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 МЕТОДИК ОБУЧЕНИЯ ТЕХНИЧЕСКИМ
ДИСЦИПЛИНАМ

Разработка рекомендаций по противодействию утечке информации по техническим каналам в системах связи 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 очная

Проверка на объём заимствований:
91,93 авторского текста
Работа рекомендована к защите
«1» 06 2022 г.
зав. кафедрой АТ, ИТ и МОТД
_____ В.В. Руднев

Выполнил:
студент группы ОФ-209-210-2-1,
Исаев Андрей Николаевич
Научный руководитель:
к.п.н., доцент кафедры
АТ, ИТ и МОТД
_____ Гафарова Е. А.

Челябинск

2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

К защищаемой информации относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Это, как правило, информация ограниченного доступа, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера.

Защита информации ограниченного доступа от утечки по каналам связи осуществляется на основе Конституции Российской Федерации, требований законов Российской Федерации «Об информации, информатизации и защите информации», «О государственной тайне», «О коммерческой тайне», других законодательных актов Российской Федерации, «Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденного Постановлением Совета Министров – Правительства РФ от 15.09.93 № 912-51, «Положения о лицензировании деятельности предприятий, организаций и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», утвержденного Постановлением Правительства РФ от 15 апреля 1995 г. № 333, и других нормативных документов.

Режим защиты информации ограниченного доступа устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством Российской Федерации.

Мероприятия по защите конфиденциальной информации от утечки по техническим каналам являются составной частью деятельности образовательной организации и осуществляются во взаимосвязи с другими мерами по обеспечению их информационной безопасности.

Защита конфиденциальной информации от утечки по каналам связи должна осуществляться посредством выполнения комплекса организационных и технических мероприятий, составляющих систему технической защиты информации на защищаемом объекте (СТЗИ), и должна быть дифференцированной в зависимости от установленной категории объекта информатизации или выделенного (защищаемого) помещения.

Организационные мероприятия по защите информации от утечки по каналам связи, в основном, основываются на учете ряда рекомендаций при выборе помещений для установки технических средств обработки конфиденциальной информации (ТСОИ) и ведения конфиденциальных переговоров, введении ограничений на используемые ТСОИ, вспомогательные технические средства и системы (ВТСС) и их размещение, а также введении определенного режима доступа сотрудников организации на объекты информатизации и в выделенные помещения.

Образовательные организации в настоящее время сталкиваются с серьезными проблемами в обеспечении информационной безопасности своих информационных ресурсов. Информационные ресурсы и информационные системы относятся к ряду основных защищаемых элементов во всех сферах жизнедеятельности современных организаций профессионального образования.

Защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести недопустимый ущерб субъектам информационных отношений является первоочередной задачей образовательных организаций.

На сегодняшний день в образовательных организациях существует широкий круг систем хранения и обработки информации, в которых в процессе их функционирования фактор информационной безопасности

хранения информации имеет особое значение. К таким информационным системам отнесем системы безопасного документооборота, базирующихся на технических каналах связи, поэтому значимой становится проблема обеспечения безопасности при передаче информационных ресурсов при их передаче по каналам связи.

Несмотря на большое количество работ по проблематике информационной безопасности, следует отметить, что практические методики по формированию оптимального механизма информационной безопасности в образовательных организациях не всегда соответствуют условиям и потребностям конкретной образовательной организации, в частности, не всегда актуальна система защиты информации при модернизации систем связи.

Специфика образовательных организаций состоит в отсутствии стандартного подхода при проведении информатизации объектов профессионального образования, в связи с чем, каждая образовательная организация имеет уникальную корпоративную сеть, со своими особенностями, сложившимися пользовательскими традициями, разной степенью обеспеченностью квалифицированными кадрами, различными техническими характеристиками и разнородными архитектурными решениями.

Обновление и усовершенствование программно-аппаратного базиса корпоративной сети образовательной организации в связи с постоянно обновляющимися угрозами информационной безопасности должно происходить с учетом специфики такой сети и в соответствии с эффективными трендами обеспечения информационной безопасности, реализуемыми при комплексном подходе.

Необходимо отметить, что технические стороны информационной безопасности систем различной природы отражены в работах Г.А. Бузова, С.В. Калинина, А.В. Кондратьева, А.П. Зайцева, Р.В. Мещерякова, А.А

Шелупанова, А.П. Тимофеева, А.В. Соколова, В.Г. Проскурина, О.Ю. Макарова и других.

Однако, потребность в создании оптимальной системы информационной безопасности посредством разработки и исследовании методов противодействия утечки информации по каналам связи в образовательной организации остается **актуальной** и представляет, как научный, так и практический интерес.

Набор мер и методов противодействия не может быть типовым, а зависит от условий конкретной образовательной организации, специфики оборота защищаемых информационных ресурсов организации, уровня технической оснащенности систем связей и других.

Таким образом, **проблема исследования** состоит в необходимости обновления теоретических знаний и практических разработок по противодействию утечки информации по техническим каналам в системах связи в образовательной организации при обновлении аппаратно-технологического базиса каналов связи.

Объектом исследования выступает система информационной безопасности образовательной организации среднего профессионального образования (СПО), а **предметом исследования** – организация защиты информации от утечки по техническим каналам в системах связи образовательной организации в образовательном процессе организации СПО.

Целью исследования является разработка рекомендаций по противодействию утечке информации по техническим каналам в системах связи образовательной организации. ГБПОУ «ЮУГК».

В соответствии с целью, объектом и предметом исследования были поставлены следующие **задачи**:

1. Определить глоссарий, основные понятия, использованные в магистерском исследовании.

2. Описать классификацию технических каналов утечки информации (далее – ТКУИ), угрозы и меры защиты.

3. Определить информационные ресурсы образовательной организации, подлежащие защите от утечки информации по ТКУИ.

4. Проанализировать состояние защиты информации от утечки в системах связи в ГБПОУ «Южно-Уральский государственный колледж».

5. Разработать меры по противодействию утечке информации в системах связи образовательной организации.

6. Привести экономическое обоснование рекомендаций по противодействию утечке информации в системах связи образовательной организации.

Гипотеза исследования состоит в предположении о том, что эффективность защиты информации от утечки в системах связи образовательной организации возможно повысить, если внедрить разработанные рекомендации по противодействию утечки информации, а также обеспечить их своевременное обновление, учитывая технические требования и минимизацию финансовых затрат.

Научная новизна проведенного исследования заключается в представлении варианта частичной модернизации системы информационной безопасности образовательной организации.

Теоретическая значимость проведенного исследования состоит в обосновании модернизации системы информационной безопасности образовательной организации ГБПОУ «ЮУГК» посредством внедрения практической разработки защиты технических каналов связи.

Практическая значимость работы заключается в разработке рекомендаций по противодействию утечке информации по техническим каналам в системах связи образовательной организации ГБПОУ «ЮУГК».

Проведенные исследования и полученные результаты могут быть использованы для повышения эффективности комплексной системы защиты информационных ресурсов в иных образовательных организациях.

База исследования: ГБПОУ СПО «Южно-Уральский государственный колледж».

Личное участие соискателя состоит в анализе информационной безопасности системы связи ГБПОУ «ЮУГК» и разработке рекомендаций по защите информации от утечки в системах связи.

Структура магистерской диссертации состоит из введения, двух глав, заключения, списка использованных источников, приложения.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАЗРАБОТКИ РЕКОМЕНДАЦИЙ ПО ЗАЩИТЕ ТЕХНИЧЕСКИХ КАНАЛОВ В СИСТЕМАХ СВЯЗИ

1.1 Глоссарий, основные понятия, использованные в магистерском исследовании

Основные определения понятийного аппарата нашего диссертационного исследования определяет Федеральный закон от 27 июля 2006г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3].

– **атака** – действие, предпринимаемое нарушителем, в поиске и использовании той или иной уязвимости информационной системы с целью получения доступа к информации.

– **владелец ресурсов, технологий и систем** – субъект с полномочиями владения и пользования указанными объектами.

– **документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

– **доступ к информации** - возможность получения информации и ее использования;

– **защищаемая информация** – информация, подлежащая защите в соответствии с требованиями правовых документов или требованиями, выдвигаемыми собственником информации.

– **информационный актив** – это материальный или нематериальный объект, который:

1. Является информацией или содержит информацию.
2. Служит для обработки, хранения или передачи информации.

3. Имеет ценность для организации.

– **идентификация пользователя** – однозначное распознание уникального имени субъекта информационной системы;

– **информационная безопасность** - меры, принятые для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним;

– **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

– **информационная система персональных данных (ИСПДн)** информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без наличия таких средств;

– **информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

– **информационные процессы** – процессы сбора, накопления, обработки хранения, распределения и поиска информации;

– **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

– **информация** - сведения (сообщения, данные) независимо от формы их представления;

– **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации,

требование не передавать такую информацию третьим лицам без согласия ее обладателя;

– **непреднамеренное воздействие на защищенную информацию** – воздействие на нее из-за ошибок пользователя, сбой техники, или программных средств, природных явлений и других непреднамеренных воздействий (например, уничтожение документа на накопителе на жестком диске);

– **несанкционированное воздействие на защищенную информацию** – воздействие с нарушением правил ее изменения (например, подмена электронных документов);

– **несанкционированный доступ** – получение защищенной информации заинтересованным субъектом с нарушением правилом доступа к ней;

– **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

– **обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

– **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

– **оператор персональных данных** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие

и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки;

– **персональные данные (ПДн)** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу – субъекту ПДн;

– **побочные электромагнитные излучения и наводки (ПЭМИН)** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания;

– **пользователь информационной системы** – субъект, обращающийся к информационной системе за получением нужной информации и пользующийся ею;

– **предоставление информации** - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

– **распространение информации** - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

– **собственник информационных ресурсов, технологий и систем** – субъект с правом владения, пользования и распределения указанных объектов;

– **технический канал утечки информации (ТКУИ)** - совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

– **угроза информационной безопасности в информационной системе** – события или действия, которые могут вызвать изменения

функционирования информационной системы, связанные с нарушением защищенности информации, обрабатываемой в ней;

– **утечка информации** – неконтролируемое распространение защищенной информации путем ее разглашения, несанкционированного доступа;

– **утечка (информации) по техническому каналу** - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

– **уязвимость информации** – это возможность возникновения на каком-либо этапе жизненного цикла информационной системы такого ее состояния, при котором создастся условия для реальной угрозы безопасности в ней;

– **шифрование информации** – преобразование информации, в результате, которого содержание информации становится непонятным для субъекта, не имеющего соответствующего доступа;

– **электронное сообщение** – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Все вышеперечисленные ключевые понятия были использованы при описании проведенного магистерского исследования.

