МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Разработка рекомендаций по повышению эффективности защиты конфиденциальной информации в образовательной организации

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
81,74% авторского текста

Работа рекомендована к защите
«26» декабря 2022 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Коновалов Юрий Александрович

Научный руководитель:
д.т.н., профессор
Дмитриев М.С.

Челябинск
2023

АННОТАЦИЯ
НА МАГИСТЕРСКУЮ ДИССЕРТАЦИЮ
Коновалова Юрия Александровича

Тема работы: «**Разработка рекомендаций по повышению эффективности защиты конфиденциальной информации в образовательной организации**»

Определены ключевые угрозы, уязвимости и риски информационной безопасности в образовательной организации Рассматривая информацию как объект информационных правоотношений, делается вывод: конфиденциальная информация – это информация, доступ к которой ограничивается в соответствии с законодательством РФ.

Рассмотрен порядок работы персонала с конфиденциальной информацией в образовательной организации и выявлены угрозы утечки конфиденциальной информации, а также предложены меры устранения угроз, выполнение которых позволит повысить эффективность средств защиты и сократит риск потери и искажения информации в образовательной организации.

Разработан комплекс предложений по совершенствованию организационных и технических мер защиты для образовательной организации конфиденциальной информации, включая алгоритм оценки эффективности мер и средств защиты конфиденциальной информации; порядок контроля эффективности системы защиты конфиденциальной информации; методику контроля защищенности конфиденциальной информации ИСПДн от несанкционированного доступа.

Магистрант_____ _____Коновалов Ю.А.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На сегодняшний день информация являешься важнейшим продуктом общественного производства, постоянно наращиваемый ресурс человечества.

Деятельность организаций неразрывно связана с получением и использованием различного рода информации. В современных условиях информация представляет собой товар, имеющий определенную ценность. Разглашение такой информации может привести к угрозам безопасности различной степени тяжести. Боязнь лишиться таких активов заставляет организации создавать различные системы защиты, в т.ч. и организационную, а главное - правовую.

В связи, с чем информация разделяется на три группы: информация для открытого пользования любым потребителем в любой форме; информация ограниченного доступа - только для органов, имеющих соответствующие законодательно установленные права (полиция, налоговая инспекция, прокуратура); информация только для работников (либо руководителей) организации.

Информация, относящаяся ко второй и третьей группам, является конфиденциальной и имеет ограничения в распространении. Часть этой информации составляет особый блок и может быть отнесена к коммерческой тайне.

Конфиденциальная информация является важнейшей составляющей любых информационных отношений. Вопросы правового регулирования по поводу использования и распространения информации в последнее время занимают одно из значительных мест в юридической литературе. Это обусловлено, прежде всего, тем, что содержание юридически значимой тайны заключается в том, что ее предмет образует информация, не предназначенная для широкого круга лиц, а ее разглашение может повлечь

нежелательные последствия для владельцев и обладателей тайны.

Проблема защиты конфиденциальной информации в организациях любой формы в настоящее время стоит наиболее остро, так как угрозы нарушения информационной безопасности носят глобальный характер. Способы реализации угроз информационной безопасности и формы их проявления постоянно совершенствуются, высокая технологичность этих угроз требует адекватных мер противодействия, предъявляет требования к квалификации специалистов по информационной безопасности, материально-техническому и кадровому обеспечению.

С этих позиций обусловливается актуальность настоящего исследования, на примере рассмотрения конфиденциальной информации в образовательной организации.

Анализ состояния проблемы позволил выявить *противоречие* между необходимостью обеспечения качественных методов и средств защиты конфиденциальной информации и отсутствием разработанных предложений по улучшению мер защиты конфиденциальной информации в образовательной организации МБУ ДО «ЦВР "Юность" г. Челябинска», для дальнейшего внедрения в систему защиты конфиденциальной информации.

Выявленное противоречие позволило сформулировать *проблему* необходимости разработки предложений по совершенствованию системы защиты конфиденциальной информации в образовательной организации.

Поиск путей решения проблемы определил *тему исследования*: «Защита конфиденциальной информации в образовательной организации».

Решение указанной проблемы определило *цель исследования* - рассмотрение особенностей работы с конфиденциальной информацией, а именно персональными данными; разработка предложений по совершенствованию мер системы защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска».

Объект исследования – Методическое обеспечение процесса защиты конфиденциальной информации в образовательной организации.

Предмет исследования - Методическое обеспечение процесса защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность".

Рабочее предположение диссертационного исследования заключается в следующем, что можно улучшать уровень защиты конфиденциальной информации, если при разработке комплекса предложений по защите конфиденциальной информации сделать уклон именно на организационные и технические меры.

Задачи исследования:

1. Изучить понятия, свойства, аспекты безопасности информации, ис-следовать основные источники правового регулирования конфиденциальной информации, рассмотреть организацию доступа и порядок работы персонала с персональными данными в образовательной организации, выявить угрозы и меры по предупреждению утечки конфиденциальной информации

2. Проанализировать меры и средства защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска»

3. Разработать предложения по совершенствованию организационных и технических мер защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска»

4. Оценить эффективность комплекса организационных и технических мер защиты конфиденциальной информации в МБУ ДО «ЦВР "Юность" г. Челябинска».

Для решения поставленных задач были использованы следующие *методы исследования:* изучение и анализ теоретико-методической литературы по теме исследования; документоведческий метод как анализ документации образовательного учреждения; анализ и сопоставление

имеющихся средств для защиты данных; анализ и классификация собранных данных с последующим моделированием и проектированием политики защиты конфиденциальной информации; метод апробации результатов; метод экспертной оценки качества разработанных мер защиты.

Теоретико-методологическая основа исследования – основные положения об обработке и защите персональных данных; научные, учебные, практические, методические рекомендации по организации защиты конфиденциальной информации ведущих специалистов в этой области таких как А.И. Алексенцев [22, 23] и Е.А. Степанов [67; 68].

Нормативно-правовая основа - Конституция как основном законе Российской Федерации [1]; статья 23 Конституции РФ гарантирует право на личную, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщении; ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 №149 [8]; основными в области безопасности конфиденциальной информации также являются законы РФ: «О государственной тайне» от 22 июля 2004 г. [4]; «О коммерческой тайне» от 29 июля 2004 (он содержит в себе информацию, составляющую коммерческую тайну, режим коммерческой тайны, разглашение информации, составляющую коммерческую тайну) [5]; «Об утверждении Перечня сведений конфиденциального характера» [9]; «О персональных данных» от 27 июля 2006 №152 – ФЗ [6]; Об утверждении Перечня сведении, которые не могут составлять коммерческую тайну" [10]; стандарт, закрепляющий основные термины и определения в области защиты информации - ГОСТ Р 50922-96 [21].

Основные *этапы исследования*:

На первом этапе формулировалась тема исследования, проводился сбор информации по теме исследования из различных источников,

осуществлялась формулировка гипотезы, постановка цели, задач.

Второй этап – в ходе данного этапа осуществлялся анализ методов и средств, которые задействуются в организации по защите персональных данных, а также проводился анализ научной литературы и отбор информации по теме исследования, осуществлялось написание и публикация научной статьи по теме исследования.

Третий этап заключался в том, что осуществлялась оценка эффективности разработанной политики по защите конфиденциальной информации, осуществлялся сбор и анализ данных, полученных в результате исследования, а также последующая оценка полученных результатов.

Положения, выносимые на защиту:

1. В ходе исследования обоснована необходимость пересмотра мер и средств защиты конфиденциальной информации, а именно персональных данных, в образовательной организации.

2. Для улучшения уровня защиты персональных данных в образовательной организации следует пересмотреть организационные и технические меры защиты и усовершенствовать их.

3. В ходе исследования выдвинута гипотеза: при отсутствии практически-усовершенствованной политики по защите конфиденциальной информации в образовательной организации, не осуществляется полноценная защита персональных данных. Гипотеза была выдвинута в ходе преддипломной практики и анализа организационно-правовых, технических и физических мер защиты конфиденциальной информации на базе исследования.

4. На основании изложенного, разработан комплекс предложений организационного и технического мер по защите конфиденциальной информации и выявлена эффективность разработанного комплекса.

Сформулированные выше задачи определили структуру дипломной работы, которая состоит из введения, трех глав, заключения, списка литературы (76 наименований). В тексте работы представлено 2 таблицы, 12 рисунков.

Во введении обоснована актуальность темы исследования, представлен научный аппарат исследования темы.

В теоретической главе раскрыты понятия, свойства, аспекты безопасности конфиденциальной информации, а также основные источники правового регулирования конфиденциальной информации.

В практической главе разработан комплекс предложений по совершенствованию организационных и технических мер защиты конфиденциальной информации для образовательной организации, проведена оценка эффективности комплекса предложений.

База исследования: МБУ ДО «ЦВР "Юность" г. Челябинска».

ГЛАВА 1. ИНФОРМАЦИЯ КАК ОБЪЕКТ ИНФОРМАЦИОННЫХ ПРАВООТНОШЕНИЙ

1.1. Информация: понятия, свойства, аспекты безопасности

На сегодняшний день информация является важнейшим ресурсом и одной из движущих сил развития человеческого общества. Информационные процессы, происходящие в материальном мире, живой природе и человеческом обществе, изучаются всеми научными дисциплинами от философии до маркетинга.

Исторически сложилось так, что исследованием непосредственно информации занимаются две комплексные отрасли науки — кибернетика и информатика.

Информация как объект правоотношений должна быть конкретизирована, организована должным образом, «привязана» к ситуации и конкретному виду отношений, классифицирована по видам и тому подобным образом «подготовлена» для осуществления по ее поводу действий, регулируемых нормами права.

В практическом смысле определение информации дал С.И. Ожегов: информация — это:

1. сведения об окружающем мире и протекающих в нем процессах;
2. сообщения, осведомляющие о положении дел, о состоянии чего-либо.

До середины 20-х гг. XX в. под информацией (в переводе с латыни — ознакомление, разъяснение, изложение) действительно понимались «сообщения и сведения», передаваемые людьми устным, письменным или другим способом. А уже с середины XX в. информация определяется как общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в

животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму как генетическая информация, одно из основных понятий кибернетики [73].

В связи с развитием средств связи и телекоммуникаций, вычислительной техники и их использованием для обработки и передами информации возникла необходимость измерять количественные характеристики информации. Появились разные теории, и понятие «информация» начало наполняться разным содержанием.

В 1949 г. К. Шеннон и У. Уивер опубликовали статью «Математическая теория связи», в которой были предложены вероятностные методы для определения количества передаваемой информации. Однако такие методы описывают лишь знаковую структуру информации и не затрагивают заложенного в ней смысла (в сообщении, сведениях) [39].

В 1948 г. Н. Винер предложил «информационное видение» кибернетики как науки об управлении в живых организмах и технических системах. Под информацией стали понимать не просто сведения, а только сведения новые и полезные для принятия решения, обеспечивающего достижение цели управления [37]. Остальные сведения не считались информацией.

На сегодняшний день определений информации существует множество, причём академик Н. Н. Моисеев даже полагал, что в силу широты этого понятия нет и не может быть строгого и достаточно универсального определения информации [73].

В международных и российских стандартах даются следующие определения:

– знания о предметах, фактах, идеях и т. д., которыми могут обмениваться люди в рамках конкретного контекста;

– знания относительно фактов, событий, вещей, идей и понятий, которые в определённом контексте имеют конкретный смысл;

– сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации [35].

