МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ЮУрГГПУ»
Профессионально-педагогический институт
Кафедра автомобильного транспо́рта, информационных технологий
и методики обучения техническим дисциплинам

Разработка рекомендаций по противодействию утечки информации в системах связи образовательной организации СПО

Магистерская диссертация
по направлению 44.04.04 Профессиональное обучение
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»

Выполнил:
студент группы ЗФ-309/210-2-1,
Худякова Ольга Юрьевна
Научный руководитель:
д.т.н., профессор
кафедры АТ, ИТ и МОТД
Дмитриев Михаил Сергеевич

Проверка на объём заимствований:
70,8 авторского текста

Работа рекомендована к защите
«01» февраля 2019 г.
Зав. кафедрой АТ, ИТ и МОТД
_____В.В. Руднев

Челябинск, 2019

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ЮУрГГПУ»
Профессионально-педагогический институт
Кафедра автомобильного транспорта, информационных технологий
и методики обучения техническим дисциплинам

Направление подготовки: 44.04.04. –
Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании

ЗАДАНИЕ

на магистерскую диссертацию

Магистранту группы ЗФ-309/210-2-1 заочного отделения Худяковой Ольге Юрьевне, обучающейся по программе магистратуры «Управление информационной безопасностью в профессиональном образовании».

Научный руководитель выпускной квалификационной работы: Дмитриев М.С., д.т.н., профессор кафедры АТ, ИТ и МОТД.

1.Тема квалификационной работы: «Разработка рекомендаций по противодействию утечки информации в системах связи образовательной организации СПО», утверждена приказом Южно-уральского государственного гуманитарно-педагогического университета № 580-сз от «26» апреля 2017 г.

2. Материалы для выполнения магистерской диссертации:

2.1. Учебная, научно-техническая, педагогическая, методическая литература по теме магистерской диссертации: отчет по преддипломной практике в ГБПОУ «Мишкинский профессионально-педагогический колледж», нормативная и законодательная документация, специальная литература, периодические издания, Интернет.

3. Основные части магистерской диссертации (перечень подлежащих разработке вопросов) и сроки их выполнения представлены в нижеприведенной таблице:

Календарный план работы

	Перечень вопросов, подлежащих разработке в диссертации	Сроки
1	ВВЕДЕНИЕ Оговаривается значение и актуальность темы работы, объект и предмет исследования,	15.05.2017

	проблема, цель и задачи работы, пути их решения. Указываются методы исследования.	
2	Глава 1. Теоретические основы разработки рекомендаций по противодействию утечки информации в системах связи Выводы по главе 1	16.10.2017
3	Глава 2. Обеспечение информационной безопасности в профессиональной образовательной организации Выводы по главе 2	23.04.2018
4	Глава 3. Разработка рекомендаций по противодействию утечки информации в системах связи образовательной организации Выводы по главе 3	29.12.2018
5	ЗАКЛЮЧЕНИЕ (объем в пределах 3 стр.) Содержит кратко и четко сформулированные выводы, и рекомендации.	29.12.2018
6	СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ (Законы и нормативные акты, справочно-статистические материалы, монографии, учебники, сборники брошюры, статьи из периодической печати, иностранная литература.	29.12.2018
7	ПРЕЗЕНТАЦИЯ (НАГЛЯДНЫЕ МАТЕРИАЛЫ) предоставляется в виде слайдов рекомендаций Microsoft PowerPoint, 10-12 слайдов, раскрывающих содержание магистерской диссертации	28.01.2019
	ПРЕДВАРИТЕЛЬНАЯ ЗАЩИТА	28.01.2019
	СДАЧА МАГИСТЕРСКОЙ ДИССЕРТАЦИИНА КАФЕДРУ	18.02.2019

Дата выдачи задания «27» апреля 2017 года

Заведующий кафедрой АТ, ИТ и МОТД
Наименование кафедры

_Руднев В.В., доцент, к.т.н._____
Ф.И.О., ученое звание и степень Подпись заведующего кафедрой

Задание выдал: _Дмитриев М.С., профессор, д.т.н._____
Ф.И.О., ученое звание и степень Подпись научного руководителя

Задание принял__Худякова О.Ю._____
Ф.И.О магистранта Подпись магистранта

Аннотация
на магистерскую диссертацию
Худяковой Ольги Юрьевны

Тема магистерской диссертации «Разработка рекомендаций по противодействию утечки информации в системах связи образовательной организации СПО».

Магистерская диссертация содержит 85 страниц, 8 таблиц, 4 рисунка, 55 источник литературы.

Ключевые слова: защита информации, утечка информации, каналы связи, системы связи, техническая защита информации.

Объектом исследования является деятельность образовательной организации по обеспечению информационной безопасности.

Цель магистерской диссертации –является разработка рекомендаций для повышения эффективности защиты информации от утечки в системах связи образовательной организации.

В процессе исследования изучены теоретические аспекты: описаны системы связи в образовательной организации, информационные ресурсы образовательной организации, подлежащие защите от утечки, меры противодействия утечки информации в системах связи. Проанализировано состояние защиты информации от утечки в системах связи в ГБПОУ «Мишкинский профессионально-педагогический колледж».

В результате проведенного исследования разработаны рекомендации по противодействию утечки информаци в системах связи в ГБПОУ «Мишкинский профессионально-педагогический колледж», проведен расчет экономической эффективности внедрения рекомендаций.

Магистрант _Худякова О.Ю._ _____
(Ф.И.О.) Подпись

Оглавление

ВВЕДЕНИЕ

К защищаемой информации относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации [3]. Это, как правило, информация ограниченного доступа, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера.

Защита информации ограниченного доступа (далее - защищаемой информации) 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 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, «Положения о государственном лицензировании деятельности в области защиты информации», утвержденного Постановлением Правительства РФ от 27 апреля 1994 г. № 10, «Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации» утвержденного Постановлением Правительства РФ от 27 мая 2002 г. № 348, с изменениями и дополнениями от 3 октября 2002 г. № 731, «Положения о сертификации средств защиты информации», утвержденного Постановлением Правительства РФ от 26 июня 1995 г. № 608, Постановлений Правительства Российской Федерации «О лицензировании деятельности по

технической защите конфиденциальной информации» (от 30 апреля 2002 г. № 290, с изменениями и дополнениями от 23 сентября 2002 г. № 689 и от 6 февраля 2003 г. № 64), «О лицензировании отдельных видов деятельности» (от 11 февраля 2002 г. № 135), а также «Положения по аттестации объектов информатизации по требованиям безопасности информации», утвержденного Председателем Гостехкомиссии России 25 ноября 1994 г., и других нормативных документов.

Наряду с существующими нормативно-правовыми документами теоретическую базу исследований составляют труды известных ученых в области защиты информации от утечки по техническим каналам: В.В. Домарева [21], А.А. Хорева [38-40] и др.

Режим защиты информации ограниченного доступа, не содержащей сведений, составляющих конфиденциальную информацию, устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством Российской Федерации.

Мероприятия по защите конфиденциальной информации от утечки каналам связи 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 (далее – объекта защиты).

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.

Таким образом, проблема исследования заключается в разработке и исследованию методов противодействия утечки информации по каналам связи в образовательной организации, что является актуальной и представляет, как научный, так и практический интерес.

Целью магистерской диссертационной работы является разработка рекомендаций для повышения эффективности защиты информации от утечки в системах связи образовательной организации.

Объектом исследования является деятельность образовательной организации по обеспечению информационной безопасности.

Предметом исследования выступает организация защиты информации от утечки в системах связи образовательной организации.

Гипотеза исследования состоит в предположении о том, что повышение эффективности защиты информации от утечки в системах связи возможна, если внедрить разработанные рекомендации по противодействию утечки информации и обеспечения их оптимального обновления с учетом максимального соответствия техническим требованиям и минимальных финансовых затрат.

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

1. Описать системы связи в образовательных организациях.
2. Выявить меры противодействия утечки информации в системах связи.
3. Разрабаотать рекомендации по совершенствованию защиты информации от утечки в системах связи колледжа.
4. Провести разчет экономической эффективности мероприятий по защите информации от утечки в системах связи ГБПОУ «Мишкинский профессионально-педагогический колледж».

Методы исследования. В работе использованы методы системного анализа, теории математической статистики, теории информационной безопасности, законодательные и нормативно-правовые документы РФ, разработки в области обеспечения информационной безопасности.

Научная новизна исследования состоит в том, что описаны меры противодействия утечки информации в системах связи и разработаны рекомендации по противодействию утечки информации в системах связи образовательной организации, что позволит снизить риски утечки конфиденциальной информации по каналам связи.

Практическая значимость работы заключается в разработке рекомендаций по защите информации от утечки в системах связи образовательной организации.

База исследования: ГБПОУ «Мишкинский профессионально-педагогический колледж».

Результаты работы докладывались на конференциях и семинарах различного уровня, в том числе на:

- Международной научно - практической конференции «Новая наука: история становления, современное состояние, перспективы развития» (2017 г., г. Волгоград);

- XV Всероссийской научно-практической конференции «Актуальные вопросы развития России в исследованиях студентов: управленческий, правовой и социально-экономический аспекты» (27-28 апреля 2017 года, г. Челябинск).

Структура магистерской диссертации состоит из введения, трех глав, заключения, библиографического списка, состоящего из 55 наименований, приложения. Работа содержит 4 рисунка, 8 таблиц. Общий объем работы составляет 85 страниц.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАЗРАБОТКИ РЕКОМЕНДАЦИЙ ПО ПРОТИВОДЕЙСТВИЮ УТЕЧКИ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ

1.1. Описание систем связи в образовательных организациях

Обеспечение имущественной и личной безопасности невозможно без средств и систем связи. Они являются элементами управления и составной частью технических систем охраны. Используются: радиоканалы (радиосистемы); проводные каналы (проводные системы); оптические каналы (оптические системы).

Любая техническая система связи помимо канала связи содержит устройство ввода и вывода информации, обеспечивающее представление сообщений в удобном виде. В зависимости от передаваемых и принимаемых сообщений и вида устройства ввода и вывода информации существующие технические системы связи подразделяются на: телефонные, телеграфные, телефаксные, телевизионные и компьютерные системы.

Таким образом, технические системы связи, используемые охранными структурами, могут быть классифицированы по виду канала связи, виду передаваемого сигнала, а также форме представления сообщения.

В образовательных организациях коммуникация персонала между отделами невозможна без применения современных систем связи. Именно их использование позволяет максимально сократить время, потраченное на передачу информации от одного сотрудника к другому.

Система связи – это комплекс технических и программных средств, позволяющих осуществлять коммуникацию между сотрудниками и группами сотрудников в пределах объекта.

В зависимости от технологии и функций, системы связи разделяются на следующие разновидности:

Системы телефонной связи. Является наиболее распространённым и широко применяемым способом обмена речевой информацией. В центре такой сети всегда имеется автоматическая телефонная станция или АТС. Станция

хранит данные о каждом абоненте. Кроме того, используются специальные абонентские аппараты – телефоны. В зависимости от применяемой технологии, связь абонентов может осуществляться проводным или беспроводным способом, а голосовой сигнал может быть передан как в аналоговом, так и в цифровом виде.

1. *Системы радиосвязи.* Для организации данной сети требуется базовая станция и специальные абонентские аппараты. В зависимости от нужд заказчика и территориальных масштабов объекта, может быть выбрана базовая станция с различным радиусом действия.

2. *Системы оперативной диспетчерской связи***.** Позволяют создать возможность быстрой и удобной речевой коммуникации персонала. Устанавливается один или несколько пультов руководителя, с помощью которых можно следить за состоянием абонентов, организовывать групповое общение, осуществлять общение в режиме «директор – секретарь» и многое другое. Зачастую имеют выход на внешние телефонные линии общего пользования.

3. *Системы оповещения.* Данная технология незаменима на крупных и потенциально опасных объектах. Позволяет осуществлять оповещение персонала в различных помещениях или их группах. Оповещение работает как в автоматическом режиме, например, при возникновении дыма или пожара, так и в ручном.

4. *Системы радиотрансляции.* Позволяют транслировать различную звуковую информацию как служебного, так и развлекательного характера. Имеет возможность программирования сигналов на определенное время или помещения.

5. *Системы обеспечения связи конференций***.** Представляют собой набор аппаратных и программных средств для реализации удобной взаимосвязи во время конференций, заседаний и другого рода собраний. Современные варианты предполагают наличие на каждом месте

мультимедийного устройства, с помощью которого можно работать с файлами, менять параметры звука и знакомиться с материалами конференции.

6. *Технологические сети связи.* Служат для передачи служебной информации, управления операциями и процессами. Созданы для переработки производственной и технологической информации в рамках одного объекта.

7. *Локальная вычислительная сеть.* Локальные вычислительные сети обеспечивают:

1. Распределение данных (Data Sharing). Данные в ЛВС хранятся на центральном ПК и могут быть доступны на рабочих станциях, поэтому на каждом рабочем месте не надо иметь накопители для хранения одной и той же информации.

2. Распределение информационных и технических ресурсов (Resource Sharing):

- логические диски и другие внешние запоминающие устройства (накопители на CD-ROM, DVD, ZIP и так далее);
- каталоги (папки) и содержащиеся в них файлы;
- подключенные к ПК устройства: принтеры, модемы и другие внешние устройства (позволяет экономно использовать ресурсы, например, печатающие устройства, модемы).

3. Распределение программ (Software Sharing). Все пользователи локальных вычислительных сетей могут совместно иметь доступ к программам (сетевым версиям), которые централизованно устанавливаются в сети.

