

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

Организация режима защиты конфиденциальной информации в
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,
Пичуров Николай Александрович
Научный руководитель:
к.т.н., доцент
кафедры АТ, ИТ и МОТД
Руднев Валерий Валентинович

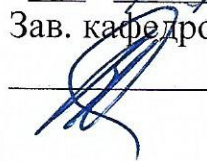
Проверка на объём заимствований:

68.06 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 Пичурову Николаю Александровичу, обучающемуся по программе магистратуры «Управление информационной безопасностью в профессиональном образовании».

Научный руководитель выпускной квалификационной работы: Руднев В.В., к.т.н., доцент кафедры АТ, ИТ и МОТД.

1. Тема квалификационной работы: «Организация режима защиты конфиденциальной информации в 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 «ЮУрГТК», 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 защиты конфиденциальной информации в образовательной организации Выводы по главе 1	16.10.2017
3	Глава 2. Анализ информационной безопасности в организации профессионального образования Выводы по главе 2	23.04.2018
4	Глава 3. Меры совершенствования защиты конфиденциальной информации в организации профессионального образования 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 MicrosoftPowerPoint, 10-12 слайдов, раскрывающих содержание магистерской диссертации, либо схемы, таблицы, графики, диаграммы в виде раздаточного материала	28.01.2019
	ПРЕДВАРИТЕЛЬНАЯ ЗАЩИТА	28.01.2019
	СДАЧА МАГИСТЕРСКОЙ ДИССЕРТАЦИИ НА КАФЕДРУ	18.02.2019

Дата выдачи задания

«27» апреля 2017 года

Заведующий кафедрой АТ, ИТ и МОТД

Наименование кафедры

Ф.И.О., ученое звание и степень

Подпись заведующего кафедрой

Задание выдал:

Ф.И.О., ученое звание и степень

Подпись научного руководителя

Задание принял

Ф.И.О магистранта

Подпись магистранта

Аннотация
на магистерскую диссертацию
Пичурова Николая Александровича

Тема магистерской диссертации «Организация режима защиты конфиденциальной информации в образовательной организации СПО».

Магистерская диссертация содержит 93 страницы, 8 рисунков, 11 таблиц, 70 источников литературы.

Ключевые слова: защита информации, конфиденциальная информация, режим защиты конфиденциальной информации.

Объектом исследования является организация защиты конфиденциальной информации в образовательной организации.

Цель магистерской диссертации – разработка рекомендации по совершенствованию защиты конфиденциальной информации с учетом комплексной оценки уровня защищенности и требований нормативно-правовой базы Российской Федерации.

В процессе исследования изучены теоретические основы защиты конфиденциальной информации, нормативно-правовое обеспечение защиты конфиденциальной информации и организация защиты информации в образовательных организациях СПО.

В результате проведенного исследования проведена оценка существующих и планируемых средств защиты конфиденциальной информации и разработаны рекомендации по совершенствованию защиты конфиденциальной информации в ГБПОУ «Южно-Уральский государственный технический колледж».

Магистрант Пичуров Николай Александрович
(Ф.И.О.)

Подпись

Оглавление

ВВЕДЕНИЕ	6
ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ.....	11
1.1. Конфиденциальная информация и значение ее защиты в образовательной организации	11
1.2. Нормативно-правовое обеспечение защиты конфиденциальной информации	16
1.3. Организация защиты конфиденциальной информации в образовательной организации	22
Выводы по Главе I.....	27
ГЛАВА 2. АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ.....	29
2.1 Общие сведения об организации профессионального образования.....	29
2.2. Конфиденциальная информация организации профессионального образования - компонент информационных ресурсов	34
2.3. Оценка существующих средств защиты конфиденциальной информации в ГБПОУ «Южно-Уральский государственный технический колледж»	37
Выводы по главе II	47
ГЛАВА 3. МЕРЫ СОВЕРШЕНСТВОВАНИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ГБПОУ «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ».....	48
3.1. Рекомендации по совершенствованию защиты конфиденциальной информации	48
3.2. Расчет экономической эффективности мероприятий по защите конфиденциальной информации	74
Выводы по Главе III	79
Заключение	81
Список использованной литературы.....	85

ВВЕДЕНИЕ

Актуальность исследования. В современных условиях развития информационных технологий и их глубокой интеграции в жизнь людей особую актуальность приобретает защита конфиденциальной информации. Проектирование и внедрение систем защиты информации на объекте является достаточно ресурсозатратной процедурой. К тому же, в нормативно-правовых документах по созданию систем защиты указывается только необходимость наличия определенных средств защиты, но не предусматривается динамическое состояние угроз. Дополнительно усложняет задачу отсутствие хорошо зарекомендовавших себя критериев оценки эффективности систем защиты информации.

Система защиты информации в общем случае включает в себя правовой, организационный и технический компоненты. Правовой компонент определяется нормативно-правовыми актами, государственными стандартами и требованиями государственных органов контроля в сфере информационной безопасности. В случае наличия в организации информации подлежащей защите, все действия с такой информацией должны совершаться в соответствии с установленными государством требованиями. Организационный компонент определяется наличием и соблюдением требований, определяемых организационно-распорядительными документами в сфере защиты конфиденциальной информации. Это направление особенно распространено на территории Российской Федерации. Однако, в силу перенасыщения рынка технических средств защиты по функционалу, задача выбора конкретных технических средств защиты и оценка эффективности их функционирования приобретает особую сложность

Данная магистерская диссертационная работа посвящена разработке системы защиты конфиденциальной информации в организациях профессионального образования. Одной из наиболее важных проблем при построении системы защиты информации является проблема оценки уровня

защищенности объекта и эффективности функционирования системы защиты информации.

Проблемы моделирования и проектирования СЗИ в частности были рассмотрены в трудах Гарсия Оз, В.И. Аверченкова, С.М. Климова, В.А. Герасименко, М.Ю. Рытова, С.С. Корта, А.Г. Корченко, А.А. Горокина, В.И. Ярочкина, В.В. Доморева и др.

Методы моделирования и автоматизации сложных организационно-технических систем рассматривались в трудах И.П. Норенкова, А.А. Рындина, В.П. Спицендаля и др.

Анализ этих работ показывает ограниченные возможности при одновременности реализации атак злоумышленников и своевременной реакции средств защиты на них. При этом целесообразно оценивать эффективность системы защиты информации в динамике протекающих процессов.

При оценивании качества функционирования систем защиты информации, в связи с особенностью свойств рассматриваемых объектов, возникает необходимость в создании адаптивных алгоритмов оценивания и реагирования на атаки с возможностью своевременного наращивания потенциала защищенности. Необходимо также учитывать, что в Российской Федерации определены федеральные законы, постановления Правительства РФ, государственные стандарты, а также ведомственные указания в области защиты конфиденциальной информации, которые указывают на необходимость применения средств защиты, но не предусматривают динамическое состояние объекта.

Это определяет актуальность создания системы защиты информации на объекте, ориентированной на угрозы безопасности, представленные в документах ФСТЭК и ФСБ России.

Целью исследования является разработка рекомендации по совершенствованию защиты конфиденциальной информации с учетом

комплексной оценки уровня защищенности и требований нормативно-правовой базы Российской Федерации.

Объектом исследования является организация защиты конфиденциальной информации в образовательной организации.

Предметом исследования является защита конфиденциальной информации.

Гипотеза исследования состоит в предположении о том, что повышение эффективности защиты конфиденциальной информации возможно на основе оценки уязвимостей существующих средств защиты и обеспечения их оптимального обновления с учетом максимального соответствия техническим требованиям и минимальных финансовых затрат.

Для достижения поставленной цели были сформулированы следующие **задачи**:

- изучить понятие «конфиденциальная информация» и значение ее защиты в образовательной организации;
- провести оценку существующих средств защиты конфиденциальной информации в колледже;
- разработать рекомендации по совершенствованию защиты конфиденциальной информации в колледже;
- провести расчет экономической эффективности мероприятий по защите конфиденциальной информации в ГБПОУ «ЮУрГТК».

Методы исследования. При выполнении теоретических исследований и реализации поставленной цели использовались теория и методология защиты информации, анализ публикационного массива по теме, описание, наблюдение, изучение законодательных актов и нормативно-методических документов, регламентирующих организацию защиты конфиденциальных данных.

Использование законодательных актов и нормативно-методических документов было продиктовано темой исследования.

Основополагающие нормы, регулирующие отношения по поводу

персональных данных, содержатся в Федеральном законе «О персональных данных» [6].

Федеральный закон «Об информации, информационных технологиях и защите информации» [5] определяет, процессы функционирования информации и документации в обществе, в системе государственного и хозяйственного управления. Настоящий закон регулирует отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

В качестве методического материала по защите персональных данных, использованы научные, учебные, практические материалы, подготовленные ведущими специалистами: Т. В. Кузнецовой [30], В.И. Петренко [42], О. В. Силакова [45]; регламентация работы с персональными данными – С. А. Борисова [25], М.А. Федосова [46] и др.

Научная новизна: проведение оценки средств защиты конфиденциальной информации в образовательной организации СПО и разработка рекомендаций по совершенствованию защиты конфиденциальной информации в образовательной организации.

Практическая значимость работы заключается в разработке рекомендаций по совершенствованию системы информационной безопасности ГБПОУ «ЮУрГТК», разработанной на основе анализа частной модели угроз названной организации, которое может быть применено в других образовательных организациях СПО.

База исследования: Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж».

Апробация исследования: результаты исследования были опубликованы на Международной научно-практической конференции «Инновации в информационных технологиях, машиностроении и автотранспорте», г. Кемерово, 2017; на XV Всероссийской научно-практической конференции «Актуальные вопросы развития России в исследованиях студентов: управленческий, правовой и социально-экономический аспекты», г. Челябинск, 2017.

Структура магистерской диссертации состоит из введения, трех глав, заключения, библиографического списка, состоящего из 70 наименований, приложения. Работа содержит 8 рисунков, 11 таблиц. Общий объем работы составляет 93 страницы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1. Конфиденциальная информация и значение ее защиты в образовательной организации

Конфиденциальная информация — любые сведения, составляющие служебную, коммерческую тайну, включая персональные данные сотрудников и студентов. Владелец конфиденциальной информации — лицо, которое владеет информацией, составляющей конфиденциальную информацию, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальной информации [1]. Владелец информации, составляющей конфиденциальную информацию, является образовательная организация.

Организация режима защиты конфиденциальной информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации любой организации, в частности образовательной.

Роль и место организации режима защиты информации в общей системе мер, направленных на защиту конфиденциальной информации образовательной организации, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учётом имеющихся в его распоряжении сил, средств, методов и способов защиты информации и на основе действующего нормативно-методического аппарата.

Среди основных направлений режима защиты информации выделяют организационную, правовую и инженерно-техническую защиту информации. Однако организационной защите информации среди этих направлений отводится особое место.

Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-

технические и инженерно-геологические) реализовать на практике спланированные руководством образовательной организации меры по защите конфиденциальной информации. Эти меры принимаются в зависимости от конкретной обстановки в образовательной организации, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к её утечке.

Под угрозой безопасности информации понимается потенциальная возможность нарушения основных качественных характеристик (свойств) информации при её обработке техническими средствами: конфиденциальности, целостности, доступности. Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями [3].

Таковыми действиями являются: ознакомление с конфиденциальной информацией различными путями и способами без нарушения её целостности; модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений; разрушение (уничтожение) информации как акт вандализма в целях прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению её конфиденциальности, полноты, достоверности и доступности, что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации. Каждая угроза влечёт за собой определённый ущерб – моральный или материальный, а защита и противодействие угрозе призвано снизить его величину, в идеале – полностью, реально – значительно или хотя бы частично. Но и это удаётся далеко не всегда [2].

Для организации режима защиты конфиденциальной информации в образовательной организации используются следующие методы.

Препятствие. Метод представляет собой использование физической силы с целью защиты информации от преступных действий злоумышленников с помощью запрета на доступ к информационным носителям и аппаратуре.

Управление доступом. Метод, который основан на использовании регулирующих ресурсов автоматизированной системы, предотвращающих доступ к информационным носителям. Управление доступом осуществляется с помощью таких функций, как идентификация личности пользователя, работающего персонала и систем информационных ресурсов такими мерами, как присвоение каждому пользователю и объекту личного идентификатора; аутентификация, которая устанавливает принадлежность субъекта или объекта к заявленному им идентификатору; проверка соответствия полномочий, которая заключается в установлении точного времени суток, дня недели и ресурсов для проведения запланированных регламентом процедур; доступ для проведения работ установленных регламентом и создание необходимых условий для их проведения; реагирование на попытку несанкционированных действий в виде шумовой сигнализации, отключения, отказа в запросе и в задержке работ [1].

Маскировка. Метод криптографического закрытия, защищающий доступ к информации в автоматизированной системе.

Регламентация – метод информационной защиты, при котором доступ к хранению и передаче данных при несанкционированном запросе сводится к минимуму.

Принуждение – это метод, который вынуждает пользователей при доступе к закрытой информации соблюдать определенные правила. Нарушение установленного протокола приводит к штрафным санкциям, административной и уголовной ответственности.

Побуждение. Метод, который основан на этических и моральных нормах, накладывающих запрет на использование запрещенной информации, и побуждает соблюдать установленные правила.

Все перечисленные методы защиты направлены на обеспечение максимальной безопасности всей информационной системы образовательной организации и осуществляются с помощью разных защитных механизмов, создание которых основано на таких средствах, как:

1. *Физические средства защиты* используются в качестве внешней охраны для наблюдения за территорией объекта и защиты автоматизированной информационной системы в виде специальных устройств.

2. *Аппаратные средства защиты* – это все виды электронных и электромеханических устройств, встроенных в блоки информационной автоматизированной системы, которые представлены как самостоятельные устройства, соединенные с этими блоками.

Обеспечение режима защиты конфиденциальной информации с помощью аппаратных средств включает:

- обеспечение запрета неавторизованного доступа удаленных пользователей и АИС (автоматизированная информационная система);
- обеспечение надежной защиты файловых систем архивов и баз данных при отключениях или некорректной работе АИС;
- обеспечение защиты программ и приложений.

Вышеперечисленные задачи обеспечения организации режима защиты конфиденциальной информации обеспечивают аппаратные средства и технологии контроля доступа (идентификация, регистрация, определение полномочий пользователя).