Хотя информация должна обрести некоторую форму представления, то есть превратиться в данные, чтобы ею можно было обмениваться, информация есть в первую очередь интерпретация такого представления. Поэтому в строгом смысле информация отличается от данных, хотя в неформальном контексте эти два термина очень часто используют как синонимы.

Термин «информация» и связанные с ним термины сегодня широко применяются и законодателем.

Различают основные виды информации, которые *классифицируют* по ее форме представления, способам ее кодирования и хранения:

– графическая

– звуковая (акустическая)

– текстовая – кодирует речь человека с помощью специальных символов – букв (для каждого народа свои)

– числовая – кодирует количественную меру объектов и их свойств в окружающем мире с помощью специальных символов – цифр

– видеоинформация – способ хранения «живых» картин окружающего мира, который появился с изобретением кино.

По степени доступа информация подразделяется на открытую и информацию ограниченного доступа, распространение которой возможно в условиях конфиденциальности или секретности (hис. 1.1).

Информация

Открытая (общедоступная):

– Информация как объект гражданских прав (произведения, патенты и авторские свидетельства, другая информация, создаваемая с целью извлечения прибыли);

– Массовая информация;

– Информация о выборах, референдуме;

– Официальные документы;

– Обязательно представляемая информация;

– Другая открытая информация.

Ограниченного доступа:

– Государственная тайна, служебная тайна

– Ноу-хау (секреты производства) и коммерческая тайна

– Персональные данные (в порядке защиты личной тайны)

– Другие виды тайн.

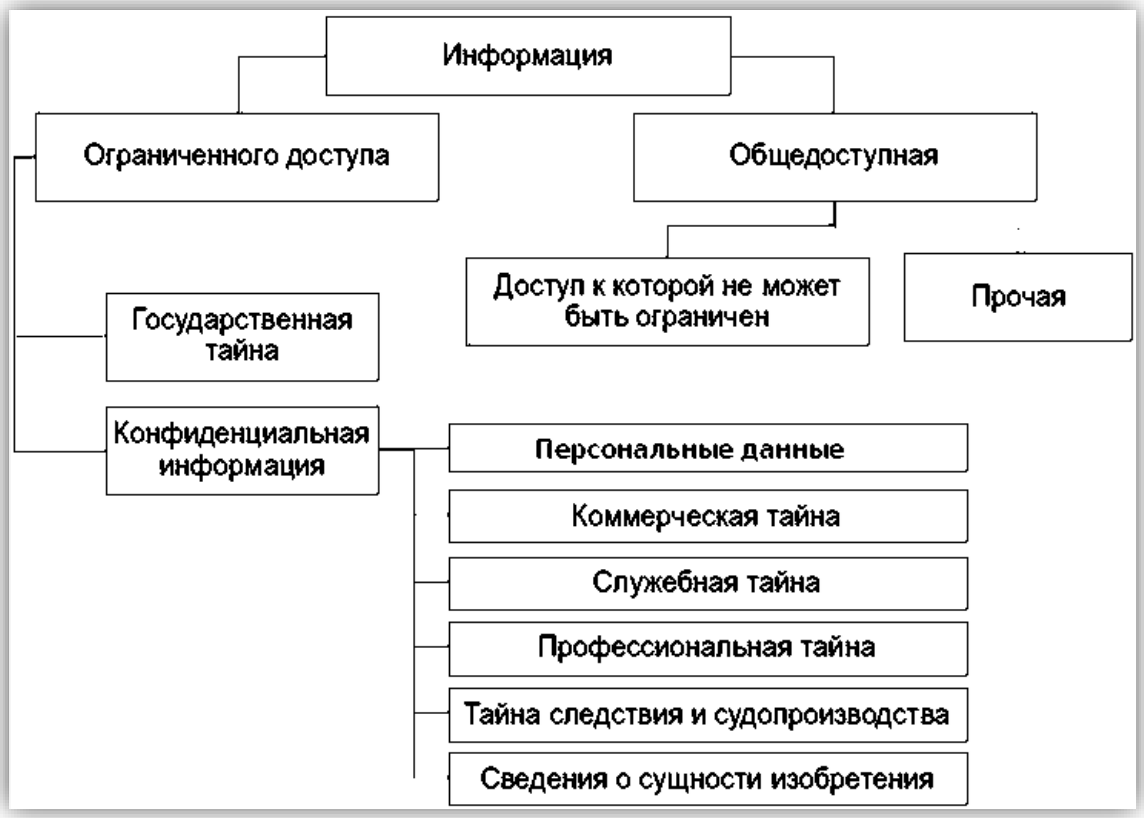

Рис. 1.1 – Подразделение информации

Также информация, как и любой объект, обладает свойствами, наиболее важными являются [40]:

– Объективность. Объективная информация – существующая независимо от человеческого сознания, методов ее фиксации, чьего-либо мнения или отношения.

– Достоверность. Информация, отражающая истинное положение дел, является достоверной. Недостоверная информация чаще всего приводит к неправильному пониманию или принятию неправильных решений. Устаревание информации может из достоверной информации сделать недостоверную, т.к. она уже не будет отражением истинного положения дел.

– Полнота. Информация является полной, если она достаточна для понимания и принятия решений. Неполная или избыточная информация может привести к задержке принятия решения или к ошибке.

– Точность информации – степень ее близости к реальному состоянию объекта, процесса, явления и т. п.

– Ценность информации зависит от ее важности для принятия решения, решения задачи и дальнейшей применимости в каких-либо видах деятельности человека.

– Актуальность. Только своевременность получения информации может привести к ожидаемому результату.

– Понятность. Если ценную и своевременную информацию выразить непонятно, то она, скорее всего, станет бесполезной. Информация будет понятной, когда она, как минимум, выражена понятным для получателя языком.

– Доступность. Информация должна соответствовать уровню восприятия получателя. Например, одни и те же вопросы по-разному излагаются в учебниках для школы и вуза.

– Краткость. Информация воспринимается гораздо лучше, если она представлена не подробно и многословно, а с допустимой степенью сжатости, без лишних деталей. Краткость информации незаменима в справочниках, энциклопедиях, инструкциях. Логичность, компактность, удобная форма представления облегчает понимание и усвоение информации.

Рассмотрим аспекты информационной безопасности, можно выделить следующие:

Целостность информации. Целостность информации – это её физическая сохранность, защищённость от разрушения и искажения, а также её актуальность и непротиворечивость.

Целостность информации подразделяется на:

– статическую

– динамическую.

Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации.

Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными и так далее.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Доступность информации

Доступность информации – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Доступность информации подразумевает, что субъект информационных отношений (пользователь) имеет возможность за приемлемое время получить требуемую информационную услугу.

Например, создавая информационную систему с информацией об обучающихся образовательной организации, мы рассчитываем, что с помощью этой системы в любое время в течение нескольких секунд сможем получить требующуюся информацию (список студентов любой группы, полную информацию о конкретном студенте и так далее).

Конфиденциальность информации

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность информации – это гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Конфиденциальная информация – это информация, на доступ к которой имеет право ограниченный круг лиц.

Если же доступ к конфиденциальной информации получает лицо, не имеющее такого права, то такой доступ называется несанкционированным и

рассматривается как нарушение защиты конфиденциальной информации. Лицо, получившее или пытающееся получить несанкционированный доступ к конфиденциальной информации, называется злоумышленником.

Обеспечение конфиденциальности информации является наиболее проработанным разделом информационной безопасности.

Конфиденциальная информация подразделяется на:

– предметную,
– служебную.

Предметная информация - это сведения о какой-то области реального мира, которые, собственно, и нужны злоумышленнику, например, чертежи подводной лодки или сведения о месте нахождения.

Служебная информация не относится к конкретной предметной области, а связана с параметрами работы определенной системы обработки данных. К служебной информации относятся в первую очередь пароли пользователей для работы в системе. Получив служебную информацию (пароль), злоумышленник с ее помощью может затем получить доступ к предметной конфиденциальной информации.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Необходимо представлять, откуда могут исходить и в чем состоять угрозы информационной безопасности, какие меры могут быть предприняты для защиты информации, и уметь грамотно применять эти меры.

1.2. Основные источники правового регулирования конфиденциальной информации

Обеспечение защиты конфиденциальной информации складывается из следующих составляющих:

1. Нормативные правовые акты РФ.
2. Нормативно-методические и методические документы.
3. Стандарты.

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

– Акты федерального законодательства

– Международные договоры РФ;

– Конституция РФ;

– Законы федерального уровня (включая федеральные конституционные законы, кодексы);

– Указы Президента РФ;

– Постановления правительства РФ;

– Нормативные правовые акты федеральных министерств и ведомств;

– Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Рассмотрим примеры:

Основные направления правового регулирования информационных отношений - конституционное и гражданско-правовое. Ч. 4 ст. 29 Конституции РФ закрепляет право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом [1]. Перечень сведений, составляющих государственную тайну, определяется соответствующим федеральным законом. Этому праву

корреспондирует общая обязанность органов государственной власти и местного самоуправления, располагающих такого рода информацией, предоставлять ее по соответствующим запросам.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" - назначение закона обеспечение защиты информации, регулирования отношений при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации, за исключением отношений в области охраны результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации [4].

Пункт 3 ст. 5 Федерального закона № 149 - ФЗ об информации содержит классификацию информации в зависимости от порядка ее предоставления или распространения. Так, по этому основанию информация подразделяется [8]:

1. на информацию, свободно распространяемую, например, посредством средств массовой информации;

2. на информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3. на информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4. на информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Конфиденциальная информация определена в п. 7 ст. 2 ФЗ № 149 через требование не передавать такую информацию третьим лицам без согласия ее обладателя [4]. Также данный Федеральный закон напрямую относит к категории конфиденциальной информации персональные данные (информацию о гражданах).

Федеральным законом № 152-ФЗ от 27 июля 2006 "О персональных данных" регулируются отношения, связанные с обработкой персональных данных федеральными органами государственной власти, органами государственной власти субъектов РФ, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими и физическими лицами с использованием средств автоматизации или без их использования, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации [6].

Федеральные законы "О коммерческой тайне", "Об информации, информационных технологиях и о защите информации" и часть 4 ГК РФ - ввели, как говорилось выше, и новые понятия, и изменили содержание некоторых прежних понятий, относящихся к данному вопросу. Ст. 139 ГК РФ, определявшая коммерческую тайну, отменена.

В ст. 3 Федерального Закона № 98-ФЗ "О коммерческой тайне" коммерческая тайна определяется как режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду[13].

Федеральные законы от 06 апреля 2011 г. № 63-ФЗ "Об электронной подписи" и от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи" - данные законы призваны обеспечить конфиденциальность информации в электронном виде - подписи, которая рассматривается как личная подпись субъекта.

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании" - закон призван обеспечить защиту сведений,

составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют государственную тайну, продукции (работ, услуг) и объектов, для которых устанавливаются требования, связанные с обеспечением ядерной и радиационной безопасности в области использования атомной энергии, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации, захоронения указанной продукции и указанных объектов (ст. 5 ФЗ № 184-ФЗ).

Федеральный закон от 8 августа 2001 г. № 128-ФЗ "О лицензировании отдельных видов деятельности" - закон регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, юридическими лицами и индивидуальными предпринимателями в свете обеспечения защиты конфиденциальной информации при осуществлении лицензирования отдельных видов деятельности [12].

Иные федеральные законы в том или ином аспекте также могут регулировать деятельность, касающуюся информации, информационных технологий и защиты информации. Так, глава 13 Кодекса РФ об административных правонарушениях № 195-ФЗ от 30 декабря 2001 г. устанавливает ответственность за административные правонарушения в области связи и информации.