4. Обмен сообщениями по электронной почте (Electronic Mail). Все пользователи сети могут оперативно обмениваться информацией между собой посредством передачи сообщений.

В настоящее время для передачи информации по каналам связи используются в основном: коротковолновые, ультракоротковолновые, радиорелейные, тропосферные и космические каналы связи; различные виды телефонной радиосвязи (например, сотовая связь), а также кабельные и

волоконно-оптические линии связи, которые при определенных условиях (при отсутствии средств криптозащиты) образуют естественные и доступные для противника каналы утечки информации.

Возможные пути утечки конфиденциальной информации:

– электронное письмо с ценной информацией может быть отослано по почтовым протоколам;

– информация может быть отправлена посредством клиентов для мгновенного обмена сообщениями (ICQ, MSN Messenger, QIP, Jabber);

– голосовые или текстовые сообщения, отправленные через Skype, также могут содержать персональные данные;

– информация может быть размещена на форумах, блогах, передана по социальным сетям. Передана по FTP-протоколу;

– также ценные данные могут быть переписаны на съёмный носитель (USB-флешку или CD/DVD диски);

– информация может быть распечатана на принтере.

Зачастую, для предотвращения утечек информации, образовательная организация запрещает сотрудникам использовать удобные и популярные каналы ее передачи и общения с внешним миром.

Например, для безопасности обычно разрешено использовать только корпоративную электронную почту, а такие средства как ICQ, Skype запрещены, несмотря на то, что они во многих случаях могли бы существенно увеличить эффективность работы.

Современная система информационной безопасности должна позволять сотруднику использовать все каналы для передачи информации, однако перехватывать и анализировать информационные потоки, идущие по этим каналам.

Информационная безопасность должна способствовать работе образовательной организации, а не препятствовать ей. Все каналы передачи информации должны быть открытыми.

1.2. Информационные ресурсы образовательной организации, подлежащие защите от утечки

Эффективная защита информационных ресурсов является неотъемлемой частью комплексной системы обеспечения информационной безопасности и способствует оптимизации финансовых затрат на организацию защиты информации.

К целям защиты информации относятся: предотвращение утечки, хищения, утраты, искажения, подделки информации и предотвращение других несанкционированных негативных воздействий.

К задачам защиты информации относятся:

- предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения;

- защита носителей информации от уничтожения в результате различных природных и техногенных воздействий;

- предотвращение утечки информации по различным техническим каналам.

Принципы проектирования систем технической защиты, следующие [4]:

- непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности;

- многозональность и многорубежность защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности;

- избирательность, заключающаяся в предотвращении угроз в первую очередь для наиболее важной информации;

- интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности;

- создание централизованной службы безопасности в интегрированных системах.

Одной из основных угроз безопасности информации ограниченного доступа относится *утечка информации по каналам связи*, под которой понимается неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего прием информации.

Угрозы информационной безопасности могут быть разделены на угрозы, не зависящие от деятельности человека (естественные угрозы физических воздействий на информацию стихийных природных явлений), и угрозы, вызванные человеческой деятельностью (искусственные угрозы), которые являются гораздо более опасными.

В зависимости от целей преднамеренных угроз безопасности информации угрозы могут быть разделены на три основные группы:

– угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа;

– угроза нарушения целостности, т. е. преднамеренного воздействия на информацию;

– угроза нарушения доступности информации, т.е. отказа в обслуживании, вызванного преднамеренными действиями одного из пользователей (нарушителя), при котором блокируется доступ к некоторому информационному ресурсу со стороны других пользователей (постоянно или на большой период времени).

Результатом реализации угроз информационной системе может быть: утрата (разрушение, уничтожение); утечка (извлечение, копирование, подслушивание); искажение (модификация, подделка) информации или блокирование информационной среды [7].

Результат реализации любой из перечисленных угроз представляет серьезную опасность для образовательной системы.

Блокирование информационной системы может быть достигнуто путем DoS- и DDoS-атак, внедрения компьютерных вирусов, сетевых червей.

DoS – атаки от Denial of Service (отказ в обслуживании) - специфический тип атак, направленный на выведение сети или сервера из работоспособного состояния. Такие атаки перегружают каналы трафиком и мешают прохождению, а зачастую и полностью блокируют передачу по нему полезной информации. Особенно актуально это для образовательных организаций, занимающихся дистанционным образованием т.к. результатом отказов системы может стать срыв учебного процесса, и, как следствие, потеря доверия к организации дистанционного образования [12].

Реализация авторских учебных курсов, практикуемая образовательными организациями, предусматривает защиту интеллектуальной собственности, поэтому серьезную угрозу могут представлять троянские программы, способствующие утечке конфиденциальной информации, к которой должны быть отнесены кроме непосредственно учебных материалов, сведения о потребителях образовательных услуг образовательной организации.

Велика опасность и преднамеренного искажения информации, вследствие активности вредоносных программ.

Нельзя выпускать из вида и человеческий фактор. Причем защищать информационные системы необходимо не только от внешних злоумышленников, но и от так называемых внутренних угроз.

К з*ащищаемым данным* относятся данные, являющиеся предметом собственности и подлежащие 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.

В таблице 1 представлена карта ведомственных информационных систем образовательной организации, которые содержат сведения конфиденциального характера и подлежат защите от утечки по каналам связи.

Таблица 1

Карта ведомственных информационных систем образовательной организации

№ п/п	Наименование информационной системы	Описание информационной системы	Перечень содержания информационной системы
1	«1С Колледж проф»	Программный продукт представляет собой комплексное решение для управления деятельностью учреждений начального и среднего профессионального образования и охватывает все уровни управленческой деятельности основных подразделений колледжа.	- Паспортные данные студента - Паспортные данные родителей (родственников) студента - СНИЛС студента - СНИЛС (родственников) студента - Данные аттестата студента - Контактный телефон - Электронная почта - Достижения - Группы здоровья - Специальность - Приказы о зачислении, отчислении, академических отпусках - Паспортные данные, СНИЛС, ИНН, контактный телефон, стаж работы сотрудников образовательной организации - Образовательные программы, рабочие программы, КТП, расписание занятий, успеваемость студентов
2	Региональная АИС «Сетевой город образования»	Автоматизированная информационная система «Сетевой Город. Образование», модуль «Профессиональная образовательная организация Модуль для профессиональных образовательных организаций АИС ПОО позволяет решать административные задачи профессиональных образовательных организаций и проводить мониторинг текущего учебного процесса.	- Паспортные данные студента - Паспортные данные родителей (родственников) студента - СНИЛС студента - СНИЛС (родственников) студента - Данные аттестата - Контактный телефон - Электронная почта - Достижения - Группы здоровья - Специальность - Приказы о зачислении, отчислении, академических отпусках - Паспортные данные, СНИЛС, ИНН, телефон, стаж работы сотрудников образовательной организации - Образовательные программы, рабочие программы, КТП, расписание занятий, успеваемость студентов

3	ФИС ГИА и Приема	Федеральная информационная система обеспечения проведения единого государственного экзамена и приема граждан в образовательные учреждения среднего профессионального образования и образовательные учреждения высшего образования	-Паспортные данные студента - Данные аттестата - Направление подготовки - Специальность - Приказ о зачислении
4	ФРДО	Фед. Реестр сведений документов об образовании или о квалификации, документах об обучении	- Название документа - Вид документа - Статус документа - Подтверждение утраты - Подтверждение обмена - Уровень образования - Серия документа - Номер документа - Дата выдачи - Регистрационный номер - Код профессии, специальности - Наименование профессии, специальности - Наименование квалификации - Образовательная программа - Год поступления - Год окончания - Срок обучения, лет - Имя получателя - Отчество получателя - Дата рождения получателя - Пол получателя
5	Сайт образовательной организации		- ФИО преподавателей - Фотографии преподавателей - Краткая биография преподавателей - Все документы об образовательной организации - Фото с мероприятий, в том числе массовые фото студентов
6	СТЭК Документооборот	Программный продукт «СТЭК – Документооборот» помогает структурировать и автоматизировать движение документов в организации с момента их создания	ФИО сотрудника, его должность, подразделение

		или получения до завершения исполнения или отправления.	
7	ПП «Комплексная бухгалтерская система» СТЭК	ПП «Комплексная Бухгалтерская Система» СТЭК версия для государственных(муниципальных) учреждений предназначена для автоматизации бухгалтерского учета государственных учреждений любого типа: казенных, бюджетных и автономных, состоящих на самостоятельном балансе, финансируемых из федерального, регионального (субъекта РФ) или местного бюджетов, а также из бюджета государственного внебюджетного фонда, ведущих учет согласно приведенным выше Планам счетов и инструкциям по их применению.	*Подсистема: «СТЭК – Бухгалтерия»* ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников - должность - банковские реквизиты Подсистема: «СТЭК – Склад» ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников Подсистема: «СТЭК – Учёт основных средств» ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников Подсистема: «СТЭК – Зарплата» ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников - лицевой счет

			Прочие участники (например, которые работают по договору подряда) *Подсистема: «СТЭК – Налогоплательщик»* ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Контактный телефон сотрудников - лицевой счет Прочие участники (например, которые работают по договору подряда) Подсистема: «СТЭК – Учет персонала предприятия» ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников Подсистема: «СТЭК – Учет расчётов по жилфонду» ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников Подсистема: «СТЭК – Общежитие» ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников ФИО студентов - Паспортные данные студентов:

			(Серия, номер, когда, кем выдан) - дата рождения студентов - СНИЛС студентов - ИНН студентов - Адрес по прописке студентов - Место рождения студентов - Контактный телефон студентов - лицевой счет Подсистема: «СТЭК – Расчёты со студентами» ФИО студентов - Паспортные данные студентов: (Серия, номер, когда, кем выдан) - дата рождения студентов - СНИЛС студентов - ИНН студентов - Адрес по прописке студентов - Место рождения студентов - Контактный телефон студентов - лицевой счет ФИО родителей - Паспортные данные родителей: (Серия, номер, когда, кем выдан) - дата рождения родителей - СНИЛС родителей - ИНН родителей - Адрес по прописке родителей - Место рождения родителей - Контактный телефон родителей - Лицевой счет родителе
8	«Контур-Экстерн» — отчётность через интернет	Описание системы защищённого электронного документооборота, позволяющей сдавать отчётность в ФНС, ПФР, ФСС и др. контролирующие органы. Тарифы. Заявка на подключение.	ФИО студентов **- Паспортные данные студентов:** (Серия, номер, когда, кем выдан) - Дата рождения студентов - СНИЛС студентов - ИНН студентов - Адрес по прописке студентов - Место рождения студентов ФИО сотрудников **- Паспортные данные сотрудников:** (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов

Таким образом, высокая эффективность использования вычислительной техники и информационных ресурсов определяется комплексом следующих задач:

- информационное сопровождение и контроль учебного процесса, деятельности структурных подразделений колледжа;
- организация и проведение учебных занятий, организация внеаудиторной самостоятельной работы обучающихся;
- сопровождение дополнительных образовательных услуг;
- мониторинг результатов освоения учебной программы обучающимися.

Администрированием сети и разграничением прав пользователей занимается технический отдел колледжа. Политика безопасности домена предписывает пользователям регулярно изменять свои пароли, контролирует не повторяемость и непохожесть паролей.

В локальной сети колледжа для сотрудников доступны шаблоны различных документов, так же сеть используется для обмена текущими документами. Для этого используются общие папки Windows. Доступ к общим папкам ограничен в зависимости от статуса сотрудника. Сотрудник колледжа может изменять хранящиеся в них документы только в том случае, если у него есть доступ к данной и папке, и он зашел под той ученой записью, в которой был создан данный документ.

Сотрудники колледжа имеют доступ в Интернет через шлюз в корпоративной сети. С помощью электронной почты ведётся обмен документами с другими образовательными организациями и Министерством образования Челябинской области.

1.3. Меры противодействия утечки информации в системах связи

Утечка информации является серьезной опасностью для многих организаций. Она может произойти в результате умысла третьих лиц или по неосторожности сотрудников. Умышленная организация утечки совершается

с двумя целями: первой из них становится нанесение ущерба государству, обществу или конкретной организации, эта цель характерна для проявлений кибертерроризма; второй целью является получение преимущества в конкурентной борьбе.

Непреднамеренная утечка происходит чаще всего по неосторожности сотрудников организации, но также может привести к серьезным неблагоприятным последствиям. Создание системы защиты информационных активов от утраты в компаниях всех типов должно осуществляться на профессиональном уровне, с использованием современных технических средств. Для этого необходимо иметь представление о каналах утечки и способах блокировки этих каналов, а также о требованиях, предъявляемых к современным системам безопасности.

Утечка - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. Технический *канал утечки информации* (ТКУИ), так же, как и канал передачи информации, состоит из источника сигнала, физической среды его распространения и приемной аппаратуры злоумышленника. На рисунке 1 приведена структура технического *канала утечки информации*.

Рис.1. - Структура технического канала утечки информации

Технические каналы утечки информации – каналы утечки защищаемых данных, обусловленные техническими характеристиками используемых для передачи информации средств.

К техническим средствам передачи, обработки, хранения и отображения информации ограниченного доступа (*ТСПИ*) относятся:

- технические средства автоматизированных систем управления, электронно-вычислительные машины и их отдельные элементы (средства вычислительной техники – СВТ);
- средства изготовления и размножения документов;
- аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода;
- системы внутреннего телевидения;
- системы видеозаписи и видеовоспроизведения;
- системы оперативно-командной связи;
- системы внутренней автоматической телефонной связи, включая соединительные линии перечисленного выше оборудования и т. д.