1.2 Классификация технических каналов утечки информации, угрозы и меры защиты

Информация передается полем или веществом. Это может быть либо акустическая волна, либо электромагнитное излучение, либо лист бумаги с текстом и т.п. Другими словами, используя те или иные физические поля, человек создает систему передачи информации или систему связи. Система связи в общем случае состоит из передатчика, канала передачи информации, приемника и получателя информации. Легитимная система

связи создается и эксплуатируется для правомерного обмена информацией. Однако ввиду физической природы передачи информации при выполнении определенных условий возможно возникновение системы связи, которая передает информацию вне зависимости от желания отправителя или получателя информации - технический канал утечки информации.

Классификация ТКУИ отражена на рисунке 1 [26].

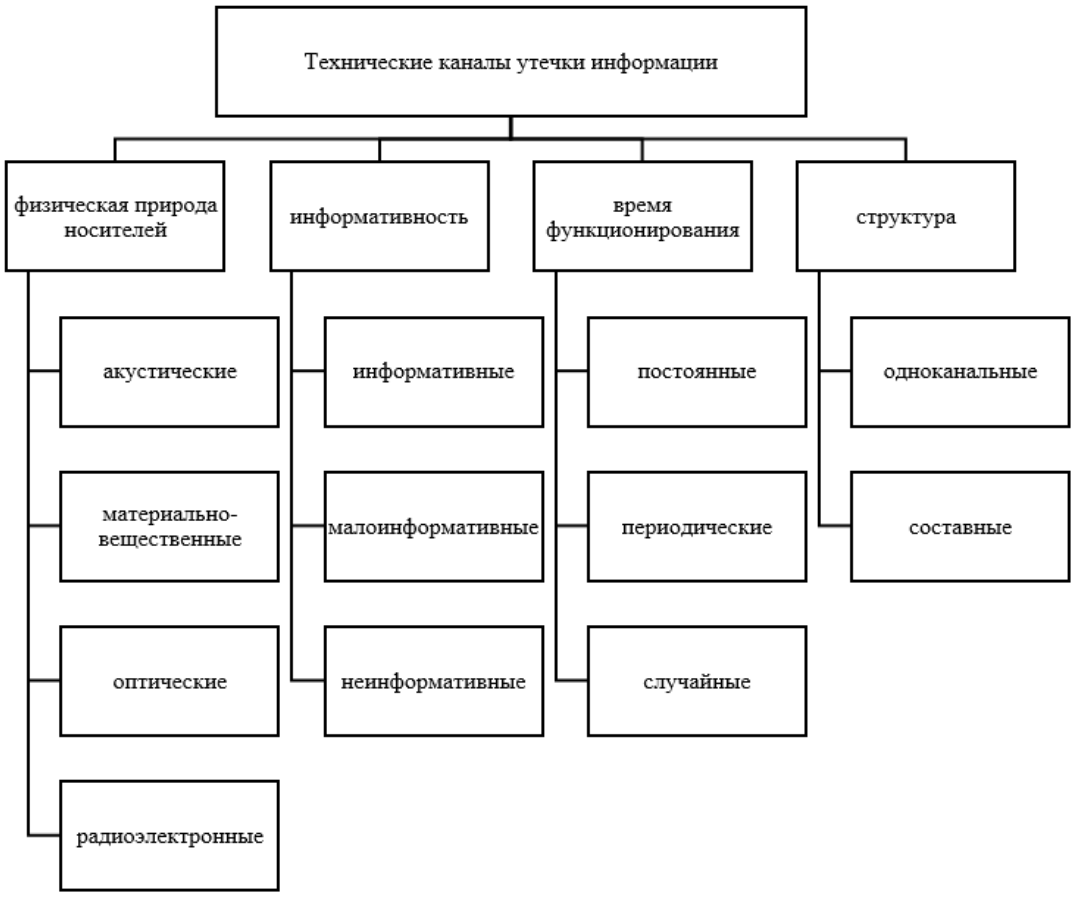

Рисунок 1 – Общая классификация технических каналов утечки информации

Через акустический канал информация передаётся звуковыми волнами в инфразвуковом, звуковом и ультразвуковом частотных диапазонах, которые распространяются через атмосферу, воду и твёрдую поверхность.

По материальному каналу утечка происходит из-за несанкционированного распространения информации на физических носителях за пределы организации.

Носителем информации в оптическом канале является электромагнитное поле.

В случае утечки информации по радиоэлектронному каналу носителем являются электрические, магнитные и электромагнитные поля.

Оценка информативности канала производится исходя из важности информации, которая передается по каналу.

При постоянном функционировании канала утечка информации называется систематической.

Во время периодического функционировании канала утечка происходит с определённым интервалом времени.

При случайном функционировании канала утечка происходит нерегулярно.

Канал утечки информации будет называться одноканальным, если он состоит из передатчика, среды распространения и приемника.

Утечка информации через составной канал возможна, если она происходит через параллельные или последовательные каналы.

Описание угрозы утечки информации по ТКУИ:

1. Источник угрозы (приемник информативного сигнала).
2. Среда (путь) распространения информационного сигнала.
3. Источник (носитель) информации.

Источники угроз утечки информации по ТКУИ:

1. Физические лица, не имеющие доступа к ИС.
2. Зарубежные спецслужбы или организации.
3. Криминальные группировки.

ТКУИ, приводящие к возникновению угроз безопасности информации:

1. Угрозы утечки акустической (речевой) информации.
2. Угрозы утечки видовой информации.
3. Угрозы утечки информации по каналам ПЭМИН.

Технические каналы утечки информации при ее передаче по каналам связи можно увидеть на рисунке 2.

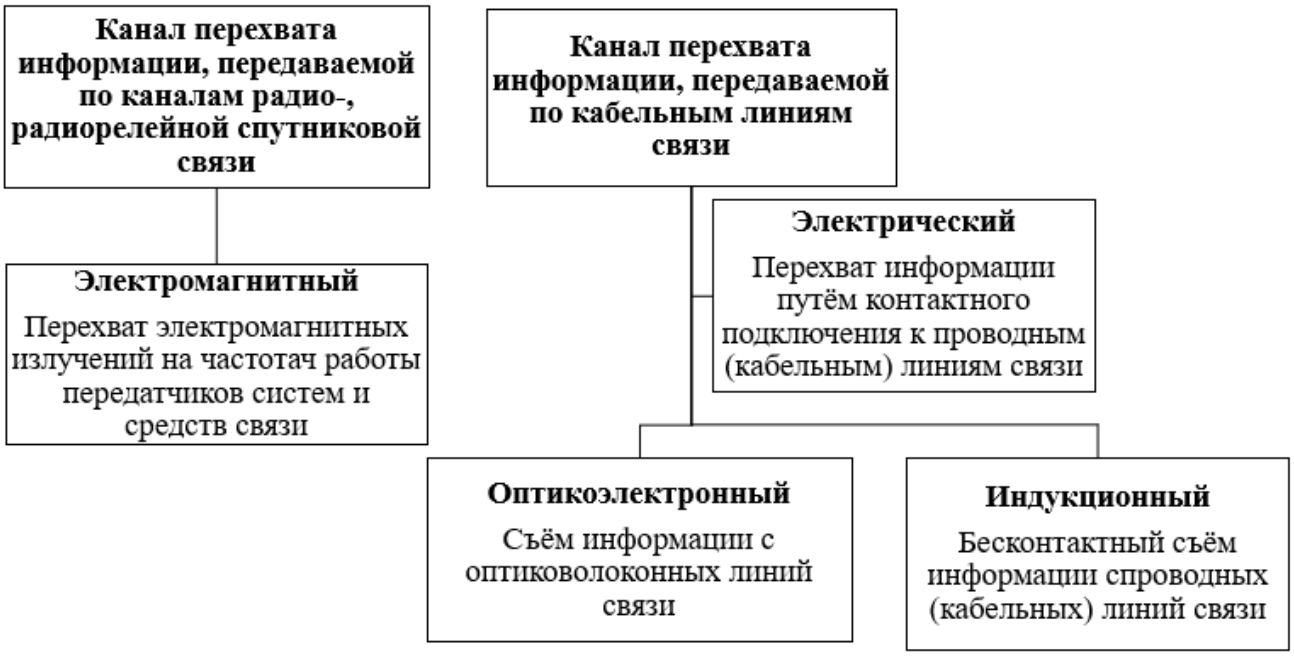

Рисунок 2 – Технические каналы утечки информации по каналам связи

Задачи защиты информации от утечки:

– выявление источника утечки информации;

– защита информации от утечки;

– оценка причинённого ущерба.

Методы, применяемые для защиты информации от утечки по ТКУИ:

1. Информационное скрытие – достигается изменением информационной структуры сообщения или объекта наблюдения.

Информационное скрытие семантической (смысловой) информации наиболее эффективно обеспечивается средствами криптографической защиты (шифрования).

Информационное скрытие объектов наблюдения осуществляется маскировкой.

2. Энергетическое скрытие – достигается снижением отношения сигнал/шум на входе приемного устройства нарушителя ниже допустимого (нормированного) значения.

Приводит к сокращению размеров зоны доступности (электромагнитной, акустической и т.п.) информационных сигналов для средств разведки нарушителя.

Классификация технических способов защиты информации в зависимости от используемых средств:

1. Пассивные:

– ослабление ПЭМИ;

– ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны;

– ослабление проникновения информационных сигналов в цепи электропитания аппаратных средств ИС, выходящие за пределы контролируемой зоны.

2. Активные:

– создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств;

– создание маскирующих электромагнитных помех в цепях электропитания аппаратных средств ИС;

– создание маскирующих электромагнитных помех в цепях заземления ИС.

При организации защиты информации от утечки необходимо учитывать некоторые особенности:

– утечку сложно обнаружить в результате уменьшения количества информации источника;

– утечка может произойти только при попадании к злоумышленнику.

Первая особенность не позволяет вовремя обнаружить утечку информации. В данных обстоятельствах сложно найти прямые свидетельства утечки: физические носители на месте, нет следов

проникновения. Утечка информации такого рода может быть обнаружена по косвенным признакам: появление на рынке похожего товара, не исполнение договора. Задержка в проявлении признаков утечки информации затрудняет устранение последствий хищения.

Суть второй особенности в том, что факт передача сведений, составляющих конфиденциальную информацию, распространения физических носителей за пределы охраняемой зоны не всегда приводят к утечке информации. В качестве примера можно привести беседу в кабинете директора образовательной организации, когда сообщается конфиденциальная информация, а в это время в приемной находится посетитель, который случайно слышит разговор, но решает не использовать полученную информацию, в этом случае утечки не произошло.

Система связи – совокупность среды передачи (канала связи), оконечного оборудования (терминальное устройство) источника и получателя данных (сообщения), характеризующаяся определенными способами преобразования передаваемого сообщения в сигнал и восстановления сообщения по принятому сигналу [18].

Основываясь на понятии ТКУИ и систем связи можно уточнить понятие ТКУИ в образовательной организации: «Технический канал утечки информации в системах связи образовательной организации – это путь сигнала от источника сообщения по каналам утечки, таким как телефонные линии, локальная и беспроводная сеть, к принимающему устройству злоумышленника» [27].