3. *Программные средства защиты* входят в состав программного обеспечения или являются элементами аппаратных систем защиты. Такие средства осуществляют режим защиты конфиденциальной информации путем реализации логических и интеллектуальных защитных функций и относятся к наиболее популярным инструментам защиты. Это объясняется их доступной ценой, универсальностью, простотой внедрения и возможностью доработки под конкретную организацию или отдельного пользователя. В то

же время, обеспечение режима защиты конфиденциальной информации с помощью программного обеспечения является наиболее уязвимым местом автоматизированной информационной системы образовательной организаций [3].

Большинство современных операционных систем содержат программные решения для обеспечения блокировки повторного доступа к информации. При отсутствии таких средств могут использоваться различные коммерческие программные обеспечения.

Для режима защиты особо важной информации используется метод хранения данных с использованием системы сигнатур. В качестве сигнатуры может применяться система, включающая сочетание защитного байта с его размером, временем изменения и именем. При любом обращении к этому файлу система анализирует сочетание информации с оригиналом. Необходимо уточнить, что надежное обеспечение безопасности информации возможно только при использовании шифрования данных.

Таким образом, организация защиты конфиденциальной информации представляет в настоящее время одно из ведущих направлений обеспечения безопасности государства, общества и отдельной личности. Проблемы различных аспектов безопасности становятся всё более актуальными с дальнейшим развитием информационно-коммуникационных технологий. Динамика развития законодательства в области информационной безопасности предполагает постоянное изменение методов и форм обеспечения режима защиты конфиденциальной информации, в том числе непрерывно развиваются и методы организации защиты информации в соответствии с вновь принимаемыми законами РФ, указами президента РФ, постановлениями правительства РФ.

1.2. Нормативно-правовое обеспечение защиты конфиденциальной информации

Обеспечение защиты конфиденциальной информации складывается из следующих составляющих:

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

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

- Акты федерального законодательства;
- Международные договоры РФ;
- Конституция РФ;
- Законы федерального уровня (включая федеральные конституционные законы, кодексы);
- Указы Президента РФ;
- Постановления правительства РФ;
- Нормативные правовые акты федеральных министерств и ведомств;
- Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Основные направления правового регулирования информационных отношений - конституционное и гражданско-правовое. Как продолжение свободы мысли и слова, которая закреплена в ч. 1 ст. 29 Конституции РФ, ч. 4 ст. 29 Конституции РФ закрепляет право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется соответствующим федеральным законом. Этому праву корреспондирует общая обязанность органов государственной власти и местного самоуправления, располагающих такого рода информацией, предоставлять ее по соответствующим запросам. Возможные исключения из этого общего правила должны обязательно иметь форму федерального закона

(ч. 3 ст. 55 Конституции РФ). Ст. 42 Конституции РФ говорит о праве каждого на достоверную информацию о состоянии окружающей среды. Ст. 19 Основ законодательства РФ «Об основах охраны здоровья граждан Российской Федерации» конкретизирует это установление закреплением определенного механизма реализации прав граждан на информацию о факторах, влияющих на их здоровье (п.5 пп.7 ст. 19).

Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности» (ред. от 26.06.2008) - данный закон призван защитить интересы личности, общества и государства от возможных внешних и внутренних угроз, посягающих на права, свободу, материальные и духовные интересы. Информационная безопасность - есть защита любой информации, и, в первую очередь, конфиденциальной.

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

Качество современного уровня правового регулирования отношений по поводу информации во многом определяется степенью учета законодателем этих признаков (свойств).

Конфиденциальная информация определена в п. 7 ст. 2 Федерального закона от 27 июля 2006 года № 149-ФЗ через требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Под конфиденциальной информацией будем понимать легально полученную информацию, которая в силу закона или иного акта, имеющего юридическое значение, доступна строго определенному кругу лиц, и в отношении которой установлен режим той или иной степени секретности.

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

- 1) на информацию, свободно распространяемую, например, посредством средств массовой информации;
- 2) на информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 3) на информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- 4) на информацию, распространение которой в Российской Федерации ограничивается или запрещается. Например, информация, составляющая коммерческую или государственную тайну.

В п. 2 этой статьи приводится разделение информации в зависимости от категории доступа к ней. По этому основанию информация может быть общедоступной; ограниченного доступа.

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

ФСТЭК предлагает выделять персональные данные из информационных систем, содержащих информацию ограниченного доступа и защищаемых в режиме тайны, что во многих случаях не реализуемо. Выделение персональных данных из общего массива охраняемой

информации создает для оператора проблему соотношения требований по технической защите информации, а также проблему соотношения прав и обязанностей субъектов в отношении защищаемой информации.

В контексте рассматриваемого вопроса нельзя обойти Федеральный закон «О коммерческой тайне» № 98-ФЗ, принятый 29 июля 2004 года и приведенный в соответствие с частью четвертой ГК РФ.

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

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

Федеральные законы от 06 апреля 2011 г. № 63-ФЗ (ред. от 01.07.2011 г.) «Об электронной подписи» и от 10 января 2002 г. № 1-ФЗ (ред. от 08.11.2007 г.) «Об электронной цифровой подписи» - данные законы призваны обеспечить конфиденциальность информации в электронном виде - подписи, которая рассматривается как личная подпись субъекта.

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

Указ Президента РФ от 12 мая 2004 г. № 611 (ред. от 03.03.2006 г.) «О мерах по обеспечению информационной безопасности Российской

Федерации в сфере международного информационного обмена» - указ регламентирует меры обеспечения информационной безопасности Российской Федерации при осуществлении международного информационного обмена посредством информационных систем, сетей и сетей связи, включая международную ассоциацию сетей «Интернет». Особое внимание уделяется обеспечению безопасности «закрытой» информации.

Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (в ред. от 9 июля 1997 г.) установил, что основными направлениями государственной политики в сфере информатизации являются: обеспечение единства государственных стандартов в сфере информатизации, их соответствие международным рекомендациям и требованиям. Указ Президента Российской Федерации № 188 от 6 марта 1997 г. (в редакции Указа Президента РФ № 1111 от 23 сентября 2005 г.) установил перечень сведений конфиденциального характера.

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

Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» - данное Постановление утвердило Положение об обеспечении безопасности персональных данных в соответствии со ст. 19 ФЗ № 152-ФЗ. Положение содержит требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных

данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 (ред. от 21.04.2010 г.) «О сертификации средств защиты информации» - данное Постановление утвердило Положение об обязательной сертификации средств защиты информации, где отражен порядок сертификации средств защиты информации в Российской Федерации.

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

Доктрина информационной безопасности Российской Федерации № ПР-1895 от 9 сентября 2000 г. развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере и представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления ее обеспечения и служит основой для формирования государственной политики и подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации, а также для разработки ее целевых программ.

Подводя итог вышеизложенному материалу можно сделать вывод, что конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и

представляет собой коммерческую, служебную, профессиональную или личную тайны, охраняющиеся её владельцем.

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

1.3. Организация защиты конфиденциальной информации в образовательной организации

Развитие новых информационных технологий, приводит к необходимости правового регулирования общественных отношений, так или иначе связанных с процессами использования и передачи информации, которая становится одним из самых ценных ресурсов современного общества.

Указанные процессы, развиваясь по восходящей, приводят к необходимости пересмотра ряда представлений о правовом характере информации. Одним из наиболее показательных примеров в этом контексте может считаться правовое регулирование режимов конфиденциальной информации.

Согласно общему определению, конфиденциальная информация – это сведения, содержащие государственную, коммерческую тайну, тайну следствия и судопроизводства, служебную тайну, врачебную, адвокатскую, нотариальную тайну, тайну переписки, телефонных переговоров, иных почтовых и телеграфных отправок, а также другие сведения о частной личной (неслужебной) жизни и деятельности граждан. Конфиденциальность, при этом, понимается как предотвращение возможности использования информации лицами, которые к ней не причастны.

Информация признается конфиденциальной именно потому, что она является объектом исключительного владения, пользования и распоряжения

конкретного лица. Одним из существенных проявлений несовершенства современного российского законодательства, в этом контексте, является отсутствие четких законодательных критериев для определения конфиденциальной информации, порядка и условий отнесения информации к конфиденциальной. Такие пробелы затрудняют реализацию права на информацию, ставят проблемы в деле построения системы ее защиты.

С развитием компьютерной техники и программного обеспечения защита конфиденциальной информации в образовательных организациях становится особенно актуальной.

Образовательная организация - инфраструктура, обладающая огромным банком данных, содержащим информацию разного характера. Это не только дидактический и методический материал в электронном виде, но и важные проектно-исследовательские наработки. Рост преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей образовательных организаций и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в рамках образовательного учреждения. Эти составляющие определяют единую политику обеспечения безопасности информации в образовательной организации, в частности колледже.

Источниками возможных угроз информации являются: компьютерные учебные аудитории, в которых происходит учебный процесс.

Специфика защиты информации в образовательной системе заключается в том, что колледж - публичное заведение с постоянно меняющейся аудиторией. Основную группу потенциальных нарушителей здесь составляют студенты, некоторые из них имеют достаточно высокий уровень знания компьютеров, сетей.

Студенты имеют доступ только в компьютерные учебные аудитории, от них и исходит внутренняя угроза. Работа студентов, преподавателей в таких аудиториях должна быть регламентирована приказом (актом) администрацией образовательной организации.

Существует немалое количество средств обеспечения защиты конфиденциальной информации, а именно информационной безопасности всей образовательной организации.

К ним можно отнести комплекс инженерно-технической защиты (ИТЗ), состоящей из:

- Физических средств защиты.
- Аппаратных средств защиты.
- Программной защиты информации.
- Криптографических средств защиты.

К физическим средствам защиты можно отнести разнообразные приспособления, конструкции, изделия, и прочие устройства для создания барьеров на пути злоумышленников. К подобным средствам защиты относятся устройства любого типа, воспрепятствующие несанкционированный доступ (НСД) и других несущих вред действий. Подобные средства применяются для охраны территории зданий, помещений, оборудования, а также для наблюдения за ними. Согласно учебному пособию Корнюшина П.Н., Костерина А.С. «В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

- охранные и охранно-пожарные системы;
- охранное телевидение;
- охранное освещение;
- средства физической защиты» [1].

Следующий набор средств - аппаратные средства защиты информации. Аппаратные средства защиты информации включают в себя разного рода технические устройства, созданные для защиты информации от утечки,

разглашения и несанкционированного доступа. К ним относятся самые разнообразные по принципу работы и возможностям технические средства, обеспечивающие пресечение разглашения, защиту от утечки и противодействие НСД к источникам конфиденциальной информации.

Употребление аппаратных средств защиты информации позволяет решать такие задачи как проведение специальных исследований технических средств на наличие возможных каналов утечки информации, могут помочь в раскрытии каналов утечки информации и локализовать их, и останавливают НСД к конфиденциальной информации. Классифицируются аппаратные средства защиты информации на средства обнаружения, средства активного и пассивного противодействия и средства поиска и детальных измерений. Аппаратные средства и методы защиты информации распространены очень широко, однако при раскрытии принципов действия могут потерять значительную часть своей полезности.

Еще одна существенная часть комплекс инженерно-технической защиты - программная защита информации. Она состоит из специальных программ, реализующих принципы информационной безопасности. Имеется 4 линии программ, направленных на защиту информации. Первая направленность - это защита информации от несанкционированного доступа. Состоит из трех основных функций:

- «идентификация субъектов и объектов;
- разграничение доступа к вычислительным ресурсам и информации;
- контроль и регистрация действий с информацией и программами.»

[2]

Самым известным методом идентификации является парольная идентификация. Однако надо учитывать, что пароль можно и взломать.

Второе направление - это защита от копирования. Средства защиты от копирования предотвращают незаконное копирование программного обеспечения и являются на данный момент единственно надежным средством, которое защищает авторское право разработчиков.

Последнее направление - это защита от разрушения информации. Из-за того что причины разрушения информации весьма разнообразны, проведение защитных мероприятий обязательно для всех, кто пользуется компьютером.

Программные средства и методы защиты являются одними из самых надежных.

Четвертая часть комплекса инженерно-технической защиты - это криптографические средства. Это специальные математические средства защиты информации, передаваемой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования. Криптографические методы занимают почти самое важное место и выступают самым надежным средством обеспечения защиты информации на длительные периоды.

Степень защищенности сетей и серверов большинства образовательных организаций России оставляет желать лучшего. Причин тому много, но одна из главных - плохая организация мер по разработке и обеспечению политики информационной безопасности, что естественным образом влияет и на защиту конфиденциальной информации. Администрация образовательной организации просто недооценивает важности этих мероприятий. Вторая проблема заключается в том, что ни государство, ни администрация колледжа не заинтересованы в выделении средств на закупку оборудования и внедрение новых технологий в сфере информационной безопасности.

Выводы по Главе I

По итогам первой главы магистерской диссертации главы можно сделать следующие выводы.

1. Раскрыто понятие «конфиденциальная информация» и значение ее защиты в образовательной организации.

Конфиденциальная информация — любые сведения, составляющие служебную, коммерческую тайну, включая персональные данные сотрудников и студентов. Владелец конфиденциальной информации - лицо, которое владеет информацией, составляющей конфиденциальную информацию, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальной информации.

Организация режима защиты конфиденциальной информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации любой организации, в частности образовательной.

2. Описана организация защиты конфиденциальной информации в образовательной организации.

Образовательная организация - инфраструктура, обладающая огромным банком данных, содержащим информацию разного характера. Рост преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей образовательных организаций и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в рамках образовательной организации. Эти составляющие определяют единую политику обеспечения безопасности информации в образовательной организации, в частности колледже.

Степень защищенности сетей и серверов большинства образовательных организаций России оставляет желать лучшего. Причин тому много, но одна из главных - плохая организация мер по разработке и обеспечению политики информационной безопасности, что естественным образом влияет и на защиту конфиденциальной информации. Администрация образовательной организации просто недооценивает важности этих мероприятий. Еще одна из проблем заключается в том, что ни государство, ни администрация колледжа не заинтересованы в выделении средств на закупку оборудования и внедрение новых технологий в сфере информационной безопасности.

ГЛАВА 2. АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

2.1 Общие сведения об организации профессионального образования

Базой исследования стал ГБПОУ «Южно-Уральский государственный технический колледж» Политехнический комплекс, располагающийся по адресу: г. Челябинск ул. Гагарина, 7.