Данные технические средства и системы в ряде случаев именуются основными техническими средствами и системами (*ОТСС*).

Наряду с техническими средствами и системами, обрабатывающими информацию ограниченного доступа, в помещениях устанавливаются и другие технические средства, и системы, которые в обработке информации ограниченного доступа непосредственно не участвуют. К ним относятся:

- системы и средства городской автоматической телефонной связи;
- системы и средства передачи данных в системе радиосвязи;
- системы и средства охранной и пожарной сигнализации;
- системы и средства оповещения и сигнализации;
- контрольно-измерительная аппаратура;
- системы и средства кондиционирования;

– системы и средства проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, телевизоры и радиоприемники и т. д.);

– средства электронной оргтехники;

– системы и средства электро-часофикации и иные технические средства и системы.

Такие технические средства и системы называются вспомогательными техническими средствами и системами (*ВТСС*).

Классификация технических каналов утечки информации приведена на рисунке 2.

Рис. 2. - Классификация технических каналов утечки информации

Существуют определенные принципы, на которых должна основываться комплексная система мер по защите конфиденциальной информации от утечек:

– непрерывность работы системы в пространстве и времени. Используемые способы защиты должны контролировать весь и материальный, и информационный периметр круглосуточно, не допуская возникновения тех или иных разрывов или снижения уровня контроля;

– многозональность защиты. Информация должна ранжироваться по степени значимости, и для ее защиты должны применяться разные по уровню воздействия методы;

– расстановка приоритетов. Не вся информация одинаково важна, поэтому наиболее серьезные меры защиты должны применяться для сведений, имеющих наивысшую ценность;

– интеграция. Все компоненты системы должны взаимодействовать между собой и управляться из единого центра. Если компания холдинговая или имеет несколько филиалов, необходимо настроить управление информационными системами из головной компании;

– дублирование. Все наиболее важные блоки и системы связи должны быть продублированы, чтобы в случае прорыва или уничтожения одного из звеньев защиты ему на смену пришел контрольный.

Построение систем такого уровня не всегда требуется небольшим торговым фирмам, но для крупных компаний, особенно сотрудничающих с государственным заказчиком, оно является насущной необходимостью.

Административно-организационные меры. За их соблюдение должен нести ответственность руководитель компании, а также один из его заместителей, в чьем ведении находится служба безопасности. Почти 70% от общей степени безопасности сведений зависит именно от административно-технических мер, так как в деятельности служб коммерческого шпионажа использование случаев подкупа сотрудников встречается гораздо чаще, чем использование специальных технических средств хищения сведений, требующих высокой квалификации и раскрытия информации третьим лицам, непосредственно не участвующим в конкурентной борьбе.

Разработка документации. Все нормативно-правовые акты организации, посвященные защите конфиденциальных сведений, должны соответствовать самым строгим требованиям, предъявляемым к аналогичным документам, необходимым для получения лицензии. Это связано не только с тем, что они наиболее проработаны, но и с тем, что качественная подготовка

этого типа документации даст в будущем возможность защиты позиции образовательной организации в суде при возникновении споров об утечке информации.

Работа с персоналом. Персонал является наиболее слабым звеном в любой системе защиты информации от утечек. Это приводит к необходимости уделять работе с ним максимальное внимание. Для организаций, работающих с государственной тайной, предусмотрена система оформления допусков. Иным организациям необходимо принимать различные меры для обеспечения ограничения возможности работы с конфиденциальными данными. Необходимо составить перечень сведений, составляющих коммерческую тайну, и оформить его в качестве приложения к трудовому договору. При работе с информацией, содержащейся в базе данных, должны быть разработаны системы допуска.

Необходимо ограничить все возможности копирования и доступ к внешней электронной почте. Все сотрудники должны быть ознакомлены с инструкциями о порядке работы со сведениями, содержащими коммерческую тайну, и подтвердить это росписями в журналах. Это позволит при необходимости привлечь их к ответственности.

Пропускной режим, существующий на объекте, должен предполагать не только фиксацию данных всех посетителей, но и сотрудничество только с охранными предприятиями, которые также соответствуют всем требованиям безопасности. Ситуация, когда сотрудник ЧОПа дежурит в ночное время на объекте, в котором сотрудники для удобства системного администратора записывают свои пароли и оставляют их на рабочем столе, может являться столь же опасной, как и работа хакера-профессионала или заложенные в помещении технические средства перехвата.

Планировочные и технические решения. При планировании архитектуры помещения, в котором проводятся переговоры или находится защищаемая информация, должны соблюдаться все требования ГОСТа по способам защиты. Помещения переговорных должны быть способны пройти

необходимую аттестацию, должны применяться все современные способы экранирования, звукопоглощающие материалы, использоваться генераторы помех.

Технические средства и системы предотвращения утечек. Для защиты информации от утечки или хищения необходимо применять широкий спектр мер аппаратно-технического характера. Современные технические средства подразделяются на четыре группы:

- инженерные;
- аппаратные;
- программные;
- криптографические.

Инженерные. Эта категория средств защиты применяется в рамках реализации планировочно-архитектурных решений. Они представляют собой устройства, физически блокирующие возможность проникновения посторонних лиц к охраняемым объектам, системы видеонаблюдения, сигнализации, электронные замки и другие аналогичные технические приспособления.

Аппаратные. К ним относятся измерительные приборы, анализаторы, технические устройства, позволяющие определять места нахождения закладных приборов, все, что позволяет выявить действующие каналы утечки информации, оценить эффективность их работы, выявить значимые характеристики и роль в ситуации с возможной или произошедшей утратой сведений. Среди них присутствуют индикаторы поля, радиочастотометры, нелинейные локаторы, аппаратура для проверки аналоговых телефонных линий. Для выявления диктофонов используются детекторы, которые обнаруживают побочные электромагнитные излучения, по тому же принципу работают детекторы видеокамер.

Программные. Наиболее значимая группа, так как с ее помощью можно избежать проникновения в информационные сети посторонних лиц, блокировать хакерские атаки, предотвратить перехват информации. Среди них

необходимо отметить специальные программы, обеспечивающие системную защиту информации. Это DLP-системы и SIEM-системы, наиболее часто применяемые для создания механизмов комплексной информационной безопасности. DLP (Data Leak Prevention, системы предотвращения утечек данных) обеспечивают полную защиту от утраты конфиденциальной информации. Сегодня они настраиваются в основном на работу с угрозами внутри периметра, то есть исходящими от пользователей корпоративной сети, а не от хакеров.

Системы применяют широкий набор приемов выявления точек утраты или преобразования информации и способны блокировать любое несанкционированное проникновение или передачу данных, автоматически проверяя все каналы их отправки. Они анализируют трафик почты пользователя, содержимое локальных папок, сообщения в мессенджерах и при выявлении попытки переправить данные блокируют ее.

SIEM-системы (Security Information and Event Management) управляют информационными потоками и событиями в сети, при этом под событием понимается любая ситуация, которая может повлиять на сеть и ее безопасность. При ее возникновении система самостоятельно предлагает решение об устранении угрозы.

Программные технические средства могут решать отдельные проблемы, а могут и обеспечивать комплексную безопасность компьютерных сетей.

Криптографические. Эта категория обеспечивает алгоритмы шифрования всей информации, которая передается по сетям или хранится на сервере. Даже при утрате она не будет представлять интерес для гипотетического конкурента.

Комплексное применение всего диапазона методов защиты может быть избыточным, поэтому для организации систем защиты информации в образовательной организации нужно создавать собственный проект, который окажется оптимальным с ресурсной точки зрения.

Выводы по Главе I

По итогам первой главы магистерской диссертации можно сделать следующие выводы.

1. Описаны системы связи в образовательной организации.

Система связи – это комплекс технических и программных средств, позволяющих осуществлять коммуникацию между сотрудниками и группами сотрудников в пределах объекта.

В зависимости от технологии и функций, системы связи разделяются на следующие разновидности: системы телефонной связи; системы радиосвязи; системы оперативной диспетчерской связи**;** системы оповещения; системы радиотрансляции; системы обеспечения связи конференций**; т**ехнологические сети связи; локальная вычислительная сеть.

2. Описаны информационные ресурсы образовательной организации, подлежащие защите от утечки по каналам связи.

Под утечкой информации по каналам связи понимается неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего прием информации.

К защищаемым данным в образовательной организации относятся данные, являющиеся предметом собственности и подлежащие защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Это, как правило, информация ограниченного доступа, содержащая сведения конфиденциального характера.

3. Выявлены меры противодействия утечки информации в системах связи.

Существуют определенные принципы, на которых должна основываться комплексная система мер по защите конфиденциальной информации от утечек: непрерывность работы системы в пространстве и времени;

многозональность защиты; расстановка приоритетов; интеграция; дублирование.

Таким образом, для комплексной защиты информации от утечки в системах связи необходимы следующие методы защиты: административно-организационные меры; разработка документации; работа с персоналом; планировочные и технические решения; технические средства и системы предотвращения утечек.

Комплексное применение всего диапазона методов защиты может быть избыточным, поэтому для организации систем защиты информации в образовательной организации нужно создавать собственный проект, который окажется оптимальным с ресурсной точки зрения.

ГЛАВА 2. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1. Характеристика Государственного бюджетного образовательного учреждения «Мишкинский профессионально-педагогический колледж»

Объектом исследования является ГБПОУ «Мишкинский профессионально-педагогический колледж».

ГБПОУ «Мишкинский профессионально – педагогический колледж» находится: Курганская область, р.п. Мишкино, ул. Павших борцов, 4 (корпус 1 отделение ПССЗ).

Колледж готовит специалистов разного уровня квалификации и проф. направлений.

ГБПОУ «Мишкинский профессионально-педагогический колледж» располагает достаточной материальной базой для организации работы образовательного процесса.

Лаборатории: архитектуры вычислительных систем, технических средств информатизации, информационных систем, компьютерных сетей, инструментальных средств разработки. Каждая лаборатория оснащена необходимой компьютерной техникой, мультимедийным оборудованием, лицензионным программным обеспечением, все ПК объединены сетью и имеют выход в Интернет.

Минимальное оснащение любой лаборатории: АРМ студента - ПК – 14 шт., ПК – рабочее место преподавателя, АРМ преподавателя: ПК, мультимедиа проектор, акустическая система, экран, лицензионное ПО:

1. MicrosoftOffice 2007 (удалённый доступ);
2. MS VisualStudio 2010 (удалённый доступ);
3. PhotoShop;
4. Corel Draw;
5. Компас 3D;
6. Flash CS3;
7. NotePad++;

8. MS Windows XP;

9. Opera;

10. Chrom;

11. Клавиатурный тренажер Stamina.

С любого компьютера колледжа в соответствии с политикой доступа можно воспользоваться сетью Интернет со скоростью до 15 Мбит/с. В библиотеке колледжа функционирует специальная зона для самостоятельной работы студентов и преподавателей, к которой так же можно получить доступ к сети Интернет. Для обучающихся действуют специальные ограничения в соответствии с федеральным законом № 139-ФЗ от 28 июля 2012 года.

В связи с обновлениями аудиторий, в колледже постоянно ведется работа по составлению и актуализации паспортов компьютерных аудиторий, для получения которых проводятся специальные измерения критических показателей для соответствия требованиям СанПиН, пожарной безопасности и охраны труда.

Объект имеет три режима:

- рабочий;
- обеденный;
- не рабочий.

Доступ на территорию и в само здание по пропускам и студенческим билетам.

Технические каналы утечки информации:

1. Оптический канал утечки информации:

- окна, двери и закладные устройства.

2. Акустический канал утечки информации:

- двери, стены, потолок, пол, окна, вентиляция, батареи, электроприборы, закладные устройства.

3. Радиоэлектронный канал утечки информации:

- электросети, радиосети, закладные устройства.

Наиболее опасный из всех рассмотренных каналов утечки является радиоэлектронный, так как ПЭМИ выходит за границы объекта исследования, но и другими каналами утечки информации не стоит пренебрегать.

2.2. Анализ состояния защиты информации от утечки в системах связи в ГБПОУ «Мишкинский профессионально-педагогический колледж»

Как правило, во многих образовательных организациях каналам утечки информации по каналам связи (телефонные сети и ЛВС) практически не уделяется внимания. Многие руководители не считают нужным затрачивать на это время и деньги. Однако, для опытных взломщиков не составит никакого труда получить все необходимые данные, используя, например, телефонную сеть. Именно поэтому защита каналов связи является одной из приоритетных задач при построении системы защиты информации.

Система обеспечения информационной безопасности в колледже осуществляется комплексно и включает в себя меры следующих уровней:

1 уровень: Нормативно–правовой, включающий законы, постановления правительства и указы президента, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации ограниченного доступа, а также вводятся меры ответственности за нарушения этих правил.

Основными законодательными актами, регулирующими вопросы информационной безопасности колледжа, являются:

– Гражданский кодекс РФ ст.139;

– Уголовный кодекс гл.28 ст.272, 273, 274, 138, 183;

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в действующей редакции.

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в действующей редакции.

– Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2 уровень - Организационно-административный.

Организационные меры являются решающим звеном формирования и реализации комплексной защите информации. Эти меры 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 пользователей или персонала защиты.

Организационные меры защиты информации в колледже реализованы следующим образом:

– организован контроль, соблюдение временного режима труда и пребывания сотрудников колледжа на территории организации;

– организована работа с документами и документированной информацией, т.е. ведется учет, исполнение, возврат, хранение носителей конфиденциальной информации;

– администрирование сети и разграничением прав пользователей. Политика безопасности домена предписывает пользователям регулярно изменять свои пароли, контролирует не повторяемость и непохожесть паролей.