Выделяют следующие виды систем связи:

– кабельные линии связи;
– беспроводные линии связи;
– телекоммуникационные сети.

Кабельная линия связи – линия связи, состоящая из кабеля, кабельной арматуры и кабельных сооружений.

Беспроводные линии связи образуются с помощью передатчика и приемника радиоволн.

Телекоммуникационная сеть – множество средств телекоммуникации, связанных между собой и образующих сеть определённой топологии. Телекоммуникационными сетями являются:

– телефонные сети для передачи телефонных данных;

– радиосети для передачи аудиоданных;

– телевизионные сети для передачи видеоданных;

– цифровые сети или сети передачи данных для передачи цифровых данных [18].

К методам защиты информации от утечки в системах связи можно отнести:

– ограничение доступа на физическом уровне;

– изменение формы сигнала для затруднения восприятия злоумышленником информации;

– организационные меры;

– применение нормативно-законодательной базы в области защиты информации;

– сочетание программных и аппаратных методов защиты информации;

– использование криптографических методов защиты информации.

Организационными мерами защиты называют нормативно-правовые акты, которые регулируют процессы функционирования системы обработки данных, использование ее ресурсов, взаимоотношение пользователей и системы таким образом, чтобы усложнить или предотвратить появление угроз информационной безопасности.

Комплекс организационных мероприятий включает разработку следующей необходимой документации:

1. Должностные инструкции.
2. Положения об обработке персональных данных.
3. Приказы.
4. Журналы:

– журнал регистрации выявленных нарушений;

– журнал регистрации используемого программного обеспечения;

– журнал по учету носителей информации, содержащих персональные данные.

К аппаратным средствам защиты информации относятся механические, электромеханические, электронные устройства, реализующие защиту информации на физическом уровне. Они позволяют предотвратить физическое проникновение, ибо лимитировать допуск ко сведениям.

Устранение допуска гарантируют электрические замки, приборы с целью ввода идентифицирующей пользователя информации, сигнализация.

К устройствам, ограничивающим доступ к данным, можно отнести сетевые фильтры, сканирующие радиоприемники и множество других устройств, которые устраняют возможные каналы утечки информации.

Программные средства защиты данных — это специализированные программы и сложные комплексы программ, исполняющие функции защиты и входящие в структуру программного обеспечения систем обработки данных.

Программные методы позволяют защитить информацию от несанкционированного доступа, копирования и заражения вирусами.

Криптографические методы защиты информации — это специальные методы шифрования, кодирования или иного преобразования информации,

в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования.

1.3 Информационные ресурсы образовательной организации, подлежащие защите от утечки информации по техническим каналам

К наиболее значимым информационным активам, которые могут передаваться по ТКУИ, в образовательной организации можно отнести:

– персональные данные студентов и преподавателей;

– информация, которая обеспечивает образовательный процесс.

Оценим безопасность названных информационных активов с помощью методики, изложенной в ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий» [12].

Коллегиально было установлено, что наиболее вероятными угрозами могут быть:

1. Неисправности в системе электроснабжения.
2. Нелегальное проникновение злоумышленников под видом санкционированных пользователей.
3. Незаконное использование программного обеспечения.
4. Доступ несанкционированных пользователей к сети.
5. Перехват информации.
6. Несанкционированное проникновение к средствам связи.

К уязвимостям системы обеспечения информационной безопасности в образовательной организации можно отнести:

1. Отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц (возможна, например, угроза хищения).
2. Подверженность воздействию влаги.

3. Незащищенные подключения к сетям общего пользования (возможна, например, угроза использования программного обеспечения несанкционированными пользователями).

4. Незащищенные потоки конфиденциальной информации (возможна, например, угроза перехвата информации).

5. Незащищенные линии связи.

Проанализируем угрозы с помощью ранжирования по мерам риска для выбранных информационных активов согласно ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий» [12].

В столбец *a* мы записываем угрозы, в столбец *b* записываем оценку воздействия (ценности актива) по шкале от 1 до 5, в столбец *c* записывается вероятность возникновения угрозы также по шкале от 1 до 5, в столбце *d* рассчитывается мера риска, путём умножения столбцов *b* и *c*, в столбце *e* происходит ранжирование угроз исходя из результатов столбца *d*. Полученные результаты отражены в таблице 1.

Таблица 1 – Ранжирование угроз по мерам риска

Дескриптор угроз *a*	Оценка воздействия (ценности актива) *b*	Вероятность возникновения угрозы *c*	Мера риска *d*	Ранг угрозы *e*
Неисправности в системе электроснабжения	2	3	6	4
Нелегальное проникновение злоумышленников под видом санкционированных пользователей	3	3	9	3
Незаконное использование программного обеспечения	3	2	6	5
Доступ несанкционированных пользователей к сети	3	2	6	6
Перехват информации.	4	4	16	1
Несанкционированное проникновение к средствам связи	4	3	12	2

По результатам применения алгоритма оценки наиболее значимых рисков информационной безопасности можно определить, что перехват информации является лидирующей угрозой для информационных активов, на втором месте несанкционированное проникновение к средствам связи, на третьем месте нелегальное проникновение злоумышленников под видом санкционированных пользователей.

Учитывая важность сохранения конфиденциальности ПДн в образовательной организации, необходимо обратить внимание на защиту именно этого актива в контексте исследования, то есть по ТКУИ.

Образовательная организация, как оператор персональных данных (конфиденциальной информации), обязана в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ (ред. от 24.04.2020) «О персональных данных» обеспечивать защиту персональных данных во внедряемых информационных системах с момента их ввода в эксплуатацию.

Действия образовательной организаций по внедрению и функционированию системы информационной безопасности персональных данных основываются на всей совокупности нормативно-методических документов и требований по организации защиты персональных данных в образовательной организации, действующих на территории РФ.

В Постановлении Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» перечислены категории персональных данных [8].

Всего их четыре: общие (или общедоступные), специальные, биометрические и иные.

Общие персональные данные.

К ним законодательство о персональных данных относит базовые личные данные: ФИО, место регистрации, информация о месте работы, номер телефона, email. Обычно эти данные и так известны некоторым

другим людям, могут быть опубликованы в общедоступных источниках. Например, о месте работы человека могут знать его друзья в социальных сетях.

Специальные персональные данные.

Информация о личности человека: расовая и национальная принадлежность, политические, религиозные и философские взгляды, состояние здоровья, подробности интимной жизни, информация о судимостях.

Специальные категории персональных данных отличаются от общих тем, что обычно находятся в закрытом доступе. Их можно узнать только лично у человека, либо сделав официальный запрос в больницу, полицию или суд. Чаще всего сообщать эти данные человек не обязан, они — его личное дело.

Биометрические персональные данные.

Это физиологические или биологические особенности человека, которые используют для установления его личности. К ним могут относиться фотографии, отпечатки пальцев, группа крови, генетическая информация.

Однако все эти данные не всегда являются биометрическими. Согласно разъяснению правительства, они становятся такими, только если вы храните их с целью идентификации личности.

Например, если на проходной стоит камера с распознаванием лиц, фотографии сотрудников будут биометрическими данными — именно по ним вы определяете личность человека.

А если к личному делу сотрудника или профилю клиента прикреплена его фотография – эти данные не биометрические. В организации не используется фото для идентификации, а является лишь дополнением к ПДн.

То же самое касается других подобных данных, в том числе медицинских. Если их используют просто для сбора информации о пациенте, они не биометрические, а общие или специальные.

Иные персональные данные.

В эту категорию ПДн относят всё, что нельзя отнести к общедоступным, специальным или биометрическим данным: принадлежность к определенной социальной группе, к примеру, членство в клубе, или корпоративные данные, например, то, что хранится в бухгалтерии: зарплата, периоды отпусков, стаж и так далее.

Иные данные сложнее всего отличить от специальных. Разница в следующем:

Специальные данные характеризуют человека как личность, часто человеку важно, чтобы посторонние их не знали.

Иные данные – это просто дополнительная информация, они часто могут меняться.

Важной частью образовательного процесса является защита информации образовательной организации.

Система защиты информации образовательной организации должна обеспечивать безопасность баз данных и конфиденциальной информации.

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты.

Персональные данные субъектов ПДн в образовательной организации, как правило состоят из следующих реквизитов-полей:

– фамилия, имя, отчество;
– дата рождения;
– место рождения;
– пол;
– возраст;

– номер лицевого счета, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета;

– данные документа, удостоверяющего личность (свидетельство о рождении/паспорт);

– адрес проживания;

– адрес регистрации;

– гражданство;

– семейное положение;

– социальное положение;

– реквизиты документа, подтверждающие наличие льготы (название документа и номер документа);

– сведения о здоровье (медицинская группа здоровья, медицинская группа здоровья для занятия физической культурой, инвалидность, сведения об ограниченности возможностей здоровья, наличие потребности в длительном лечении);

– сведения о дошкольном образовании (зачисление в образовательную организацию, образовательная программа, форма обучения, форма финансирования, группа, прекращение образовательных отношений);

– сведения о начальном, основном и среднем общем образовании (зачисление в образовательную организацию, образовательная программа, форма обучения, форма финансирования, учебный класс, учебная смена, годовая успеваемость, результаты обучения, итоговая успеваемость, мероприятия по профессиональной ориентации обучающихся, внеурочная деятельность, прекращение образовательных отношений, документ об образовании);

– сведения о среднем профессиональном образовании (зачисление в образовательную организацию, образовательная программа, профессия или специальность, форма обучения, форма финансирования,

учебная группа, результаты обучения, прекращение образовательных отношений, документ об образовании);

– сведения о высшем образовании (зачисление в образовательную организацию, отчисление из образовательной организации);

– сведения о дополнительном образовании (зачисление в образовательную организацию, образовательная программа, форма обучения, форма финансирования, результаты освоения образовательной программы, прекращение образовательных отношений, документ об образовании);

– сведения о дополнительном профессиональном образовании (зачисление в образовательную организацию, образовательная программа, форма обучения, форма финансирования, прекращение образовательных отношений, документ об образовании и/или о квалификации);

– сведения о профессиональном обучении (зачисление в образовательную организацию, образовательная программа, форма обучения, форма финансирования, прекращение образовательных отношений, документ об образовании и/или о квалификации);

– портфолио (уровень образования, на котором обучающийся получил достижение, уровень мероприятия, название мероприятия, дата участия, результаты участия, полученные награды, присвоенные разряды и пр.);

– сведения о документе об образовании (наименование документа об образовании, номер и серия бланка документа об образовании, регистрационный номер и дата выдачи документа об образовании, наименование организации, выдавшей документ об образовании, наименование образовательной программы, наименование профессии, специальности, направления подготовки (при наличии),

наименование присвоенной квалификации (при наличии), срок обучения, год поступления на обучение, год окончания обучения);

– тип законного представителя;

– реквизиты документа, подтверждающего полномочия законного представителя по отношению к ребенку;

– место работы;

– контактный телефон;

– электронная почта;

– идентификационный номер налогоплательщика;

– должность;

– сведения об аттестации;

– сведения о приеме (увольнении);

– количество занимаемых ставок.