В Южно-Уральском государственном техническом колледже сегодня учится более 4000 студентов. Директор колледжа Тубер Игорь Иосифович – заслуженный учитель РФ, кандидат педагогических наук, почетный строитель России.

Учредитель ГБПОУ «Южно-Уральский государственный технический колледж»: Министерство образования и науки Челябинской области.

Организационная структура управления ГБПОУ «Южно-Уральский государственный технический колледж» представлен на рисунке 1.

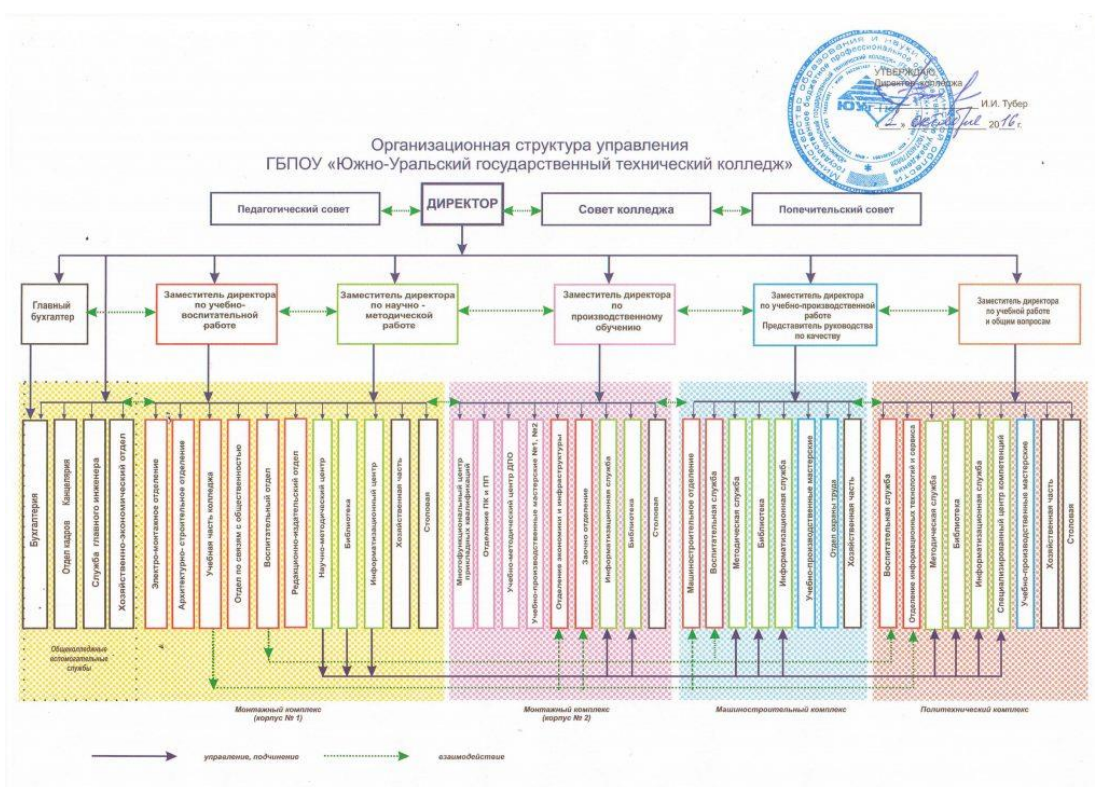


Рис. 1. – Организационная структура управления ГБПОУ «ЮУрГТК»

В основу успехов колледжа на современном этапе заложена сертифицированная в соответствии со стандартом ГОСТ Р ИСО 9001-2001

система менеджмента качества. Она стимулирует педагогический коллектив к постоянному совершенствованию, внедрению инновационных технологий, нацеливает на успех. Высокий уровень подготовки специалистов в колледже подтверждается победами на олимпиадах, конкурсах и выставках регионального и российского значения.

Сегодня в своей деятельности Южно-Уральский государственный технический колледж опирается на современные образовательные технологии – их внедрению уделяется большое внимание, а также на требования работодателей – заказчиков кадров. Система социального партнерства с базовыми предприятиями была выстроена еще в 60-е годы прошлого века. Сегодня подготовка специалистов ведется в колледже с учетом тех требований, которые предъявляются предприятиями, на которых работают выпускники.

Рассмотрим структуру службы информационной безопасности Южно-Уральского государственного технического колледжа (ЮУрГТК).

Проанализировав структуру колледжа, выявили подразделение, отвечающее за информационную безопасность в данном колледже. Таким подразделением является Информатизационный центр.

Информатизационный центр (ИЦ) – структурное подразделение, отвечающее за состояние единой информационной среды колледжа. В его сферу деятельности входят:

- Все рабочие станции в сети.
- Все сервисы доступны с любого компьютера в соответствии с политикой безопасности.
- Корпоративная сеть на основе оптоволокна.
- 7 современных физических серверов.
- 28 виртуальных серверов.
- Два канала доступа к сети Интернет.
- Собственный web-хостинг.
- Лицензионное программное обеспечение.

- Организация ИТ-службы по международному стандарту ITIL.
- Собственное вычислительное облако [3].

Согласно положению информатизационного центра главной целью деятельности ИЦ является организация и предоставление доступа к электронным сетевым сервисам для повышения эффективности работы подразделений колледжа.

В своей деятельности данный центр руководствуется: Конституцией РФ; Законом Российской Федерации от 29 декабря 2012 г. № 273-1 «Об образовании в Российской Федерации»; Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»; Уставом колледжа; документацией внутриколледжной системы менеджмента качества; документацией внутриколледжной системы менеджмента охраны труда и техники безопасности;

- законодательными и нормативными актами по охране труда, пожарной безопасности и обеспечения защиты персональных данных.

Информатизационный центр осуществляет свою деятельность как структурное подразделение колледжа. Структура ИЦ состоит из лабораторий, специализирующихся по направлениям: лаборатория технического обеспечения; лаборатория информационных технологий.

Руководство лабораторией осуществляет заведующий лабораторией, который подчиняется непосредственно руководителю ИЦ. Руководство ИЦ осуществляет руководитель ИЦ, который подчиняется непосредственно заместителю директора по информационным технологиям.

Руководитель ИЦ и заведующие лабораториями, назначаются на должность и освобождаются от нее приказом директора колледжа. Структуру и штатную численность ИЦ утверждает директор колледжа. Сотрудники ИЦ являются штатными сотрудниками колледжа.

Сотрудники:

- Руководитель центра.

Монтажный комплекс:

- Заведующий ЛТО.
- Администратор сети.
- Инженер АСУ.
- Инженер ИЦ.
- Техники ИЦ Техник ИЦ (2-ой корпус).

Машиностроительный комплекс:

- Инженер ИЦ.
- Оператор ЭВМ ИЦ.

Политехнический комплекс:

- Инженер ИЦ.
- Техник ИЦ [3].

Информатизационный центр решает следующие задачи:

1. Разработка и осуществление единой технической политики и практического использования современных достижений информационных технологий в бизнес-процессах колледжа.

2. Выполнение работ по созданию и развитию единой информационной сети колледжа.

3. Выполнение работ, ориентированных на создание новых информационных технологий в целях информационного обеспечения учебного процесса и управления в колледже.

За обеспечение информационной безопасности в колледже отвечает лаборатория информационных технологий.

В ее функции входит: создание, обслуживание и развитие защищенного центрального серверного центра колледжа; проектирование и развитие компьютерной сети с использованием современных достижений в данной области; установка, настройка и сопровождение сетевых программных продуктов; создание надежных условий для доступа всех пользователей к компьютерной сети колледжа; предоставление сетевых сервисов в целях обеспечения учебных и управленческих работ; организация централизованной антивирусной защиты информационных ресурсов;

предоставление сетевых ресурсов для автоматизации управленческой деятельности подразделений; проектирование, разработка, размещение и поддержка внешних и внутренних Web-серверов; подбор, адаптация, разработка нового и внедрение программного обеспечения с целью создания, и развития автоматизированной системы управления колледжем; адаптация и внедрение программного обеспечения для организации процесса дистанционного образования и независимой проверки знаний; организация работ по обеспечению защиты информационных систем персональных данных.

Администратор сети в данном центре несет ответственность по обеспечению информационной безопасности и защиты от вирусов, а также безопасности информационных систем персональных данных.

Администратор сети должен проводить работы с ресурсами ИСПДн, которые заключаются в следующем: проверка работоспособности и настройка системы доступа к ресурсам ИСПДн; проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ); антивирусная защита ресурсов ИСПДн; хранение дистрибутивов программного обеспечения СЗИ; проверка целостности системного и прикладного ПО; резервное копирование и восстановление информации; конфигурирование ИСПДн; вывод ресурсов ИСПДн из эксплуатации; реагирование на сбои при регистрации событий безопасности.

При нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации [4].

Таким образом, можно сделать вывод, что информатизационный центр является подразделением службы информационной безопасности в ГБПОУ «Южно-Уральский государственный технический колледж» и обеспечивает в колледже комплексную защиту информации.

2.2. Конфиденциальная информация организации профессионального образования - компонент информационных ресурсов

Защите в колледже подлежат сведения конфиденциального характера, обрабатываемые сотрудниками колледжа на основании Устава ГБПОУ «ЮУрГТК», Трудового кодекса РФ и других положений действующего законодательства.

Отнесение информации к конфиденциальной производится директором на основании Указа Президента РФ от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера», Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и других нормативных актов.

Конфиденциальная информация может включать следующие сведения:

- персональные данные сотрудников ГБПОУ «ЮУрГТК»,
- персональные данные обучающихся и их законных представителей,
- технологическая информация эксплуатируемых в колледже автоматизированных и информационных систем,
- сведения о программно-технических средствах обработки,
- сведения о средствах защиты конфиденциальной информации,
- сведения о каналах информационного обмена и телекоммуникации,
- сведения об объектах и помещениях, в которых расположены компоненты системы защиты информации или компоненты эксплуатируемых автоматизированных и информационных систем.

Конфиденциальная информация подлежит защите вне зависимости от формы обработки и хранения, в том числе,

- речевая и видео-информация,
- информация, хранящаяся на файловых серверах (виртуальных и физических), серверах репликации данных, ленточных библиотеках резервного копирования,

– информация, передаваемая по каналам связи, локальным вычислительным сетям, эксплуатируемым автоматизированным и информационным сетям,

- информация на бумажных, магнитных и других материальных носителях.

Обработка, в том числе накопление и систематизация конфиденциальной информации, производится с помощью автоматизированных и неавтоматизированных ресурсов, при этом объектами защиты являются все компоненты информационных ресурсов.

В состав объектов защиты входят: информация и содержащие ее информационные ресурсы, эксплуатируемые в ГБПОУ «ЮУрГТК», содержащие зафиксированные на материальном носителе сведения, используемые в процессе сбора, обработки, накопления, хранения, в рамках оказания государственных услуг ГБПОУ «ЮУрГТК». Поэтому информация не может быть рассмотрена в отрыве от элементов содержащих ее информационных ресурсов ГБПОУ «ЮУрГТК», на которых она обрабатывается (хранится).

Объекты защиты включают:

– конфиденциальную информацию в любой форме представления: персональные данные; технологическую информацию по автоматизированным и информационным системам, сведения о программно-технических средствах обработки и защиты ПДн, о каналах информационного обмена и телекоммуникаций, о помещениях, в которых размещены компоненты эксплуатируемых систем и т.д.;

– информационные ресурсы (далее - ИР): информационные и автоматизированные системы; средства защиты информации, используемые при обработке ПДн в ИСПДнГБПОУ «ЮУрГТК»;

– помещения, здания, объекты, сооружения, предназначенные для работы с информацией;

– оборудование информационных систем (серверные комплексы, рабочие станции пользователей, технические средства ввода/вывода информации, комплексы сканирования документов, принтеры, средства хранения и архивирования данных, источники бесперебойного питания);

– телекоммуникационные сети и системы,

– программные средства (операционные системы, системы управления базами данных, другое общесистемное, специальное и прикладное программное обеспечение);

– технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации);

– средства обеспечения жизнедеятельности объектов (основные и резервные/бесперебойные системы электропитания и заземления объектов, системы пожарной и охранной сигнализации, электронные системы контроля управления доступом на территорию и в помещения, системы громкоговорящей связи и оповещения, системы кондиционирования, отопления, вентиляции и пожаротушения).

Для организации защиты объектов защиты должен быть организован их учет, идентифицирующий каждый из объектов единственным образом, а также установлен порядок и правила их эксплуатации.

Содержание, эксплуатация и учет объектов защиты информации должны быть организованы в соответствии с требованиями действующего законодательства и эксплуатационной документации.

Построение системы защиты ПДн ГБПОУ «ЮУрГТК» и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность;

– системность;

- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

Обеспечение требуемого уровня защищенности должности достигается с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности объектов защиты подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

2.3. Оценка существующих средств защиты конфиденциальной информации в ГБПОУ «Южно-Уральски государственный технический колледж»

Активы (ресурсы) – это все, что имеет ценность или находит полезное применение для организации, ее деловых операций и обеспечения их непрерывности. Надлежащее управление и учет активов должны являться одной из основных обязанностей руководителей всех уровней [1].

Без инвентаризации активов на уровне служебной деятельности невозможно ответить на вопрос, что именно нужно защищать.

Были выявлены следующие потоки информации:

- личные дела преподавателей, персонала и студентов;
- данные о материальном обеспечении колледжа;
- данные по приказам, распоряжениям, мероприятиям, распорядку ГБПОУ «ЮУрГТК»;
- бухгалтерская и управленческая отчетность.

Перечень информационных активов, обязательное ограничение доступа, к которым регламентируется действующим законодательством РФ, сведены в таблицу 1.

Таблица 1

Перечень сведений конфиденциального характера

№ п/п	Наименование сведений	Гриф конфиденциальности	Нормативный документ, реквизиты, № статей
1	Сведения, раскрывающие характеристики средств защиты ЛВС колледжа от несанкционированного доступа	Конфиденциально	Устав колледжа (ГБПОУ «ЮУрГТК»)
2	Требования по обеспечению сохранения служебной тайны сотрудниками образовательной организации	Конфиденциально	Гражданский кодекс РФ ст. 1465
3	Персональные данные преподавателей, персонала и студентов (и их родителей)	Конфиденциально	Федеральный закон 152-ФЗ

Результат ранжирования активов представляет собой интегрированную оценку степени важности актива для образовательной организации, взятую по пятибалльной шкале и представленную в таблице 2.