В числе нормативных правовых актов, частично регулирующих рассматриваемые отношения, следует назвать также Закон "Об архивном деле в Российской Федерации" [3]. Пользователь архивных документов имеет право использовать, передавать, распространять информацию, содержащуюся в них, а также копии архивных документов для любых

законных целей и любым законным способом. Кроме того, приняты и иные нормативные правовые акты в данной области.

Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти" - данное постановление регламентирует порядок обращения и работы с конфиденциальной информацией федеральными органами исполнительной власти с целью предотвращения угрозы утечки информации и обеспечения защиты информации [16].

Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных". Положение содержит требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПД) [13].

Постановления: Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 "О лицензировании деятельности по технической защите конфиденциальной информации" [12] и Постановление Правительства Российской Федерации от 31 августа 2006 г. № 532 "О лицензировании деятельности но разработке и (или) производству средств защиты конфиденциальной информации" призваны обеспечить защиту конфиденциальной информации путем обязательного лицензирования технических средств защиты [12].

В завершении анализа нормативно правовых норм можно прийти к выводу, что конфиденциальная информация – это информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную, профессиональную или личную тайны, охраняющиеся её владельцем.

Вывод по Главе 1

В первой главе было изучено понятие информации, выявлены её свойства. Стало известно, что выделяют такие аспекты информационной безопасности, как целостность, доступность и конфиденциальность.

В первой главе рассмотрены основные источники правового регулирования конфиденциальной информации.

Отношения по поводу информации в целом и конфиденциальной информации в частности, регулируются правом. При этом информация как таковая и конфиденциальная информация являются предметом регулирования различных отраслей права и нормативных правовых актов РФ, важнейшее место среди которых занимает Конституция РФ.

Также было выявлено, что обеспечение защиты конфиденциальной информации складывается из следующих составляющих:

1. Нормативные правовые акты РФ
2. Нормативно-методические и методические документы
3. Стандарты.

Кроме того в первой главе были проанализированы нормативно-правовые акты Российской Федерации в области информационной безопасности и было выяснено, что Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите и информации" напрямую относит к категории конфиденциальной информации *персональные данные*. Также важным является Федеральный закон № 152-ФЗ от 27 июля 2006 "О персональных данных", в котором регулируются отношения, связанные с обработкой персональных данных федеральными органами государственной власти, органами государственной власти субъектов РФ.

Рассматривая в главе информацию как объект информационных

правоотношений, можно сделать вывод, что *конфиденциальная информация* – это информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

ГЛАВА 2. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1. Организация доступа и порядок работы персонала с конфиденциальной информацией в образовательной организации

В каждой образовательной организации (далее – Организация) разрабатывается Положение о конфиденциальной информации, с целью регулирования порядка распространения и защиты конфиденциальной информации.

В основе данного Положения лежит Конституция РФ, федеральный закон № 149-ФЗ от 27.07.2006 года «Об информации, информационных технологиях и защите информации», федеральный закон № 98-ФЗ от 29.07.2004 года «О коммерческой тайне», положение статьи 1464 Гражданского Кодекса РФ, статей 102 и 313 Налогового Кодекса РФ, статьи 7 федерального закона № 152-ФЗ от 27.07.2006 года «О персональных данных». Настоящее положение является локальным актом Организации, обязательным для соблюдения всеми работниками, как основными, так и совместителями.

К конфиденциальной информации образовательной организации (далее Организация) относятся [47]:

– персональные данные (далее – ПДн) работников, обучающихся и их родителей, в соответствии с нормами 152-ФЗ от 27.07.2006 года и Положением о порядке использования и хранения ПДн, являющимся локальным актом организации;

– сведения о финансово-хозяйственной деятельности организации, за исключением информации о количестве и общей сумме заключенных гражданско-правовых договоров, подлежащих обязательному размещению на официальных сайтах в сети «Интернет» в соответствии с законодательством о контрактной системе и законодательстве в сфере закупок;

– сведения о доходах работников Организации, за исключением, установленных федеральным законодательством для Руководителя Организации или лиц, предоставление сведений о доходах которых обязательно в рамках судебного или исполнительного производства;

– сведения бухгалтерского баланса;

– сведения, содержащийся в поступающих по почте (в том числе, в электронной форме) документах от вышестоящих и контролирующих организаций;

– внутренние документы Организации (приказы по основной деятельности, переписка с контрагентами по договорам, жалобы от участников образовательного процесса и др.);

– сведения о поступлении и расходовании бюджетных средств;

– сведения о типе и характеристиках компьютерного оборудования и установлению программного обеспечения;

– коды и пароли доступа;

– сведения о личной жизни сотрудников, а так же сведения о состоянии их здоровья;

– коммерческая, служебная и банковская тайна;

– содержание регистров бухгалтерского учета;

– содержание внутренней бухгалтерской отчетности;

– сведения об открытых в кредитных организациях расчетных и иных счетах, в том числе в иностранной валюте, о движении средств по этим счетам, и об остатке средств на этих счетах, сведения об имеющихся вкладах в банках, в том числе в иностранной валюте;

– сведения о методах управления Организацией.

Устав Организации, сведения о лицензировании, локальные акты, регулирующие образовательную деятельность (за исключением персональных данных обучающихся), прейскурант на оказание дополнительных платных услуг, являются открытой к доступу информацией и подлежат обязательному размещению на официальном сайте образовательной организации.

Обращение с конфиденциальной информацией

Конфиденциальная информация подлежит обработке, хранению и защите. Каждый сотрудник образовательной организации вправе использовать по своему усмотрению в ходе работы сведения, являющиеся конфиденциальными, самостоятельно определяя способ и степень их использования, в то же время учитывая, что информация с ограниченным доступом не подлежит публичному обнародованию, передаче сторонним физическим и юридическим лицам, включая сотрудников организации, которым данная информация не предназначена и напрямую не затрагивает их интересы.

Иначе говоря, использование конфиденциальной информации образовательной организации, его работников, обучающихся и их родителей (законных представителей) допускается только теми работниками Организации, которым доступ к такой информации необходим в силу выполняемых ими функций.

Сотрудник Организации без разрешения директора не вправе

передавать сведения, ставшие ему известными в ходе работы, другим сотрудникам, которым данная информация не предназначена и напрямую не затрагивает их интересы.

При приеме на работу, работники письменно ознакомляются с настоящим положением, обязуясь таким образом хранить конфиденциальность полученных ими в ходе работы сведений и защищать информацию от передачи третьим лицам. Контрагенты по договорам, в процессе подписания договора, уведомляются о необходимости сохранения конфиденциальности, ставшей им известной информации, о чем может быть прописано в договоре.

Предоставление конфиденциальной информации Организации третьим лицам возможно не иначе как с разрешения директора Организации, а конфиденциальной информации работников Организации, обучающихся и их родителей (законных представителей) возможно только с их письменного согласия, также передача конфиденциальной информации допускается только по письменному запросу вышестоящих и контролирующих органов, судов, службы судебных приставов, службы исполнения наказаний, правоохранительных органов, прокуратуры.

Защита конфиденциальной информации

Организация состоит в принятии комплекса мер, направленных на ограничение доступа к конфиденциальной информации третьих лиц, на предотвращение несанкционированного разглашения конфиденциальной информации, выявление нарушений режима конфиденциальной информации, пресечение нарушений режима конфиденциальной информации, привлечение лиц, нарушающих режим конфиденциальной информации к установленной ответственности. Обязательным условием трудовых договоров, заключаемых с сотрудниками Организации, является условие о соблюдении сотрудником служебной и коммерческой тайны.

Каждый сотрудник Организации при принятии на работу предупреждается под расписку об ответственности за нарушение режима служебной и коммерческой тайны. В случае попытки посторонних лиц получить от сотрудника сведения, относящиеся к коммерческой тайне Организации, сотрудник обязуется незамедлительно сообщить об этом Директору Организации в письменной или устной форме. Заключаемые Организацией в лице любых уполномоченных лиц договоры должны содержать условие о сохранении контрагентами конфиденциальности.

За несанкционированное разглашение конфиденциальной информации, неправомерное использование которой может нанести материальный и моральный ущерб Организации либо деловым партнерам и гражданам, на виновное лицо в соответствии с Трудовым кодексом РФ может быть наложено дисциплинарное взыскание (вплоть до увольнения) [17], а также взысканы убытки согласно ст. 139 Гражданского кодекса РФ [2]. Кроме того, виновное лицо может быть привлечено в установленных законом случаях к административной ответственности, а также к уголовной ответственности.

1.2. Угрозы и меры по предупреждению утечки конфиденциальной информации

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Можно сказать, что сотрудники Организации являются главным источником различных угроз в работе с конфиденциальной информацией. Способы осуществления угроз информационной безопасности могут быть различны. Сотрудник, например, может действовать целенаправленно или неосознанно по собственной инициативе, а также под чьим-то влиянием [61].

Основные виды реализации угроз информационной безопасности:

1. завладение конфиденциальными данными, вследствие чего у злоумышленника оказывается их копия. Получение конфиденциальной информации может происходить при помощи разных методов: подслушивание разговоров сотрудников данной Организации, использование технических средств (подслушивающих устройств), копирование секретных данных.

2. кража служебных документов, в результате чего злоумышленник овладевает секретными сведениями, а предприятие в свою очередь их лишается.

3. повреждение или полная ликвидация информации, в результате чего злоумышленник приносит вред предприятию.

4. изменение работником секретной информации, вследствие чего специалисты предприятия могут принять неверные руководящие действия.

Таким образом, вышесказанное ещё раз подтверждает, что самой часто встречающейся причиной осуществления угроз по защите безопасности является безответственность сотрудников организации. Это прослеживается в нарушении сотрудников условий по защите информационной безопасности, что приводит к утечке секретной информации [71].

Утечка информации – это несанкционированный доступ к закрытым данным и неконтролируемое распространение секретных сведений в результате их разглашения.

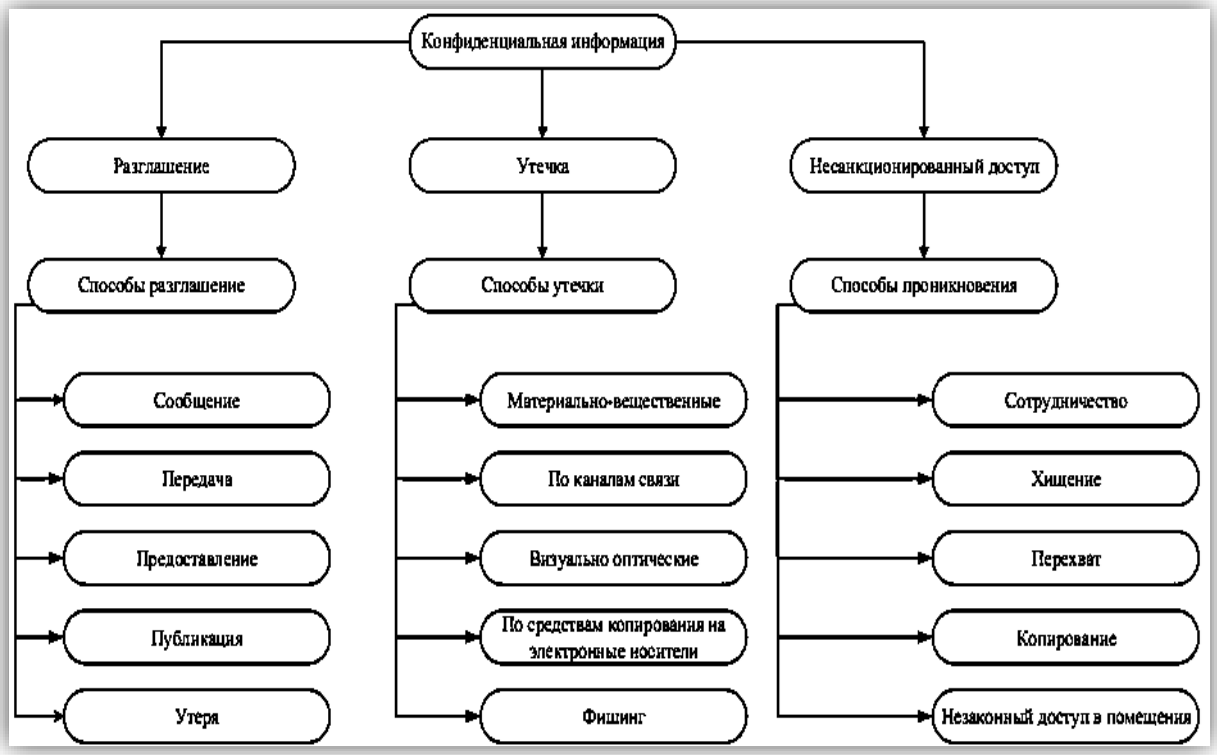

Рис. 2.1 – Способы утечки конфиденциальной информации

Главные причины утечки информации:

– нарушение сотрудниками требований в работе с источниками служебной информации и правил использования систем защиты;

– недочёты в конструировании систем защиты;

– проведение злоумышленником технической и агентурной разведок.