Система защиты информационных активов от утечек по техническим каналам должна разрабатываться на высоком уровне, применяя новые технические средства защиты данных, рассматривая в качестве наиболее защищаемого актива ПДн.

Вывод по первой главе

В первом параграфе был представлен глоссарий основных понятий, использованных в ходе магистерского исследования, основанный на Федеральном законе от 27 июля 2006г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Второй параграф исследования описывает классификацию ТКУИ, угрозы ТКУИ и возможные методы, средства и меры защиты информации от утечки.

В третьем параграфе были определены информационные активы образовательной организации, подлежащие защите от утечки по ТКУИ, проведена оценка безопасности активов и была определена потенциально опасная угроза для этих активов.

ГЛАВА 2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ПРОТИВОДЕЙСТВИЮ УТЕЧКИ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ГПБОУ «ЮУГК»

2.1 Анализ состояния защиты информации от утечки в технических каналах систем связи в ГБПОУ «Южно-Уральский государственный колледж»

Колледж является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа. Главная цель и направление деятельности ГБПОУ «Южно-Уральский государственный колледж» – повышение качества знаний и уровня профессиональных компетенций выпускников колледжа за счет разработки, создания и внедрения инновационных образовательных технологий, основанных на E-Learning, электронных учебно-методических комплексах, компетентностном подходе. Данные технологии и формы обучения позволили реально повысить качество профессиональной подготовки, прежде всего практического обучения, и сделали выпускников колледжа востребованными на рынке труда.

На протяжении ряда лет Южно-Уральский государственный колледж (бывший Челябинский колледж информационно-промышленных технологий и художественных промыслов, бывший Челябинский экономический колледж) занимается разработкой и внедрением в учебном процессе интенсивных информационных образовательных технологий, основанных на широком использовании компьютерной и коммуникационной техники, электронных обучающих программ, проектной культуры. Это позволяет колледжу активно решать проблемы доступности, эффективности и качества профессиональной подготовки современных специалистов для отраслей предприятий России. Педагоги колледжа имеют опыт практической работы по соответствующей

специальности и глубокую теоретическую подготовку, необходимую для успешной реализации профессиональных образовательных программ. Среди них – кандидаты наук, заслуженные работники образования РФ, преподаватели высшей категории.

Для эффективного взаимодействия с учетом большого контингента обучающихся и месторасположением учебных зданий после реорганизации были определены образовательные комплексы (по территориальному признаку и направлениям подготовки):

1. Образовательный комплекс Информационных технологий и экономики (г. Челябинск, ул. Курчатова, д.7).
2. Образовательный комплекс Промышленной автоматики (г. Челябинск, ул. Доватора, д.38).
3. Образовательный комплекс Промышленного дизайна и торговли (г. Челябинск, ул. Блюхера, д.1А).
4. Отделение Дизайна (г. Челябинск, ул. Блюхера, д.3А).

Объекты для проведения практических занятий

В колледже имеется 57 оборудованных учебных аудитории и лабораторий, 33 компьютерных класса, учебные полигоны, залы дипломного проектирования, слесарные мастерские, электромонтажные мастерские, механообрабатывающие мастерские, участок станков с ЧПУ, ювелирные мастерские, литейная мастерская, камнерезная мастерская. Количество и перечень кабинетов, лабораторий, мастерских и других помещений соответствует требованиям ГОС и ФГОС по направлениям подготовки.

ГБПОУ «Южно-Уральский государственный колледж» обладает специализированным и лабораторным оборудованием, соответствующим реализации профессиональных образовательных программ.

Наличие оборудованных учебных кабинетов

Обеспеченность кабинетов учебных дисциплин общеобразовательного цикла лабораторным оборудованием соответствует

реализуемым образовательным программам по профилю подготовки профессионального образования.

В соответствии с рабочей программой часть занятий по иностранному языку проводится в лингафонных кабинетах, оборудованных комплектом мультимедиа аппаратуры.

Важная задача комплексной информационной безопасности в образовательном учреждении – это обеспечение организации защиты персональных данных.

Одним из элементов защиты персональных данных является разграничение прав доступа к персональным данных. Так студенты должны получить доступ только к своим персональным данным, тогда как посторонний человек не должен получить доступ к данным студентов, не говоря уже о сотрудниках образовательной организации. В ГБПОУ «ЮУГК» применяется разграничение прав доступа при входе в операционную систему и при работе с различными информационными системами.

В ГБПОУ «ЮУГК» реализован Web-сервис обмена данными между сайтом и 1С Колледж ПРОФ. Он позволяет студентам и их родителям (законным представителям), использующим пару логин-пароль, получить доступ только к своим оценкам и посещаемости через сайт колледжа, но при этом данные студентов не хранятся в базе данных сайта, а поступают напрямую от базы данных 1С Колледж ПРОФ в момент обращения пользователя к сайту.

Связь между базами организована по индивидуальному номеру, присваиваемому каждому студенту в 1С Колледж ПРОФ при зачислении в образовательную организацию.

После формирования приказа о зачислении в 1С Колледж ПРОФ на электронную почту студента, указанную в анкете при поступлении, отправляется данные для входа на сайт колледжа.

В ГБПОУ «ЮУГК» используется несколько программных продуктов для защиты информации от утечки информации по техническим каналам в системах связи:

1. Ideco.
2. ViPNet.
3. Dallas Lock.
4. Средство антивирусной защиты Kaspersky Endpoint Security для Windows.

Ideco UTM (Unified Threat Management – Унифицированное управление угрозами) — российское программное UTM-решение, предназначенное для защиты сетевого периметра, контроля и фильтрации Интернет-трафика в корпоративных и частных сетях. Сертифицирован ФСТЭК [36].

Компания-разработчик — «Айдеко» основанной в 2005 году в Екатеринбурге.

Ideco UTM служит для распределения, учёта и контроля доступа в Интернет на предприятиях, в частных и провайдерских сетях. Ideco UTM основан на операционной системе Fedora. Установка может производиться как на отдельный сервер, так и на виртуальную машину. Управление интернет-шлюзом осуществляется через графический веб-интерфейс из-под любой распространенной операционной системы (Windows, Linux, Mac OS), а также через локальное меню в консоли. Может поставляться с коммерческими антивирусными продуктами.

Включает в себя следующие модули:

1. VPN-сервер.
2. Система авторизации пользователей.
3. Система предотвращения вторжений.
4. Контент-фильтр.
5. Контроль приложений.
6. Управление полосой пропускания.

7. Кластеризация.

8. Антивирусная и антиспам-проверка трафика.

9. Маршрутизация.

Сертифицирован ФСТЭК РФ. Номер сертификата 4503, срок действия 28.12.2026. Соответствует требованиям документов: Требования доверия (4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ(Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ).

Программно-аппаратный комплекс Ideco UTM обладает следующими особенностями и функциональными возможностями:

1. Система предотвращения вторжений — предназначена для выявления и предотвращения вредной и потенциально опасной сетевой активности в защищаемой сети. Осуществляется в том числе предупреждение вирусной активности внутри сети, блокирование атак, DoS, шпионских программ, телеметрии Windows, командных центров ботнетов, криптомайнеров. Также выполняется блокировка неблагонадёжных регионов по GeoIP и репутации IP-адресов.

2. Контент-фильтр — осуществляет анализ посещаемых пользователем веб-ресурсов с целью предотвращения доступа к запрещённым или вредоносным ресурсам.

3. Контроль приложений — обеспечивает определение программ независимо от используемого сетевого порта на 7-м уровне модели OSI. Многоуровневая антивирусная и антиспам-проверка трафика — обеспечивается антивирусный анализ внешними антивирусными фильтрами от «Лаборатории Касперского».

ИнфоТеКС (Информационные Технологии и Коммуникационные Системы) — российский разработчик программно-аппаратных VPN-решений и средств криптографической защиты информации. Компания основана 6 сентября 1991 года группой специалистов по информационной

безопасности во главе с Андреем Чапчаевым. ИнфоТеКС входит в ТОП-5 крупнейших компаний России в сфере защиты информации (согласно рейтингу CNews «Крупнейшие компании России в сфере защиты информации 2019») [38].

Флагманская разработка ИнфоТеКС — технология ViPNet, гибкое VPN-решение для безопасной передачи данных в защищённой сети.

Технология ViPNet

Для защиты информации, передаваемой по открытым каналам связи, поддерживающим протоколы TCP/IP, компания «Инфотекс» предлагает семейство продуктов ViPNet.

Технология ViPNet предназначена для создания целостной системы доверительных отношений и безопасного функционирования технических средств и информационных ресурсов корпоративной сети, взаимодействующей также и с внешними техническими средствами и информационными ресурсами.

Программное обеспечение ViPNet Client предназначено для использования в сетях ViPNet, управляемых с помощью ПО ViPNet Administrator. ViPNet Client выполняет функции VPN-клиента в сети ViPNet и обеспечивает защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях.

Программное обеспечение ViPNet Client может быть установлено для защиты трафика на любом компьютере с ОС Windows, будь то стационарный, удаленный, мобильный компьютер или сервер.

Возможности:

1. VPN-клиент (шифрование и защита IP-пакетов от навязывания ложных данных).
2. Контроль сетевой активности приложений и компонентов операционной системы.
3. ViPNet Client работает в составе сети ViPNet и совместим со всеми продуктами линейки ViPNet Network Security.

Dallas Lock — система защиты информации от несанкционированного доступа в процессе её хранения и обработки. Представляет собой программный комплекс средств защиты информации в автоматизированных системах [40].

Компания «Конфидент» работает на российском рынке услуг в области информационной безопасности с 1992 года.

Центр защиты информации компании «Конфидент» – российский разработчик линейки сертифицированных средств защиты информации. Продукты компании применяются для защиты конфиденциальной информации, в том числе содержащейся в ГИС, ИСПДн, АСУ ТП и значимых объектах КИИ, а также сведений, составляющих государственную тайну до уровня «совершенно секретно» включительно.

Решения компании «Конфидент» регулярно проходят инспекционный контроль, подтверждая надежность и качество новых функциональных возможностей. Они одинаково эффективны для защиты как малых сетей, так и масштабных сетевых инфраструктур.

ЦЗИ компании «Конфидент» активно развивает партнерскую сеть. Сегодня в ее состав входят более 700 партнеров по всей территории России, включая ведущих интеграторов и региональные аттестационные центры.

Центр защиты информации осуществляет свою деятельность на основании лицензий ФСТЭК России, ФСБ России, Роскомнадзора и Минобороны России.

Kaspersky Endpoint Security от «Лаборатории Касперского» — решение для обеспечения многоуровневой защиты и реализации расширенных возможностей управления ИТ-средой организации.

Ключевые возможности продукта:

– выявление аномалий в корпоративной сети в автоматическом режиме;

– защита от угроз даже без регулярных обновлений;

– нейтрализация попыток майнинга на рабочих устройствах;

– обнаружение вредоносных программ; предотвращение вторжений и настройка политик информационной безопасности с использованием облака – все это в единой веб-консоли управления защитой всех узлов сети [42].