Таблица 2

Результаты ранжирования активов

Наименование актива	Ценность актива (ранг)
Программное обеспечение	10
Сотрудники	11
Компьютерные средства	9
Информационные услуги	4
Текстовые сообщения	12
Личные дела преподавателей, персонала, студентов	1
Переписка внутри колледжа	8
Расходные накладные	7
Данные по приказам, распоряжениям, мероприятиям, распорядку колледжа	4
Инвентаризационная ведомость	5
Приходные накладные	6
Бухгалтерская и налоговая отчетность	8

Таким образом, были выделены активы, имеющие наибольшую ценность: личные дела сотрудников, персонала и обучающихся.

Оценка уязвимости активов проведена на основании требований стандарта ГОСТ Р ИСО/МЭК ТО 13335-3-2007 [4].

Уязвимость – это событие, которое возникает как результат некоторого стечения обстоятельств, когда в силу каких-то причин используемые в системах обработки данных средства защиты информации не в состоянии оказать достаточного сопротивления различным дестабилизирующим факторам и нежелательного их воздействия на информацию, подлежащую защите.

Уязвимости информационной системы организации можно выявить несколькими способами. Их может описать сотрудник компании (инженер, системный администратор или специалист службы информационной безопасности) на основании собственного опыта. Кроме того, могут быть

приглашены сторонние специалисты для проведения технологического аудита информационной системы и выявления ее уязвимостей.

Показателем уязвимости некоторого актива является степень уязвимости в порядковой шкале оценок (пример степеней: высокая, средняя, низкая).

Перечень уязвимостей, с указанием оценки степени вероятности возможной реализации отмеченных уязвимостей, представлены в таблице 3.

Таблица 3

Оценка уязвимости активов

Группа уязвимостей	Личные дела преподавателей, персонала и студентов	Переписка внутри колледжа	Данные о материальном обеспечении	Расходные накладные	Данные по приказам, распоряжениям	Инвентаризационная ведомость	Приходные накладные	Бухгалтерская и налоговая отчетность	ПО
1. Среда и инфраструктура									
Нестабильная работа электросети									низкая
2. Аппаратное обеспечение									
Недостаточное обслуживание	высокая	средняя	средняя	средняя	средняя	средняя	средняя	низкая	средняя
Отсутствие контроля изменения конфигурации	высокая	высокая	высокая	высокая	высокая	высокая	низкая	низкая	высокая
3. Программное обеспечение									
Отсутствие механизмов идентификации	высокая	высокая	высокая	высокая	высокая	высокая	низкая	низкая	высокая

и аутентификации									
Незащищенные таблицы паролей	высокая	высокая	высокая	низкая	высокая	низкая	низкая	низкая	высокая
Плохое управление паролями	высокая	высокая	высокая	высокая	высокая	низкая	низкая	низкая	высокая
Неправильное присвоение прав доступа	высокая	высокая	средняя	низкая	средняя	низкая	низкая	низкая	средняя
Отсутствие регистрации конца сеанса при выходе	высокая	высокая	высокая	низкая	высокая	низкая	низкая	низкая	средняя
Отсутствие эфф. контроля внесения изменений	высокая	высокая	средняя	средняя	средняя	низкая	низкая	низкая	высокая
Отсутствие резервных копий	высокая	высокая	средняя	высокая	средняя	средняя	низкая	низкая	средняя
4. Коммуникации									
Неадекватное управление сетью	высокая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая
Незащищенные подключения к сетям	высокая	средняя	средняя	средняя	средняя	средняя	средняя	средняя	средняя
5. Документы (документооборот)									

Хранение в незащищенных местах	низкая	высокая	высокая	высокая	высокая	средняя	низкая	низкая	
Недостаточная внимательность при уничтожении	низкая	высокая	высокая	высокая	высокая	средняя	низкая	низкая	
Бесконтрольное копирование	низкая	высокая	высокая	высокая	высокая	средняя	низкая	низкая	
6. Персонал									
Неправильное исполнение ПО и АО	высокая	средняя	средняя	средняя	средняя	средняя	низкая	средняя	средняя
7. Общие уязвимые места									
Неадекватные результаты проведения тех. обслуживания	высокая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая

Угроза – это потенциальная причина инцидента, который может нанести ущерб системе или организации.

Инцидент информационной безопасности – это любое непредвиденное или нежелательное событие, которое может нарушить деятельность организации или информационную безопасность.

Существуют пассивные и активные угрозы. Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов информационной системы, не оказывая при этом влияния на саму информацию, не вызывая искажений и нарушений информации. К пассивной угрозе можно, например, отнести прослушивание каналов связи, просмотр баз данных.

Цель активных угроз - нарушение нормальной работы информационной системы путем целенаправленного воздействия на ее составляющие. Активные угрозы портят информацию, воздействуют на саму информационную систему. Так, к активным угрозам можно отнести искажение информации, вывод из строя компьютерной техники, воздействие вирусов.

Оценка угроз активам проведена на основании требований стандарта ГОСТ Р ИСО/МЭК ТО 13335-3-2007 [4]. Перечень угроз, с указанием оценки, приведены в таблице 4.

Таблица 4

Оценка угроз активам

Группа уязвимостей	Личные дела преподавателей, персонала и студентов	Переписка внутри колледжа	Данные о материальном обеспечении	Расходные накладные	Данные по приказам, распоряжениям	Инвентаризационная ведомость	Приходные накладные	Бухгалтерская и налоговая отчетность	ПО
1. Угрозы, обусловленные преднамеренными действиями									
Вредное ПО	высокая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая
Доступ несанкц. пользователей к сети	высокая	средняя	средняя	средняя	средняя	средняя	средняя	средняя	средняя
Использование ПО несанкц. пользователями	высокая	высокая	высокая	высокая	высокая	высокая	высокая	низкая	высокая
2. Угрозы, обусловленные случайными действиями									
Ошибки операторов	высокая	высокая	высокая	высокая	высокая	высокая	высокая	средняя	средняя
Неадекватное	средняя	высокая	высокая	высокая	средняя	высокая	средняя	низкая	средняя

использование ресурсов									
Ошибки при обслуживании	высокая	средняя	средняя	средняя	низкая	средняя	средняя	средняя	средняя
3. Угрозы, обусловленные естественными причинами (природные, техногенные факторы)									
Ухудшение состояния носителей данных	низкая	высокая	высокая	высокая	средняя	высокая	высокая	средняя	средняя
Колебания напряжения	низкая	высокая	высокая	высокая	высокая	высокая	низкая	средняя	средняя

Активы, имеющие ценность и характеризующиеся определенной степенью уязвимости, всякий раз подвергаются риску в присутствии угроз. Задача анализа риска состоит в определении и оценке рисков, которым подвергается система информационных технологий и ее активы, с целью определения и выбора целесообразных и обоснованных средств обеспечения безопасности.

Для каждого актива рассматривают уязвимые места и соответствующие им угрозы. Если имеются уязвимые места без соответствующей угрозы или угрозы без соответствующего уязвимого места, то считают, что в данное время риск отсутствует. Затем идентифицируют соответствующий ряд матрицы по ценности актива, а соответствующую колонку – по степени угрозы и уязвимости. Ценность настоящего метода состоит в ранжировании соответствующих рисков (таблица 5).

Таблица 5

Результаты оценки рисков информационным активам организации

Риск	Актив	Ранг риска
Утрата целостности	Данные по приказам, распоряжениям, мероприятиям, распорядку колледжа	9

Утрата целостности	Информационные услуги	9
Утрата конфиденциальности	Внутренняя переписка	8
Утрата конфиденциальности	Приходные накладные	8
Утрата конфиденциальности	Расходные накладные	7
Утрата конфиденциальности	Инвентаризационная ведомость	6
Утрата конфиденциальности	Личные дела преподавателей, обучающихся, персонала	6
Нарушение целостности	Программное обеспечение	4
Утрата доступности	Данные материальном обеспечении колледжа	4
Утрата доступности	Бухгалтерская и налоговая отчетность	1

Данная таблица содержит риски по наиболее ценным информационным активам, ранжированные в порядке убывания.

Результаты оценки рисков являются основанием для выбора и формулировки задач по обеспечению информационной безопасности предприятия, и выбора защитных мер.

Таким образом, на основе анализа можно выявить такие основные проблемы:

1. Отсутствие антивирусного ПО на самих АРМ.
2. Устаревшее антивирусное ПО на сервере.
3. Отсутствие системы контроля доступа сотрудников к чужим АРМам.
4. Отсутствие системы видеонаблюдения в кабинетах.

Все эти проблемы должны учитываться при планировании комплексной системы защиты в образовательной организации.

Задачи по защите информации возложены на сотрудников информатизационного центра, а также на руководителей подразделений. Результаты оценки действующей системы безопасности информации, отражают, насколько полно выполняются однотипные объективные функции

при решении задач обеспечения защиты конфиденциальной информации (таблица 6).

Таблица 6

Анализ выполнения задач по обеспечению информационной безопасности

№ п/п	Основные задачи по обеспечению информационной безопасности	Степень выполнения
1	обеспечение безопасности процесса управления образовательной организации СПО, защита информации и сведений, являющихся конфиденциальной;	средняя
2	организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите конфиденциальной информации;	средняя
3	организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся конфиденциальной;	средняя
4	предотвращение необоснованного допуска и открытого доступа к сведениям и работам, составляющим конфиденциальность;	низкая
5	выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (авария, пожар и др.) ситуациях;	средняя
6	обеспечение режима безопасности при осуществлении таких видов деятельности, как различные встречи, переговоры, совещания, заседания и другие мероприятия, связанные с деловым сотрудничеством на национальном и международном уровне;	средняя
7	обеспечение охраны территории, зданий помещений, с защищаемой информацией.	средняя

В первую очередь необходимо обратить внимание на те аспекты защиты информации, которые характеризуются низкой и средней степенью выполнения. Кроме того, важно обеспечить комплексный характер защиты.

Но, следует отметить, что остаются слабые места в системе, которые не защищены никакими средствами. Задача состоит в том, чтобы обеспечить надежной защитой все моменты, описанные в частной модели угроз (приложение 1).

Выводы по главе II

Во второй главе магистерской диссертации проведен анализ информационной безопасности Южно-Уральского государственного технического колледжа.

На основании оценки рисков наиболее ценным информационным активам были выбраны основные задачи по совершенствованию информационной безопасности.

Обеспечение целостности, а также конфиденциальности активов возможно за счет внедрения программно-аппаратных средств и антивирусной защиты.

Внедрением системы защиты в колледже будет заниматься системный администратор (подбор, установка, настройка и обслуживание технических и программных средств защиты), а также начальник информатизационного центра (разработка положений, приказов, распоряжений).

Решение задачи обеспечения информационной безопасности является очень важной для функционирования колледжа. Потеря информации приведет к выходу всей системы из строя, потере эффективности работы, разглашению служебной информации.

ГЛАВА 3. МЕРЫ СОВЕРШЕНСТВОВАНИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ГБПОУ «ЮЖНО- УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

3.1. Рекомендации по совершенствованию защиты конфиденциальной информации

На основании проведенного анализа и в соответствии с приказом ФСТЭК России №21 [20] определяем необходимые требования по защите ПДн в ГБПОУ «ЮУрГТК». К ним можно отнести:

- идентификацию и аутентификацию пользователей системы (настройка ОС);
- защиту от сетевых атак и вторжений;
- управление доступом пользователей к ПЭВМ (электронные замки);
- регистрацию событий безопасности (встроенный журнал безопасности ОС);
- контроль и управление физическим доступом к ТС, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие НСД к данным средствам (установка запирающихся сейфов, шкафов для защиты бумажных носителей и установка СЗИ от НСД для защиты ТС самой ИСПДн).
- передача ПДн в сторонние организации должна осуществляться в зашифрованном виде.

Защита конфиденциальной информации должна содержать:

1. Анализ информационных ресурсов (определение состава, содержания, местонахождения; способов обработки конфиденциальной информации, подлежащей защите; наличия средств защиты информации).
2. Выявление уязвимостей и возможных угроз безопасности информации:
 - составление перечня уязвимостей и возможных угроз безопасности информации;

- оценка актуальности угроз безопасности информации;
- создание частной модели угроз безопасности информации;

3. Классификацию систем, обрабатывающих конфиденциальную информацию.

4. Обоснование требований по защите КИ, обрабатываемой на объекте информатизации (ОИ).

5. Оценку достаточности фактически реализованных мер защиты (подготовят заключение об их целесообразности и рекомендации по их совершенствованию).

6. Создание (модернизация) системы защиты конфиденциальной информации:

- разработка системы защиты информации;
- поставка, установка, наладка, опытная эксплуатация, устранение недостатков по результатам опытной эксплуатации и ввод в эксплуатацию системы защиты информации;

7. Разработку организационно-распорядительной документации по организации защиты конфиденциальной информации на ОИ.

8. Аттестацию ОИ по требованиям безопасности информации (оценку соответствия требованиям безопасности информации).

9. Техническое обслуживание и сопровождения системы защиты конфиденциальной информации.

Согласно данным требованиям были разработаны мероприятия по совершенствованию системы информационной безопасности колледжа, которая состоит из:

1. Комплекс организационных мер обеспечения информационной безопасности колледжа, разработка частной модели угроз.

2. Комплекс проектируемых программно-аппаратных средств обеспечения информационной безопасности колледжа.

*Комплекс организационных мер обеспечения информационной безопасности
колледжа*

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

- 1) Конституция РФ;
- 2) Законы федерального уровня (включая федеральные конституционные законы, кодексы);
- 3) Указы Президента РФ;
- 4) Постановления правительства РФ;
- 5) Нормативные правовые акты федеральных министерств и ведомств;
- 6) Нормативные правовые акты субъектов РФ, органов местного самоуправления и т.д.

К нормативно-методическим документам можно отнести:

1. Методические документы государственных органов России:

- 1) Доктрина информационной безопасности РФ;
- 2) Руководящие документы ФСТЭК (Гостехкомиссии России);
- 3) Приказы ФСБ;

2. Стандарты информационной безопасности, из которых выделяют:

- 1) Международные стандарты;
- 2) Государственные (национальные) стандарты РФ;
- 3) Рекомендации по стандартизации;
- 4) Методические указания.