Виды утечки информации:

– разглашение;

– несанкционированный доступ к информации;

– получение секретной информацией разведками.

Все каналы утечки конфиденциальной информации делятся на косвенные и прямые. Косвенные каналы не требуют прямого доступа к техническим средствам информации. Прямые каналы – непосредственный доступ к источнику информации.

Примеры косвенных каналов утечки:

– похищение или потеря носителей информации;

– фотографирование, прослушивание на расстоянии;

– перехват электромагнитных излучений.

Примеры прямых каналов утечки [66]:

– утечка информации из-за нарушения сотрудниками служебных требований;

– непосредственное копирование.

Одна из самых сложно решаемых угроз любой информационной системы — присутствие «инсайдера», официального специалиста организации, имеющего доступ к конфиденциальной информации, и, по каким-либо причинам (психологического характера или с целью наживы) осуществляющего кражу такой информации.

Соответственно, для предотвращения этой угрозы ведется планомерное обучение сотрудников и педагогов образовательной организации информационной культуре на заседаниях педагогического совета и тематических заседаниях методических комиссий по всем дисциплинам. Прививаются понятия «корпоративной» этики, ведется

мониторинг психологической стабильности работников, в коллективе поддерживается «теплый» психологический климат.

Защита персональных данных представляет собой комплекс мер технического, организационного, организационно-технического, морально-этнического и правового характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу – субъекту персональных данных (работнику) [71].

Определение актуальных (наиболее опасных) угроз осуществляется на основе анализа расположения объектов защиты и структуры построения ИС, а также информационных ресурсов, подлежащих защите (рис. 2.2) [8].

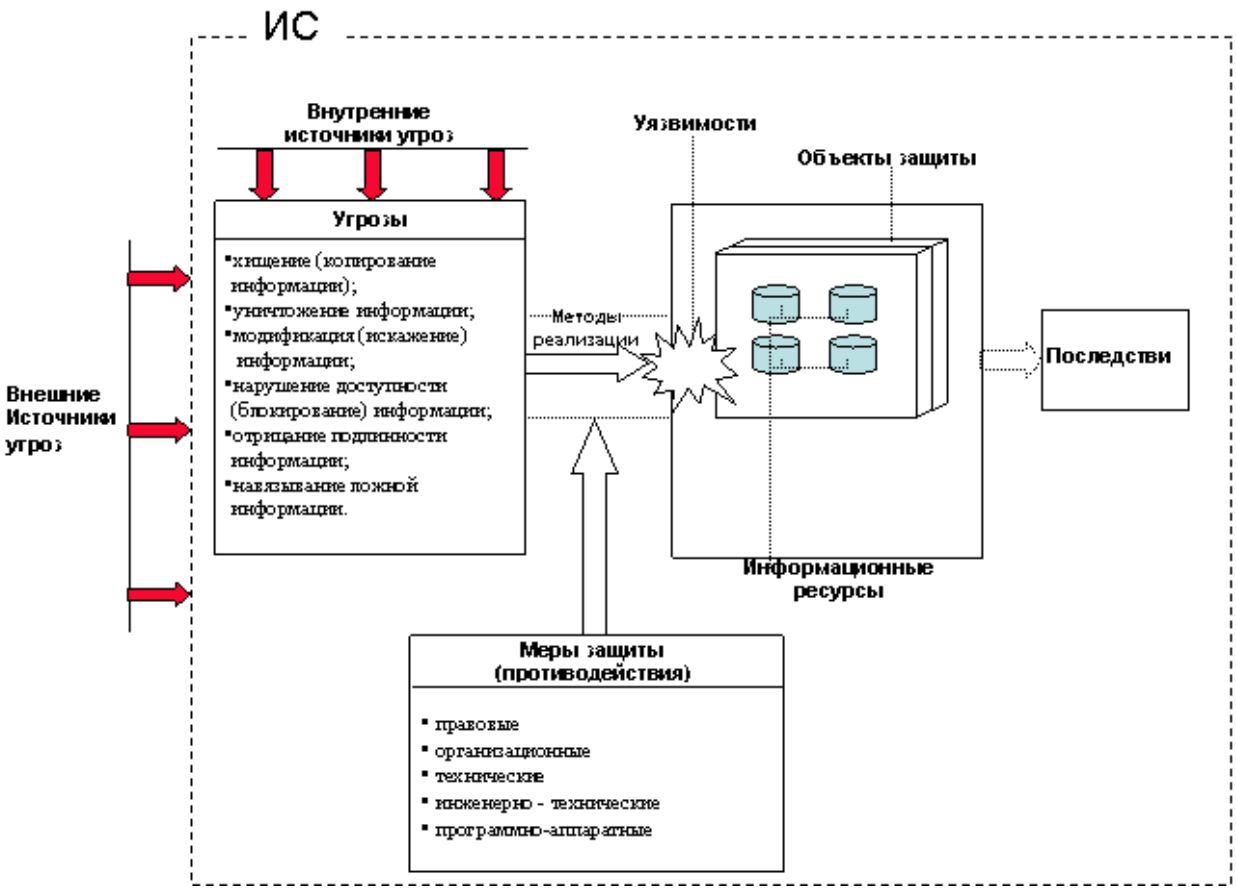

Рис. 2.2 – Модель реализации угроз информационной безопасности ИС

Во исполнение Закона в первую очередь должны быть разработаны: приказ об ответственных лицах по сотрудникам, а также положение о

защите персональных данных. Такое положение является основным локальным актом, его отсутствие может быть квалифицировано государственным органом контроля и надзора как нарушение работодателем трудового законодательства. Этот документ определяет: порядок обработки персональных данных работников; обеспечение защиты прав и свобод работников при обработке их персональных данных; ответственность лиц, имеющих доступ к персональным данным работников, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных работников.

Далее, для предупреждению утечки конфиденциальной информации может быть создана рабочая группа. Поскольку главным условием защиты персональных данных является четкая регламентация функций сотрудников.

Рабочей группой проводятся следующие мероприятия: уточняются все ситуации, когда требуется проводить обработку ПДн, четко выделяются процессы, в которых обрабатываются ПДн, продумывается разработка пакета организационно-распорядительных документов для обеспечения полноценной защиты.

В общем, защита персональных данных работников образовательной организации сводится к созданию режима обработки персональных данных, включающего:

– создание внутренней документации по работе с персональными данными;

– организацию системы защиты персональных данных;

– внедрение технических мер защиты персональных данных.

Также не стоит забывать, что специфика учебной организации такова, что обработке подвергаются не только данные сотрудников, но и обучающихся и их родителей. Соответственно, должна быть разработана и

внедрена система получения согласия родителей на обработку персональных данных их самих и их детей (в случае, если обучающийся совершеннолетний, то он сам дает такое согласие).

С технической стороны защиты персональных данных необходимо использовать единую базу данных с организацией доступа по паролю. Также, необходимо определить возможные каналы утечки информации и возможные угрозы информационной системе, построить модель угроз нарушителя, и уже на их основании строить модель защиты. Проделать эту работу неспециалисту чрезвычайно трудно, соответственно возникает проблема – либо обучаться самостоятельно, либо платить деньги за обучение сотрудника, либо полностью передать вопрос защиты ПДн стороннему интегратору. Не стоит забывать, что еще один необходимый шаг в организации технической стороны защиты персональных данных – обязательная сертификация программного обеспечения для ИСПД [72].

Если осуществляется обработка ПДн, то обязана обеспечиваться и защита. Поскольку потенциальные угрозы безопасности информации весьма многообразны, следовательно цели защиты информации могут быть достигнуты путем создания комплексной системы защиты информации, под которой понимается совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в образовательной организации.

Итак, исходя из вышесказанного, можно подвести итог и составить перечень методов и средств обеспечения требуемого уровня защищенности персональных данных.

1. Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. *Все меры обеспечения безопасности ИСПДн подразделяются на:*

1.1. Законодательные (правовые) меры защиты. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

1.2. Морально-этические меры защиты. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

1.3. Организационные и административные меры защиты. Организационные и административные меры защиты - это меры организационного характера, регламентирующие процессы

функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации. К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн. На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн.

1.4. Физические меры защиты. 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 зданий,

помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

1.5. Аппаратно-программные средства защиты ПДн. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Взаимосвязь рассмотренных выше мер обеспечения безопасности приведена на рис. 3.1.

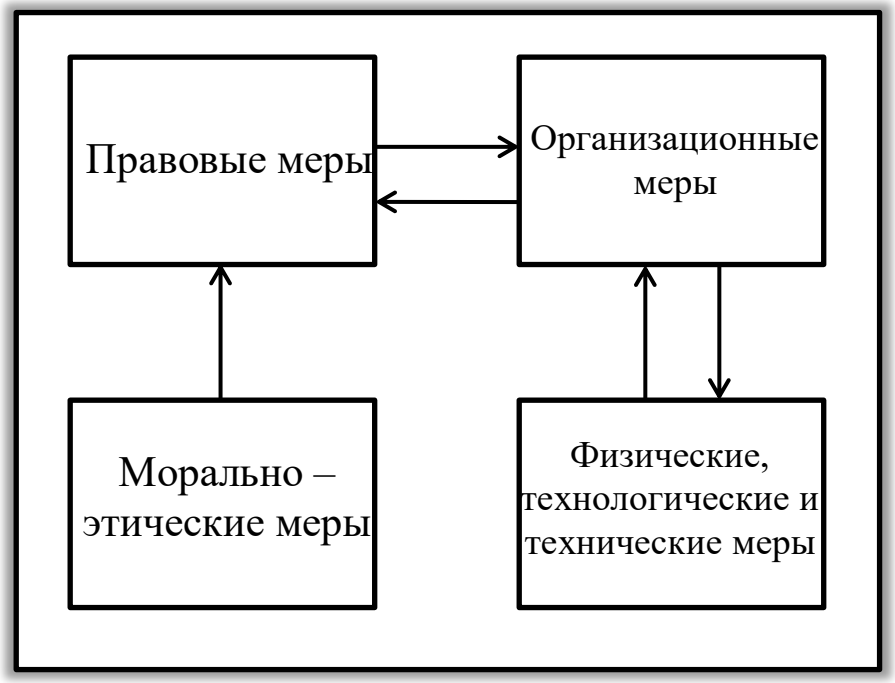

Рис. 3.1 –Взаимосвязь мер обеспечения информационной безопасности

2. Контроль эффективности системы защите персональных данных (далее – СЗРДн) должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

3. Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

4. Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

5. Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

6. Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководитель образовательной организации. Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.