На сегодняшний день такое состояние защиты от утечки информации по ТКУИ имеет ГБПОУ «ЮУГК».

2.2 Меры по противодействию утечке информации в технических каналах систем связи ГБПОУ «Южно-Уральский государственный колледж»

В широком смысле принимаемые меры для защиты информации от утечки по ТКУИ можно разделить на две большие категории:

1. Организационные.
2. Технические.

Организационные меры по защите информации – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией, и включает в себя организацию режима охраны, организацию работы с сотрудниками, с документами, организацию использования технических средств и работу по анализу угроз информационной безопасности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, т.к. возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются не техническими аспектами, а злоумышленными действиями, небрежностью и халатностью

пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы несанкционированный доступ к конфиденциальной информации.

Организационная защита информации:

– организация работы с персоналом;

– организация внутриобъектного и пропускного режимов и охраны;

– организация работы с носителями сведений;

– комплексное планирование мероприятий по защите информации;

– организация аналитической работы и контроля;

– регулярный инструктаж по информационной безопасности.

Технические меры защиты информации – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

В ГБПОУ «ЮУГК» имеются следующие системы связи:

– телефонные линии;

– беспроводные сети;

– локальные сети.

Беспроводные сети – это часть ИТ-инфраструктуры, позволяющая передавать данные на большие и малые расстояния без использования проводов.

Для организации корпоративных WLAN (беспроводных локальных сетей) используется технология Wi-Fi и оборудование, которое соответствует стандарту IEEE 802.11.

В состав оборудования могут входить: роутеры, точки доступа, беспроводные мосты, коммутаторы, сетевые адаптеры. В качестве конечных устройств выступают рабочие станции, ноутбуки, мобильные телефоны, планшеты и другие схожие устройства.

Каждый из элементов беспроводной сети — потенциально опасный источник утечки данных, который может повлиять на работу всей локально-вычислительной сети. Поэтому оставлять сети «открытыми» — без шифрования — категорически нельзя.

В случае, если беспроводная сеть является открытой, тогда согласно требованиям ФЗ N-97 от 05.05 2014 г. «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» необходимо проводить обязательную аутентификацию пользователей.

Виды угроз для беспроводных сетей.

Возможные виды угроз:

1. Подслушивание. Организуется двумя способами: перехват радиосигнала (анонимное подслушивание) и при помощи MITM-атаки («человек посередине»).

2. DDoS-атаки. При их организации сигналы точек доступа и клиентских терминалов просто глушатся.

3. Подмена MAC-адресов клиентских устройств. Злоумышленники подменяют MAC-адрес своего устройства, выдавая его за уже зарегистрированное в сети, и получают к ней доступ.

4. Ложные точки доступа (атака Evil Twin). Организуются с целью сбора аутентификационных данных с устройств для подключения к конкретной сети.

Все беспроводные сети рано или поздно подключаются к проводным сетям, и место этого подключения может стать слабым звеном, часто это происходит из-за неправильной сегментации VLAN.

Методы защиты беспроводных сетей.

Для обеспечения защиты беспроводных сетей используется несколько методов:

1. Фильтрация по MAC-адресам. MAC-адрес – уникальный адрес Wi-Fi адаптера. То есть, у каждого устройства он свой. В настройках роутера можно прописать MAC-адреса тех устройств, которые могут подключаться к вашей сети (создать белый список адресов). Если MAC-адреса устройства в списке нет – оно к сети не подключиться. Неудобство лишь в том, что при подключении новых устройств придется заходить в настройки роутера и прописывать их MAC-адреса.

2. Повысить уровень защищённости Wi-Fi можно при помощи технологий безопасной аутентификации. Это может быть:

– аутентификация при помощи внешнего сервера;

– использование двухфакторной аутентификации.

Безопасность беспроводных локальных вычислительных сетей во многом зависит от правильных настроек сети и грамотного управления политиками. В частности, рассчитывать на высокий уровень защищённости можно при использовании таких мер, как:

1. Отключение WPS (Wi-Fi Protected Setup).

2. Использование сложных паролей и их ежеквартальная смена. сложным считается пароль от 10 символов, состоящий из букв и специальных символов.

3. Скрытый SSID. В настройках Wi-Fi сети на маршрутизаторе есть такая функция как «Скрыть SSID» (Hide SSID), или «Отключить широковещание SSID». После ее активации устройства перестанут видеть вашу Wi-Fi сеть. А чтобы к ней подключиться, нужно будет указать не только пароль, но и имя самой сети (SSID).

Средства защиты данных в беспроводных сетях.

Усилить защиту можно при помощи программных, аппаратных и аппаратно-программных средств.

Беспроводная система предотвращения вторжений (Wireless Intrusion Prevention System, сокращённо WIPS) — корпоративные системы обнаружения вторжения по Wi-Fi. Обнаруживают ложные точки доступа, выявляют признаки атак, MITM и другие виды угроз. Режим WIPS поддерживается многими точками доступа от известных производителей. Эти системы обычно реализуются как наложение на существующую инфраструктуру беспроводной локальной сети

VoIP (англ. Voice over IP – голос через IP) – это разновидность IP-телефонии, то есть передача голоса через интернет-протокол. Технология позволяет совершать звонки в обход аналоговых телефонных линий или мобильной сети — данные передаются по интернету.

Современные атаки VoIP-сетей

Среди актуальных типов атак, которым может подвергаться передаваемая информация, выделяют:

1. Перехват телефонного трафика.

Наиболее опасный способ атак, при котором сведения могут передаваться третьему лицу. Для перехвата информации используются современные устройства и технологии, которые внедряют между адресантом и получателем информации третье лицо – злоумышленника, который может прослушивать переговоры. Актуальный способ для недоброжелателей или конкурентов компании, он позволяет отследить отправленные сведения и перехватить их до момента получения. При этом, злоумышленник будет осведомлен в лишней информации и сможет ее использовать в личных целях. Отсутствие шифрования голосовых данных делает IP-телефонию уязвимой.

2. Замена или взлом.

Несанкционированный доступ со стороны третьих лиц к передаваемой информации может привести к подмене сведений. Обычно это возможно при взломе аккаунтов, данная угроза может отразиться на деятельности компании, вызвать большие финансовые траты, сорвать

важный контракт или даже повлиять на репутацию компании. Замена сведений осуществляется путем взлома, но при отсутствии защищенных каналов связи, данные могут распространяться и без наличия несанкционированного доступа со стороны мошенников или заинтересованных лиц.

3. Искажение.

Нередко передаваемая информация может искажаться или передаваться в неполной мере. Так вот прослушивание и искажение данных выполняется при отсутствии механизмов аутентификации, что приводит к нарушению безопасности. Далее могут последовать финансовые траты, использование телефонной сети, использование сведений в личных целях.

4. Запрет доступа.

Запрет доступа к передаче данных – это вполне реальная угроза, осуществляемая путем так называемой «перегрузки линии». При высокой нагрузке на сети они отказываются функционировать и исключают возможность работы IP-телефонии. Иными словами, это отсутствие связи между абонентами.

Помимо простого программного брандмауэра, установленного на каждой машине в образовательной организации, можно установить аппаратный брандмауэр, иначе называемый межсетевой экран. В отличие от программного брандмауэра, который устанавливается на каждом отдельном компьютере, аппаратный брандмауэр — это физическое устройство, сопровождаемое программным обеспечением и подключенное непосредственно к сети образовательной организации.

Подготовка, конфигурирование, мониторинг и обслуживание могут затем выполняться с одного компьютера, управляющего сетью, что позволяет быстрее внедрять и значительно меньше действий, предпринимаемых отдельными пользователями.

В то время как аппаратный брандмауэр потребует меньше действий от каждого отдельного пользователя на его собственной машине, начальная настройка, а также техническое обслуживание и мониторинг должны выполняться ИТ-специалистом.

Типы межсетевых экранов по ФСТЭК:

1. «А» — аппаратные, установленные на физических границах сети. Например, программно-аппаратные комплексы в месте физического подключения сети компании к интернету через кабель.
2. «Б» — программные и аппаратные, установленные на логических границах сети, например, встроенные в маршрутизатор.
3. «В» — программные, установленные на узлы, например, компьютеры сотрудников.
4. «Г» — аппаратные и программные, работающие с протоколами http и https, то есть с веб-трафиком.
5. «Д» — аппаратные и программные, которые работают с промышленными протоколами передачи данных.

В настоящее время интернет широко используется практически во всех образовательных учреждениях, повсеместно растет используемая ширина канала, увеличивается количество устройств, имеющих доступ в интернет.

При этом образовательные учреждения обязаны не только обеспечивать безопасность своей растущей ИТ-инфраструктуры, но также и соответствовать ряду специальных требований законодательства, имея зачастую при этом весьма ограниченные финансовые возможности.

Дополнительно к этому UserGate поддерживает максимальный набор функций, связанных с интернет-фильтрацией - фильтрацию по категориям, морфологический анализ содержимого страниц, безопасный поиск, фильтрацию баннеров и скриптов отслеживания, контроль закачек, мониторинг и статистику использования интернета.

Все это позволяет блокировать опасные сайты, связанные с порнографией, наркотиками, суицидом, экстремизмом, а также обеспечить исполнение любых политик доступа.

Сети любого размера должны быть защищены от внешних атак, вирусов и разнообразных современных киберугроз. UserGate является компактным и удобным в настройке сетевым устройством, способным обеспечить безопасность сетей небольших организаций или филиалов с числом пользователей от нескольких десятков до сотни и более.

На рисунке 3 представлен межсетевой экран.

Рисунок 3 – Межсетевой экран UserGate C100

Доступность и удобство

UserGate C100 предлагается по минимальным ценам, что делает его доступным для небольших организаций, а также для использования в филиалах, таких, например, как точки продаж. Данное устройство поставляется практически готовым к использованию, и его настройка может быть произведена обычным системным администратором. UserGate C100 может использоваться в сетях с шириной канала пропускания до 2 Гб/с.

Комплексная безопасность

Несмотря на компактность и невысокую стоимость модели UserGate C100, работа устройства основана на тех же технологиях, которые используются и для защиты сетей крупных компаний. С его помощью можно обеспечить не только базовую функциональность межсетевого экранирования, но и обеспечить защиту от современных атак, анализ и

фильтрацию трафика по контенту, контроль интернет-приложений, блокирование опасных скриптов и приложений, защиту от вирусов и спама, а также другие функции безопасности. Кроме этого, UserGate C100 может обеспечить защиту гостевого Wi-Fi и дает возможность контроля персональных устройств, таких как смартфоны и планшет.