Защита конфиденциальной информации предполагает выбор различных мер. По статистике, нарушения информационной безопасности совершаются, в основном, работниками учреждения (81%) или бывшими его сотрудниками (6%). Соотношение нарушений информации, произведенных разными группами лиц, представлено на рисунке 2.

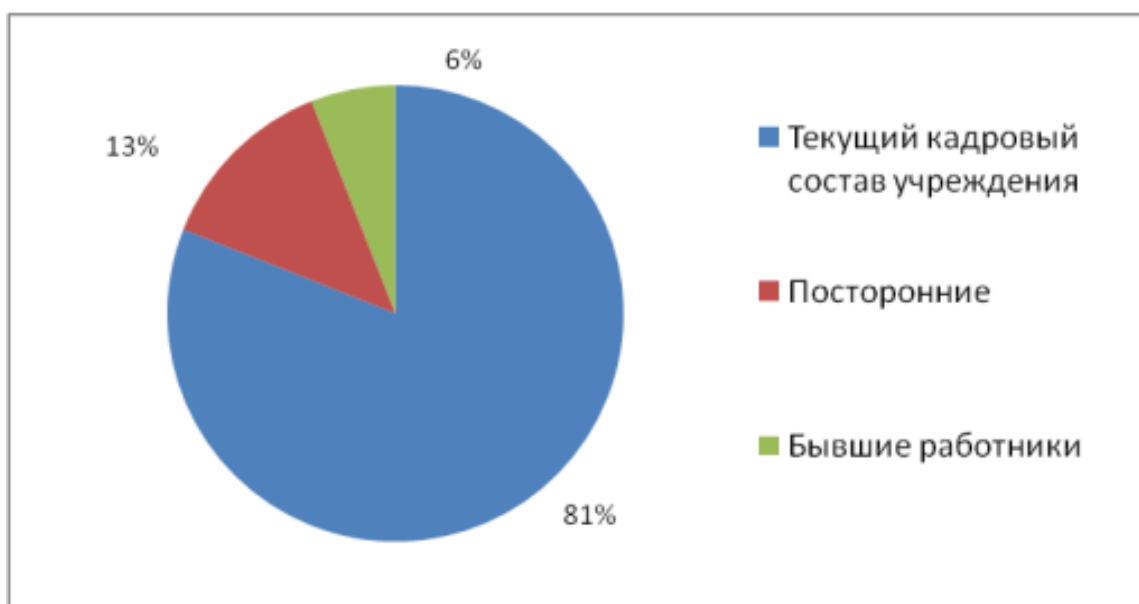


Рис. 2. – Соотношение нарушений информации, произведенных разными группами лиц

Таким образом, около 80% всех преступлений в сфере нарушения конфиденциальной информации совершается либо сотрудниками организации, либо с их помощью, а иногда и вследствие халатности и невнимательности работников. Именно поэтому очень важным направлением обеспечения защиты конфиденциальной информации является административная информационная безопасность, которая обеспечивается за счет применения организационных мер. Организационные меры предполагают внедрение безопасных способов ведения документации, применение методов разработки, внедрения и тестирования прикладных программных средств, а также процедур обработки инцидентов в случаях нарушения систем безопасности. Обеспечение административной составляющей информационной безопасности предполагает также выбор определенной стратегии защиты информации в компании.

К организационно-административным мероприятиям защиты информации относятся:

– выделение специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;

- выделение специальных ЭВМ для обработки конфиденциальной информации;
- организация хранения конфиденциальной информации на специальных промаркированных магнитных носителях;
- использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;
- организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации;
- организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной информации;
- установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;
- разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки, хранения, передачи и использования информации;
- постоянный контроль за соблюдением установленных требований по защите информации.

На основе анализа существующей системы безопасности было принято решение реализовать такие административные меры безопасности:

1) Разработать и утвердить приказом по колледжу:

- положение о защите сведений, содержащих конфиденциальность, и другой информации ограниченного пользования, определённые законодательством РФ;

- инструкцию по делопроизводству с документами ограниченного пользования.

2) Издать приказ по колледжу, в котором:

- на руководителей подразделений возложить обязанность проведения мероприятий, направленных на обеспечение сохранности конфиденциальной информации;

- определить меры административного наказания за нарушение правил работы с документами и сведениями, содержащими конфиденциальную информацию;

- на службу безопасности возложить обязанность по выявлению возможных нарушений, в результате которых возможна утечка охраняемых сведений.

3) Ввести запрет на хранение личной информации на компьютере.

4) Установить правила копирования документов, исключающих изготовление копий важных документов без санкции руководителя.

5) От работников, по должности обладающих сведениями конфиденциальности, при заключении трудового договора брать письменные обязательства о неразглашении. В случае увольнения работника, требовать от него передачи всех носителей информации, составляющих конфиденциальную информацию, которая находилась в его распоряжении.

6) Изготовить выписки, содержащие выдержки из положения о конфиденциальной информации для использования работниками в повседневной деятельности;

7) Разработать журнал учета персональной информации;

8) Разработать правила работы с электронной почтой.

9) При включении компьютера перед вводом пароля программным способом выдавать пользователю сообщение, напоминающее пользователю о правилах работы с компьютером.

10) Разработана частная модель угроз (приложение 1).

Организационно-административные меры защиты информации позволят избежать части непреднамеренных угроз, а также преднамеренных угроз безопасности информации со стороны работников колледжа. Кроме того, жесткий регламент обращения с информационными ресурсами дисциплинирует коллектив, приучает их более внимательно работать с данными и относиться к ней как к ценному ресурсу.

*Комплекс проектируемых программно-аппаратных средств обеспечения
информационной безопасности колледжа*

Одной из главных задач при разработке системы защиты информации является построение модели угроз (приложение 1). Это позволяет в полном объеме оценить слабые места автоматизированной системы. В соответствии с пунктом 2 статьи 19 ФЗ «О персональных данных» обеспечение безопасности персональных данных достигается, в частности определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, т.е. разработкой модели угроз.

Основными группами угроз, на противостояние которым направлены цели и требования безопасности, являются:

1. Угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией при ее обработке и хранении.
2. Угрозы, связанные с несанкционированным копированием (хищением) информации.
3. Угрозы, связанные с осуществлением доступа к информации, содержащей сведения о персональных данных, без разрешения на то ее владельца (субъекта персональных данных).
4. Угрозы, связанные с нарушением доступности информации, содержащей сведения, передаваемой заинтересованным лицам.
5. Угрозы, связанные с перехватом информации, содержащей сведения, из каналов передачи данных с использованием специализированных программно-технических средств.

6. Угрозы, связанные с потерей (утратой) информации, вследствие сбоев (отказов) программного и аппаратного обеспечения.

7. Угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения.

8. Угрозы, связанные с осуществление несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.).

Модель угроз является обязательным пунктом в построении системы защиты информации. Данная мера необходима для выявления слабых мест АС и ИСПДн, эффективной постановки задачи.

Из вышеперечисленного списка угроз можно сделать вывод, что основными направлениями разработки системы защиты информации будут защита от НСД при приеме, передачи и хранении конфиденциальной информации.

В приложении 1 приведен пример Частной модели угроз безопасности персональных данных в информационной системе персональных данных «Региональная АИС «Сетевой город образования»».

Виды средств защиты информации

Примеры основных средств защиты персональных данных в ИСПДн:

Обязательные

- Средство защиты информации от несанкционированного доступа (СЗИ от НСД).

- Антивирусное средство защиты.

При взаимодействии с иными компьютерными

- Межсетевой экран (защита от сетевых угроз)

При передаче ПДн за пределы контролируемой зоны (в т.ч. Интернет)

- Средство шифрования информации (криптографические, СКЗИ)

Дополнительные:

- Сетевые сканеры безопасности (контроль и анализ уязвимостей).

- Система обнаружения вторжений (обнаружение компьютерных атак).

Программно-технические средства защиты информации

Сервис безопасности:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

1. От несанкционированного копирования, в том числе:

- средства защиты носителей данных;
- средства предотвращения копирования программного обеспечения,

установленного на ПЭВМ

2. Средства криптографической и стенографической защиты информации

3. Средства прерывание работы программы пользователя при нарушении им правил доступа, в том числе:

- принудительное завершение работы программы;
- блокировка компьютера

4. Средства стирания данных, в том числе:

– стирание остаточной информации, возникающей в процессе обработки данных в оперативной памяти и на магнитных носителях;

– надежное стирание устаревшей информации с магнитных носителей

5. Средства выдачи сигнала тревоги при попытке несанкционированного доступа к информации, в том числе:

- средства регистрации некорректных обращений пользователей к защищаемой информации;

- средства организации контроля за действиями пользователей ПЭВМ

6. Средства обнаружения и локализации действия программных и программно-технических закладок.

Технические средства защиты информации

- системы охранной и пожарной сигнализации;

- системы цифрового видео наблюдения;

- системы контроля и управления доступом (СКУД). Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

- использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;

- установкой на линиях связи высокочастотных фильтров;

- создание контролируемых зон.

Программные средства защиты информации

- средства собственной защиты;

- средства защиты в составе вычислительной системы;

- средства защиты с запросом информации;

- средства активной защиты;

- средства пассивной защиты.

Направления использования программ для обеспечения безопасности конфиденциальной информации:

- защита информации от несанкционированного доступа;

- защита информации от копирования;

- защита программ от копирования;

- защита программ от вирусов;
- защита информации от вирусов;
- программная защита каналов связи

Программные средства защиты информации имеют следующие разновидности специальных программ:

- идентификация технических средств, задач, массивов и пользователей;
- определение прав технических средств, задач и пользователей;
- контроль работы технических средств и пользователей;
- регистрация работы технических средств и пользователей при обработке закрытой информации;
- уничтожение информации в ЗУ после завершения работы;
- сигнализация о несанкционированных действиях;
- вспомогательные программы различного назначения (контроль работы механизма защиты, автоматическое проставление грифа и т.п.).

Программно-аппаратные средства защита системы персональных данных 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).

Средства защиты от несанкционированного доступа (НСД) обеспечивают защиту информации, хранимой и обрабатываемой на персональных компьютерах, рабочих станциях и серверах.

Основная задача средств защиты от НСД - идентификация и аутентификация пользователей, позволяющая регламентировать доступ к защищаемым информационным ресурсам.

Используемые средства защиты от НСД:

Программные:

- Secret NetStudio;
- Dallas Lock 8.0-C;
- Панцирь-К.

Программно-аппаратные (модули доверенной загрузки):

- ПАК СЗИ НСД «Аккорд-АМДЗ»%
- ПАК «Соболь»;
- плата «Secret Net Card».

Операционные системы:

- Windows 7/8/ Server 2008/2012
- ALT Linux;
- РОСА;
- Astra Linux.

Для решения задачи обеспечения информационной безопасности была выбрана система Dallas Lock 8.0-C.

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.

Варианты использования Dallas Lock:

1. Защита автоматизированных рабочих мест без централизованного управления – защита небольшого количества (10-50) рабочих станций и серверов. Автоматизированные рабочие места могут администрироваться либо локально, либо удаленно.

2. Защита автоматизированных рабочих мест с централизованным управлением в сетях (не требуется наличия Active Directory) – применение политик безопасности, а также централизованное разворачивание Dallas Lock – используется Сервер безопасности Dallas Lock.

Система защиты Dallas Lock может работать на любом компьютере, работающем под управлением следующих ОС:

- Windows Server 2008 (SP 2) (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 (R2) (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home).

Система защиты Dallas Lock поддерживает 32-х и 64-х битные версии операционных систем.

Dallas Lock позволяет защищать информационные ресурсы рабочего пространства Windows To Go операционной системы Windows 8 на USB-накопителе.

Минимальная и оптимальная конфигурация ПК определяется требованиями к версии операционной системы Windows, на которую установлена система защиты Dallas Lock. Для размещения файлов системы и ее работы требуется не менее 30 Мбайт пространства на системном разделе жесткого диска. Для использования Dallas Lock на компьютерах в составе ЛВС необходимо установить сетевой протокол TCP/IP. Для использования аппаратных идентификаторов требуется наличие в аппаратной части ПК соответствующих портов: USB-порта или COM-порта.

Средства антивирусной защиты

Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

Требования к средствам антивирусной защиты», утверждены Приказом ФСТЭК России от 20 марта 2012 г. N 28.

В колледже имеется потребность в развертывании антивирусной защиты, поэтому нужно выбрать антивирусное программное обеспечение.

В таблице 7 представлена спецификация профилей защиты средств антивирусной защиты для каждого типа средства антивирусной защиты и класса защиты средства антивирусной защиты.

Таблица 7

Спецификация профилей защиты средств антивирусной защиты

Тип САВЗ	Класс защиты					
	6	5	4	3	2	1
тип «А»	ИТ.САВЗ. А6.ПЗ	ИТ.САВЗ. А5.ПЗ	ИТ.САВЗ . А4.ПЗ	ИТ.САВЗ. А3.ПЗ	ИТ.САВЗ. А2.ПЗ	ИТ.САВЗ. А1.ПЗ
тип «Б»	ИТ.САВЗ.Б 6.ПЗ	ИТ.САВЗ. Б5.ПЗ	ИТ.САВЗ .Б4.ПЗ	ИТ.САВЗ.Б3. ПЗ	ИТ.САВЗ.Б2 .ПЗ	ИТ.САВЗ. Б1.ПЗ
тип «В»	ИТ.САВЗ.В 6.ПЗ	ИТ.САВЗ. В5.ПЗ	ИТ.САВЗ .В4.ПЗ	ИТ.САВЗ.В3. ПЗ	ИТ.САВЗ.В 2.ПЗ	ИТ.САВЗ. В1.ПЗ
тип «Г»	ИТ.САВЗ.Г 6.ПЗ	ИТ.САВЗ. Г5.ПЗ	ИТ.САВЗ .Г4.ПЗ	ИТ.САВЗ.Г3. ПЗ	ИТ.САВЗ.Г2 .ПЗ	ИТ.САВЗ. Г1.ПЗ

Исходя из результатов проведенных тестов, антивирус Касперского можно с уверенностью считать наилучшим вариантом для защиты информации в колледже, к тому же цена на продукт лаборатории Касперского не является самой высокой.

В колледже должна быть разработана стратегия антивирусной защиты. Стратегия антивирусной защиты образовательной организации направлена на осуществление многоуровневой защиты всех уязвимых элементов в ИТ структуре организации (рисунок 3).