7. Сфера ответственности руководителя включает следующие направления обеспечения безопасности ПДн:

7.1. Планирование и реализация мер по обеспечению безопасности ПДн;

7.2. Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;

7.3. Контроль защищенности ИТ инфраструктуры образовательной организации от угроз ИБ путем;

7.4. Обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;

7.5. Предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

7.6. Анализ угроз безопасности ПДн;

Достоинства и недостатки различных видов мер защиты.

Законодательные и морально-этические меры

Эти меры определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение.

Законодательные и морально-этические меры противодействия, являются универсальными в том смысле, что принципиально применимы для всех каналов проникновения.

В некоторых случаях они являются единственно применимыми, как, например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией.

Организационные меры

Очевидно, что в организационных структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто бессмысленно. Прежде всего, надо решить правовые и организационные вопросы. Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем. Организационные

меры - это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. Однако это вовсе не означает, что систему защиты необходимо строить исключительно на их основе.

Этим мерам присущи серьезные *недостатки*, такие как:

– низкая надежность без соответствующей поддержки физическими, техническими и программными средствами (люди склонны к нарушению любых установленных дополнительных ограничений и правил, если только их можно нарушить);

– дополнительные неудобства, связанные с большим объемом рутинной и формальной деятельности.

Организационные меры необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными физическими и техническими средствами.

Физические и технические средства защиты

Физические и технические средства защиты призваны устранить недостатки организационных мер, поставить прочные барьеры на пути злоумышленников и в максимальной степени исключить возможность неумышленных (по ошибке или халатности) нарушений регламента со стороны персонала и пользователей системы.

Даже при допущении возможности создания абсолютно надежных физических и технических средств защиты, перекрывающих все каналы, которые необходимо; перекрыть, всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих средств (администратора АС, администратора безопасности и т.п.). Вместе с самими средствами

защиты эти люди образуют так называемое ядро безопасности. В этом случае, стойкость системы безопасности будет определяться стойкостью персонала из ядра безопасности системы, и повышать ее можно только за счет организационных (кадровых) мероприятий, законодательных и морально-этических мер. Но, даже имея совершенные законы и проводя оптимальную кадровую политику, проблему защиты все равно решить до конца не удастся.

– Во-первых, потому, что вряд ли удастся найти персонал, в котором можно было быть абсолютно уверенным, и в отношении которого невозможно было бы предпринять действий, вынуждающих его нарушить запреты.

– Во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

Вывод по Главе 2

Во второй главе был рассмотрен порядок работы персонала с конфиденциальной информацией в образовательной организации и выявлены угрозы утечки конфиденциальной информации, а также предложены меры устранения угроз, выполнение которых позволит повысить эффективность средств защиты и сократит риск потери и искажения информации в образовательной организации.

Для решения проблемы сохранности конфиденциальной информации необходимо применение законодательных, организационных, морально-этических и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в образовательной организации приобретает все большее значение. Также у каждых из мер защиты бывают свои достоинства и недостатки, которые тоже важно учитывать, при

разработке системы защиты.

Технический аспект связан с выбором программного обеспечения, организационный – с проведением мероприятий для реализации закона № 152-ФЗ «О персональных данных», а документационный – с созданием локальных актов образовательной организации.

Таким образом, можно говорить о том, что обеспечение информационной безопасности учебного процесса в современных условиях становится одним из главных видов деятельности образовательной организации. Поэтому на основании этого заключения, в Главе 3 диссертационного исследования описывается процесс разработки рекомендаций по совершенствованию мер защиты конфиденциальной информации, а также их дальнейшая эффективность.

Глава 3

3.1

Федеральным законом № 152 и Приказом ФСТЭК № 21 предусмотрена оценка эффективности мер по обеспечению безопасности ПДн — комплекс мероприятий организационно-технического характера, по итогам которого составляется официальный протокол. На его основании можно начинать эксплуатацию ИСПДн.

В нормативно-правовых актах предусмотрено два способа организации проверочных мероприятий — усилиями самой организации либо путем привлечения сторонних специалистов, причем во втором случае допускается сотрудничество исключительно с лицензиатами ФСТЭК.

Цели и особенности оценки эффективности защиты ПДн

Проверка информационной системы персональных данных осуществляется в обязательном и добровольном порядке и позволяет определить, насколько продуктивно она функционирует, точнее — справляются ли предусмотренные меры защиты со своими задачами, а именно:

присутствуют ли все предусмотренные действующим законодательством элементы, насколько корректно они настроены и инсталлированы;

имеется ли полный перечень документов по защите личной информации, отвечает ли он действующим правовым нормативам;

назначены ли ответственные лица за обеспечение безопасности ПДн, насколько они компетентны и справляются с поставленными задачами;

осведомлены ли пользователи системы в сфере защиты персональных данных;

насколько в целом эффективна СЗПДн.

Для составления окончательного вердикта специалистам необходимо проанализировать соответствие организационно-техническим требованиям и произвести испытания внедренных защитных мер от потенциальных угроз. По итогам каждого теста и этапа заполняются протоколы, а выводы отражаются в итоговом заключении.

Что включают в себя оценочные мероприятия?

Перед началом работ сотрудники Центра разрабатывают методику, в которой описывается порядок исследований, описание объекта, список запланированных процедур, критерии и требования, которыми будут руководствоваться.

Непосредственно оценка эффективности защиты персональных данных включает в себя анализ:

структурных особенностей системы;

технологических нюансов обработки персональных данных субъектов;

достаточности внутренней документации, её соответствия прописанным в нормативно-правовых актах требованиям;

соответствия между структурой, составом программно-технической базы ИСПДн и подготовленной организационно-технической документацией;

правильности определения уровней защищенности персональных данных и способов защиты для каждого из них;

подготовленности персонала и распределения ответственности;

наличия и результативности физической охраны ИСПДн;

состояния и выполнения работ по поддержанию безопасности информационной системы.

Что нужно проверять

Полную документацию по объекту.

Анализ структуры ИСПДн и техпроцесс обработки информации.

Оценка уровня защиты.

Проверка структуры ИСПДн согласно заявленной документации.

Оценка организации рабочего процесса и общего выполнения требований по защите.

Вопросы охраны проверяемого объекта.

Есть ли штатные средства защиты, как они настроены.

Оценка уровня компетентности лиц, ответственных за защиту ПДн.

Проверка знаний персонала ИСПДн по информационной безопасности.

Проверка прав доступа.

Регистрация и учет.

Обеспечение целостности.

Антивирус и все базы.

Общий анализ уровня защиты.

Обнаружение вторжений.

Файрвол и его настройки.

Уровень защиты каналов связи.

Проверка защиты ИСПДн сканером безопасности.

По итогам вышеописанных манипуляций составляется протокол оценки эффективности системы защиты ПД. Он служит основой составления итогового заключения о состоянии защиты данных.

Если ИСПДн не прошла испытания на соответствие требованиям по созданию эффективной защиты обрабатываемой информации, то разрабатываются предложения по устранению недостатков и, по возможности, недостатки устраняются еще до окончания процедуры оценки.

Порядок проведения испытаний информационных систем ПДн

Чтобы удостовериться в том, что ИСПДн надежно защищена от несанкционированного проникновения, утечки данных и прочих угроз,

наши сотрудники проводят с помощью специального оборудования и ПО испытания всех подсистем:

учета и регистрации;

контроля доступа;

антивирусной защиты;

поддержания целостности;

межсетевого экранирования;

выявления вторжений;

каналов связи;

оценки защищенности.

Оценочные работы включают также определение наличия предусмотренной законом документации (проектной, эксплуатационной), её соответствия комплексу программно-технических средств и степени выполнения правил использования СЗИ.

3.2. Контроль эффективности системы защиты ИСПДн

Контроль эффективности СЗПДн должен осуществляется на периодической основе.

Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.).

Оценка обстановки (рис. 3.1) является этапом, во многом определяющим эффективность решения задач обеспечения безопасности ПДн. Она основывается на результатах комплексного обследования ИСПДн, в ходе которого, прежде всего, проводится определение защищаемой информации и ее категорирование по важности.

Рис. 3.1 – Содержание оценки обстановки

Немаловажной составляющей контроля эффективности защиты ИСПДн является оценочное прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн с разработкой, по меньшей мере, превентивных мероприятий.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Виды контроля в соответствии с ГОСТ Р50922–96

В соответствии со стандартом ГОСТ Р50922-96 контроль подразделяется на следующие виды:

Организационный контроль;

Технический контроль.

Для технического контроля используются средства контроля (программные или аппаратные). В качестве организационного

контроля выступает организационно-распорядительная документация.

Применение способов контроля на практике называется методом контроля.

Наиболее надежным является технический контроль эффективности защиты информации. Для реализации технического контроля применяются следующие методы:

Инструментальные;

Инструментально-расчетные;

Расчетные.

К инструментальным методам относятся программные, программно-аппаратные и аппаратные средства. Следовательно, можно организовать надежный контроль защиты информации. С использованием исходных данных о состоянии системы защиты возможно использовать расчётный метод и узнать, насколько контроль эффективен.

Состав контрольных мероприятий

2.2.1.Основными составляющими Контроля являются:

2.2.1.1. Автоматизированный контроль на основе мониторинга событий ИБ.

2.2.1.2. Проверка правильности и полноты проводимых мероприятий по обеспечению соответствия обработки и защиты ПДн требованиям законодательства РФ.

2.2.1.3. Проверка работоспособности и эффективности СЗИ. Проверка работоспособности СЗИ в рамках контрольных мероприятий проводится в соответствии с программой проведения контроля состояния СЗПДн.

2.2.1.4. Проверка своевременности внесения изменений в проектную, техническую и нормативно-техническую документацию по обеспечению безопасности ПДн.

2.2.1.5. Принятие на основе результатов Контроля мер по устранению последствий нарушений требований безопасности ПДн, вплоть до полного

или частичного приостановления эксплуатации ИСПДн, если иными мерами невозможно устранить нарушения требований безопасности ПДн.

2.2.1.6. Проведение в ходе мероприятий по государственному контролю разъяснительной работы по применению требований законодательства РФ и нормативных документов в области защиты ПДн в ИСПДн.

2.2.2.Основные контрольные мероприятия и периодичность их проведения приведены в таблице 3.1.

2.2.3.Периодичность проведения того или иного мероприятия устанавливается по решению Комиссии. Некоторые мероприятия следует проводить внепланово, в случае изменения внешних факторов, например, изменения законодательства РФ в области ПДн.

Таблица 3.1.

Перечень основных контрольных мероприятий

Мероприятие	Периодичность
Контроль соответствия полномочий пользователей ИСПДн матрицам доступа	Ежемесячно
Контроль соблюдения порядка и требований обработки ПДн	Еженедельно
Контроль соблюдения требований парольной защиты	Ежемесячно
Контроль соблюдения требований антивирусной защиты	Еженедельно
Контроль соблюдения требований ИБ в сфере информационного обмена	Еженедельно
Контроль соблюдения требований работы с МНИ	Ежемесячно

Окончание таблицы 3.1.