В качестве недостатков данного уровня защиты можно указать следующие факты.

В колледже отсутствует обучение пользователей ИС, периодические инструктажи, наказания/поощрения пользователей, что ведет к небрежности сотрудников, выраженная в недостаточном знании правил защиты конфиденциальной информации, непониманием необходимости тщательного

их выполнения и студентов, заключающаяся в частоте блокирование системы из-за неправильности введенных данных.

А также на административном уровне политика информационной безопасности пока не утверждена.

3 уровень - Программно-аппаратный.

Программно-технические меры защиты информации - это совокупность аппаратных и программных средств и мероприятий по их использованию в интересах защиты конфиденциальности информации.

В колледже осуществляется управление доступом путем деления информации по соответствующим должностям и полномочиям доступа к ней, т.е. спецификация и контроль действий пользователей над информационными ресурсами колледжа.

Программно-аппаратные средства защиты информации.

ViPNet Client (Клиент) — это программный комплекс, выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

ViPNet Client функционирует под управлением операционных систем MS Windows: Windows XP SP3 (32-разрядная) / Windows Server 2003 (32-разрядная) / Windows Vista SP2 (32/64-разрядная) / Windows Server 2008 (32/64-разрядная) / Windows 7 (32/64-разрядная)/Windows Server 2008 R2 (64-разрядная).

Программный комплекс ViPNet Client 3.2 представлен в двух исполнениях для соответствия требованиям СКЗИ разных классов (КС2 и КС3).

Преимущества

– Высокая производительность шифрования и фильтрации трафика позволяет в реальном времени осуществлять защиту трафика служб голосовой

и видеосвязи в сетях TCP/IP, а также обеспечивать одновременную работу с ресурсами разных сегментов корпоративной сети.

– Равный доступ к ресурсам корпоративных информационных систем независимо от места и способа подключения пользователя к телекоммуникационной сети.

– Защита канала не влияет на работу сторонних приложений на компьютере пользователя.

– Ключи шифрования, политики безопасности и обновления ПО ViPNet доставляются на компьютер через надежный защищенный канал.

1. Антивирусная система Kaspersky Anti-Virus для защиты от компьютерных вирусов. Производится нерегулярное обновление баз и сканирование рабочих станций.

Таким образом, можно сделать вывод, что система обеспечения информационной безопасности в колледже существует, но имеет уязвимости.

Самым уязвим местом в системе безопасности можно назвать сотрудников колледжа и программно-аппаратные средства. В частности в колледже: не выполняется резервное копирование данных на персональных компьютерах сотрудников колледжа - при отказах оборудования некоторые важные данные могут быть потеряны; не выполняется обновление операционной системы MS Windows и использующегося ПО, что может привести к несанкционированному доступу к хранящейся на ПК информации или её повреждению из-за ошибок в ПО; доступ сотрудников к ресурсам Интернета не контролируется, из-за этого может произойти утечка данных; деловая электронная переписка ведётся через Интернет по незащищённым каналам, сообщения электронной почты хранятся на серверах почтовых служб в Интернете; некоторые сотрудники имеют недостаточные навыки работы с автоматизированными системами, используемыми в колледже, что может привести к появлению в системе неверных данных; отсутствуют нормативные документы по безопасности.

Выводы по Главе II

Во второй главе магистерской диссертации проведен анализ информационной безопасности ГБПОУ «Мишкинский профессионально-педагогический колледж».

Система обеспечения информационной безопасности в колледже осуществляется комплексно и включает в себя меры следующих уровней:

1 уровень: Нормативно–правовой, включающий законы, постановления правительства и указы президента, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации ограниченного доступа, а также вводятся меры ответственности за нарушения этих правил.

2 уровень - Организационно-административный.

Организационные меры защиты информации в колледже реализованы следующим образом:

– организован контроль, соблюдение временного режима труда и пребывания сотрудников колледжа на территории организации;

– организована работа с документами и документированной информацией, т.е. ведется учет, исполнение, возврат, хранение носителей конфиденциальной информации;

– администрирование сети и разграничением прав пользователей.

3 уровень - Программно-аппаратный.

Программно-аппаратные средства защиты информации:

– ViPNet Client (Клиент);

– Антивирусная система Kaspersky Anti-Virus.

Таким образом, можно сделать вывод, что система обеспечения информационной безопасности в колледже существует, но имеет уязвимости.

ГЛАВА 3. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ПРОТИВОДЕЙСТВИЮ УТЕЧКИ ИНФОРМАЦИИ В СИСТЕМАХ СВЯЗИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

3.1. Проект рекомендаций по противодействию утечки информаци в системах связи в ГБПОУ «Мишкинский профессионально-педагогический колледж»

Мероприятия по защите конфиденциальной информации от утечки по системам связи (далее - технической защите информации) являются составной частью деятельности образовательной организации и осуществляются во взаимосвязи с другими мерами по обеспечению их информационной безопасности.

Защита конфиденциальной информации от утечки по техническим каналам 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 (далее – объекта защиты).

Организационные мероприятия по защите информации от утечки по техническим каналам 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 образовательной организации на объекты информатизации и в выделенные помещения.

Технические мероприятия по защите информации от утечки по техническим каналам основываются на применении технических средств защиты и реализации специальных проектных и конструкторских решений.

Техническая защита информации осуществляется подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководителями организаций для проведения таких работ. Для разработки мер по защите информации могут привлекаться сторонние организации, имеющие лицензии ФСТЭК или ФСБ России на право проведения соответствующих работ.

Для защиты информации рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства защиты. Порядок сертификации определяется законодательством Российской Федерации.

Перечень необходимых мер защиты информации определяется по результатам специального обследования объекта защиты, сертификационных испытаний и специальных исследований технических средств, предназначенных для обработки конфиденциальной информации.

Уровень технической защиты информации должен соответствовать соотношению затрат на организацию защиты информации и величины ущерба, который может быть нанесен собственнику информационных ресурсов.

Защищаемые объекты должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России на соответствие установленным нормам и требованиям по защите информации. По результатам аттестации дается разрешение (аттестат соответствия) на обработку конфиденциальной информации на данном объекте.

Ответственность за обеспечение требований по технической защите информации возлагается на руководителей организаций, эксплуатирующих защищаемые объекты.

В целях своевременного выявления и предотвращения утечки информации по техническим каналам должен осуществляться контроль состояния и эффективности защиты информации. Контроль заключается в

проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Защита информации считается эффективной, если принятые меры соответствуют установленным требованиям и нормам. Организация работ по защите информации возлагается на руководителей подразделений, эксплуатирующих защищаемые объекты, а контроль за обеспечением защиты информации - на руководителей подразделений по защите информации (служб безопасности).

Установка технических средств обработки конфиденциальной информации, а также средств защиты информации должна выполняться в соответствии с техническим проектом или техническим решением. Разработка технических решений и технических проектов на установку и монтаж ТСОИ, а также средств защиты информации производится подразделениями по защите информации (службами безопасности предприятий) или проектными организациями, имеющими лицензию ФСТЭК, на основании технических заданий на проектирование, выдаваемых заказчиками.

Технические решения по защите информации от утечки по техническим каналам являются составной частью технологических, планировочных, архитектурных и конструктивных решений и составляют основу системы технической защиты конфиденциальной информации.

Непосредственную организацию работ по созданию СТЗИ осуществляет должностное лицо, обеспечивающее научно-техническое руководство проектированием объекта защиты.

Разработка и внедрение СТЗИ может осуществляться как силами образовательной организации, так и другими специализированными организациями, имеющими лицензии ФСТЭК и (или) ФСБ России на соответствующий вид деятельности.

В случае разработки СТЗИ или ее отдельных компонентов специализированными организациями в организации - заказчике определяются подразделения или отдельные специалисты, ответственные за

организацию и проведение мероприятий по защите информации, которые должны осуществлять методическое руководство и участвовать в специальном обследовании защищаемых объектов, аналитическом обосновании необходимости создания СТЗИ, согласовании выбора ТСОИ, технических и программных средств защиты, разработке технического задания на создание СТЗИ, организации работ по внедрению СТЗИ и аттестации объектов защиты.

Порядок организации на предприятии работ по созданию и эксплуатации объектов информатизации и выделенных (защищаемых) помещений определяется в специальном «Положении о порядке организации и проведения на предприятии работ по защите информации от ее утечки по техническим каналам» с учетом конкретных условий, которое должно определять:

- порядок определения защищаемой информации;
- порядок привлечения подразделений организации, специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и СТЗИ, их задачи и функции на различных стадиях создания и эксплуатации защищаемого объекта;
- порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;
- порядок разработки, ввода в действие и эксплуатацию защищаемых объектов;
- ответственность должностных лиц за своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СТЗИ.

В образовательной организации должен быть документально оформлен перечень сведений, подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа персонала к такого рода сведениям.

При организации работ по защите утечки по техническим каналам информации на защищаемом объекте можно выделить три этапа [6, 9]:

1. Первый этап (подготовительный, предпроектный).

2. Второй этап (проектирование СТЗИ).

3. Третий этап (этап ввода в эксплуатацию защищаемого объекта и системы технической защиты информации).

Подготовительный этап создания системы технической защиты информации

На первом этапе осуществляется подготовка к созданию системы технической защиты информации на защищаемых объектах, в процессе которой проводится специальное обследование защищаемых объектов, разрабатывается аналитическое обоснование необходимости создания СТЗИ и техническое (частное техническое) задание на ее создание.

В качестве объекта защиты мы выбрали кабинет директора колледжа (ГБПОУ «Мишкинский профессионально-педагогический колледж). На первом этаже здания размещены кабинет директора колледжа, приемная, столовая, спортивный зал, бухгалтерия, кабинет заместителя директора по учебной работе, кабинет заместителя директора по АХЧ, учебные аудитории и охрана. Библиотека, актовый-зал, учебные кабинеты, кабинет заместителя директора по научно-методической работе, преподавательская расположены на втором этаже. Территория вокруг здания обнесена забором. Вход людей в здание осуществляется по пропускам и студенческим билетам.

Площадь кабинета руководителя составляет 40 м^2. В помещении – есть два окна, выходящих на улицу, и дверь в кабинет секретаря (приемная).

Для описания факторов, влияющих на защищенность информации в кабинете, проводится его обследование по 6 группам факторов (таблица 2):

1. общая характеристика помещения;

2. характеристика ограждения;

3. предметы мебели и интерьера;

4. средства и системы информатизации, участвующие в обработке информации - основные технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи информации ограниченного доступа, программные средства;

5. технические средства и системы, не обрабатывающие непосредственно информацию, но размещенные в помещениях, где она обрабатывается - вспомогательные технические средства и системы;

6. средства коммуникации.

Таблица 2

Результаты обследования кабинета

Общая характеристика помещения	
Этаж	1
Площадь, м^2	40
Смежные помещения	слева – кабинет секретаря; справа – бухгалтерия; вверху – учебные аудитории; внизу – мед. пункт
Ограждения	
Стены	наружная – железобетон 600 мм, на стене укреплены две стальные штампованные батареи отопления, соединенные металлическими трубами с трубой в боковой стене; смежная с коридором – железобетонная толщиной 300 мм; смежная с приемной – железобетонная толщиной 400 мм
Потолок	железобетонная плита толщиной 200 мм с фальшпотолком
Пол	железобетонная плита толщиной 200 мм с фальшполом
Окна	количество – 2, двух камерные с 1 фрамугой, обращены на улицу, толщина стекла 3 мм

Продолжение таблицы 2

1	2
Дверь	типовая деревянная, выход к секретарю
Предметы мебели и интерьера	
Стол для заседаний	1 шт., рассчитан на 6 человек
Стулья	деревянные полужесткие, 6 шт.
Кресло кожаное	8 шт.
Журнальный-стеклянный стол	1 шт.
Основные технические средства и системы	
Компьютер	Системный блок, монитор, мышь, клавиатура. Подключение к локальной сети и выход в интернет
Принтер	1 шт.
Вспомогательные технические средства и системы	
Телефон	внутренней и районной АТС
Электронные часы	на стене смежной с приёмной
Извещатели пожарные	2 шт. на потолке
Светильники	4 шт.
Средства коммуникации	
Розетка электропитания	2 шт., возе письменного стола
Телефонная розетка	одна под письменным столом
Электропроводка	скрытая в потолке и полу
Кабель телефонной линии	внутренний, плоский два провода – 6 м, укреплён в стене возле письменного стола

Кабель локальной сети ЭВМ	оптоволокно (с сердечником 50 мк и оболочкой 125 мк) – 6,5 метров, укреплён в стене возле письменного стола
Шлейф пожарной сигнализации	внутренний, на потолке

План кабинета директора колледжа представлен на рисунке 3.