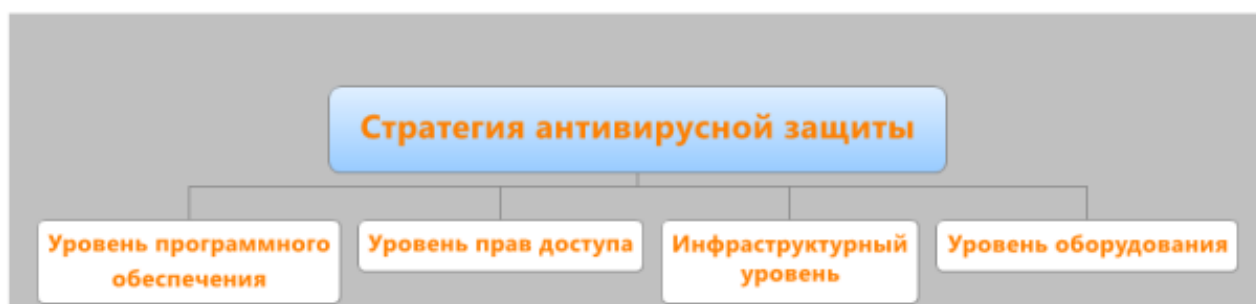


Рис. 3. – Стратегия антивирусной защиты

Рассмотрим подробнее стратегию антивирусной защиты:

1. Инфраструктурный уровень. Выбирается структура сети, обеспечивающая необходимую защиту от вторжений для самых критичных и уязвимых элементов сети. Она включает защиту сети от атак через установку сетевого шлюза с файерволом корпорации, фильтрация внешнего трафика сети (в том числе входящей электронной корреспонденции), загружаемых интернет-страниц и служб мгновенных сообщений, которые чаще всего становятся источниками заражения.

2. Уровень программного обеспечения. Проводится работа по выявлению уязвимых приложений, регулярное своевременное обновление ПО с целью закрытия обнаруженных уязвимостей. Устанавливается нужное программное обеспечение, в зависимости от потребностей образовательной организации.

3. Уровень оборудования. Исследуется возможность и порядок применения внешних запоминающих устройств (Flash-накопители, оптические носители и прочее) с целью сокращения числа возможных источников заражения вирусами.

4. Уровень прав доступа. Регламентируются права пользователей системы, сводя к минимуму возможность проникновения вредоносных программ. Организовывается регулярное резервное копирование всей критичной информации для быстрого восстановления при необходимости. Проводится планомерный контроль состояния антивирусных программ, аудит безопасности сети и полные антивирусные проверки.

Комплексная защита сети от вирусов колледжа выполняет следующие функции:

1. Защита персональных компьютеров предотвращает проникновение вредоносных программ из разных источников. Так обеспечивается проактивная защита от неизвестных в базе вирусов.

2. Защита шлюзов и сервера электронной почты, системы обмена e-mail и обеспечение безопасного коллективного доступа к документам колледжа. Антивирус на почтовом сервере контролирует и проверяет электронную почту, лечит или удаляет поврежденные файлы. Система защиты не пропускает зараженные письма на персональные компьютеры, где бороться с вирусами гораздо сложнее;

3. Защита интернет-трафика. Антивирус проверяет весь трафик, поступающий из Интернета, и удаляет вирусы. Этот этап существенно повышает общую защищенность сети и является весомым дополнением к антивирусной защите рабочих мест и серверов, но не гарантирует полную безопасность;

4. Защита файлового сервера. В этом случае антивирус проверяет открываемые или изменяемые файлы. Проводится распределение системой серверных ресурсов между антивирусом и прочими серверными приложениями, предоставляя возможность минимального влияния на ключевые серверные службы;

5. Регулярное автоматическое обновление ПО позволяет устранять уязвимости в программных продуктах, предотвращая заражение, а не борясь с его последствиями.

6. Обеспечение централизованного доступа к управлению элементами антивирусной защиты. Этот этап является ключевым в обеспечении безопасности корпоративной системы.

Регулярный мониторинг всех элементов защиты позволяет администратору максимально быстро выявить проблему на одной компьютере, исключая ее переход на следующие устройства. Отличие

персональных антивирусных программ от корпоративных решений заключается именно в возможности централизованного мониторинга и администрирования. Даже в небольших сетях такая возможность необходима для обеспечения безопасности. Ранее было обосновано использование средств антивирусной защиты Kaspersky Internet Security. Однако, существуют разные версии и комплектации программного обеспечения Kaspersky. Обоснуем выбор конкретного продукта. Для этого проведем сравнительный анализ. Результаты сравнения приведены в таблице 8.

Таблица 8

Сравнительный анализ продуктов KIS

Тип защищаемого узла сети	Kaspersky Security для предприятия				Защита отдельных узлов сети				
	Стартовый	Стандартный	Расширенный	Total	KIS для почтовых серверов	Kaspersky Systems Management	KIS для интернет-шлюзов	KIS для серверов совме/работы	KIS для вирт. сред
Рабочие станции	+	+	+	+					
Файловые серверы		+	+	+					
Мобильные устройства		+	+	+					
Системное Администрирование			+	+		+			
Серверы совм. работы				+				+	
Почтовые серверы				+	+				
Интернет-шлюзы				+			+		
Виртуальная инфраструктура									+

На основе данного сравнительного анализа был выбран пакет «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.

Также Kaspersky Endpoint Security (версии 8 и 10) является сертифицированным антивирусным средством защиты.

При наличии действующей лицензии достаточно приобрести только один сертифицированный установочный комплект (стоимость от 900 до 2500 руб).

Качественная установка и настройка системы защиты локальной сети от вирусов в колледже является непростой задачей, требующей вовлечения профессионального IT-инженера. Ведь услуга комплексной антивирусной защиты обеспечивает образовательной организации надежность и высокую безопасность функционирования информационных систем, гарантированно снижая риски вирусного заражения компьютерных систем организации.

Межсетевые экраны

Межсетевой экран (МЭ) представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в ИС и/или выходящей из ИС, и обеспечивает защиту ИС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) ИС.

Функция МЭ –защита от несанкционированного доступа по компьютерной сети.

Устанавливается 5 классов защищенности МЭ, самый низкий класс защищенности – пятый.

Сценарии использования:

1. Защита клиент-серверных и многозвенных ИСПДн (рис. 4):

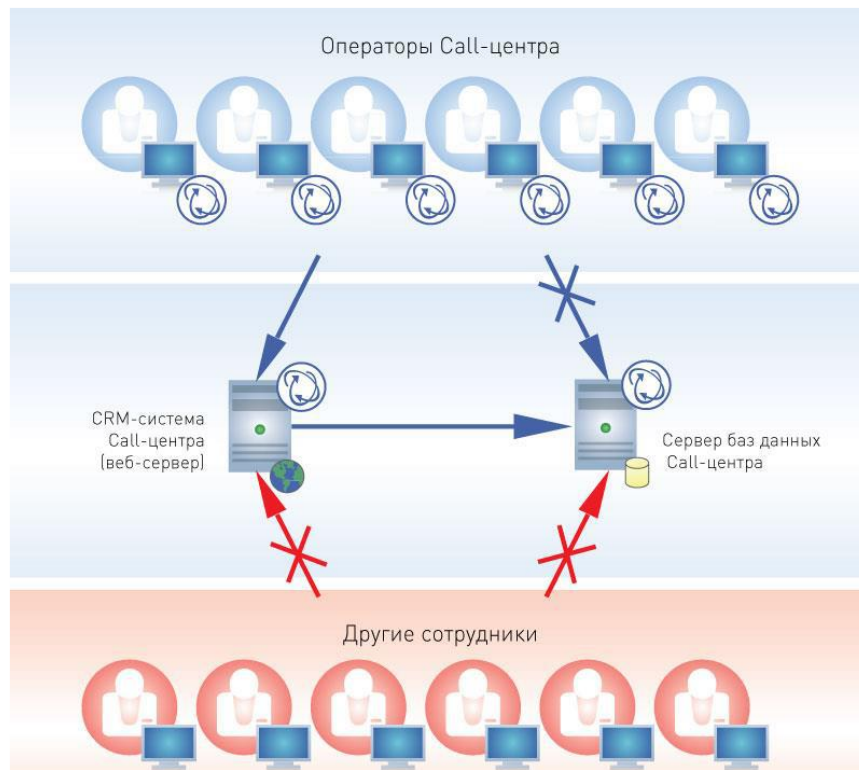


Рис. 4. - Защита клиент-серверных и многозвенных ИСПДн

2. Разграничение доступа к файл-серверу на уровне общих папок (рис. 5):

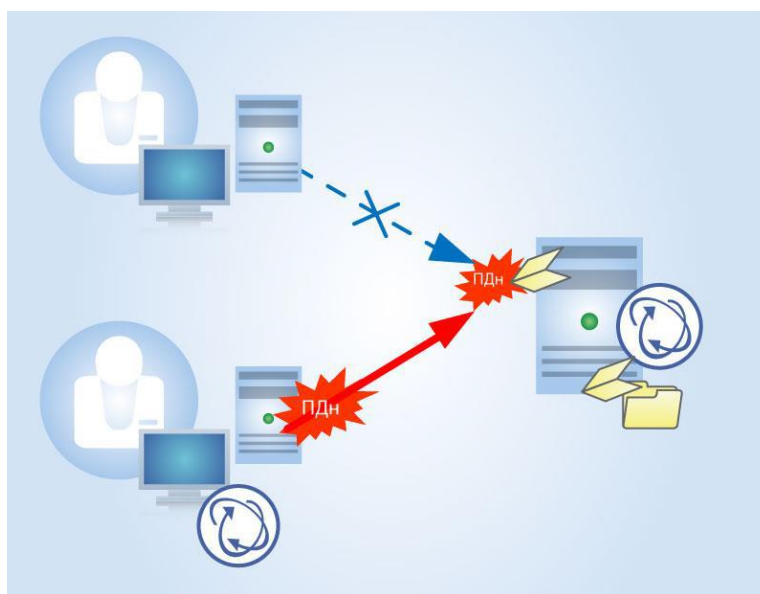


Рис. 5. – Разграничение доступа к файл-серверу

3. Разграничения доступа пользователей к серверам (рис. 6):

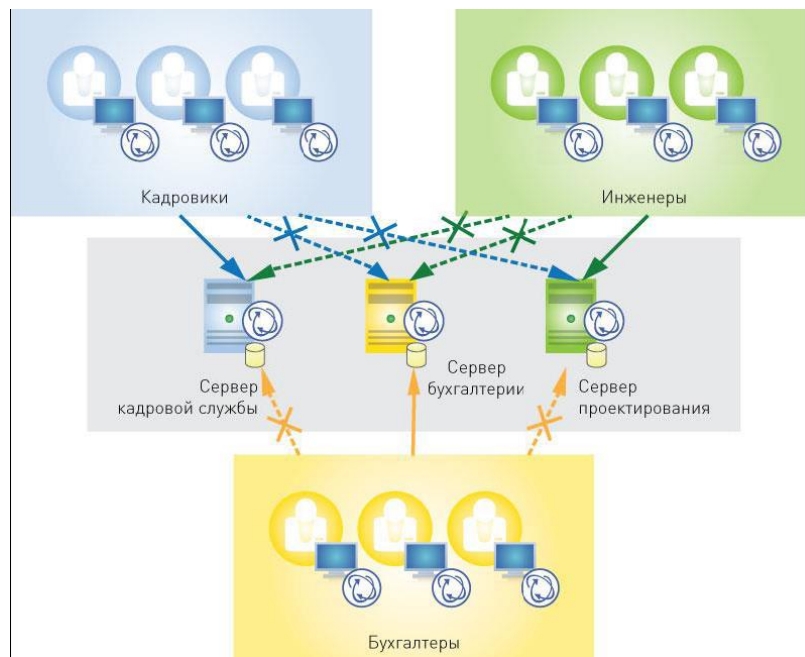


Рис. 6. – Разграничения доступа пользователей к серверам

4. Защита терминальных соединений (рис. 7):

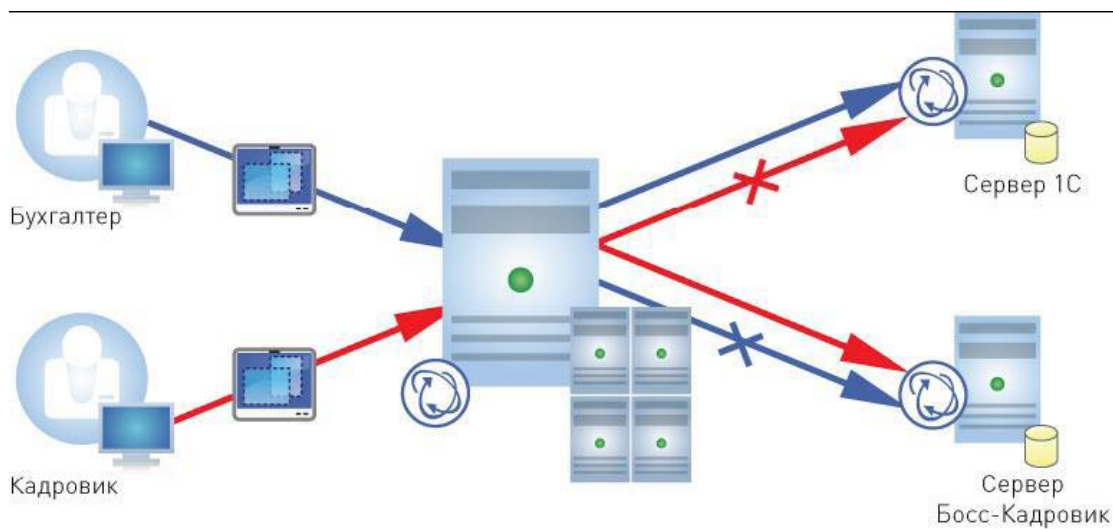


Рис. 7. – Защита терминальных соединений

Требования к МЭ для ИСПДн (согласно Приказам ФСТЭК) представлены на рисунке 8.

