

5.7. Мероприятия по антивирусной защите информационных ресурсов Учреждения

Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы Учреждения от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей Учреждения к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

Основополагающими требованиями к системе антивирусной защиты Учреждения являются:

- решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях)

ничего не известно;

- решение задачи антивирусной защиты должно осуществляться в реальном времени.

Мероприятия, направленные на решение задач по антивирусной защите:

- необходимо проводить политику, требующую установки только лицензированного программного обеспечения;
- антивирусные программные средства должны регулярно обновляться и использоваться для профилактических проверок (желательно ежедневных);
- непрерывный контроль над всеми возможными путями проникновения вредоносных программ в ИТКС Учреждения, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИТКС;
- ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИТКС программного обеспечения ОС и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика ПО и других специализированных экспертных антивирусных служб.
- проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.
- необходимо проводить регулярную проверку целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;
- дискеты, диски, дисковые накопители любого типа неизвестного происхождения следует проверять на наличие вирусов до их использования;
- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения АИС компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;
- следует иметь планы обеспечения бесперебойной работы организации для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

В рамках создания системы антивирусной защиты информационных ресурсов Учреждения необходимо разработать следующие организационно-распорядительные и нормативно-технические документы:

- Положение об антивирусном контроле, включая определение основных целей и области применения системы антивирусной защиты, требования к персоналу, степень ответственности, структуру и необходимый уровень защищенности от вредоносных программ, статус и должностные обязанности сотрудников

Должностные инструкции администраторов и сотрудников безопасности, которые должны включать:

- Порядок установки и настройки средств антивирусной защиты;
- Порядок эксплуатации средств антивирусной защиты, в т.ч. обновление ПО, мониторинг и управление;
- Порядок действия в период вирусных эпидемий;
- Порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты;
- Порядок действия для устранения последствий заражений.
- Технологические инструкции

5.8. Мероприятия по обнаружению компьютерных атак на информационные ресурсы и телекоммуникационные системы Учреждения

Основополагающими требованиями к системе обнаружения компьютерных атак на информационные ресурсы и телекоммуникационные системы Учреждения являются:

- система обнаружения компьютерных атак должна быть сертифицирована;
- система обнаружения компьютерных атак должна быть способна выявлять атаки, направленные на нарушение конфиденциальности, целостности и доступности информационных ресурсов.

Система обнаружения компьютерных атак должна обеспечивать возможность выполнения следующих основных функций:

- выявление информационных атак на прикладном уровне стека TCP/IP посредством анализа пакетов данных, передаваемых в ИТКС;
- блокирование пакетов данных, нарушающих заданную политику безопасности;
- мониторинг трафика, циркулирующего на сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем;
- выявление аномалий сетевого трафика;
- оповещение администратора безопасности об обнаруженных атаках или аномалиях сетевого трафика.

5.9. Мероприятия по совершенствованию организационно-штатной структуры подразделений, отвечающих за обеспечение информационной безопасности Учреждения

Основные мероприятия по совершенствованию организационно-штатной структуры подразделений защиты информации:

- оснащение программно-техническими средствами для проведения контроля состояния ИБ в Учреждения
- проведение мероприятий по повышению квалификации сотрудников.

5.10. Мероприятия по повышению квалификации специалистов в области защиты информации

Подготовка и переподготовка пользователей и специалистов Учреждения по защите информации требует создание системы повышения уровня технической грамотности и информированности пользователей в области информационной безопасности, а также переподготовки специалистов по защите информации. Для этого необходимо регулярно проводить тренинги для персонала и контроль готовности новых сотрудников по применению правил информационной защиты, а также периодически осуществлять переподготовку специалистов подразделений защиты информации. Особенно важно проводить тренинги при изменении конфигурации информационной системы (внедрении новых технологий и прикладных автоматизированных систем, смены оборудования, операционной системы, ключевых приложений, принятии новых правил или инструкций и т.д.)

5.11. Мероприятия по внутреннему аудиту информационных систем Учреждения

Внутренний аудит информационных систем Учреждения производится сотрудниками, ответственными за информационную безопасность, по распоряжению руководителя Учреждения. Сроки и режим проведения внутреннего аудита устанавливаются руководителем Учреждения.

Целью внутреннего аудита является оценка текущего состояния системы информационной безопасности ИТКС, разработка или актуализация организационных и технических требований к системе информационной безопасности Учреждения, прогнозирование на основе этого требуемых затрат на ее поддержание и модернизацию.

Требования к системе информационной безопасности разрабатываются на основе анализа существующих угроз информационно-телекоммуникационной системы, идентификации существующих уязвимостей и оценки величины возможного ущерба.

Результаты аудита должны содержать отчёты по обеспечению безопасности информационной системы подразделения в целом или её логических компонентов. Описания, выявленные факты и рекомендации,

полученные в ходе проведения аудита, должны быть использованы для дальнейшей оценки защищенности информационной системы.

Аудит проводятся независимо от сотрудников, ответственных за функционирование общей системы поддержки. Необходимые проверки могут быть осуществлены как изнутри, так и извне информационной системы.

Комплексные проверки мер по обеспечению информационной безопасности проводятся не реже одного раза в год. Отдельные проверки систем на потенциальные повреждения осуществляются с периодичностью, необходимой для поддержания требуемого уровня оперативности статистических данных.