Контроль соблюдения порядка доступа в выделенные помещения	Ежеквартально
Контроль соблюдения порядка проведения резервного копирования, хранения и корректности создаваемых резервных копий	Ежемесячно
Контроль соблюдения порядка использования СЗИ	Еженедельно
Контроль соблюдения требований хранения материальных носителей ПДн (бумажных и машинных)	Ежеквартально
Контроль соблюдения требований работы в ИСПДн	Ежемесячно
Контроль соответствия состава обрабатываемых ПДн заявленным целям их обработки	Ежегодно
Контроль реагирования на обращения (запросы) субъектов ПДн об исполнении из законных прав	Ежемесячно
Контроль исполнения требований Комиссии	Ежеквартально
Контроль (тестирование) работоспособности и корректной настройки СЗПДн	Ежеквартально
Контроль удаления ПДн и уничтожения их материальных носителей	Ежеквартально
Контроль соблюдения порядка предоставления ПДн и их материальных носителей третьим лицам	Ежемесячно
Выявление изменений порядка и условий обработки и защиты ПДн	Ежегодно
Контроль обновления ПО и соответствия программного и технического состава ИСПДн заявленному (техническому паспорту)	Ежемесячно
Анализ и переоценка УБПДн, предсказание появления новых, еще не известных угроз	Ежегодно
Контроль исполнения требований законодательства РФ в области ПДн	Ежеквартально
Контроль актуальности ЛНА, регламентирующих обработку и защиту ПДн	Ежеквартально
Контроль ведения журнальных форм	Ежеквартально
Внутренний аудит обеспечения безопасности ПДн	1 раз в 3 года

Планирование контрольных мероприятий

2.3.1.Внутренние мероприятия по Контролю могут быть: – плановыми;

– внеплановыми. 2.3.2.Плановые мероприятия

2.3.2.1. Плановые мероприятия устанавливаются ЛНА Учреждения, регламентирующими обработку и защиту ПДн, включая настоящий регламент.

2.3.2.2. Перечень плановых мероприятий формируется Комиссией и утверждается директором в виде годового плана.

2.3.3.Внеплановые мероприятия

2.3.3.1. Решение о проведении внеплановых мероприятий принимается председателем Комиссии, и оформляется приказом директора.

13

2.3.3.2. Внеплановость мероприятий подразумевает:

– максимально короткий срок между выходом приказа о проведении и проведением;

– минимизация круга лиц, которые заранее знают о готовящемся мероприятии;

– отсутствие периодичности в сроках проведения таких мероприятий.

2.3.3.3. Внеплановые мероприятия могут осуществляться, в частности, в следующих случаях:

– при изменении законодательства РФ в области ПДн;

– при возникновении или после возникновения инцидента ИБ (например, утечки ПДн);

– появления жалоб субъектов ПДн;

– изменения структуры процессов обработки ПДн.

2.3.3.4. Внеплановые мероприятия могут осуществляться, в частности, в целях:

– реагирования на инциденты ИБ и их предупреждения;

– определения текущего состояния СЗПДн;

– определения уровня подготовки работников в области защиты ПДн;

– тестирования СЗПДн.

2.3.3.5. В качестве внеплановых мероприятий могут выступать любые мероприятия из входящих в состав плановых, а также иные.

3.3. Методика контроля защищенности конфиденциальной информации ИСПДн от несанкционированного доступа

Несанкционированный доступ (НСД) — это доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или

автоматизированными системами (АС). Под штатными средствами здесь понимается совокупность технического, программного и микропрограммного обеспечения СВТ или АС [2].

Одним из принципов защиты информации от несанкционированного доступа (НСД) является контроль эффективности средств защиты информации (СЗИ), а именно – проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам по безопасности информации с применением штатных средств, под которыми понимается совокупность технического, программного и микропрограммного обеспечения средств вычислительной техники (СВТ) или автоматизированных систем (АС). Такой контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами. Проверка функционирования системы защиты информации от НСД осуществляется с помощью программных или программно-технических средств на предмет соответствия требованиям по безопасности с учетом классификации АС и степени секретности обрабатываемой информации. В случае конфиденциальной информации контролю подлежат три из четырех подсистем системы защиты информации от НСД, а именно:

– подсистема управления доступом; – подсистема регистрации и учета;

– подсистема обеспечения целостности.

Методика контроля защищенности конфиденциальной информации в АС от НСД состоит из трех основных этапов:

– Планирование.

– Тестирование.

– Анализ результатов.

На этапе планирования проводится анализ всех исходных данных и документации по АС, в частности анализ защищаемых информационных

ресурсов, структуры АС, а также целей и задач системы защиты конфиденциальной информации в АС от НСД. Перед началом тестирования необходимо установить, что в документации на объект испытаний декларируется соответствие АС требованиям руководящих документов.

Заказчик должен предоставить комиссии, проводящей контроль защищенности, описание технологического процесса обработки информации в АС, включающее в себя следующую информацию:

– перечень объектов доступа;

– перечень субъектов доступа; – перечень штатных средств доступа к информации;

– перечень используемых средств защиты информации;

– описание реализованных правил разграничения доступа (матрицу доступа);

– схему или описание информационных потоков.

На этапе тестирования проводится комплекс организационно-технических мероприятий по оценке показателей защищенности конфиденциальной информации в АС от НСД.

Тестирование включает проверку каждой из подсистем системы защиты:

1. Проверка подсистемы управления доступом. В рамках проверки подсистемы управления доступом контролируются организационные мероприятия, устанавливающие требования к парольной политике, проводится анализ установленных параметров функционирования средств идентификации и аутентификации, осуществляется контроль корректности функционирования механизмов идентификации и аутентификации, а также контролируется процедура смены паролей пользователями. Поскольку методика контроля защищенности представляет собой обоснованную последовательность действий, то порядок проверки выполнения каждого требования (нор-

мы) удобнее всего представить в виде таблицы (таблица 3.2).

Таблица 3.2.

Порядок проверки подсистемы управления доступом

Проверяемое требование	Порядок действий при проверке
1. Проверка механизма идентификации и аутентификации субъектов доступа при входе в систему	1. На исследуемом АРМ выполнить запросы на идентификацию и проведение аутентификации с использованием различных сочетаний учетных данных: зарегистрированный (незарегистрированный) идентификатор, верный (неверный) пароль. 2. Проверить реакцию системы защиты на вход в ОС с неправильно введенным идентификатором (логином). 3. Проверить реакцию системы защиты на вход в ОС с неправильно введенным паролем. 4. Проверить реакцию системы защиты на вход в ОС с правильно введенным логином и паролем.
2. Проверка соблюдения требований к паролю (длина пароля должна быть не менее 6 символов, пароль должен включать буквы и цифры)	1. Проверить наличие эксплуатационной документации на АС, в которой регламентирован порядок проведения парольной защиты АС. Проверить наличие: – требования к паролям; – обязанности администратора безопасности парольной политики $ИСПД_{Н}$ (генерация и распределение паролей); – обязанности пользователей парольной политики $ИСПД_{Н}$ (генерация паролей, смена паролей).

Продолжение 1 Таблицы 3.2

Проверяемое требование	Порядок действий при проверке
2. Проверка соблюдения требований к паролю (длина пароля должна быть не менее 6 символов, пароль должен включать буквы и цифры)	2. Определить значения, установленные средствами СЗИ от НСД, для следующих параметров: минимальная длина пароля, сложность пароля (алфавит паролей), максимальный срок действия пароля, максимальное число неудачных попыток входа пользователей в ОС, после которого осуществляется блокировка работы пользователя, реакция СЗИ на превышение максимального числа неудачных попыток входа пользователя. 3. Под учетными записями пользователей произвести попытки установить пароль, не соответствующий нормативным требованиям. Для этого осуществить: – попытку установить пароль, длина которого менее 6 символов; – попытки установить пароль, состоящий исключительно из цифр, либо только из букв.
3. Проверка механизма идентификации по именам внешних устройств	1. Проверить возможность загрузки ОС с внешних носителей (с flash-накопителя или CD-диска) в обход системы защиты информации в АС. Попытки загрузки с внешних устройств должны быть проигнорированы системой защиты информации ИСПД$_{Н}$.

Окончание Таблицы 3.2

Проверяемое требование	Порядок действий при проверке
4. Проверка механизма идентификации программ, каталогов, файлов, записей, полей записей по именам при обращении к ним средствами ОС и средствами установленных на СЗИ от НСД	1. Провести идентификацию программ запуском их (через «Проводник») и проверить их соответствие заданным параметрам. 2. Провести идентификацию каталогов (папок), в которых расположены защищаемые файлы путем обращения к ним с помощью штатных средств ОС (программа «Проводник»). 3. Проверка механизма идентификации записей и полей записей проводится только в том случае, если в $ИСПД_{Н}$ присутствуют системы управления базами данных (СУБД).
5. Проверка правильности предоставления доступа к конкретным субъектам, к защищаемым объектам (каталогам, файлам) в соответствии с установленными правами (матрицей доступа)	1. Проверить наличие матрицы доступа в числе документации на $ИСПД_{Н}$. 2. Дальнейшая проверка производится при помощи специализированных программных средств: – «Ревизор 1 XP»; – «Ревизор 2 XP» или их аналогов: – ER Win Data Modeller; – Secret Net 7; – Фикс 2.0.2; – Terrier 3.0; – XSpider 7.8; – Cisco Packet Tracer.

2. Проверка подсистемы регистрации и учета.

При проверке подсистемы регистрации и учета АС контролируется регистрация и учет событий средствами установленного СЗИ от НСД на всех этапах технологического процесса обработки и хранения информации (вход и выход субъектов в ОС, запуск и завершение программ, попытки доступа программ к защищаемым файлам, каталогам, узлам сети, терминалам, линиям связи), выдача защищаемых материалов на печать, порядок регистрации и учета носителей защищаемой информации, а также качество очистки освобождаемых областей памяти внешних накопителей и оперативной памяти. Порядок проверки подсистемы регистрации и учета представлен в таблице 3.3.

Таблица 3.3.

Порядок проверки подсистемы регистрации и учета

Проверяемое требование	Порядок действий при проверке
1. Проверка регистрации входа/выхода пользователя в/из ОС, входа/выхода компьютера из спящего режима	1. Произвести выход из системы, вход в систему от имени пользователя или администратора. 2. Произвести попытку предоставления неправильного идентификатора (или ввода неправильного имени пользователя), пароля. 3. Ввести компьютер, на котором осуществляется проверка, в спящий режим и вывести из него. 4. Зайти в журнал «Безопасность» ОС Windows или в соответствующий журнал используемого СЗИ от НСД. Проверить наличие записей о каждом из событий пунктов 1–3.

Продолжение 1 Таблицы 3.3.

Проверяемое требование	Порядок действий при проверке
2. Проверка регистрации запуска и завершения программ	1. Запустить и завершить программы, используемые для обработки защищаемой информации. 2. Зайти в журнал «Безопасность» ОС Windows или в соответствующий журнал используемого СЗИ от НСД. 3. Проверить наличие записей о каждом из событий п. 1.
3. Проверка регистрации попыток доступа к защищаемым файлам и каталогам	1. Открыть и закрыть файлы и папки, содержащие защищаемую информацию (согласно матрице доступа). 2. Попробовать создать (удалить) файлы и папки (согласно матрице доступа). 3. Зайти в журнал «Безопасность» ОС Windows или в соответствующий журнал используемого СЗИ от НСД. 4. Проверить наличие записей о всех (каждом) из событий п. 1,2.
4. Проверка регистрации выдачи защищаемых материалов на печать	1. Проверить, что пользователю, осуществляющему печать, разрешен доступ к порту, к которому подключен принтер. 2. Проверить, что факт вывода документа на печать, дата и время выдачи, имя файла, уровень конфиденциальности, количество экземпляров документа, листов в экземпляре, имя файла, с которого выполнена печать документа, идентификатор пользователя, запросившего документ, регистрируется установленным СЗИ от НСД. 3.Проверить, что бракованные листы уничтожаются в установленном в образовательной организации порядке.