Наличие сертификата ФСТЭК России

Межсетевой экран UserGate сертифицирован ФСТЭК России по требованиям к Межсетевым Экранам (4-й класс, профили А и Б) и к Системам Обнаружения Вторжений (4-й класс), а также по 4 уровню доверия. Таким образом, UserGate может использоваться в составе автоматизированных систем (АС) до класса защищенности 1Г, значимых объектов КИИ I категории, информационных системах персональных данных (ИСПДн) 1 уровня защищенности, государственных информационных системах (ГИС) 1 класса защищенности, автоматизированных систем управления технологическими процессами 1 класса защищенности и информационных системах общего пользования II класса.

Локально вычислительная сеть (ЛВС) – это система взаимосвязанных вычислительных ресурсов (компьютеров, серверов, маршрутизаторов, программного обеспечения и др.), распределенных по сравнительно небольшой территории (офис или группа зданий), служащая для приема-передачи, хранения и обработки информации различного рода.

ЛВС представляет собой соединение нескольких ПК с помощью соответствующего аппаратного и программного обеспечения. В локальных сетях скорость передачи данных высока, протоколы в сравнении с протоколами глобальных сетей относительно просты, отсутствует избыточность каналов связи.

Защита ЛВС требует соответствующей комбинации организационных мер защиты, технических средств защиты, обучения и инструктажей пользователей и плана обеспечения непрерывной работы.

Одним из методов защиты ЛВС является установка межсетевого экрана.

Для выбора межсетевого экрана необходимо учитывать следующие требования:

– обязательная сертификация ФСТЭК;

– должно присутствовать достаточное количество портов Fast Ethernet;

– осуществление контроля на прикладном уровне с учетом состояния, контроля прикладного протокола;

– проверка пакетов на соответствие заданным условиям;

– обнаружение и предотвращение несанкционированного доступа;

– высокая производительность.

Выбор меж сетевого экрана для защиты ЛВС был сделан в пользу ALTELL NEO.

Аппаратный межсетевой экран ALTELL NEO для защита локальной сети представлен на рисунке 4.

Рисунок 4 – Межсетевой экран ALTELL NEO 110

ALTELL NEO — российские аппаратные межсетевые экраны нового поколения, сертифицированные ФСТЭК на самые высокие классы защиты. Главная особенность этих устройств — сочетание возможностей фильтрации трафика с функциями построения защищенных каналов связи (VPN), обнаружения и предотвращения вторжений (IDS/IPS) и контент-фильтрации (антивирусы, веб- и спам-фильтры, контроль приложений), что обеспечивает полное соответствие современной концепции унифицированной защиты сети (Unified Threat Management, UTM, шлюз безопасности).

Преимущества ALTELL NEO

1. Полное соответствие требованиям российского законодательства в области ИБ (сертификаты ФСТЭК и ФСБ).
2. Богатые функциональные возможности (антивирусный шлюз, почтовый фильтр, веб-фильтр).
3. Высокая производительность.
4. Контроль приложений в реальном времени.
5. Работа в конвергентных сетях (данные, голос, видео).
6. Встроенный учет трафика.
7. Бесплатная трехлетняя гарантия работоспособности устройства.
8. Бесплатная годовая техническая поддержка;
9. Автоматическое обновление в режиме PUSH.
10. Возможно использование отечественного UEFI BIOS.

На основе проведенной оценки исходной защищенности ИС и анализа нормативно-правовых требований действующего законодательства считаем необходимым рекомендовать следующие меры в ГБПОУ «ЮУГК».

Совершенствование защиты информации от утечки информации по техническим каналам в системах связи организации можно разделить на несколько этапов.

Этап 1. Разработка организационно-распорядительных и технических документов по защите персональных данных.

1. Алгоритм по применению комплекта документов по защите персональных данных в образовательной организации.
2. Акт классификации информационной системы персональных данных.
3. Акт об уничтожении бумажных носителей персональных данных субъектов персональных данных.
4. Акт об уничтожении электронных носителей персональных данных субъектов персональных данных.
5. Журнал учета паролей пользователей информационной системы персональных данных.
6. Журнал учета машинных носителей информации.
7. Журнал учета средств защиты информации, эксплуатационной и технической документации к ним.
8. Журнал учёта ключей от сейфов и помещений.
9. Журнал учета обращений субъектов информационной системы персональных данных.
10. Журнал учета проверок юридического лица.
11. Журнал учета работ в информационной системе персональных данных.
12. Инструкция администратора безопасности информационной системы персональных данных.
13. Инструкция о порядке работы с персональными данными.
14. Инструкция ответственного за организацию обработки персональных данных.
15. Инструкция по организации антивирусной защиты.
16. Инструкция по организации парольной защиты.
17. Инструкция по физической охране, контролю доступа в помещения.

18. Инструкция пользователя информационной системы персональных данных.

19. Перечень сведений, содержащих персональные данные.

20. Перечень информационных систем персональных данных.

21. Перечень автоматизированных рабочих мест.

22. Перечень общесистемного и прикладного программного обеспечения, используемого в информационной системе персональных данных.

23. Перечень серверного коммутационного и сетевого оборудования.

24. План внутренних проверок состояния защиты информационных систем персональных данных.

25. План мероприятий по защите персональных данных.

26. Политика обработки и защиты персональных данных.

27. Положение об обработке персональных данных с использованием средств автоматизации.

28. Положение об обработке персональных данных без использования средств автоматизации.

29. Правила работы с обезличенными данными.

30. Приказ о введении в действие организационно-распорядительных документов по защите персональных данных.

31. Приказ об организации работ по обеспечению безопасности персональных данных.

32. Приказ об утверждении мест хранения материальных носителей персональных данных.

33. Приказ об утверждении списка должностных лиц, которым необходим доступ к персональным данным, обрабатываемым в информационной системе.

34. Регламент резервного копирования и восстановления данных.

35. Согласия субъектов на обработку персональных данных.

36. Список лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей.

37. Список мест хранения материальных носителей персональных данных.

38. Оценка вреда субъектам ПДн ИСПДн (Акт).

39. Описание технологического процесса обработки персональных данных.

40. Справка по информационным системам персональных данных.

41. Схема внешних и внутренних потоков передачи персональных данных.

Этап 2. Повышение осведомленности/ознакомление работников в области персональных данных.

Инструктаж работников, непосредственно осуществляющих обработку персональных данных.

Этап 3. Установка и настройка технических средств защиты информации.

Техническая защита системы персональных данных осуществляется и заключается в следующем:

1. Закупить и установить средства защиты информации, сертифицированных ФСТЭК России и ФСБ России.

2. Разработать эксплуатационную документацию на технические средства защиты персональных данных.

Для обеспечения безопасности передачи информации по каналам связи необходимо и целесообразно использовать сочетание аппаратных и организационных мер защиты информации от утечки по ТКУИ.

2.3 Экономическое обоснование рекомендаций по противодействию утечке информации в системах связи образовательной организации

Приведём экономический расчёт аппаратных средств защиты информации от утечки по ТКУИ в таблице 2.

Таблица 2 – Расчёт стоимости защиты ПДн СПО ГБПОУ «ЮУГК»

Наименование	Цена, руб.	Количество	Стоимость, руб.
Аппаратный межсетевой экран UserGate C100	79000	1	79000
Аппаратный межсетевой экран ALTELL NEO 110	99000	1	99000
Аттестация информационных систем по требованиями ФСБ и ФСТЭК	30000	1	30000
		Итого	208000

В случае выявления нарушений в области обработки и обеспечения безопасности ПДн, в случае утечки информации в организации к руководителям и юридическим лицам может быть применена уголовная и административная ответственность (таблица 3), которая может применяться одновременно и в отношении организации, и в отношении руководителя организации, подразделения или виновного работника.

Таблица 3 – Нарушения в области обработки и обеспечения безопасности ПДн

Статья	Содержание статьи	Сумма штрафа, тыс. руб.
		Юр. лицо
Уголовная ответственность		
137 УК РФ	Нарушение неприкосновенности частной жизни	
ч.1	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации	до 200
ч.2	Те же деяния, совершенные лицом с использованием своего	100-300

	служебного положения	
ч.3	Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия	150-350
272 УК РФ	Неправомерный доступ к компьютерной информации	
ч.1	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации	до 200
Административная ответственность		
13.11 КоАП	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	
ч.1	Обработка персональных данных в случаях, не предусмотренных законодательством , либо обработка персональных данных, несовместимая с целями сбора персональных данных	60-100
ч 1.1	Повторное нарушение части 1	100-300
ч.2	Обработка персональных данных без согласия в письменной форме, либо обработка персональных данных с нарушением требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных	30-150
ч. 2.1.	Повторное нарушение части 2	300-500
ч. 3	Не публиковано или не обеспечен иным образом неограниченный доступ к политике в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных	30-60
ч. 4	Невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	40-80
ч. 5	Невыполнение оператором в сроки требования об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	50-90
ч. 5.1	Повторное нарушение части 5	300-500
ч. 6	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к	50-100

	ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных	
ч. 8	Невыполнение оператором при сборе персональных данных через Интернет обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации	1-6 млн
ч. 9	Повторное нарушение части 8	6-18 млн

Сопоставляя данные таблиц 2 и 3, мы видим, что экономический ущерб от утечки информации для организации значительно превышает возможные затраты на модернизацию системы защиты технических каналов связи. В данное обоснование не включены оценки репутационных рисков образовательной организации, которые зачастую оценить достаточно сложно в краткосрочной и долгосрочной перспективах.

Вывод по второй главе

В первом параграфе было проанализировано состояние защиты информации от утечки в технических каналах систем связи базы исследования с подробным описанием использующихся программным методов защиты.

Были описаны системы связи образовательной организации.

Во втором параграфе были описаны меры защиты от утечки информации по Wi-Fi, IP-телефонии и локальной сети.

В третьем параграфе исходя из предложенных мер защиты ПДн от утечки был произведён расчёт стоимости защиты ПДн СПО ГБПОУ «ЮУГК», а также рассмотрены штрафы за нарушения в области обработки и обеспечения безопасности ПДн и, таким образом, была оценена экономическая эффективность предложенных мер.

ЗАКЛЮЧЕНИЕ

В магистерской диссертации предложены рекомендации по противодействию утечке информации по техническим каналам в системах связи ГБПОУ «Южно-Уральский государственный колледж».

Основными результатами диссертационного исследования можно назвать следующее:

1. Составлен глоссарий основных понятий, использующихся в магистерском исследовании. Основанием для составления глоссария послужил Федеральный закон от 27 июля 2006г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» Статья 2. Основные понятия, используемые в настоящем Федеральном законе.

2. Описана классификация технических каналов утечки информации, рассмотрены угрозы утечки информации по ТКУИ и возможные меры защиты информации от утечки.

3. Определены информационные ресурсы образовательной организации, подлежащие защите от утечки информации по ТКУИ. Такими ресурсами являются персональные данные и информация, которая обеспечивает образовательный процесс. Оценена безопасность названных информационных активов, определены наиболее вероятные угрозы. Были проанализированы угрозы с целью выявления потенциально опасной угрозы утечки информации по ТКУИ.