Тип межсетевого экрана	Класс защиты					
	6	5	4	3	2	1
Межсетевой экран типа «А»	ИТ.МЭ. А6.ПЗ	ИТ.МЭ. А5.ПЗ	ИТ.МЭ. А4.ПЗ	ИТ.МЭ. А3.ПЗ	ИТ.МЭ. А2.ПЗ	ИТ.МЭ. А1.ПЗ
Межсетевой экран типа «Б»	ИТ.МЭ. Б6.ПЗ	ИТ.МЭ. Б5.ПЗ	ИТ.МЭ. Б4.ПЗ	ИТ.МЭ. Б3.ПЗ	ИТ.МЭ. Б2.ПЗ	ИТ.МЭ. Б1.ПЗ
Межсетевой экран типа «В»	ИТ.МЭ. В6.ПЗ	ИТ.МЭ. В5.ПЗ	ИТ.МЭ. В4.ПЗ	ИТ.МЭ. В3.ПЗ	ИТ.МЭ. В2.ПЗ	ИТ.МЭ. В1.ПЗ
Межсетевой экран типа «Г»	ИТ.МЭ. Г6.ПЗ	ИТ.МЭ. Г5.ПЗ	ИТ.МЭ. Г4.ПЗ	-	-	-
Межсетевой экран типа «Д»	ИТ.МЭ. Д6.ПЗ	ИТ.МЭ. Д5.ПЗ	ИТ.МЭ. Д4.ПЗ	-	-	-

Рис. 8. – Требования к МЭ для ИСПДн

Используемые средства защиты от НСД:

Программные:

- DallasLock с модулем «Межсетевой экран»;
- Secret Net Studio с модулем персонального межсетевого экрана;
- ViPNet Client.

Программные (прокси):

- Трафик Инспектор 3.0;
- Ideco ICS 6.

Программно-аппаратные (шлюзы):

- ПАК ViPNet Coordinator HW;
- АПКШ «Континент»;
- ПАК МЭ «Застава».

В качестве межсетевого экрана для совершенствования защиты информации была выбрана программа ViPNet Client. 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.

ViPNet Client поддерживает работу на компьютерных устройствах под управлением ОС Microsoft Windows, Linux и OS X.

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)

Шифровальные (криптографические) средства:

а) средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты–аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи –аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой

подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

Криптопровайер —это предоставляющая специальный API и специальным образом зарегистрированная в операционной системе библиотека, которая позволяет расширить список поддерживаемых в ОС криптоалгоритмов. Посредник между операционной системой, которая может управлять им с помощью стандартных функций CryptoAPI, и исполнителем криптографических операций (программа, аппаратный комплекс).

Применяемый алгоритм шифрования ГОСТ 28147-89.

Сценарий использования: защищенная сеть на базе VipNet представлена на рисунке 9.



Рис. 9. - Защищенная сеть на базе VipNet

Требования к СКЗИ для ИСПДн (согласно требованиям ФСБ) представлены в таблице 9.

Требования к СКЗИ для ИСПДн

Тип нарушителя	Н1	Н2	Н3	Н4	Н5	Н6
Класс СКЗИ	КС1	КС2	КС3	КВ1	КВ2	КА1

№ п/п	СКЗИ сертифицированные	Уровни защищенности ПДн			
		IV	III	II	I
1	Классы средств криптографической защиты информации (СКЗИ)	Класс КС1 и выше	Класс КС1 и выше (актуальные угрозы 3-го типа) класс КВ и выше (актуальные угрозы 2-го типа)	Класс КС1 и выше (актуальные угрозы 3-го типа) класс КВ и выше (актуальные угрозы 2-го типа) Класс КА (актуальные угрозы 1-го типа)	Класс КА (актуальные угрозы 1-го типа) Класс КВ и выше (актуальные угрозы 2-го типа)

Для совершенствования СКЗИ был выбран 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).

Таким образом, для ГБПОУ «ЮУрГТК» были предложены следующие меры по совершенствованию защиты конфиденциальной информации:

I. Организационные меры защиты информации

В колледже обновлены и доработаны документы, регламентирующие вопросы обеспечения информационной безопасности. Организационно-административные меры защиты информации позволят избежать части непреднамеренных угроз, а также преднамеренных угроз безопасности информации со стороны работников колледжа.

Кроме того, жесткий регламент обращения с информационными ресурсами дисциплинирует коллектив, приучает их более внимательно работать с данными и относиться к ней как к ценному ресурсу.

II. Технические меры защиты информации

Закуплены и установлены сейфы для хранения конфиденциальной и внутренней информации.

III. Программные меры защиты информации.

В колледже есть потребность организации комплексной антивирусной защиты. На основе анализа было выбрано программное средство «Kaspersky Endpoint Security для бизнеса расширенный». Наиболее удобной будет такая система антивирусной защиты: на сервере устанавливается антивирус-сервер, а на рабочих местах – клиентские приложения, работой которых управляет сервер. Это сравнительно недорогое решение, а главное, что администратор сможет управлять проверкой всех компьютеров с сервера.

Кроме того, спланирована установка системы Dallas Lock 8.0-C., СКЗИ ViPNet CSP 4.2, межсетевой экран ViPNet Client, которые обеспечат комплексное решение проблем обеспечения безопасности информации. Выполнено разграничение доступа к документам на сервере, определено выделение разного количества трафика разным группам пользователей интернета, а также определение некоторого набора ресурсов, к которым можно получить доступ.

3.2. Расчет экономической эффективности мероприятий по защите конфиденциальной информации

Оценка эффективности является важным элементом разработки проектных и плановых решений, позволяющим определить уровень прогрессивности действующей структуры, разрабатываемых проектов или плановых мероприятий и проводится с целью выбора наиболее рационального варианта структуры или способа ее совершенствования. Эффективность защитных мероприятий (ЗМ) должна оцениваться на стадии проектирования, для получения наилучших показателей работоспособности системы в целом.

При разработке проекта важны экономические показатели, которые наряду с техническими результатами будут определять эффективность системы. В состав затрат на разработку и исследование включаются затраты на проведение всех этапов работ.

Затраты на обеспечение информационной безопасности следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной безопасности организации.

Совокупная стоимость владения для системы ИБ в общем случае складывается из стоимости: проектных работ; закупки и настройки программно-технических средств защиты, включающих следующие основные группы: межсетевые экраны, средства криптографии, антивирусы и

AAA (средства аутентификации, авторизации и администрирования); затрат на обеспечение физической безопасности; обучения персонала; управления и поддержки системы (администрирование безопасности); аудита ИБ; периодической модернизации системы ИБ [8].

При этом затраты на приобретение и ввод в действие программно-технических средств могут быть получены из анализа накладных, записей в складской документации и т.п.

Величина выплат сотрудникам может быть взята из ведомостей. Объемы выплат заработной платы должны учитывать реально затраченное время на проведение работ по обеспечению информационной безопасности.

Суммарно ежегодные затраты на информационную безопасность складываются из трех показателей: затраты на административно-организационные мероприятия; затраты на технические мероприятия; затраты на ликвидацию последствий.

Затраты на административно-организационные мероприятия (АОМ) в организациях профессионального обучения обычно меньше затрат на технические средства (таблица 10).

Таблица 10

Расходы на предложенные АОМ по защите конфиденциальной информации в колледже

Мероприятие	Бюджет
Система поощрений сотрудников за соблюдение правил в области защиты ИР в ИСПДн (АИС) (500 руб. /в мес)	10000 руб.
Комплекс профилактических мер по соблюдению сотрудниками требований по ИБ (1000 руб. / в мес)	10000 руб.
Плановая проверка и обслуживание всех информационных систем и информационной инфраструктуры на работоспособность (1000 руб. / в мес)	12000 руб.
Всего: 30000 руб. в год	Всего: 32000 руб. в год

Суммарно расходы на административно-организационные мероприятия по повышению эффективности защиты информации в ГБПОУ «ЮУрГТК» составят 32000 рублей.

Предварительные расходы на программно-аппаратные средства в ГБПОУ «ЮУрГТК» представлены в таблице 11.

Таблица 11

Расходы на предложенные программно-аппаратные средства по защите информации

Мероприятие	Бюджет
Установка DALLASLOCK 8.0 – К - 4 500, 00 руб. (1 лицензия, 1 экз. на 1 рабочее место).	40000 руб.
Создание защищенной виртуальной частной сети, которая соответствует заявленным требованиям (750 руб. / мес.)	10000 руб.
Установка СКЗИ программного комплекса ViPNet Client 4 (1 канал на 1 рабочее место) (7000 руб.)	15000 руб.
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	5000 руб.
Всего: 33000 руб. в год	Всего: 70000 руб.

Суммарно расходы на программно-аппаратные средства по повышению эффективности защиты конфиденциальной информации в ГБПОУ «ЮУрГТК» составят 70 тысяч рублей.

Рассчитаем отдачу от инвестиций на административно-организационные мероприятия и программно-аппаратные средства защиты конфиденциальной информации в ГБПОУ «ЮУрГТК» по формуле (1.1)

$$rosi(t, aom) = \frac{\Delta \text{Доходы} - \Delta \text{Расходы}}{\Delta \text{Инвестиции}}$$

где $rosi(t, aom)$ - отдача от инвестиций на программно-аппаратные средства и административно-организационные меры, $\Delta \text{ Доходы}$ - изменения в доходах, обусловленные инвестициями ИБ (возможных поступлений средств от предотвращенных потерь), $\Delta \text{ Расходы}$ - изменения в расходах, обусловленные инвестициями ИБ, $\Delta \text{ Инвестиции}$ - инвестиции, сделанные в информационную безопасность.

$$rosi(t) = \frac{250000 - 33000}{70000} \approx 3,1$$

$$rosi(aom) = \frac{250000 - 30000}{32000} \approx 6,8$$

Далее, вычислим показатель отдачи от инвестиций в информационную безопасность после внедрения изменений в систему ИБ по формуле (1.2)

$$ROSI(t, aom) = ROSIold \frac{Iold - \Delta \text{ Расходы}}{Iold + \Delta I} + rosi(t, aom) \frac{\Delta I}{Iold + \Delta I}$$

где $ROSI(t, aom)$ - показатель отдачи от инвестиций в информационную безопасность после внедрения программно-аппаратных средств и административно-организационных изменений в систему ИБ, $ROSIold$ - показатель отдачи от инвестиций до внесения изменений в систему ИБ, $Iold$ - уже сделанные инвестиции, $\Delta \text{ Расходы}$ - изменения в расходах, обусловленные инвестициями ИБ, $rosi(t, aom)$ - отдача от инвестиций на программно-аппаратные средства и административно-организационные меры.

$$ROSI(t) = 2,55 \frac{0 - 33000}{0 + 70000} + 2,05 \frac{70000}{0 + 70000} \approx 0,8$$

$$ROSI(aom) = 4,73 \frac{0 - 30000}{0 + 32000} + 3,5 \frac{32000}{0 + 30000} \approx -0,7$$

В обоих случаях, видно, что $rosi(t, aom) > ROSI(t, aom)$, следовательно, внедрение проекта приведет к увеличению ROSI в ГБПОУ «ЮУрГТК» (в ИБ).

Итак, в результате анализа совокупных показателей существует возможность сделать обоснованный выбор в пользу предложенных

мероприятий по совершенствованию защиты конфиденциальной информации колледжа.

Таким образом, предложенные мероприятия по совершенствованию защиты конфиденциальной информации колледжа несут в себе не только положительные моменты, такие как устранение основных проблем в организации среднего профессионального образования, касающихся информационной безопасности, но при этом они потребуют дополнительных вложений на разработку нормативных документов, касающихся политики безопасности. Потребуется дополнительных затрат труда и не исключат стопроцентно риски.

Всегда будет иметь место человеческий фактор, форс-мажорные обстоятельства. Но если такие меры не предпринять затраты на восстановление информации, потерянные возможности по стоимости превзойдут те затраты, что требуются для разработки системы безопасности.

Выводы по Главе III

В третьей главе магистерской диссертации в соответствии с оценкой существующих средств защиты конфиденциальной информации в ГБПОУ «ЮУрГТК» были предложены рекомендации по совершенствованию защиты конфиденциальной информации, в результате выполнения которых колледж позволит повысить эффективность средств защиты и сократит риск потери и искажения информации. Следует обратить внимание на то, что только при совместном взаимодействии сотрудников, программно-аппаратных средств и организационных мер по защите информации возможна эффективность данных мероприятий.

Согласно требованиям ФСТЭК России №21 были разработаны мероприятия по совершенствованию системы информационной безопасности колледжа, которая состоит из:

1. Комплекс организационных мер обеспечения информационной безопасности колледжа, разработка частной модели угроз.
2. Комплекс проектируемых программно-аппаратных средств обеспечения информационной безопасности колледжа.

Для ГБПОУ «ЮУрГТК» были предложены следующие меры по совершенствованию защиты конфиденциальной информации:

I. Организационные меры защиты информации

В колледже обновлены и доработаны документы, регламентирующие вопросы обеспечения информационной безопасности. Организационно-административные меры защиты информации позволят избежать части непреднамеренных угроз, а также преднамеренных угроз безопасности информации со стороны работников колледжа.

Кроме того, жесткий регламент обращения с информационными ресурсами дисциплинирует коллектив, приучает их более внимательно работать с данными и относиться к ней как к ценному ресурсу.

II. Технические меры защиты информации

Закуплены и установлены сейфы для хранения конфиденциальной и внутренней информации.

III. Программные меры защиты информации.

В колледже есть потребность организации комплексной антивирусной защиты. На основе анализа было выбрано программное средство «Kaspersky Endpoint Security для бизнеса расширенный». Наиболее удобной будет такая система антивирусной защиты: на сервере устанавливается антивирус-сервер, а на рабочих местах – клиентские приложения, работой которых управляет сервер. Это сравнительно недорогое решение, а главное, что администратор сможет управлять проверкой всех компьютеров с сервера.

Кроме того, спланирована установка системы Dallas Lock 8.0-С., СКЗИ ViPNet CSP 4.2, межсетевой экран ViPNet Client, которые обеспечат комплексное решение проблем обеспечения безопасности информации.

Проведен расчет экономической эффективности мероприятий по защите конфиденциальной информации в ГБПОУ «Южно-Уральский государственный технический колледж».

В результате анализа совокупных показателей существует возможность сделать обоснованный выбор в пользу предложенных мероприятий по совершенствованию защиты конфиденциальной информации колледжа.

Таким образом, предложенные мероприятия несут в себе не только положительные моменты, такие как устранение основных проблем в организации среднего профессионального образования, касающихся информационной безопасности, но при этом они потребуют дополнительных вложений на разработку нормативных документов, касающихся политики безопасности и закупку, и установку программно-аппаратных средств защиты.

Заключение

Внедрение системы информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности. Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, а также определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим определённую степень ценности.