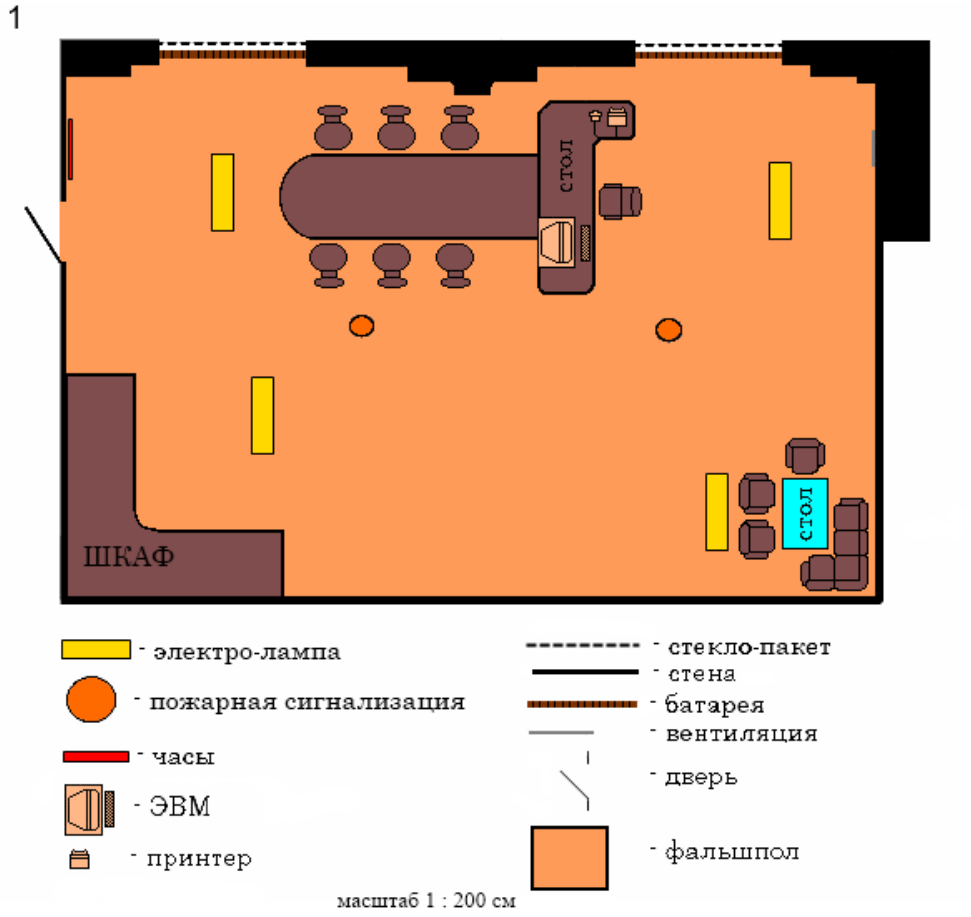

Рис. 3 – План кабинета директора колледжа

План сетей кабинета директора колледжа представлен на рисунке 4.

Рис. 4. - План сетей кабинета директора колледжа

После проведения предпроектного специального обследования защищаемого объекта, проводится аналитическое обоснование необходимости создания СТЗИ, в процессе которого:

– определяется перечень сведений, подлежащих защите (перечень сведений конфиденциального характера утверждается руководителем образовательной организации);

– проводится категорирование сведений конфиденциального характера, подлежащих защите;

– определяется перечень лиц, допущенных до сведений конфиденциального характера, подлежащих защите;

– определяется степень участия персонала в обработке (обсуждении, передаче, хранении и т.п.) информации, характер их взаимодействия между собой и со службой безопасности;

– разрабатывается матрица допуска персонала к сведениям конфиденциального характера, подлежащих защите;

– определяется (уточняется) модель вероятного противника (злоумышленника, нарушителя);

– проводятся классификация и категорирование объектов информатизации и выделенных помещений;

– проводится обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации, для проектирования и внедрения СТЗИ;

– проводится оценка материальных, трудовых и финансовых затрат на разработку и внедрение СТЗИ;

– определяются ориентировочные сроки разработки и внедрения СТЗИ.

Основным признаком конфиденциальной информации является ее ценность для потенциального противника. Поэтому, определяя перечень сведений конфиденциального характера, их обладатель должен определить эту ценность через меру ущерба, который может быть нанесен образовательной организации при их утечке (разглашении). В зависимости от величины ущерба (или негативных последствий), который может быть нанесен при утечке (разглашении) информации, вводятся следующие категории важности информации:

1 категория – информация, утечка которой может привести к потере экономической или финансовой самостоятельности образовательной организации или потери ее репутации;

2 категория – информация, утечка которой может привести к существенному экономическому ущербу или снижению ее репутации;

3 категория – информация, утечка разглашение которой может нанести экономический ущерб образовательной организации.

Следовательно, целесообразно установить шесть уровней конфиденциальности информации (таб. 3).

Таблица 3

Уровни конфиденциальности информации

Величина ущерба (негативных последствий), который может быть нанесен при разглашении конкретной информации	Уровень конфиденциальности информации	
	информация, не подлежащая передаче другим ОО	информация, предназначенная для передачи другим ОО или полученная от них
Утечка информации может привести к потере экономической или финансовой самостоятельности ОО или потери ее репутации	1.1	1.2
Утечка информации может привести к существенному экономическому ущербу или снижению репутации ОО	2.1	2.2
Утечка информации может нанести экономический ущерб ОО	3.1	3.2

Введение категорий конфиденциальности информации необходимо для определения объема и содержания комплекса мер по ее защите.

При установлении режима доступа к конфиденциальной информации необходимо руководствоваться принципом - чем больше ущерб от разглашения информации, тем меньше круг лиц, которые к ней допущены.

Режимы доступа к конфиденциальной информации должны быть увязаны с должностными обязанностями сотрудников.

В целях ограничения круга лиц, допущенных к сведениям, составляющим коммерческую тайну, целесообразно введение следующих режимов доступа к ней:

режим 1 – обеспечивает доступ ко всему перечню сведений конфиденциального характера. Устанавливается руководящему составу образовательной организации;

режим 2 – обеспечивает доступ к сведениям при выполнении конкретных видов деятельности (финансовая, производственная, кадры,

безопасность и т.п.). Устанавливается для руководящего состава отделов и служб;

режим 3 – обеспечивает доступ к определенному перечню сведений при выполнении конкретных видов деятельности. Устанавливается для сотрудников - специалистов конкретного отдела (службы) в соответствии с должностными обязанностями.

Таким образом, после составления перечня сведений конфиденциального характера необходимо установить уровень их конфиденциальности, а также режим доступа к ним сотрудников.

Для обеспечения дифференцированного подхода к организации защиты информации от утечки по техническим каналам защищаемые объекты должны быть отнесены к соответствующим категориям и классам.

Классификация объектов проводится по задачам технической защиты информации и устанавливает требования к объему и характеру комплекса мероприятий, направленных на защиту конфиденциальной информации от утечки по техническим каналам в процессе эксплуатации защищаемого объекта.

Защищаемые объекты целесообразно разделить на два класса защиты (табл. 4).

К классу защиты А относятся объекты, на которых осуществляется полное скрытие информационных сигналов, которые возникают при обработке информации или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте).

К классу защиты Б относятся объекты, на которых осуществляется скрытие параметров информационных сигналов, возникающих при обработке информации или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте).

Таблица 4

Классы защиты объектов информатизации и выделенных помещений

Задача технической защиты информации	Установленный класс защиты
Полное скрытие информационных сигналов, которые возникают при обработке информации или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте)	А
Скрытие параметров информационных сигналов, которые возникают при обработке информации или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте)	Б

При установлении категории защищаемого объекта учитываются класс его защиты, а также финансовые возможности образовательной организации по закрытию потенциальных технических каналов утечки информации. Защищаемые объекты целесообразно разделить на три категории.

Моделирование оптического канала утечки информации

Утечка визуальной информации возможна по следующим оптическим каналам:

– источник визуального сигнала – окно – оптико-лазерный приемник злоумышленника;

– источник визуального сигнала – дверь – злоумышленник.

Для оценки угроз визуальной информации необходимо оценить уровень оптического сигнала в возможных местах размещения оптического приемника злоумышленника. Такими местами являются:

1. жилой дом;
2. кабинет секретаря.

Моделирование акустического канала утечки информации

Утечка речевой информации возможна по следующим акустическим каналам:

– источник речевого сигнала – стена в соседнее помещение – акустический приемник злоумышленника;

– источник речевого сигнала – приоткрытая дверь в приемную – акустический приемник;

– источник акустического сигнала – закладное устройство – радиоканал – радиоприемник злоумышленника;

– источник акустического сигнала – стекло окна – модулированный лазерный луч – фотоприемник лазерной системы подслушивания;

– источник акустического сигнала – воздухопровод – акустический приемник;

– источник акустического сигнала – случайный акустоэлектрический преобразователь в техническом средстве – побочное излучение технического средства – радиоприемник;

– источник акустического сигнала – случайный акустоэлектрический преобразователь в техническом средстве – проводные кабели, выходящие за пределы контролируемой зоны;

– источник акустического сигнала – воздушная среда помещения – диктофон у злоумышленника.

Для оценки угроз речевой информации необходимо оценить уровень акустического сигнала в возможных местах размещения акустического приемника злоумышленника. Такими местами являются:

– кабинет секретаря;

– коридор;

– смежные с кабинетом помещения;

– труба отопления, проходящая рядом с кабинетом;

– воздуховод вентиляции.

Кроме того, речевая информация в кабинете может ретранслироваться по радиоканалу или проводам телефонной линии и электропитания закладными устройствами и побочными электромагнитными излучениями

основных и вспомогательных технических средств и систем, а также средствами лазерного подслушивания. Так как носителями информации при ретрансляции являются электромагнитная волна в радиодиапазоне и электрический ток, то угрозы и меры по предотвращению перехвата рассматриваются в радиоэлектронном канале утечки информации. Также акустическая информация может быть добыта с помощью лазерного средства подслушивания, установленного в помещении противоположного дома.

В качестве критерия защищенности речевой информации используется отношение сигнал/шум, при котором качество подслушиваемой речевой информации ниже допустимого уровня. В соответствии с существующими нормами понимание речи невозможно, если отношение помеха/сигнал равно 6-8, а акустический сигнал не воспринимается человеком как речевой, если отношение помеха/сигнал превышает 8-10. Следовательно, для гарантированной защищенности речевой информации отношение сигнал/шум должно быть не более 0,1 или -10 дБ.

Уровни громкости речевой информации в возможных местах размещения акустического приемника злоумышленника при громкости источника 70 дБ указаны в таблице 5.

Таблица 5

Уровни громкости речевой информации

Характеристика речи	Громкость, дБ	Основной элемент среды распространения	Величина звукоизоляции, дБ	Место нахождения акустического приемника	Уровень шума, дБ
1	2	3	4	5	6
Спокойный разговор	50-60	Стена и дверь в приемную	27	Приемная	30
Громкая речь	60-70	Стена в коридор	51	Коридор	35-40
Шумное совещание	70-80	Стена в смежную комнату	40	Соседнее помещение	20-25
		Межэтажное перекрытие	50	Помещения на верхнем и	25-30

				нижнем этажах	
		Вентиляционный короб	0,2 дБ/м 3-7дБ на изгиб	В вентиляционном отверстии другого помещения	30
		Трубы отопления	25-35	На трубе отопления	30

Из данных таблицы 6, наибольшую угрозу создает канал утечки, приемник которого расположен в кабинете секретаря и в коробе вентиляции.

Таблица 6

Угрозы

№	Место размещения акустического приемника злоумышленника	Уровень громкости, дБ	Риск подслушивания
1	2	3	4
1	Кабинет секретаря	5-10	Очень высокий
2	Коридор	-15- (-20)	Отсутствует
3	Соседнее помещение	-5	Низкий
4	Верхнее (нижнее) помещение	-5- (-10)	Отсутствует
5	Вентиляционный короб	0-5	Средний
6	Трубы отопления	0-5	Средний

Каналом утечки, приемник которого расположен в коридоре, можно пренебречь.

Моделирование радиоэлектронного канала утечки информации

Радиоэлектронные каналы утечки информации в кабинете директора представляют собой простые каналы и части составных акусто-радиоэлектронных каналов утечки информации.

Простые каналы образованы побочными электромагнитными излучениями и наводками радиосредств и электрических приборов, размещенных в кабинете, в том числе компьютера при обработке на нем закрытой информации.

Кроме того, опасные сигналы случайных акустоэлектрических преобразователей в радиосредствах и электрических приборах могут добавить к простым оптическим и акустическим каналам радиоэлектронные каналы утечки информации и создать составные акусто-радиоэлектронные и оптико-радиоэлектронные каналы утечки. Источниками радиоэлектронных каналов утечки в составе акусто-радиоэлектронных составных являются:

– коммутационное оборудование и кабели внутренней АТС;

– электрические приборы в кабинете (вторичные часы единого времени);

– передатчики акустических и телевизионных закладных устройств.

Побочные НЧ и ВЧ излучения ОТСС имеют очень широкий диапазон частот – доли Гц – тысячи МГц (длины волн – сотни метров – десятки сантиметров). Помещение кабинета, учитывая его размеры, представляет собой ближнюю, переходную и дальнюю зону побочного излучения ОТСС. На частотах до 30 МГц помещение образует ближнюю зону. В зависимости от вида излучателя в ближней зоне может преобладать электрическое или магнитное поля.

Информация в помещении находится в безопасности, если уровни ее носителей в виде электрических сигналов и напряженности поля не превышают нормативы. Следовательно, для предотвращения подслушивания путем перехвата опасных сигналов необходимо определить эти уровни на периметре кабинета и в случае недопустимо больших значений определить рациональные меры по их уменьшению.

Уменьшение затухания электромагнитной волны в железобетонных стенах с повышением ее частоты вызвано снижением экранирующего эффекта металлической арматуры железобетона. На частоте 1 ГГц длина волны равна 30 см, соизмеримая с размерами ячеек арматуры.

При ослаблении электромагнитной волны железобетонными стенами здания на 20 дБ дальность ее распространения уменьшается на 1 порядок. Учитывая, что окна кабинета выходят на улицу, риск перехвата

радиоизлучений ПЭВМ из кабинета руководителя организации можно оценить значением «средний», а электрических сигналов акустоэлектрических преобразователей – «низкий».