Окончание Таблицы 3.3.

Проверяемое требование	Порядок действий при проверке
5. Проверка регистрации и учета носителей защищаемой информации	1.Проверить, что учет носителей защищаемой информации проводится в журнале с регистрацией их выдачи (приема). 2. Проверить, что носители защищаемой информации уничтожаются в установленном в организации порядке с записью об этом в журнале учета.
6. Проверка качества очистки освобождаемых областей памяти внешних накопителей и оперативной памяти	1. Проверка очистки (обнуления, обезличивания) освобождаемых областей внешних накопителей и оперативной памяти производится при помощи специализированных программных средств контроля защищённости, таких как «Terrier 3.0» и его аналоги.

4. Проверка подсистемы обеспечения целостности.

При проверке подсистемы обеспечения целостности АС осуществляется проверка обеспечения целостности СЗИ от НСД и неизменности программной среды компьютера, проверка проведения периодического тестирования системы защиты информации от НСД, проверка наличия средств восстановления программной среды компьютера и СЗИ от НСД, а также проверка наличия САВЗ в исследуемой АС.

Порядок проверки подсистемы обеспечения целостности представлен в таблице 3.4.

Средствами восстановления СЗИ от НСД в АС являются дистрибутивы (инсталляционные файлы) с системным и прикладным ПО. Копии дистрибутивов хранятся отдельно для обеспечения возможной полной замены (переустановки) ПО в случае каких-либо отказов (сбоев) или нарушений в работе технических средств АС. Автоматическое оперативное

восстановление функций СЗИ НСД при сбоях проверяется путем моделирования сбойных ситуаций и последующей проверки (тестирования) функций СЗИ НСД.

Помимо проверки наличия средств антивирусной защиты проводится выборочная проверка используемых в системе программных средств на наличие компьютерных вирусов.

Таблица 3.4.

Порядок проверки подсистемы обеспечения целостности

Проверяемое требование	Порядок действий при проверке
1. Проверка обеспечения целостности программных СЗИ от НСД и неизменности программной среды компьютера	1. Проверка обеспечения целостности программных СЗИ от НСД и неизменности программной среды производится при помощи специализированных средств контроля защищенности, таких как «ФИКС 2.0.1», «ФИКС 2.0.2» или их аналогов.
2. Проверка проведения периодического тестирования системы защиты информации от НСД	1. Проверить наличие организационно-распорядительной документации, определяющей периодичность и порядок тестирования всех функций СЗИ от НСД. 2. Проверить возможность периодического тестирования СЗИ путем анализа применяемых разработчиком средств контроля целостности компонентов системного ПО, реализующих функции СЗИ от НСД и наборов данных, используемых этими средствами.
3. Порядок проверки наличия средств восстановления и средств антивирусной защиты	1. Проверить наличие средств восстановления программной среды ПК, СЗИ от НСД, хранящихся отдельно, в обеспе-чение переустановки при сбоях. 2. Проверить наличие средств антивирусной защиты.

5. Заключительный этап анализа результатов

На заключительном этапе анализа результатов производится сравнение фактических значений показателей защищенности, и норм (требований), определенных в нормативно-методических документах по защите конфиденциальной информации в ИСПД$_{Н}$. от НСД.

Выводы по Главе 3.

ЗАКЛЮЧЕНИЕ

ГЛОССАРИЙ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аудит информационной безопасности (организации) – систематический, независимый и документированный процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации (ГОСТ Р 53114-2008).

База данных – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимая от прикладных программ (ГОСТ 20886-85).

Выделенные помещения – помещения (кабинеты, актовые, конференц-залы и т.д.) специально предназначенные для обработки персональных данных.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (ГОСТ Р 50922-2006).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922-2006).

Информационная безопасность (организации) – состояние защищенности интересов организации в условиях угроз в информационной сфере (ГОСТ Р 53114-2008).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 No 152-ФЗ).

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (Федеральный закон от 27.07.2006 No 149-ФЗ).

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность (ГОСТ Р ИСО/МЭК 27001-2006).

Контроль обеспечения защиты персональных данных – проверка соответствия обеспечения защиты персональных данных в организации, наличия и содержания документов требованиям нормативных документов, технической, правовой, организационно- распорядительной документации в области защиты персональных данных.

Критерий аудита информационной безопасности (организации) – совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности организации в области информационной безопасности (ГОСТ Р 53114-2008).

6

Матрица доступа – таблица, отображающая правила разграничения доступа («Защита от несанкционированного доступа к информации. Термины и определения», утверждено решением председателя Гостехкомиссии России от 30.03.1992)

Мониторинг информационной безопасности (организации) – постоянное наблюдение за процессом обеспечения информационной безопасности в организации с целью установить его соответствие требованиям по информационной безопасности (ГОСТ Р 53114-2008).

Непреднамеренное воздействие на информацию – ошибка пользователя информацией, сбой технических и программных средств информационных систем, природные явления или иные нецеленаправленные на изменение информации действия, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также утрате, уничтожению или сбою функционирования носителя информации (ГОСТ Р 51583-2000[1]).

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации (ГОСТ Р 50922- 2006).

Несанкционированный доступ (к информации) – доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации (Р 50.1.053-2005).

Носитель информации – материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (ГОСТ Р 50922-2006).

Обеспечение информационноŭ безопасности (организации) – деятельность, направленная на устранение (неитрализацию, парирование) внутренних и внешних угроз информационноŭ безопасности организации или на минимизацию ущерба от возможноŭ реализации таких угроз (ГОСТ Р 53114-2008).

Обработка персональных данных – любое деиствие (операция) или совокупность деиствиŭ (операциŭ), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (Федеральный закон от 27.07.2006 No 152-ФЗ).

[1] Заменен на ГОСТ Р 51583-2014 (с 1 сентября 2014 г.)

Объект защиты информации – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации (ГОСТ Р 50922-2006).

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно

или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (Федеральный закон от 27.07.2006 No 152-ФЗ).

Оценка соответствия требованиям по защите информации – прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации (ГОСТ Р 50922-2006).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 No 152-ФЗ).

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа («Защита от несанкционированного доступа к информации. Термины и определения», утверждено решением председателя Гостехкомиссии России от 30.03.1992).

Правило доступа (к защищаемой информации) – совокупность правил, регламентирующих порядок и условия доступа субъекта к защищаемой информации и ее носителям (ГОСТ Р 50922-2006).

Право доступа (к защищаемой информации) – совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации (ГОСТ Р 50922-2006).

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации (ГОСТ Р 53114-2008).

Система защиты персональных данных – совокупность организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах персональных данных (Постановление Правительства РФ от 01.11.2012 No 1119).

Угроза безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (Федеральный закон от 27.07.2006 No 152-ФЗ).

Угроза информационной безопасности (организации) – совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации,

8

вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации (ГОСТ Р 53114-2008).

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к

информации и получения защищаемой информации иностранными разведками (ГОСТ Р 53114-2008).

Цель защиты информации – заранее намеченный результат защиты информации (ГОСТ Р 50922-2006).

Примечание: результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию, или обеспечение соответствия требованиям в области защиты информации.

Эффективность защиты информации – степень соответствия результатов защиты информации цели защиты информации (ГОСТ Р 50922-2006).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Барабанов А. В., Марков А. С., Цирлов В. Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. — 2011. — № 3. — С. 48–53.
Программа и методики проведения аттестационных испытаний объектов информатизации (Аттестация АС) // Документы по информационной безопасности. URL: http://securitypolicy.ru/index.php/Программа_и_методики_проведения_аттестационных_испытаний_объектов_информатизации_(Аттестация_АС)

1. Риски информационной безопасности веб-приложений [Электронный ресурс] – Режим доступа: https://habrahabr.ru/company/pentestit/blog/279219/.
2. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ.
3. IT-Project Management [Электронный ресурс] – Режим доступа: https:// itproject management.wordpress.com/2008/04/17/Разбираемся-с-терминами-уязвимость-у/.
4. Вихорев С.В. Классификация угроз информационной безопасности [Электронный ресурс] – Режим доступа: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml.
5. Стандарт ISO:17799-00 (Стандарт Великобритании BS 7799-95 "Практические правила управления информационной безопасностью").
6. Руководящий документ. "Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации", Гостехкомиссия России, Сб-к руководящих документов по защите информации от несанкционированного доступа, М.: 1998., п. 4.
7. Виды угроз информационной безопасности и классификация источников угроз [Электронный ресурс] – Режим доступа: http://www.intuit.ru/studies/

courses/17846/1242/lecture/27498.

8. Угрозы безопасности для информационной системы вуза [Электронный ресурс] – Режим доступа: http://security.ase.md/publ/ru/pubru91/.

9. Домарев В. В. Безопасность Информационных Технологий. Методология создания систем защиты, Москва-Санкт-Петербург-Киев, 2002.

10. Международный стандарт ISO/IEC 17799. Информационные технологии: Свод практических правил управления защитой информации, ISO/IEC, 2000.

11. Идентификация угроз. Детальное рассмотрение процесса оценки рисков [Электронный ресурс] – Режим доступа: http://www.jetinfo.ru/stati/upravlenie-riskami-obzor-upotrebitelnykh-podkhodov-chast-2.

12. Оценка угроз безопасности информационным системам [Электронный ресурс] – Режим доступа: http://security.ase.md/publ/ru/pubru01.html.

13. Шнайдерман И.Б. Концепция системы информационной безопасности автоматизированных информационных систем / И.Б. Шнайдерман, С.А. Охрименко, Г.А. Черней // Автоматизация и современные технологии. – 1996. – № 8. – С.26–29.

14. Охрименко С.А. Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) / С.А. Охрименко, Г.А. Черней // НТИ. Сер.1, Орг. и методика информ. работы. – 1996. – № 5. –С. 5–13.

15. Черней Г.А. Безопасность автоматизированных ИС / Г.А. Черней, С.А. Охрименко, Ф.С. Ляху. – Кишинев:Ruxanda, 1996. –186 с.

16. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – кн.1,2

17. Бадретдинова Р.Р. Разработка системы оценки и мониторинга рисков информационной безопасности на примере образовательной организации

общего образования [Электронный ресурс] – Режим доступа: degree_ work_file.

18. Васильев Р.А. Курс лекций по информационной безопасности образования [Электронный ресурс] – Режим доступа: http://5_____pdf.

19. Каберник В.В. Информационная безопасность образовательных учреждений в контексте противодействия угрозам терроризма и экстремизма [Электронный ресурс] – Режим доступа: http://Informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdeniy-v-kontekste-protivodeystviya-ugrozam-terroriz ma-i-ekstremizma.

20. Астахов А. Искусство управления информационными рисками [Электронный ресурс] – Режим доступа: http://xn----7sbab7afcqes2bn.xn--p1ai/ content/octave.

21. Жаринова И.А. Диагностика сформированности конструкторско-технологических знаний и умений у будущего учителя технологии. Канд. дис., Екатеринбург, 2001.

22. Блюмберг В.А. Какое решение лучше? Метод расстановки приоритетов / В.А. Блюмберг, В.Ф. Глущенко. – Л.: Лениздат, 1982. – 89 с.