Обеспечение информационной безопасности - комплексная задача, потому что сама информационная среда есть сложный и многоплановый механизм, где могут присутствовать такие компоненты, как сотрудники, электронное оборудование, программное обеспечение и т.д.

Для решения многих проблем обеспечения информационной безопасности необходимо применение следующих мер: законодательных, организационных и программно-технических. Игнорирование хотя бы одного из аспектов этой проблемы может привести к потере (утечке) информации, которая в жизни современного общества приобретает всё более важное значение и играет немаловажные роли.

Организационные меры обеспечения защиты информации являются первоочередными, т.к. они призваны обеспечить эффективное функционирование остальных мер обеспечения конфиденциальности информации. С этой точки зрения организационные меры являются первичными по отношению к остальным мерам.

Все документы должны пройти согласование с юридической службой образовательной организации, утверждены руководством колледжа и введены в действие приказом по колледжу. При этом необходимо также учитывать, что документы должны соответствовать законам и другим правовым документам РФ в этой области, так как

на работников накладываются определённые ограничения и ответственность, вплоть до уголовной, за нарушения правил работы с конфиденциальной информацией.

По результатам анализа объекта защиты и обзора технических средств разработаны рекомендации по совершенствованию защиты конфиденциальной информации.

Предпринимаемые меры защиты должны быть адекватны вероятности осуществления данного типа угрозы и потенциальному ущербу, который может быть нанесен в том случае, если угроза осуществится (включая затраты на защиту от нее).

В процессе работы были рассмотрены теоретические и законодательные основы организации защиты конфиденциальной информации в организации профессионального образования, проанализирована специфика их защиты в современных условиях, дана краткая характеристика объекту исследования (ГБПОУ «Южно-Уральский государственный технический колледж»), произведена оценка существующих средств защиты конфиденциальной информации, выявлены уязвимости и риски в системе защиты информации колледжа, разработана частная модель угроз, разработаны рекомендации по совершенствованию защиты конфиденциальной информации и произведен расчет экономической целесообразности предлагаемых мероприятий.

Согласно требованиям ФСТЭК России №21 были разработаны мероприятия по совершенствованию системы информационной безопасности колледжа, которая состоит из:

3. Комплекс организационных мер обеспечения информационной безопасности колледжа, разработка частной модели угроз.

4. Комплекс проектируемых программно-аппаратных средств обеспечения информационной безопасности колледжа.

Для ГБПОУ «ЮУрГТК» были предложены следующие меры по совершенствованию защиты конфиденциальной информации:

I. Организационные меры защиты информации

В колледже обновлены и доработаны документы, регламентирующие вопросы обеспечения информационной безопасности. Организационно-административные меры защиты информации позволят избежать части непреднамеренных угроз, а также преднамеренных угроз безопасности информации со стороны работников колледжа.

Кроме того, жесткий регламент обращения с информационными ресурсами дисциплинирует коллектив, приучает их более внимательно работать с данными и относиться к ней как к ценному ресурсу.

II. Технические меры защиты информации

Закуплены и установлены сейфы для хранения конфиденциальной и внутренней информации.

III. Программные меры защиты информации.

В колледже есть потребность организации комплексной антивирусной защиты. На основе анализа было выбрано программное средство «Kaspersky Endpoint Security для бизнеса расширенный». Наиболее удобной будет такая система антивирусной защиты: на сервере устанавливается антивирус-сервер, а на рабочих местах – клиентские приложения, работой которых управляет сервер. Это сравнительно недорогое решение, а главное, что администратор сможет управлять проверкой всех компьютеров с сервера.

Кроме того, спланирована установка системы Dallas Lock 8.0-С., СКЗИ ViPNet CSP 4.2, межсетевой экран ViPNet Client, которые обеспечат комплексное решение проблем обеспечения безопасности информации.

Проведен расчет экономической эффективности мероприятий по защите конфиденциальной информации в ГБПОУ «Южно-Уральский государственный технический колледж».

В результате анализа совокупных показателей существует возможность сделать обоснованный выбор в пользу предложенных мероприятий по совершенствованию защиты конфиденциальной информации колледжа.

Таким образом, предложенные мероприятия несут в себе не только положительные моменты, такие как устранение основных проблем в организации среднего профессионального образования, касающихся информационной безопасности, но при этом они потребуют дополнительных вложений на разработку нормативных документов, касающихся политики безопасности и закупку, и установку программно-аппаратных средств защиты.

В заключение хотелось бы подчеркнуть, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам информационной безопасности в образовательной организации СПО.

Список использованной литературы

1. Аверченков, В. И. Организационная защита информации [Текст]: учеб. пособие / В. И. Аверченков, М. Ю. Рытов. – Брянск: БГТУ, 2014. – 184 с.
2. Ажмухамедов, И.М., Ханжина, Т.Б. Определение оптимального комплекса мер по обеспечению информационной безопасности [Текст] / И.М. Ажмухамедов, Т.Б. Ханжина // Мат. методы в технике и технологиях – ММТТ-24: сб. трудов XXII Междунар. науч. конф.: в 10 т. Т.9. Секция 13 / под общ. ред. В.С Балакирева. Саратов: Изд-во Саратовского гос. технического университета, 2011. 187с., С.73-75.
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. Анализ рисков в управлении информационной безопасностью [Электронный ресурс]. – URL: <http://www.iso27000.ru/>. Дата обращения: 12.01.2019.
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]: [Утверждена заместителем директора ФСТЭК РФ 15.02.2008 г.]. - Режим доступа: www.fstec.ru. Дата обращения: 15.01.2019.
6. Богатырева, Ю.И. Информационная безопасность образовательных организаций: проблема и пути ее решения [Текст] / Ю.И. Богатырева // Новые информационные технологии в образовании, IX международной научно-практической конференции. 2016 Издательство: Российский государственный профессионально-педагогический университет (Екатеринбург), с. 125-130.
7. Галатенко, В.А. Основы информационной безопасности [Текст] / В.А. Галатенко. - М.: Интуит, 2013.

8. Галкин, Г.А. ROI — до мелочей. Цена времени [Текст] / Г.А. Галкин. – URL: <http://www.iemag.ru/master-class/detail.php?ID=15691>. Дата обращения: 16.02.2019.

9. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 9 с.

10. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 7 с.

11. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности. Основные термины и определения. – URL: http://www.opengost.ru/iso/35_gosty_iso/35020_gost_iso/11522-gost-r-53114-2008-zaschita-informacii.-obespechenie-informacionnoy-bezopasnosti.-osnovnyie-terminy-i-opredeleniya.html. Дата обращения: 16.12.2018.

12. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.

13. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

14. ГОСТ Р ИСО/МЭК ТО 13335-3-2007. [Электронный ресурс]. – URL: http://www.opengost.ru/iso/13_gosty_iso/13110_gost_iso/4958-gost-r-iso_mek-to-13335-3-2007-it.-metody-i-sredstva-obespecheniya-bezopasnosti.-chast-3.-metody-menedzhmenta-bezopasnosti-informacionnyh-tehnologiy.html. Дата обращения: 16.02.2019.

15. Гражданский кодекс РФ ст.139. [Электронный ресурс]. – URL: <http://www.grazkodeks.ru/>. Дата обращения: 26.12.2018.

16. Давлетханов, М.А. Оценка затрат компании на ИБ [Текст] / М.А. Давлетханов. – URL: <http://www.getinfo.ru/article682.html>. Дата обращения: 05.02.2019.

17. Дворчук, О.И. Показатели экономической эффективности ИТ-проектов [Текст] / О.И. Дворчук. – URL:

http://security.ase.md/publ/ru/pubru107/Dvorciuk_O.pdf. Дата обращения: 16.02.2019.

18. Доктрина информационной безопасности Российской Федерации, № Пр-1895 от 9 сентября 2000 г.

19. Домарев, В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – Киев: «ГИД», 2012. – 912 с.

20. Ефимов Е. Н., Лапицкая Г. М. Оценка эффективности мероприятий информационной безопасности в условиях неопределенности // Бизнес-информатика. 2015. №1 (31). URL: <https://cyberleninka.ru/article/n/otsenka-effektivnosti-meropriyatiy-informatsionnoy-bezopasnosti-v-usloviyah-neopredelennosti>. Дата обращения: 15.02.2019.

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

22. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» // «Российская газета», № 182, 21.09.1993.

23. Зегжда, Д.П. Основы безопасности информационных систем [Текст]: учеб. пособие для вузов / Д. П. Зегжда, А. М. Ивашко. - М.: Горячая линия Телеком, 2000. - 452 с.

24. Иващенко, Г.В. Доктрина информационной безопасности и методические проблемы теории безопасности [Текст] / Г.В. Иващенко. // Материалы круглого стола «Глобальная информатизация и социально-гуманитарные проблемы человека, культуры, общества», МГУ, октябрь 2000 г. С. 48 — 63.

25. Изменения в Законе о персональных данных Электронный документ. - URL: https://yuridicheskaya-konsultaciya.ru/trudovoe_pravo/zakon-o-personalnyh-dannyh.html. Дата обращения: 16.12.2018.

26. Концепция обеспечения информационной безопасности предприятия [Электронный ресурс]. - Режим доступа: www.securitypolicy.ru. Дата обращения: 12.05.2017.

27. Курносов, Ю.В., Конотопов, П.Ю. Аналитика: методология, технология и организация информационно-аналитической работы [Текст] / Ю.В. Курносов, П.Ю. Конотопов. – М.: Издательство «Русаки», 2014.

28. Кустов Г.А. Управление информационными рисками организации на основе логико-вероятностного метода: автореф. дис. канд. тех. наук. – Уфа, 2008. – 18 с.

29. Малюк, А.А. Введение в защиту информации в автоматизированных системах [Текст] / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М.: Горячая линия-Телеком, 2012. – 148 с.

30. Международный стандарт ИСО/МЭК 27001. Первое издание 2005-10-15. Информационные технологии. Методы защиты. Системы менеджмента защиты информации.

31. Мельников, В.П. Информационная безопасность и защита информации [Текст]: учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М.: Издательский центр «Академия», 2013. – 336 с.

32. Меры по защите от угроз нарушения доступности [Электронный ресурс]. - URL: www.sha-danis.narod.ru. Дата обращения: 20.12.2018.

33. 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/>

34. 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.

35. 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.).

36. 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.

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

38. 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.

39. Милютин О.В. Особенности защиты информации в образовательном учреждении [Текст] / О.В. Милютин. – URL: http://www.fcoit.ru/internet_conference/information_security_training_process/features_information_security_in_an_educational_institution.php. Дата обращения: 10.12.2018.

40. Модели угроз информационной безопасности [Электронный ресурс]. - Режим доступа: www.arinteg.ru. Дата обращения: 19.12.2018.

41. 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.

42. 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.

43. 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.

44. 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.

45. Организационное обеспечение информационной безопасности [Электронный ресурс]. - Режим доступа: www.starik2222.narod.ru. Дата обращения: 12.01.2019.

46. Организационные основы защиты информации на предприятии [Электронный ресурс]. - Режим доступа: www.безопасник.рф. Дата обращения: 20.01.2019.

47. Официальный сайт ГБПОУ «Южно-Уральский государственный технический колледж». – URL: <http://sustec.ru/>

48. Оценка информационной безопасности в деятельности организаций. Способы оценки информационной безопасности [Текст]. – URL: <http://www.pvsm.ru/informatsionnaya-bezopasnost/19741>. Дата обращения: 15.02.2019.

49. Петренко, С.А., Симонов, С.В., Кислов, Р.И. Информационная безопасность: экономические аспекты [Текст] / С.А. Петренко, С.В. Симонов, Р.И. Кислов. – URL: <http://citforum.ru/security/articles/sec/index.shtml>. Дата обращения: 12.01.2019.

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

51. 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».

52. 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/>.

53. 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/>.

54. Постановление Правительства РФ от 06.07.2008 № 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 06.07.2008 № 512 // «Российская газета», № 148, 11.07.2008.

55. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // «Российская газета», № 200, 24.09.2008.

56. 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.

57. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ России и Министерства связи и массовых коммуникаций РФ

от 31 декабря 2013 г. № 151/786/461 «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». - Режим доступа: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/815-sovmestnyj-prikaz-fstek-rossii-fsb-rossii-i-minkomsvyazi-rossii-ot-31-dekabrya-2013-g-n-151-786-461>.

58. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Составы 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

59. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // «Российская газета», № 107, 22.05.2013.

60. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]: [Утвержден решением председателя Гостехкомиссии при Президенте РФ 30.03.1992 г.]. - Режим доступа: www.consultant.ru. Дата обращения: 17.04.2017.

61. Сидоров, А.О. Модель и метод структурированной оценки риска при анализе информационной безопасности [Текст]: диссертация ... кандидата технических наук: 05.13.19 / А.О. Сидоров; [Место защиты: С.-Петербург. гос. ун-т информац. технологий, механики и оптики]. - Санкт-Петербург, 2008. - 134 с.

62. Сорокин, М. Комплексная система обеспечения информационной безопасности (КСОИБ) [Текст] / М. Сорокин. - URL: <http://www.keysystems.ru/products/ProtectInf/ksoib/>. Дата обращения: 15.12.2017.

63. Специальные требования и рекомендации по технической защите конфиденциальной информации [электронный ресурс]. — URL: http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTЕК_requirements.htm. Дата обращения: 15.04.2017.

64. Стандарты информационной безопасности. – URL: <https://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html>. Дата обращения: 20.05.2017.

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

66. Структура системы защиты информации от угроз нарушения целостности [Электронный ресурс]. - URL: www.shadanis.narod.ru. Дата обращения: 20.04.2017.

67. Тронилов, И.Б. Методы оценки информационной безопасности предприятия на основе процессного подхода [Текст]: диссертация ... кандидата технических наук: 05.13.19 / И.Б. Тронилов; [Место защиты: С.-Петербург. гос. ун-т информац. технологий, механики и оптики]. - Санкт-Петербург, 2010. - 134 с.

68. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 19.07.2011)/

69. Шиляев, С. Методика оценки рисков информационной безопасности / С. Шиляев. – URL: <https://kontur.ru/articles/1691/>. Дата обращения: 15.01.2019.

70. Ярочкин, В. И. Словарь терминов и определений по безопасности и защите информации [Текст] / В.И. Ярочкин, Т.А. Ильещова. – М.: «Ось-99», 2011. – 48 с.

Приложение

Приложение 1