Таким образом, наибольший ущерб информации, содержащейся в кабинете директора колледжа, могут нанести следующие угрозы:

– подслушивание разговора в кабинете через приоткрытую дверь в кабинете секретаря;

– подслушивание громкого разговора через стену, разделяющую кабинет и коридор;

– перехват побочных электромагнитных излучений радиоэлектронных средств и электрических приборов, размещенных и работающих в кабинете во время разговора;

– перехват опасных сигналов, содержащих речевую информацию, распространяющихся по проводам телефонных линий связи, трансляции, часов единого времени, электропитания и заземления;

– подслушивание с помощью стетоскопа речевой информации акустических сигналов, распространяющихся по трубам отопления;

– подслушивание речевой информации акустических сигналов, распространяющихся по воздухопроводам;

– подслушивание с помощью акустических закладных устройств, установленных в кабинете.

На основе аналитического обоснования и действующих нормативно-методических документов по защите информации от утечки по техническим каналам, с учетом установленного класса и категории защищаемого объекта задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СТЗИ.

Техническое задание (ТЗ) на разработку СТЗИ должно содержать:

- обоснование разработки;
- исходные данные объекта защиты в техническом, программном, информационном и организационном аспектах;

– ссылку на нормативно-методические документы, с учетом которых будет разрабатываться и приниматься в эксплуатацию СТЗИ;

– конкретные требования к СТЗИ;

– перечень предполагаемых к использованию технических средств защиты информации;

– состав, содержание и сроки проведения работ по этапам разработки и внедрения;

– перечень подрядных организаций - исполнителей различных видов работ;

– перечень предъявляемой заказчику научно-технической продукции и документации.

Техническое задание на проектирование СТЗИ защищаемого объекта оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности организации-заказчика в части достаточности мер по технической защите информации и утверждается заказчиком.

Стадия проектирования системы технической защиты информации

Меры предотвращения утечки информации

Оптический канал утечки информации:

– установка трёх камерного пакета с рельефным стеклом и специальной плёнкой, жалюзи и стальных ставней на окна;

– экранирование стекла для монитора.

Акустический канал утечки информации:

– установка двойной двери с тамбуром, в котором размещена звуковая колонка, устранение щелей между дверью и дверной коробкой, покрытие двери и тамбура звукопоглощающими материалами, установка на дверь замка с автозащелкой, экранов на стены, перед батареями отопления – акселерометров и экранов на батареи, зашумления вентиляционного канала;

– использование шумогенератора, линейное и пространственное зашумление (приложение 1);

– использование защиты от прослушивания телефонной линии (приложение 2).

Радиоэлектронный канал утечки информации:

– экранирование проводных коммуникаций, в частности для ПЭВМ кабель с фильтром, между системным блоком и монитором;

– процессор компьютера со свинцовым напылением;

– подавитель сотовой связи (приложение 3).

Предотвращение перехвата радио и электрических сигналов

Предотвращение утечки информации из кабинета по радио-электронному каналу можно обеспечить:

– выключением во время разговора всех радиосредств и электрических приборов, без которых можно обойтись;

– установкой в разрыв цепей электропитания возле стен сетевых фильтров для исключения ВЧ-навязывания;

– установкой средств подавления сигналов акустоэлектрических преобразователей телефонных аппаратов;

– установкой НЧ-фильтров в цепь вторичных часов единого времени;

– использованием в кабинете генератора пространственного электромагнитного зашумления кабинета, включаемого во время проведения совещания;

– установкой в свободный слот системной платы компьютера платы генератора помех.

Кроме того, после проведения капитального ремонта и перед проведением совещания производить чистку помещения с целью обнаружения закладных устройств.

Меры по защите речевой информации от подслушивания

Для защиты от подслушивания речевой информации в кабинете секретаря необходимо существенно повысить звукоизоляцию дверей как наиболее слабого звена в акустической защите и стены до 55 дБ на частоте

1000 Гц. Такая звукоизоляция обеспечивается двойной дверью с тамбуром шириной не менее 200 мм с уплотнителями по периметру дверных полотен.

Для предотвращения утечки информации через ограждения кабинета возможны три варианта:

- повышение поверхностной плотности ограждения;
- установление дополнительной перегородки;
- зашумление ограждения.

Так как звукоизоляция пропорциональна поверхностной плотности среды распространения акустической волны, то при недостаточной звукоизоляции утолщают стены.

Наиболее удобным строительным материалом для этого является кирпич, который укладывают на ширину половины или длины целого кирпича вплотную к стенке. Возможно также укрепление на стене строительных материалов (многослойной фанеры различной толщины, стеклопластика, пемзобетонных плит и др.) Утолщенная стена из красного кирпича обеспечивает повышение звукоизоляции с 48 дБ до 53 дБ. Кладка утолщенной стены с зазором между стенками 40 мм увеличивает звукоизоляцию еще приблизительно на 4-5 дБ. Утолщение стены целесообразно проводить со стороны кабинета секретаря, так как это позволит уменьшить выступ двойной двери с тамбуром в кабинет секретаря.

Звукоизоляция стен между кабинетом и коридором, кабинетом и смежным помещением повышается путем утолщения стен и крепления к ним дополнительных перегородок. Утолщение стен производится путем кирпичной кладки у стены кабинета. В качестве дополнительных перегородок используются асбестоцементные, гипсокартонные, древесностружечные, древесноволокнистые плиты толщиной 10-20 мм. Они крепятся к стене с помощью деревянных реек и брусков толщиной 40-50 мм по периметру и поверхности стены. По периметру между перегородкой и другими ограждениями необходимо установить упругие (из губчатой резины)

прокладки, между перегородкой разместить звукопоглощающий пористый материал.

В качестве меры, повышающей энергетическое скрытие речевой информации в кабинете, на стенах укрепить виброакустические излучатели акустических генераторов помех.

Для исключения утечки информации через батареи и трубы отопления перед батареями установить акселерометры или резонансные экраны в виде деревянных перегородок с отверстиями.

Для предотвращения утечки информации через вентиляционное отверстие пред ним укрепить экран и разместить в нем глушитель звука.

В качестве мер предотвращения подслушивания рекомендуем:

– установить двойные двери с уплотнительными прокладками и тамбуром глубиной 300 мм;

– увеличить толщину стены между кабинетом и приемной, а также соседними помещениями на кирпич;

– установить на батареи отопления акселерометры резонаторных экранов или излучатели генератора виброакустического зашумления;

– закрыть окна стальными ставнями и жалюзи, установить на стекла окон излучатели генератора виброакустического зашумления (для предотвращения лазерного подслушивания при закрытых окнах);

– установить перед воздухозаборниками воздухопроводов акустические экраны;

– применить устройство для подавления сигналов скрытно работающего диктофона.

Перечень программно-аппаратных средств защиты информации

Программно-аппаратные средства защиты информации осуществляется и заключается:

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

2.Обучить ответственного за обработку и защиту персональных данных в техникуме, обучить пользователей СКЗИ.

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

К основным средствам защиты персональных данных относится:

– Средство защиты информации от несанкционированного доступа.

– Антивирусное средство защиты.

– Межсетевой экран (защита от сетевых угроз).

– Средство шифрования информации (криптографические).

– Сетевые сканеры безопасности (контроль и анализ уязвимостей).

– Система обнаружения вторжений (обнаружение компьютерных атак).

Dallas Lock 8.0-. – средство защиты от НСД.

Возможности Dallas Lock:

- однофакторная или двухфакторная аутентификация пользователей;
- контроль каналов распространения конфиденциальной информации;
- позволяет выполнять очистку остаточной информации;
- позволяет разграничить права доступа администраторов и пользователей к локальным и сетевым ресурсам;
- позволяет разграничить доступ к сменным накопителям для предотвращения возможной утечки конфиденциальной информации.
- возможность администрирования рабочих мест удаленно;
- возможность работы с помощью сервера терминального доступа;
- разграничение прав по мандатному и дискреционному принципу;
- организация доверенной информационной среды;
- Способность создать замкнутую программную среду;
- имеет трехуровневую систему управления безопасностью (компьютер-домен безопасности-лес безопасности), что позволяет применять Dallas Lock в организации с большим количеством филиалов);
- контроль целостности ресурсов компьютера и программно-аппаратной конфигурации;

– отсутствие обязательной аппаратной части;

– при использовании Сервера безопасности, возможность централизованно управлять политиками безопасности;

– дает возможность проводить оперативный мониторинг и аудит действий пользователей.

Средства антивирусной защиты - Kaspersky Endpoint Security для бизнеса расширенный. «Kaspersky Endpoint Security для бизнеса расширенный» предоставляет высокоэффективные технологии и инструменты обеспечения IT-безопасности для построения системы многоуровневой защиты. Технологии сканирования сети на наличие уязвимостей и управления установкой исправлений устраняют уязвимости в операционных системах и приложениях, а технология шифрования данных обеспечивает защиту конфиденциальной информации в случае утери ноутбука или попытки несанкционированного доступа к данным. Kaspersky Endpoint Security (версии 8 и 10) является сертифицированным антивирусным средством защиты.

Межсетевой экран (МЭ) - программный комплекс ViPNet Client предназначен для защиты рабочих мест корпоративных пользователей. ViPNet Client надежно защищает от внешних и внутренних сетевых атак за счет фильтрации трафика. Кроме того, ПК ViPNet Client обеспечивает защищенную работу с корпоративными данными через зашифрованный канал, в том числе для удаленных пользователей.

Преимущества:

1. Высокая производительность шифрования и фильтрации трафика позволяет в реальном времени осуществлять защиту трафика служб голосовой и видеосвязи в сетях TCP/IP, а также обеспечивать одновременную работу с ресурсами разных сегментов корпоративной сети.

2. Равный доступ к ресурсам корпоративных информационных систем независимо от места и способа подключения пользователя к телекоммуникационной сети (при использовании решения ViPNet Network Security).

3. Защита канала не влияет на работу сторонних приложений на компьютере пользователя.

4. Ключи шифрования, политики безопасности и обновления ПО ViPNet доставляются на компьютер через надежный защищенный канал.

Средства криптографической защиты информации (СКЗИ) - ViPNet CSP 4.2 — российский криптопровайдер, сертифицированный ФСБ России как средство криптографической защиты информации (СКЗИ) и электронной подписи.

ViPNet CSP 4.2 позволяет:

– создание ключей ЭП, формирование и проверка ЭП по ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012;

– хэширование данных по ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012;

– шифрование и имитозащита данных по ГОСТ 28147-89.

Базовый вариант ViPNet CSP 4.2 (вариант исполнения 1) обеспечивает класс защищенности КС1.

Преимущества:

1. Поддержка работы с внешними устройствами (токенами) для создания и хранения ключей и сертификатов с использованием интерфейса PKCS#11. Данная функция облегчает интеграцию новых устройств с ViPNet CSP 4.

2. Возможность экспорта и импорта ключей в формате #PKCS12, что повышает совместимость форматов ключей с решениями других производителей.

3. Поддержка вызова криптографических функций CSP сторонними приложениями через API PKCS#11, Microsoft CryptoAPI и Microsoft CNG.

4. Выделенное множество функций API позволяет клиентским приложениям ограничивать объемы сертификационных испытаний только проведением оценки влияния (согласно требованиям ФСБ).

Hide Folders (инструмент для сокрытия конфиденциальной информации от посторонних, а также разделы жёсткого диска и папки).

Ввод в эксплуатацию системы технической защиты информации

На **третьем этапе** силами монтажных и строительных организаций осуществляется выполнение мероприятий по защите информации, предусмотренных техническим проектом. К работам по монтажу технических средств обработки информации, вспомогательных технических средств, а также проведения технических мероприятий по защите информации должны привлекаться организации, имеющие лицензию ФСТЭК РФ.

Монтажной организацией или заказчиком проводятся закупка сертифицированных ТСОИ и специальная проверка несертифицированных ТСОИ на предмет обнаружения возможно внедренных в них электронных устройств перехвата информации («закладок») и их специальные исследования.

По результатам специальных исследований ТСОИ уточняются мероприятия по защите информации. В случае необходимости вносятся соответствующие изменения в технический проект, которые согласовываются с проектной организацией и заказчиком.

Проводятся закупка сертифицированных технических, программных и программно-технических средств защиты информации и их установка в соответствии с техническим проектом.

Перед установкой в выделенные помещения и на объекты информатизации мебели и предметов интерьера технические устройства и средства оргтехники должны проверяться на отсутствие закладных устройств. Одновременно целесообразно провести проверку технических средств на уровни побочных электромагнитных излучений. Такую проверку целесообразно проводить в специально оборудованном помещении или на промежуточном складе.

После отделки рекомендуется провести всесторонний анализ здания на возможность утечки информации по акустическим и вибрационным каналам. По результатам измерений с учетом реальной ситуации по режиму охраны

должны быть разработаны дополнительные рекомендации по усилению мер защиты, если имеет место невыполнение требований по защите.

После установки и монтажа технических средств защиты информации проводится их опытная эксплуатация в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации.

По результатам опытной эксплуатации проводятся приемо-сдаточные испытания средств защиты информации с оформлением соответствующего акта.

По завершении ввода в эксплуатацию СТЗИ проводится аттестация объектов информатизации и выделенных помещений по требованиям безопасности. Она является процедурой официального подтверждения эффективности комплекса реализованных на объекте мер и средств защиты информации.

Аттестация защищаемого помещения

Аттестация объектов информатизации – это комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» – подтверждается, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации [16].