23. Шляхтенко С.Г. Категории качества и количества / С.Г. Шляхтенко. – Л.: Изд. ЛГУ, 1968.

24. Глушков, В.М. Введение в АСУ. Изд. 2-е / В.М. Глушков. – Киев, Техника, 1974.

25. Черняк Ю.И. Системный анализ в управлении экономикой / Ю.И. Черняк. – М.: Экономика. 1971.

26. Новые технологии перехвата данных: ПЭМИН («TEMPEST») [Электронный ресурс] – Режим доступа: https://www.mipko.ru/blog/2011/01/ perehvat-dannyh-s-klaviatury/.

27. Макаренко С.И. Информационная безопасность: учеб. пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

28. Белевитин, В.А. Магистерская диссертация: рекомендации по подготовке и защите: учебно-методич. пособие / В.А. Белевитин, Е.А. Гнатышина, И.Г. Черновол. – Челябинск, 2016.
29. Защита компьютерной информации от утечки по ПЭМИН [Электронный ресурс] – Режим доступа: www.support17.com/component/content/39.html?.
30. Вероятность произведения событий [Электронный ресурс] – Режим доступа: www life-prog.ru/1_32219_veroyatno...niya-sobitiy.html.
31. Вероятность наступления события [Электронный ресурс] – Режим доступа: www.infourok.ru/issledovatelskaya...bitiya-993492.html/.
32. Метод и модель формирования системы обеспечения информационной безопасности [Электронный ресурс] – Режим доступа: aspirantura.ifmo.ru/file/other/FiaRFzLArW.pdf.
33. Корбаинова Е.В. Определение основных характеристик модели защиты информации, основанной на иммунных принципах / Е.В. Корбаинова, А.С. Згурский // Сб-к статей XI конференции «Фундаментальные и прикладные исследования, разработка и применение высоких технологий». Том 1 – СПб, 2011. – С. 114–116.
34. Згурский А.С. Алгоритм оценки степени потребности информационного актива в свойствах безопасности / А.С. Згурский, Е.В. Корбаинова // Научно-технический вестник Поволжья, Том №2 – Казань, 2011, С. – 95–98.
35. Згурский А.С. Основные угрозы и источники-субъекты угроз информационной безопасности организаций РФ // Сб-к тезисов седьмой междун. науч.-практич. конференции «Современные проблемы гуманитарных и ЕСтественных наук». Москва, 2011, – С. 58–59.
36. Электронный учебник по разработке информационной безопасности персональных компьютеров // Help Antivirus – URL: http://helpantivirus.ru/developmentsafety/Menu.php.

37. Галатенко В. А. Основы информационной безопасности. – М.: Интернет-университет информационных технологий – www.INTUIT.ru, 2008. – 208 с.
38. Астахов А. Анализ защищенности корпоративных автоматизированных систем // Jet Info [Электронный ресурс] – Режим доступа: – URL: www.jetinfo.ru\2002\7\1\article1.7.2002.html.
39. Доля А. Внутренние угрозы ИТ-безопасности. // Byte-Россия [Эл. ресурс] – N 12, 2004. – URL: www.bytemag.ru/?ID=603365.
40. Атака через Интернет / Медведовский И. Д., Семьянов П. В., Платонов В. В.; под ред. П. Д. Зегжды. – СПб.: изд. НПО «Мир и семья-95», 1997.
41. Мэйволд Э. Безопасность сетей: курс лекций для Интернет- университета информационных технологий / Э. Мэйволд.– М.: Интернет-университет информационных технологий [Электронный ресурс] – Режим доступа: – www.INTUIT.ru, 2006. – URL: www.intuit.ru/department/security/netsec/.
42. Васенин В.А. Информационная безопасность и компьютерный терроризм / В.А. Васенин // Научные и методологические проблемы информационной безопасности. — М.: МЦПМО, 2004.
43. Зегжда Д.П.. Как построить защищенную информационную систему / Д.П. Зегжда, А.М. Ивашко. – СПб.: Мир и семья. – 2007.
44. Расторгуев С.П. Философия информационной войны / С.П. Расторгуев. – М.: Вузовская книга. – 2001.
45. Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности личности / Г.Л. Смолян // Информационное общество. – М.:, 1999.
46. Черешкин Д.С. Сетевая информационная революция / Д.С. Черешкин, Г.Л. Смолян // Информационные ресурсы России, № 4. – 1997.
47. Антопольский А.А. Ответственность за правонарушения при работе с конфиденциальной информацией / А.А. Антопольский // Административная ответственность. – М.: ИГиП РАН, – 2001.

48. Бачило И.Л. Информационное право: основы практической информатики / И.Л. Бачило. – М.: Юринформцентр, – 2001.

49. Астахова Л.В. Информационная безопасность: герменевтический подход. – М.: РАН, 2010.

50. Ващекин Н.П. Цивилизация и Россия на пути к устойчивому развитию: проблемы и перспективы / Н.П. Ващекин, В.А. Лось, А.Д. Урсул. – М.: МГУК, 1999.

51. Ващекин Н.П. Безопасность и устойчивое развитие России / Н.П. Ващекин, М.И. Дэлиев, А.Д. Урсул. – М.: МГУК, 1998.

52. Bynum T. Ethical Challenges to Citizens of the Automatic Age: Norbert Wiener on the Information Society *II* Journal of Information, Communication and Ethics in Society. – 2004. – № 2(2).

53. Johnson D. Computer Ethics. – New Jersey: Prentice Hall, 2001.

54. Ван Дюн Дж. Роль человеческого фактора в совершении преступлений в сфере компьютеров / Дж. Ван Дюн // Компьютеризация общества и человеческий фактор. – М., 1988.

55. Капурро Р. Информационная этика / Р. Капурро // Информационное общество. – 2010. – Вып. 5.

56. Maner V. Unique Ethical Problems in Information Technology // Science and Engineering Ethics 1996. – № 2(2).

57. Moor J. Why We Need Better Ethics for Emerging Technologies // Ethics and Information Technology, 2005. – Vol. 7(3).

58. Himrna K. E. The handbook of information and computer ethics / K.E. Himrna, H.T. Tavani. – New Jersey: Wiley-Interscience, 2008.

59. Freeman L.. Information Ethics: Privacy and Intellectual Property. – Hersey: Information Science Publishing, 2005.

Приложение 1

Тест-анкета оценки угроз безопасности ИС
профессиональной образовательной организации

1. Сколько раз за последние 3 года сотрудники организации пытались получить несанкционированный доступ к хранящейся в ее ИС информации с использованием прав других пользователей?

a) Ни разу (0 баллов); b) Один или два раза (10 баллов); c) В среднем один раз в год (20 баллов); d) В среднем более одного раза в год (30 баллов); e) Неизвестно (10 баллов).

2. Какова тенденция в статистике такого рода попыток несанкционированного проникновения в информационную систему?

a) К возрастанию (10 баллов); b) Оставаться постоянной (10 баллов); c) К снижению (10 баллов).

3. Хранится ли в информационной системе информация (например, личные дела), которая может представлять интерес для сотрудников организации и побуждать их к попыткам не санкционированного доступа к ней?

a) Да (5 баллов); b) Нет (0 баллов).

4. Известны ли случаи нападения, угроз, шантажа, давления на сотрудников со стороны по сторонних лиц?

a) Да (10 баллов); b) Нет (0 баллов).

5. Существуют ли среди персонала группы лиц или отдельные лица с недостаточно высокими моральными качествами?

a) Нет, все сотрудники отличаются высокой честностью и порядочностью (0 баллов); b) Существуют группы лиц и отдельные личности с недостаточно высокими моральными качествами, но это вряд ли может спровоцировать их на несанкционированное использование системы (5 баллов); c) Существуют группы лиц и отдельные личности с настолько низкими моральными качествами, что это повышает вероятность

несанкционированного использования системы сотрудниками (10 баллов).

6. Хранится ли в информационной системе информация, несанкционированное изменение которой может принести прямую выгоду сотрудникам?

a) Да (5 баллов); b) Нет (0 баллов).

7. Предусмотрена ли в информационной системе поддержка пользователей, обладающих техническими возможностями совершить подобные действия?

a) Нет (0 баллов); b) Да (5 баллов).

8. Существуют ли другие способы просмотра информации, позволяющие злоумышленнику добраться до нее более простыми методами, чем с использованием «маскарада»?

a) Да (10 баллов); b) Нет (0 баллов).

9. Существуют ли другие способы несанкционированного изменения информации, позволяющие злоумышленнику достичь желаемого результата более простыми методами, чем с использованием «маскарада»?

a) Да (10 баллов); b) Нет (0 баллов).

10.Сколько раз за последние 3 года сотрудники пытались получить несанкционированный доступ к информации, хранящейся в других подобных системах в вашей организации?

a) Ни разу (0 баллов); b) Один или два раза (5 баллов); c) В среднем раз в год (10 баллов); d) В среднем чаще одного раза в год (15 баллов); e) Неизвестно (10 баллов).

Итог тест-анкетирования по сумме выставленных экспертами баллов: Степень угрозы при количестве баллов: До 9 баллов – Очень низкая; От 10 до 19 баллов – Низкая; От 20 до 29 баллов – Средняя; От 30 до 39 баллов – Высокая 40 и более 40 баллов – Очень высокая.

Приложение 2

Тест-анкета оценки уязвимостей безопасности ИС
профессиональной образовательной организации

1. Сколько людей имеют право пользоваться информационной системой?

a) От 1 до 10 (0 баллов); b) От 11 до 50 (4 балла); c) От 51 до 200 (10 баллов); d) От 200 до 1000 (14 баллов).

2. Пользователи информационной системой ведут себя необычным образом?

a) Да (0 баллов); b) Нет (10 баллов).

3. Какие устройства и программы доступны пользователям?

a) Только терминалы или сетевые контроллеры, ответственные за предоставление и маршрутизацию информации, но не за передачу данных (5 баллов);

b) Только стандартные офисные устройства и программы и управляемые с помощью меню подчиненные прикладные программы (0 баллов);

c) Пользователи могут получить доступ к операционной системе, но не к компиляторам (5 баллов);

d) Пользователи могут получить доступ к компиляторам (10 баллов);

4. Возможны ли ситуации, когда сотрудникам, предупрежденным о предстоящем сокращении или увольнении, разрешается логический доступ к информационной системе

a) Да (10 баллов); b) Нет (0 баллов).

5. Каковы в среднем размеры рабочих групп сотрудников пользовательских подразделе ний, имеющих доступ к информационной системе?

a) Менее 10 человек (0 баллов); b) От 11 до 20 человек (5 баллов); c) Свыше 20 человек (10 баллов).

6. Станет ли факт изменения хранящихся в информационной системе данных очевидным сразу для нескольких человек (в результате чего его будет

очень трудно скрыть

a) Да (0 баллов); b) Нет (10 баллов).

7. Насколько велики официально предоставленные пользователям возможности по про смотру всех хранящихся в системе данных?

a) Официальное право предоставлено всем пользователям (2 балла); b) Официальное право предоставлено только некоторым пользователям (0 баллов).

8. Насколько необходимо пользователям знать всю информацию, хранящуюся в системе?

a) Всем пользователям необходимо знать всю информацию (4 балла); b) Отдельным пользователям необходимо знать лишь относящуюся к ним информацию (0 баллов).

Итог тест-анкетирования по сумме выставленных экспертами баллов:

Степень уязвимости при количестве баллов: До 9 баллов – Низкая: От 10 до 19 баллов – Средняя; 20 и более баллов – Высокая.