4. Проведён анализ состояния защиты информации от утечки в системах связи ГБПОУ СПО «Южно-Уральский государственный колледж», в результате которого был определены используемые в ГБПОУ «ЮУГК» программные продукты для защиты информации от утечки информации по техническим каналам в системах связи. Были определены системы связи ГБПОУ «ЮУГК».

5. Разработаны меры по противодействию утечке информации в системах связи ГБПОУ «ЮУГК». Рассмотрены возможные угрозы утечки информации для систем связи и предложены меры по защите. Предложено сочетание организационных и технических мер защиты информации от утечки по ТКУИ.

6. Приведено экономическое обоснование рекомендаций по противодействию утечке информации по ТКУИ в системах связи ГБПОУ «ЮУГК». Произведён расчёт стоимости защиты ПДн. Рассмотрены статьи уголовного и административного кодекса с нарушениями в области обработки и обеспечения безопасности ПДн. В результате расчёт подтверждает экономическую эффективность и целесообразность использования рекомендованных мер при внедрении их в процесс информационной безопасности.

Таким образом, цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция Российской Федерации от 12.12.1993 (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) Ст. 23 // СПС КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_28399/2573feee1caecac37c442734e00215bbf1c85248/ (дата обращения: 05.03.2022).

2. Конституция Российской Федерации от 12.12.1993 (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) Ст. 24 // СПС КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_28399/bcddbd9060e44ed6085b65a1af0fb90aa3ef0175/ (дата обращения: 05.03.2022).

3. Федеральный закон от 27 июля 2006г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 05.03.2022).

4. Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ (последняя редакция) // СПС КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 05.03.2022).

5. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция) // СПС КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 05.03.2022).

6. Положения «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденного Постановлением Совета Министров – Правительства РФ от 15.09.93 № 912-51 // ИСС «Аюдар Инфо» URL: https://www.audar-info.ru (дата обращения: 05.03.2022).

7. Постановление Правительства РФ от 15 апреля 1995 г. N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" // СПС «ГАРАНТ» URL: https://base.garant.ru/104554/ (дата обращения: 05.03.2022).

8. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс» URL: http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ (дата обращения: 09.03.2022).

9. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 25.03.2022). — Текст : электронный // УК РФ Статья 137. Нарушение неприкосновенности частной жизни // СПС «КонсультантПлюс» URL: http://www.consultant.ru/document/cons_doc_LAW_10699/4234a27af714cc608ea71b7bae9400f3613c8f60/ (дата обращения: 10.05.2022).

10. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 25.03.2022). — Текст : электронный // УК РФ Статья 272. Неправомерный доступ к компьютерной информации // СПС «КонсультантПлюс» URL: http://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/ (дата обращения: 10.05.2022).

11. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 28.05.2022). — Текст : электронный // КоАП РФ Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных // СПС «КонсультантПлюс» URL:

http://www.consultant.ru/document/cons_doc_LAW_34661/1f421640c6775ff67079ebde06a7d2f6d17b96db/ (дата обращения: 10.05.2022).

12. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий // «Интернет и Право» URL: https://internet-law.ru/gosts/gost/5475/ (дата обращения: 15.03.2022).

13. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения // «Интернет и Право» URL: https://internet-law.ru/gosts/gost/48411/ (дата обращения: 15.03.2022).

14. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения // «Интернет и Право» URL: https://internet-law.ru/gosts/gost/5737/ (дата обращения: 15.03.2022).

15. ГОСТ 7.1–2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления // Библиография. – 2004. – № 3. – С. 45–72; № 4. – С. 41–64.

16. ГОСТ Р 7.0.5—2008. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления. – М.: Стандартинформ, 2008. – 19 с.

17. ГОСТ Р 7.0.11 – 2011. Система стандартов по информации, библиотечному и издательскому делу. Диссертация и автореферат диссертации. Структура и правила оформления. – М.: Стандартинформ, 2012. – 9 с.

18. Алиев, Т. И. Сети ЭВМ и телекоммуникации / Т. И. Алиев. — СПб : СПбГУ ИТМО, 2011. — 400 с.

19. Берлин А.Н. Телекоммуникационные сети и устройства : учебное пособие / А.Н. Берлин. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 395 с.

20. Вострецова, Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.

21. Громов Ю. Ю., Иванова О. Г., Мартемьянов Ю. Ф., Букурако, В. Г. Однолько Ю. К. Методы организации защиты информации : учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю. Ю. Громов и др. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с.

22. Евстифеев, А. А. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 267 с.

23. Железняк В.К. Защита информации от утечки по техническим каналам: учебное пособие / В. К. Железняк; ГУАП. – СПб., 2006. – 188 с.

24. Завгородний, В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. - 264 с : ил.

25. Зайцев А. П., Мещеряков Р. В., Шелупанов А. А., Технические средства и методы защиты информации. Учебник для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков. Под ред. А. П. Зайцева и А. А. Шелупанова. – 7-е изд., испр. – М.: Горячая линия–Телеком, 2012. – 442 с: ил.

26. Исаев, А. Н. Противодействие утечке информации по техническим каналам / А. Н. Исаев. — Текст : непосредственный // Молодой ученый. — 2021. — № 2 (344). — С. 17-19. — URL: https://moluch.ru/archive/344/77362/ (дата обращения: 30.03.2022).

27. Исаев, А. Н. Противодействие утечке информации по техническим каналам в системах связи в ГБПОУ «ЮУГК» / А. Н. Исаев, М. С. Подин. — Текст : непосредственный // МОЛОДЕЖНАЯ ПОЛИТИКА И СОЦИАЛЬНАЯ МИССИЯ ОБРАЗОВАНИЯ В ЭПОХУ

ГЛОБАЛИЗАЦИИ И ЦИФРОВИЗАЦИИ: материалы Международной научно-практической конференции. — Челябинск : «ЗАО Библиотека А. Миллера», 2022. — С. 468-471

28. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

29. Основные меры защиты информации от утечки по техническим каналам. Организационные меры защиты: временные ограничения, территориальные ограничения, Текст : электронный // Интуит : [сайт]. — URL: https://intuit.ru/studies/courses/3649/891/lecture/32347

30. Рекомендации по предотвращению утечки информации. — Текст : электронный // DELPHI PLUS : [сайт]. — URL: https://www.delphiplus.org/zashchita-ot-utechki-informatsii-po-tekhnicheskim-kanalam/kanaly-utechki-informatsii-pri-ee-peredache-po-kanalam-svyazi.html (дата обращения: 26.03.2022).

31. Комплексная защита информации в организации / М. М. Тараскин, А. Г. Захаров, Ю. И. Коваленко, Г. И. Москвитин. — Москва : РУСАЙНС, 2020. — 354 с.

32. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

33. Торокин, А. А. Инженерно-техническая защита информации / А. А. Торокин. — Москва : Гелиос АРВ, 2005. — 960 с.

34. Хорев П.Б. Программно-аппаратная защита информации. Учебное пособие / П.Б. Хорев. М.: ФОРУМ, 2019. 352 с.

35. Межсетевой экран ALTELL NEO 110. — Текст : электронный // ALTELL NEO : [сайт]. — URL: http://www.altell.ru/products/neo/models/ (дата обращения: 10.05.2022).

36. Ideco UTM. — Текст : электронный // Википедия : [сайт]. — URL: https://ru.wikipedia.org/wiki/Ideco_UTM (дата обращения: 03.04.2022).

37. Ideco UTM. — Текст : электронный // Ideco : [сайт]. — URL: https://ideco.ru (дата обращения: 03.04.2022).

38. ИнфоТеКС. — Текст : электронный // Википедия : [сайт]. — URL: https://ru.wikipedia.org/wiki/ИнфоТеКС (дата обращения: 03.04.2022).

39. ViPNet. — Текст : электронный // ИнфоТеКС : [сайт]. — URL: https://infotecs.ru/product/vipnet-client-.html#soft (дата обращения: 03.04.2022).

40. Dallas Lock. — Текст : электронный // Википедия : [сайт]. — URL: https://ru.wikipedia.org/wiki/Dallas_Lock (дата обращения: 03.04.2022).

41. Dallas Lock. — Текст : электронный // Dallas Lock : [сайт]. — URL: https://dallaslock.ru (дата обращения: 03.04.2022).

42. Обзор Kaspersky Endpoint Security 11.1 для Windows. — Текст : электронный // Anti-Malware : [сайт]. — URL: https://www.anti-malware.ru/reviews/Kaspersky-Endpoint-Security-11-Windows (дата обращения: 03.04.2022).

43. Kaspersky Endpoint Security для Windows. — Текст : электронный // «Лаборатория Касперского» : [сайт]. — URL: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-windows (дата обращения: 03.04.2022).

44. Межсетевой экран UserGate C100. — Текст : электронный // UserGate : [сайт]. — URL: https://www.usergate.com/ru/products/usergate-c (дата обращения: 10.05.2022).

45. 10 обязательных функций межсетевого экрана нового поколения. — Текст : электронный // Хабр : [сайт]. — URL: https://habr.com/post/327953/ (дата обращения: 03.04.2022).

ПРИЛОЖЕНИЕ

ИСЕВ АНДРЕЙ НИКОЛАЕВИЧ

РЕКОМЕНДАЦИИ ПО ПРОТИВОДЕЙСТВИЮ УТЕЧКЕ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ГПБОУ «ЮУГК»

Челябинск – 2022

На основе проведенной оценки исходной защищенности ИС и анализа нормативно-правовых требований действующего законодательства считаем необходимым рекомендовать следующие меры в ГБПОУ «ЮУГК».

Совершенствование защиты информации от утечки можно разделить на несколько этапов.

Этап 1. Разработка организационно-распорядительных и технических документов по защите персональных данных.

1. Алгоритм по применению комплекта документов по защите персональных данных в образовательной организации.
2. Акт классификации информационной системы персональных данных.
3. Акт об уничтожении бумажных носителей персональных данных субъектов персональных данных.
4. Акт об уничтожении электронных носителей персональных данных субъектов персональных данных.
5. Журнал учета паролей пользователей информационной системы персональных данных.
6. Журнал учета машинных носителей информации.
7. Журнал учета средств защиты информации, эксплуатационной и технической документации к ним.
8. Журнал учёта ключей от сейфов и помещений.
9. Журнал учета обращений субъектов информационной системы персональных данных.
10. Журнал учета проверок юридического лица.
11. Журнал учета работ в информационной системе персональных данных.
12. Инструкция администратора безопасности информационной системы персональных данных.
13. Инструкция о порядке работы с персональными данными.

14. Инструкция ответственного за организацию обработки персональных данных.

15. Инструкция по организации антивирусной защиты.

16. Инструкция по организации парольной защиты.

17. Инструкция по физической охране, контролю доступа в помещения.

18. Инструкция пользователя информационной системы персональных данных.

19. Перечень сведений, содержащих персональные данные.

20. Перечень информационных систем персональных данных.

21. Перечень автоматизированных рабочих мест.

22. Перечень общесистемного и прикладного программного обеспечения, используемого в информационной системе персональных данных.