Объекты информатизации вне зависимости от используемых отечественных или зарубежных технических и программных средств аттестуются на соответствие требованиям государственных стандартов России или нормативных и методических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации в пределах его компетенции.

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей

государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по желанию заказчика или владельца объекта информатизации [16].

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации в целях оценки соответствия использованного комплекса мер и средств защиты информации требуемому уровню безопасности информации [16].

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с тем уровнем секретности (конфиденциальности) и на тот период времени, которые установлены в «Аттестате соответствия» [16].

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа к информации, обрабатываемой автоматизированными средствами (в том числе от компьютерных вирусов), и от утечки информации по техническим каналам.

При необходимости по решению директора колледжа организациями, имеющими соответствующие лицензии ФСБ России, могут быть проведены специальные проверки на наличие возможно внедренных в выделенные помещения или технические средства специальных электронных устройств перехвата информации («закладных устройств»).

Основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроль и надзор за аттестацией и эксплуатацией аттестуемых объектов информатизации устанавливает «Положение по аттестации объектов информации по требованиям

безопасности информации», утвержденное председателем Гостехкомиссии России 25 ноября 1994 г. [16].

Система аттестации объектов информации по требованиям безопасности информации является составной частью единой обязательной системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке [16].

Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации, которым является Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК РФ) в пределах ее компетенции, определяемой законодательными актами Российской Федерации.

3.2. Расчет экономической эффективности внедрения рекомендаций по противодействию утечки информаци в системах связи в ГБПОУ «Мишкинский профессионально-педагогический колледж»

Основой определения эффективности защиты объекта является сопоставление отношения доходов образовательной организации и расходов, потраченных на обеспечения информационной безопасности.

Экономический эффект – разность между результатами деятельности хозяйствующего субъекта и произведенными для их получения затратами на изменения условий деятельности.

Экономическая эффективность – это соотношение полезного результата и затрат факторов производственного процесса. Для количественного определения экономической эффективности используется показатель эффективности.

Эффективность определяется с помощью различных показателей, при этом сопоставляются данные, выражающие эффект (прибыль, объем

производства, экономия от снижения издержек) с затратами, обеспечивающими этот эффект (капитальные вложения, текущие издержки).

При решении экономических задач определяется результативность каждого предприятия и производится сопоставление различных результатов.

Различают два вида экономической эффективности:

- абсолютную (соотношение результатов экономической деятельности и затрат для достижения этих результатов);
- сравнительную (показывает изменение результатов экономической деятельности по отношению к уже достигнутым результатам).

Важное значение в расчете эффективности, в том числе и эффективности защиты информации является приведение расчетных величин к сопоставимым значениям, которое производится до расчетов. Приведение обеспечивает точность экономических расчетов и их обоснованность.

Расчеты производятся в одинаковых единицах измерения, за одинаковые отрезки времени, на одинаковое количество объектов расчета.

Экономическая эффективность проекта (Э) складывается из двух составляющих:

- косвенная эффективность;
- прямого эффекта, который характеризуется снижением трудовых, стоимостных показателей.

Расчет стоимости создания системы защиты конфиденциальной информации от утечки информаци в системах связи

Расчетное время проведения мероприятий согласно разработанным рекомендациям, составляет 6 недель, 1 исполнитель (120 чел./часов) и делится на следующие этапы:

- информационное обследование – 2 дня;
- проведение оценки угроз – 7 дней;
- разработка модели угроз – 5 дней;
- выработка мер и рекомендаций – 3 дня.

Смета на научно-техническую продукцию составляется по статьям затрат:

- затраты на основные материалы (материальные затраты);
- заработная плата исполнителя;
- отчисления на социальные нужды;
- накладные расходы;
- командировочные расходы (если предусмотрены);

Затраты на основные материалы

Затраты на основные материалы рассчитываются по следующей формуле:

$$З_м = \sum_{i=1}^{m} К_{mi} * Ц_{mi}, \quad (1)$$

где $З_М$ – затраты на основные материалы соответствующего вида, руб;

$К_{mi}$ –количество материалов, шт., кг;

$Ц_{mi}$ – цена за единицу основного материала, руб;

m– количество наименований.

Полученные данные представлены в таблице 7.

Таблица 7

Затраты на основные материалы

Наименование материала	**Расход материала**	**Цена, руб**	**Стоимость**
Стационарный шумогенератор ГШ-1000М	1	9300	9300
Защита от прослушивания телефонной линии SEL-17	1	15900	15900
Подавитель сотовой связи ЛГШ-701	1	20000	20000
Установка DALLASLOCK 8.0 – К - 4 500, 00 руб. (1 лицензия, 1 экз. на 1 рабочее место).	1	4500	4500

Установка СКЗИ программного комплекса ViPNet Client 4 (1 канал на 1 рабочее место) (7000 руб.)	1	7000	7000
Установка Kaspersky Endpoint Security для бизнеса расширенный - 900 руб. (покупается один раз на все компьютеры организации), продление каждый год для образовательной организации - в пределах 180 - 200 руб. на 1 год	1	1000	1000
Итого:			57 700

Основная заработная плата исполнителя

Расчет заработной платы исполнителя ведется по формуле:

$$З_{осн} = \sum_{i=1}^{n} Ч_i * Ф_i * С_i \quad (2)$$

,

Где $Ч_i$ – число исполнителей, чел.;

$Ф_i$ – фонд рабочего времени исполнителей, час;

$С_i$ – тарифная ставка, руб.;

n – общее число исполнителей.

В данной магистерской диссертации рассматривается работа одного исполнителя. Фонд рабочего времени исполнителя равен 120 чел./часов. Тарифная ставка составляет 250 руб/час.

Подставив данные в формулу получаем, затраты на основную заработную плату:

$$З_{осн} = 1 * 250 \text{ руб./час.} * 120 \text{ чел./часов} = 30000 \text{ руб.}$$

Дополнительная заработная плата исполнителя

Дополнительная заработная плата учитывает потери времени на отпуск и болезни. Данная выплата в среднем составляет 10% от основной заработной платы исполнителя.

$$З_{доп} = З_{осн} * 10\% = 30000 \text{ руб.} * 10\% = 3000 \text{ руб.}$$

Отчисления на социальные нужды

Отчисления на социальные нужды – это обязательные отчисления по нормам, установленным законодательством государственного социального страхования, в Фонд социального страхования РФ, Пенсионный фонд РФ, фонды обязательного медицинского страхования от затрат на оплату труда работников, включаемых в себестоимость продукции (работ, услуг), по элементу «Затраты на оплату труда» (кроме тех видов оплаты, на которые страховые взносы не начисляются).

Отчисления на социальные нужды производятся согласно Федеральному закону № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования».

Законом установлены следующие тарифы страховых взносов:

– Пенсионный фонд Российской Федерации - 22 %;

– Фонд социального страхования Российской Федерации - 2,9 %;

– Федеральный фонд обязательного медицинского страхования с 1 января 2019 года - 5,1 %;

– территориальные фонды обязательного медицинского страхования с 1 января 2019 года - 0,0 %.

Расчет данного значения ведется по следующей формуле:

$$З_{отч} = (З_{осн} + З_{доп}) * q / 100, \quad (3)$$

Где q– норматив отчислений на социальные нужды (30%).

$З_{отч}$ = (30000+3000) * 0,3 = 9900 руб.

Накладные расходы

Накладные расходы включают затраты на содержание помещения, отопление, электроэнергию, управленческие и хозяйственные расходы.

При укрупненных расчетах применяется формула:

$$З_н = З_{осн} * Q_н /100, \quad (4)$$

где $Q_н$– норматив накладных расходов. В среднем данный показатель равен 120%.

$З_н$ = (30000+3000) * 120 / 100 = 39600 руб.

Итоговая сумма затрат

Итоговая сумма затрат представлена в таблице 8.

Таблица 8

Итоговая сумма затрат

№ п/п	Статьи затрат	Сумма, руб.
1	Материалы	57700
2	Основная зарплата	30000
3	Дополнительная зарплата	3000
4	Отчисления на социальные нужды	9900
5	Накладные расходы	39600
Итого:		140200

Расчет потерь при реализации угрозы

По данным Info Watch Analitics и Ponemon Institute в среднем за год организации в России теряют до 80 миллионов рублей в связи с утечкой информации. Ежегодные исследования показывают, что инсайдерские угрозы стали сложной задачей для IT-специалистов.

Число инцидентов, связанных с мошенничеством остается очень большим. Тем не менее, только 44% организаций ставят первоочередной задачей предотвращение инсайдерского мошенничества.

Подсчитав данные можно увидеть, что средний ущерб составляет 3520000 рублей в результате инсайдерских атак. Будем считать, что

реализации угроза производится умышленно (процент умышленных реализаций угроз равен 45,1).

Также с июля 2017 года ужесточилось законодательство по работе с персональными данными. Штрафы:

– за обработку данных без согласия – штраф до 75 тыс. руб.;

– оператор персональных данных (например, работодатель или интернет-сайт) обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных – штраф до 30 тыс. руб.

Расчет экономического эффекта и эффективности

Экономический эффект $Э_{эф}$ определяется через полученную дополнительную прибыль, либо сокращение убытков.

$$Э'_{эф} = З_2 – З_1, \quad (5)$$

где $З_1$– затраты на проведение мероприятий согласно разработанным рекомендациям;

$З_2$– затраты на погашение ущерба нанесенного организации.

Рассмотрим частный случай взяв за параметр $З_1$ средние максимальные затраты, рассматриваемые в данной работе –140200 рублей (сумма затрат с использованием специализированного аппаратного решения), а за $З_2$ – среднюю сумму затрат на погашения ущерба.

$Э'_{эф}$= 3520000 –140200=3379800 руб.

Экономическая эффективность $Э_э$ представляет соотношение между прибылью и капиталовложением:

$$Э_э = Э_{эф} / З_1, \quad (6)$$

$Э_э$= 35059800 /140200= 24

Значение экономической эффективности $Э_э \geq 0,2$ ($Э_э$= 24), что подтверждает целесообразность и экономическую эффективность использования предложенных рекомендаций по противодействию утечки

информаци в системах связи образовательной организации (ГБПОУ «МППК»).

Выбор способа реализации мер зависит от следующих факторов:

- размер прибыли образовательной организации;
- величина информационной системы образовательной организации;
- используемые средства защиты информации для защиты ИС;
- объем информационных активов хранимых и обрабатываемых в информационной системе образовательной организации;
- размер возможных потерь от нанесенного организации ущерба от реализации угроз информационной безопасности.

Таким образом**,** представленные в данном параграфе вычисления подтверждают экономическую эффективность и целесообразность использования рекомендованных мер при внедрении их в процесс информационной безопасности образовательной организации. Предложенные рекомендации по противодействию утечки информаци в системах связи являются экономически оправданными.

Выводы по 3 главе

В третьей главе магистерской диссертации на основе анализа состояния защиты информации от утечки в системах связи в ГБПОУ «МППК» были предложены рекомендации по противодействию утечки информаци в системах связи колледжа.

Мероприятия по защите конфиденциальной информации от утечки по системам связи (далее - технической защите информации) являются составной частью деятельности образовательной организации и осуществляются во взаимосвязи с другими мерами по обеспечению их информационной безопасности.

Защита конфиденциальной информации от утечки по техническим каналам 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 (далее – объекта защиты).

При организации работ по защите утечки по техническим каналам информации на защищаемом объекте были выделены три этапа:

1. Первый этап (подготовительный, предпроектный).

2. Второй этап (проектирование СТЗИ).

3. Третий этап (этап ввода в эксплуатацию защищаемого объекта и системы технической защиты информации).

В качестве объекта защиты был выбран кабинет директора колледжа (ГБПОУ «Мишкинский профессионально-педагогический колледж).

Для ГБПОУ «МППК» были предложены следующие рекомендации по противодействию утечки информаци в системах связи:

I. Проведение специального обследования защищаемого объекта, разрабатывается аналитическое обоснование необходимости создания СТЗИ и техническое (частное техническое) задание на ее создание.

II. Моделирование угроз утечки информации

III. Меры предотвращения утечки информации

IV. Аттестация защищаемого помещения

Проведен расчет экономической эффективности внедрения рекомендаций по противодействию утечки информаци в системах связи в ГБПОУ «Мишкинский профессионально-педагогический колледж».

В результате вычисления подтверждают экономическую эффективность и целесообразность использования рекомендованных мер при внедрении их в процесс информационной безопасности образовательной организации. Предложенные рекомендации по противодействию утечки информаци в системах связи являются экономически оправданными.

ЗАКЛЮЧЕНИЕ

В магистерской диссертации предложены рекомендации по противодействию утечки информаци в системах связи ГБПОУ «Мишкинский профессионально-педагогический колледж».

В качестве основных результатов диссертационной работы можно выделить следующие:

1. Описаны системы связи в образовательной организации, информационные ресурсы образовательной организации, подлежащие защите от утечки по каналам связи. В зависимости от технологии и функций, системы связи разделяются на следующие разновидности: системы телефонной связи; системы радиосвязи; системы оперативной диспетчерской связи**;** системы оповещения; системы радиотрансляции; системы обеспечения связи конференций**; т**ехнологические сети связи; локальная вычислительная сеть. К защищаемым данным в образовательной организации относятся данные, являющиеся предметом собственности и подлежащие защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Это, как правило, информация ограниченного доступа, содержащая сведения конфиденциального характера.