23. Перечень серверного коммутационного и сетевого оборудования.

24. План внутренних проверок состояния защиты информационных систем персональных данных.

25. План мероприятий по защите персональных данных.

26. Политика обработки и защиты персональных данных.

27. Положение об обработке персональных данных с использованием средств автоматизации.

28. Положение об обработке персональных данных без использования средств автоматизации.

29. Правила работы с обезличенными данными.

30. Приказ о введении в действие организационно-распорядительных документов по защите персональных данных.

31. Приказ об организации работ по обеспечению безопасности персональных данных.

32. Приказ об утверждении мест хранения материальных носителей персональных данных.

33. Приказ об утверждении списка должностных лиц, которым необходим доступ к персональным данным, обрабатываемым в информационной системе.

34. Регламент резервного копирования и восстановления данных.

35. Согласия субъектов на обработку персональных данных.

36. Список лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей.

37. Список мест хранения материальных носителей персональных данных.

38. Оценка вреда субъектам ПДн ИСПДн (Акт).

39. Описание технологического процесса обработки персональных данных.

40. Справка по информационным системам персональных данных.

41. Схема внешних и внутренних потоков передачи персональных данных.

Этап 2. Повышение осведомленности/ознакомление работников в области персональных данных.

Инструктаж работников, непосредственно осуществляющих обработку персональных данных.

Этап 3. Установка и настройка технических средств защиты информации.

Техническая защита системы персональных данных осуществляется и заключается:

1. Закупить и установить средства защиты информации, сертифицированных ФСТЭК России и ФСБ России.

2. Разработать эксплуатационную документацию на технические средства защиты персональных данных.

Для защиты беспроводной сети от утечки информации необходимо:

– провести фильтрацию по MAC-адресам;

– повысить уровень защищённости Wi-Fi при помощи технологий безопасной аутентификации;

– отключение WPS (Wi-Fi Protected Setup);

– использование сложных паролей и их ежеквартальная смена;

– скрыть SSID;

– усилить защиту при помощи программных и аппаратных средств.

Для защиты информации от утечки по телефонным линиям необходимо:

– приобрести межсетевой экран UserGate C100.

Для защиты информации от утечки по локальной сети необходимо:

– приобрести межсетевой экран ALTELL NEO 110.

Инструкция

пользователя по обеспечению информационной безопасности

1. Общие положения

1.1. Настоящая Инструкция определяет основные обязанности и ответственность пользователя, допущенного к обработке конфиденциальной информации.

1.2. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность конфиденциальной информации и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

2. Основные обязанности пользователя:

2.1. Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные законодательством РФ, внутренними документами организации и настоящей Инструкцией.

2.2. При работе с конфиденциальной информацией располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами.

2.3. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, базам данных, файлам и другим носителям конфиденциальной информацией при ее обработке.

2.4. Самостоятельно не устанавливать на ЭВМ какие-либо аппаратные или программные средства.

2.5. Знать штатные режимы работы программного обеспечения, основные пути проникновения и распространения компьютерных вирусов.

2.6. Помнить личные пароли и персональные идентификаторы, хранить их в тайне, не оставлять без присмотра носители, их содержащие,

и хранить в запирающемся ящике стола или сейфе. С установленной периодичностью менять свой пароль (пароли).

2.7. При применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов средствами ЭВМ.

2.8. Знать и строго выполнять правила работы с установленными на его ЭВМ средствами защиты информации (антивирус, средства разграничения доступа, средства криптографической защиты и т.п.) в соответствии с технической документацией на эти средства.

2.9. Надежно хранить и никому не передавать личную печать.

2.10. Немедленно ставить в известность сотрудника ответственного за информационную безопасность и своего непосредственного руководителя при обнаружении:

– нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах или иных фактов совершения в его отсутствие попыток несанкционированного доступа к закрепленной за ним защищенной ЭВМ;

– некорректного функционирования установленных на ЭВМ технических средств защиты;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ЭВМ, выхода из строя или неустойчивого функционирования узлов ЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения.

2.11. По завершении работ по изменению аппаратно-программной конфигурации, закрепленной за ним ЭВМ проверять ее работоспособность.

3. Обеспечение антивирусной безопасности

3.1. Основными путями проникновения вирусов в информационно-вычислительную сеть организации являются: съемные носители информации, электронная почта, файлы, получаемые из сети Интернет, ранее зараженные ЭВМ.

3.2. При возникновении подозрения на наличие компьютерного вируса (сообщение антивирусной программы, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль ЭВМ.

3.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь **ОБЯЗАН:**

– прекратить (приостановить) работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, ответственного за информационную безопасность, а также смежные подразделения, использующие эти файлы в работе;

– оценить необходимость дальнейшего использования файлов, зараженных вирусом;

– провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

3.4. Пользователю **ЗАПРЕЩАЕТСЯ:**

– отключать средства антивирусной защиты информации;

– без разрешения копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

4. Обеспечение безопасности персональных данных

4.1. Основанием для допуска работника организации к обработке персональных данных в рамках своих функциональных обязанностей является перечень должностей, утвержденным директором организации и должностная инструкция работника. Основанием для прекращения допуска к персональным данным является исключение из Перечня должностей, утвержденным директором организации и (или) изменение должностной инструкции работника.

4.2. Каждый работник организации, участвующий в процессах обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и базам данных системы организации, является пользователем и несет персональную ответственность за свои действия.

4.3. Пользователь **ОБЯЗАН***:*

– знать требования руководящих документов по защите персональных данных;

– производить обработку защищаемой информации в строгом соответствии с утвержденными технологическими инструкциями (техническими порядками);

– строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами.

4.4. Пользователю **ЗАПРЕЩАЕТСЯ***:*

– использовать компоненты программного и аппаратного обеспечения не по назначению (в неслужебных целях);

– использовать средства разработки и отладки программного обеспечения стандартных программных средств общего назначения (MS Office и др.);

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ЭВМ или устанавливать дополнительно любые программные и аппаратные средства;

– осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить персональные данные на неучтенных съемных носителях информации (гибких магнитных дисках, флэш - накопителях и т.п.), осуществлять несанкционированную распечатку персональных данных;

– оставлять включенной без присмотра свою ЭВМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

– оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, носители и распечатки, содержащие персональные данные;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушениям безопасности персональных данных. Об обнаружении такого рода ошибок - ставить в известность ответственного за безопасность информации и руководителя подразделения.

4.5. Особенности обработки персональных данных без использования средств автоматизации.

4.5.1. Обработка персональных данных считается неавтоматизированной, если она осуществляется без использования средств вычислительной техники.

4.5.2. Допуск к неавтоматизированной обработке персональных данных осуществляется в соответствии с Перечнем должностей сотрудников организации, имеющих доступ к персональным данным,

которые несут ответственность за реализацию требований по обеспечению безопасности персональных данных.

4.5.3. Персональные данные при их неавтоматизированной обработке и хранении должны обособляться от иной информации путем фиксации их на отдельных материальных носителях в специальных разделах или на полях форм (бланков).

4.5.4. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

4.5.5. Для каждой категории персональных данных используется отдельный материальный носитель.

4.5.6. Хранение материальных носителей персональных данных осуществляется в специальных шкафах (ящиках, сейфах и т.д.), обеспечивающих сохранность материальных носителей и исключающих несанкционированный к ним доступ.

5. Обеспечение информационной безопасности при использовании ресурсов сети Интернет

5.1. Ресурсы сети Интернет могут использоваться для осуществления выполнения требований законодательства Российской Федерации, дистанционного обслуживания, получения и распространения информации, связанной с деятельностью организации (в том числе, путем создания информационного web-сайта), информационно-аналитической работы в интересах организации, обмена почтовыми сообщениями, а также ведения собственной хозяйственной деятельности. Иное использование ресурсов сети Интернет, решение о котором не принято руководством организации в установленном порядке, рассматривается как нарушение информационной безопасности.

5.2. С целью ограничения использования сети Интернет в неустановленных целях выделяется ограниченное число пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для

пользователей. Наделение работников организации правами пользователя конкретного пакета выполняется в соответствии с его должностными обязанностями.

5.3. Особенности использования сети Интернет**:**

– сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;

– гарантии по обеспечению информационной безопасности при использовании сети Интернет никаким органом не предоставляются.

5.4. При осуществлении дистанционного обслуживания и электронного документооборота, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет организация применяет соответствующие средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

5.5. Почтовый обмен конфиденциальной информацией через сеть Интернет осуществляется с использованием защитных мер.

5.6. Электронная почта организации подлежит периодической архивации. Доступ к архиву разрешен только подразделению (лицу) в организации, ответственному за обеспечение информационной безопасности. Изменения в архиве не допускаются.

5.7. При взаимодействии с сетью Интернет отдел информационных технологий обеспечивает программными и аппаратными средствами противодействие атакам хакеров и распространению спама**.**

5.8. При пользовании ресурсами сети Интернет **ЗАПРЕЩАЕТСЯ:**

– использовать на рабочем месте иные каналы доступа ЭВМ к сети Интернет, кроме установленного;

– проводить самостоятельное изменение конфигурации технического и программного обеспечения ЭВМ, подключенной к сети Интернет;

– осуществлять отправку электронных почтовых сообщений, содержащих конфиденциальную информацию, по открытым каналам;

– использовать иные, кроме служебных, почтовые ящики для электронной переписки;

– открывать файлы, пришедшие вместе с почтовым сообщением, если не известен источник этого сообщения;

– осуществлять перенос полученной по сети Интернет документированной информации в электронном виде на другие компьютеры без проверки ее антивирусными программами;

– скачивать из сети Интернет, в том числе средствами электронной почты, информацию, содержащую исполняемые модули, программы, драйверы и т.п., без предварительного согласования с Департаментом информационных технологий;

– использовать сеть Интернет вне служебных задач, посещать интернет–сайты, не связанные с выполнением должностных обязанностей.

6. Организация парольной защиты.

6.1. Пароль для своей учетной записи пользователь устанавливает самостоятельно.

6.2. Запрещается использовать пароль домена локальной вычислительной сети (вводится при загрузке ЭВМ) для входа в иные автоматизированные системы.

6.3. Длина пароля должна быть не менее 7 символов. В числе символов пароля рекомендуется использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

6.4. Пароль не должен включать в себя легко вычисляемые сочетания символов (логины, имена, фамилии и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

6.5. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 позициях.

6.6. Пользователь обязан хранить в тайне свой личный пароль.

6.7. Требования к паролю и периодичность его смены устанавливаются в групповых доменных политиках.

7. Ответственность пользователей

7.1. Работники организации несут ответственность согласно действующему законодательству, за разглашение сведений, составляющих служебную, коммерческую и иную охраняемую законом тайну (в том числе персональные данные) и сведений ограниченного распространения, ставших им известными по роду работы.

7.2. Нарушения установленных правил и требований по обеспечению информационной безопасности являются основанием для применения к работнику (пользователю) мер наказания, предусмотренных трудовым законодательством.