2. Выявлены меры противодействия утечки информации в системах связи. Существуют определенные принципы, на которых должна основываться комплексная система мер по защите конфиденциальной информации от утечек: непрерывность работы системы в пространстве и времени; многозональность защиты; расстановка приоритетов; интеграция; дублирование. Также для комплексной защиты информации от утечки в системах связи необходимы следующие методы защиты: административно-организационные меры; разработка документации; работа с персоналом; планировочные и технические решения; технические средства и системы предотвращения утечек.

3. Система обеспечения информационной безопасности в колледже существует, но имеет уязвимости.

4. Анализ состояния защиты информации от утечки в системах связи в колледже позволил выявить необходимость разработки рекомендации по противодействию утечки информаци в системах связи колледжа.

5. Разработаны рекомендации по противодействию утечки информаци в системах связи ГБПОУ «Мишкинкий профессионально-педагогический колледж». В качестве объекта защиты был выбран кабинет директора колледжа.

6. Проведен расчет экономической эффективности внедрения рекомендаций по противодействию утечки информаци в системах связи в ГБПОУ «Мишкинский профессионально-педагогический колледж». В результате вычисления подтверждают экономическую эффективность и целесообразность использования рекомендованных мер при внедрении их в процесс информационной безопасности образовательной организации. Предложенные рекомендации по противодействию утечки информаци в системах связи являются экономически оправданными.

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

Список использованной литературы

1. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. – М.: Гротек, 1997, с. 248.

2. Абалмазов Э.И. Новая технология защиты телефонных разговоров [Электронный ресурс]. - URL: http://ess.ru. Дата обращения: 24.01.2019.

3. Ажмухамедов, И.М., Ханжина, Т.Б. Оценка экономической эффективности мер по обеспечению информационной безопасности [Текст] / И.М. Ажмухамедов, Т.Б. Ханжина // Вестник АГТУ. Серия: «Экономика» №1/2011, С.185-190.

4. Аппаратура защиты информации от утечки по ПЭМИН. - URL: https://npo-echelon.ru/production/79/. Дата обращения: 20.01.2019.

5. Ворона В.А., Костенко В.О. Способы и средства защиты информации от утечки по техническим каналам // Computational nanotechnology. 2016. №3. URL: https://cyberleninka.ru/article/n/sposoby-i-sredstva-zaschity-informatsii-ot-utechki-po-tehnicheskim-kanalam. Дата обращения: 23.01.2019.

6. Ворона В.А., Костенко В.О. Способы и средства получения акустической речевой информации. -М.: Вестник ВНИИНМАШ – Техническое регулирование и стандартизация, № 1 (14), с. 130-151. 2013.

7. Ворона В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. Учебное пособие. – М.: Горячая линия-Телеком. Серия «Обеспечение безопасности объектов», книга 1. 2012. с. 196.

8. Гавриш В.Ф. Практическое пособие по защите коммерческой тайны. – Симферополь: Таврида, 1994, с. 112.

9. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. (Принят и введен в действие Постановлением Госстандарта России от 12 мая 1999 г. № 160).

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

11. Завгородний, В.И. Комплексная защита информации в компьютерных системах [Текст] / В.И. Завгородний. - М.: «Логос», 2001.

12. Заикин А. Защита от утечки конфиденциальной информации. Особенности внедрения решений защиты от утечки / А. Заикин. - URL: https://www.croc.ru/upload/iblock/d00/d00cd776e7f514eead7ec506a7c4fd89.pdf. Дата обращения: 15.01.2019.

13. Защита информации от утечки. Средства защиты от утечки конфиденциальной информации. – URL: http://rus.safensoft.com/security.phtml?c=768. Дата обращения: 15.01.2019.

14. Защита информации. Техническая защита конфиденциальной информации [Электронный ресурс]. URL: http://ab-solut.net/ru/articles/tex_zashita/.

15. Защита от утечки информации DLP. - URL: https://www.open-vision.ru/solutions/information-security/data-loss-privention/. Дата обращения: 15.01.2019.

16. Защита от утечки информации. - URL: http://korpusa-trekom.ru/zaschita-ot-ytechki-informacii.html. Дата обращения: 15.01.2019.

17. Защита помещений от утечки речевой конфиденциальной информации. - URL: https://www.cibit.ru/zashhita-pomeshhenij/. Дата обращения: 20.01.2019.

18. Козиков А.Ю., Зауголков И.А. Анализ угроз утечки информации по телефонному каналу связи из защищаемого помещения / А.Ю. Козиков, И.А. Зауголков // Гаудеамус. 2012. №20. URL: https://cyberleninka.ru/article/n/analiz-ugroz-utechki-informatsii-po-telefonnomu-kanalu-svyazi-iz-zaschischaemogo-pomescheniya. Дата обращения: 24.01.2019.

19. Комарович В.Ф., Железняк В.К., Безопасность информации в телекоммуникационных системах: сб. статей / под ред. засл. деят. науки и техники РФ, проф. В. Ф. Комаровича. СПб.: ВУС. 2011. С. 15–19.

20. Максимов Ю.Н. Технические методы и средства защиты информации / Ю.Н. Максимов, В.Г. Сонников, В.Г. Петров и др. – Санкт-Петербург: ООО «Издательство Полигон», 2000, с. 320.

21. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 14.02.2008) Электронный документ. Режим доступа: http://fstec.ru/

22. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: [Утверждены руководством 8 центра ФСБ России 21.02.2008 г. №149/54-144]. - Режим доступа: www.consultant.ru. Дата обращения: 15.01.2019.

23. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. N 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 13 декабря 2013 г.).

24. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утв. ФСБ России 31.03.2015 N 149/7/2/6-432). Электронный документ. Режим доступа: http://docs.cntd.ru/document/420336137. Дата обращения: 16.01.2018.

25. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014). Электронный документ. Режим доступа: http://fstec.ru/.

26. Методы организации защиты информации [Текст]: 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 ВО «ТГТУ», 2013. – 80 с. – 100 экз. – ISBN 978-5-8265-1235-7/

27. О безопасности [Электронный ресурс]: [федеральный закон: от 05.03.1992 г. № 2446-I, в ред. от 25.12.1992 г. № 4235-I, от 24.12.1993 г. №2288, от 25.07.2002 г. № 116-ФЗ, от 07.03.2005 г. № 15-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 18.04.2017.

28. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 18.04.2017.

29. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. №149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 18.04.2017.

30. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [п. 2 Постановления Правительства Российской Федерации: от 17.11.2007 г. № 781, в ред. От 01.11.2012 г. № 1119]. - Режим доступа: www.consultant.ru. Дата обращения: 14.04.2017.

31. Основные меры защиты информации от утечки по техническим каналам. Организационные меры защиты: временные ограничения, территориальные ограничения. - URL: https://www.intuit.ru/studies/courses/3649/891/lecture/32347. Дата обращения: 20.01.2019.

32. Петраков А.В. Основы практической защиты информации. Учебное пособие / А.В. Петраков. - Солон-Пресс, 2012.

33. Планирование затрат на информационную безопасность [Электронный ресурс]. - Режим доступа: www.anti-malware.ru. Дата обращения: 12.02.2019.

34. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

35. Постановление Правительства РФ от 03.02.2012 N 79 (с изм. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации». [Электронный ресурс]. Режим доступа: http://www.garant.ru/.

36. Постановление Правительства РФ от 03.03.2012 N 171 (с изм. от 15.06.2016) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации». [Электронный ресурс]. Режим доступа: http://www.garant.ru/.

37. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 г. Москва «Об утверждении Порядка проведения классификации информационных систем персональных данных» // «Российская газета», № 4637, 12.04.2008.

38. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн при использовании средств криптографической защиты информации» // «Российская газета» от 17 сентября 2014 г. N 211

39. Противодействие экономическому шпионажу: сборник публикаций журнала «Защита информации. Конфидент» 1994 – 2000. – Санкт-Петербург: Конфидент, 2000, с. 344.

40. Рекомендации по предотвращению утечки информации. – URL: http://www.delphiplus.org/inzhenerno-tekhnicheskaya-zashchita-

informatsii/rekomendatsii-po-predotvrashcheniyu-utechki-informatsii.html. Дата обращения: 18.01.2019.

41. Система обеспечения информационной безопасности. – URL: http://www.ec-leasing.ru/products/sistemy-obespechiniya-informacionnoi-bezopasnosti/.

42. СИСТЕМЫ СВЯЗИ. - URL: http://www.smis-expert.com/pages/sistemy-svyazi.html. Дата обращения: 25.11.2018.

43. Современные технологии защиты от утечки конфиденциальной информации. - URL: https://dialognauka.ru/press-center/article/4761/. Дата обращения: 15.01.2019.

44. Стандарты информационной безопасности. – URL: https://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html.

45. Степанов, Е. А. Информационная безопасность и защита информации [Текст]: учеб. пособие / Е. А. Степанов, И. К. Корнеев. – М.: ИНФРА – М, 2013. – 304 с.

46. Структура системы защиты информации от угроз нарушения целостности [Электронный ресурс]. - URL: www.shadanis.narod.ru. Дата обращения: 15.11.2018.

47. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники. - URL: https://alterozoom.com/documents/12626.html. Дата обращения: 10.12.2018.

48. 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.

49. Торокин А.А. Инженерно-техническая защита информации: Учеб. пособие для студентов, обучающихся по специальностям в обл. информ. Безопасности / А.А. Торокин. – М.: Гелиос АРВ, 2012, с. 960.

50. Утечка информации на современном предприятии и обеспечение информационной безопасности. Анализ состояния защиты информации. - URL: http://razgovorodele.ru/security1/safety06/analytical_work01.php. Дата обращения: 20.01.2019.

51. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. - URL: http://www.analitika.info/kanalutechki.php. Дата обращения: 10.12.2018.

52. Хорев А.А. Организация защиты информации от утечки по техническим каналам / А.А. Хорев. – URL: http://www.bnti.ru/showart.asp?aid=751&lvl=04.03. Дата обращения: 20.01.2019.

53. Хорев А.А. Способы и средства защиты информации: Учеб. Пособие / А.А. Хорев. – М.: МО РФ, 2000, с. 316.

54. Хорев А.А., Железняк В.К., Макаров Ю.К. Оценка эффективности методов защиты речевой информации. Общесистемные вопросы защиты информации: монография / под ред. Е. М. Сухарева, М.: Радиотехника, 2003. Кн.1. 296 с.

55. Хореев А.А. Техническая защита информации. Том 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008.

Приложения

ПРИЛОЖЕНИЕ 1

Стационарный шумогенератор ГШ-1000М

Используется для обеспечения защиты конфиденциальной информации от утечки и негласного съема за счет ПЭМИН (0,1…1000 МГц), для маскирования побочных электромагнитных излучений и наводок работающих ПЭВМ.

Имеет сертификат Гостехкомиссии РФ и сертификат соответствия медицинским нормам.

Обеспечивает перекрытие диапазона частот 0,1…1000 МГц. Имеется возможность световой индикации режимов. Создает уровни излучаемой мощности шума на расстоянии 1 метра от шумогенератора не менее: 60 дБ (0,1-100 МГц); 70 дБ (100-300 МГц); 45 дБ (300-500 МГц); 25 дБ (500-1000 МГц). Питание осуществляется от электросети 220 В. Габаритные размеры 700х600х35 мм.

Цена: 9300 руб.

ПРИЛОЖЕНИЕ 2

Защита от прослушивания телефонной линии SEL-17

- Диапазон ВЧ-помехи при поднятой трубке:

6-10 кГц;

- Уровень ВЧ-помехи на линии 600 Ом:

не менее 15 дБ/м;

- Регулировка уровня ВЧ-помехи: 0-9 дБ;
- Диапазон НЧ-помехи при положенной

трубке: 0,3-3 кГц;

- Уровень НЧ-помехи на линии 600 Ом:

не менее 20 дБ/м;

- Контроль напряжения линии в диапазоне: 0-100 В;
- Погрешность измерения напряжения линии: не более 0,3%;
- Пороговое отклонение напряжения линии (при замкнутом шлейфе): 0,8В;
- Пороговое отклонение напряжения линии (при разомкнутом шлейфе): 2В;
- Питание: 220В (от сети переменного тока), 12В (от ИПТ);
- Размеры: 152х104х34 мм.
- Цена: 15900 руб.

ПРИЛОЖЕНИЕ 3

Подавитель сотовой связи ЛГШ-701

- Диапазон рабочих частот:
  - стандарт IMT-MC-450 (NMT-450i), стандарт CDMA2000 1x – не менее 462,5...467,475МГц;
  - стандарт GSM900 – не менее 935...960МГц;
  - стандарт DSC/GSM1800 (DECT1800) – не менее 1805...1900МГц;
- Максимальная выходная мощность на антенном разъеме:
  - стандарт IMT-MC-450 (NMT-450i), стандарт CDMA2000 1x – 33dBm (2W);
  - стандарт GSM900 – 33dBm (2W);
  - стандарт DSC/GSM1800 (DECT1800) – 30dBm (2W);
- Диапазон регулировки выходной мощности на антенном разъеме – не менее 13 dB (20 раз) по каждому выходу, плавно и независимо;
- Эффективный радиус подавления – 3...50м;
- Коэффициент усиления входящих в комплект поставки антенных устройств – около 0dBi с круговой диаграммой направленности;
- Питание – однофазная сеть переменного тока с напряжением от 85 до 264V частотой 47...63Hz;
- Мощность, потребляемая от сети 220V 50Hz – не более 20W;
- Габаритные размеры (без антенн) – 256x128x36мм;
- Цена: 20000 руб.

Диапазон регулировки выходной мощности на антенном разъеме – не менее 13 dB (20 раз) по каждому выходу, плавно и независимо.