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

Разработка методики анализа и оценки угроз информационной безопасности для образовательной организации

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,
Иванова Ирина Юрьевна
Научный руководитель:
д.т.н., профессор
кафедры АТ, ИТ и МОТД
Белевитин Владимир Анатольевич

Проверка на объём заимствований:
68,18 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 Ивановой Ирине Юрьевне, обучающейся по программе магистратуры «Управление информационной безопасностью в профессиональном образовании».

Научный руководитель выпускной квалификационной работы: Белевитин В.А., д.т.н., профессор кафедры АТ, ИТ и МОТД.

1.Тема квалификационной работы: «Разработка методики анализа и оценки угроз информационной безопасности для образовательной организации», 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 «ЮУГК», 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. Современные угрозы информационной безопасности в образовательной организации Выводы по главе 1	16.10.2017
3	Глава 2. Нормативно-правовая документация в области управления рисками информационной безопасности в образовательной организации Выводы по главе 2	23.04.2018
4	Глава 3. Разработка методики оценки риска угроз информационной безопасности ГБПОУ «Южно-Уральский государственный колледж 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 (сначала располагаются нормативно – законодательные акты, остальные источники в алфавитном порядке). Законы и нормативные акты, справочно-статистические материалы, монографии, учебники, сборники брошюры, статьи из периодической печати, иностранная литература.	29.12.2018
7	ПРЕЗЕНТАЦИЯ (НАГЛЯДНЫЕ МАТЕРИАЛЫ) предоставляется в виде слайдов рекомендаций Microsoft PowerPoint, 10-12 слайдов, раскрывающих содержание магистерской диссертации, либо схемы, таблицы, графики, диаграммы в виде раздаточного материала	28.01.2019
	ПРЕДВАРИТЕЛЬНАЯ ЗАЩИТА	28.01.2019
	СДАЧА МАГИСТЕРСКОЙ ДИССЕРТАЦИИНА КАФЕДРУ	18.02.2019

Дата выдачи задания «27»__апреля__ 2017 года

Заведующий кафедрой АТ, ИТ и МОТД
Наименование кафедры

_____
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
Ивановой Ирины Юрьевны

Тема магистерской диссертации «Разработка методики анализа и оценки угроз информационной безопасности для образовательной организации».

Магистерская диссертация содержит 79 страниц, 11 таблиц, 2 рисунка, 61 источник литературы.

Ключевые слова: угроза, защита информации, методы анализа и оценки угроз, информационная безопасность

Объектом исследования является защитные меры информационных систем, создающих, хранящих и обрабатывающих информацию, важную с точки зрения обеспечения ее конфиденциальности, целостности и доступности.

Цель магистерской диссертации – анализ информационно-телекоммуникационной инфраструктуры образовательно организации и оценка рисков, определяющая основные характеристики рисков информационной системы и ресурсов образовательной организации.

В процессе исследования изучены теоретические аспекты: изучены виды угроз информационной безопасности в образовательной организации и их характеристики; выявлены угрозы, уязвимости и риски в системе защиты информации образовательной организации. Приведено описание международных стандартов управления информационной безопасностью, а также Методика ФСТЭК определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

В результате проведенного исследования разработана методика оценки риска угроз, которая позволит повысить качество выбора защитных мер для информационной системы образовательной организации и может быть реализованы в виде модуля управления рисками безопасности информационной системы.

Магистрант _Иванова Ирина Юрьевна_ _____
(Ф.И.О.) Подпись

Оглавление

Введение

Актуальность исследования. Высокие требования к обеспечению безопасности и надежности информационных систем (ИС), обусловленные характером решаемых задач, а также регулярные изменения информационной среды, требуют тщательного подхода к формированию и постоянному совершенствованию системы защиты информации (СЗИ) информационных систем, состоящей из комплекса технических и организационных защитных мер.

В современных условиях, когда информационные системы пронизывают все сферы деятельности организации, а с учётом необходимости их связи с сетью Интернет они оказываются открытыми для реализации внутренних и внешних угроз, проблемы информационной безопасности становится не менее важной чем экономическая или физическая безопасность.

Основное предназначение информационных систем заключается в повышении эффективности деятельности образовательной организации, следовательно, формируемый комплекс защитных мер для ИС должен быть рациональным с точки зрения выгод и затрат.

Актуальность темы исследования следует из указанной выше необходимости рационального выбора защитных мер для ИС, осуществляемого на основе оценки угроз, возникающих при этом трудностей и противоречий, а также возможностей по совершенствованию применяемых на практике методов и моделей оценки угроз.

Основные теоретические аспекты проблемы оценки рисков и выбора защитных мер для информационных и автоматизированных систем и компьютерных сетей отражены в работах А.Н. Атаманова, Е.В. Дойниковой, И.А. Зикратова, Д.А. Котенко, И.В. Котенко, И.В. Машкиной, А.Г. Остапенко, И.Б. Саенко, Р.М. Юсупова, H. Joh, X. Ou, N. Poolsappasit, I. Ray, A. Singhal.

Разработано большое количество нормативных документов, регламентирующих вопросы оценки угроз и анализа защищенности информационных и автоматизированных систем.

Теоретические основы информационной безопасности отражены в трудах А.А. Варфоломеева, В.А. Герасименко, В.В. Домарева, Д.П. Зегжды, А.А Малюка, Д.С. Черешкина, А.И. Ярочкина.

Анализ работ специалистов в области оценки угроз ИБ показал, что при всей значимости проведенных исследований, проблема количественной оценки угроз и анализа безопасности ИС изучена и практически проработана не в полной мере.

В первую очередь, для повышения качества выбора защитных мер необходимо разработать методику анализа и оценки угроз.

Анализ рисков включает в себя мероприятия по обследованию организации с целью определения того, какие ресурсы и от каких угроз надо защищать. По результатам анализа и оценки рисков организация определяет факторы, влияющие на возможность реализации угроз безопасности и степени их воздействия, а также принимает осознанные решения относительно применения защитных мер, обеспечивающие желаемый уровень ИБ организации.

В настоящее время не существует стандартизированной методики анализа и оценки рисков угроз информационной безопасности для образовательных организаций. Все разработанные и активно использующиеся методики являются довольно общими для организаций, работающих в различных секторах, и они носят лишь рекомендательный характер.

В связи с этим **проблема** исследования заключается в разработке методики оценки угроз информационной безопасности образовательной организации на основе существующих стандартов и методик управления рисками информационной безопасности.

Цель исследования – анализ информационно-телекоммуникационной инфраструктуры образовательно организации и оценка рисков, определяющая основные характеристики рисков информационной системы и ресурсов образовательной организации.

Объект исследования – защитные меры информационных систем, создающих, хранящих и обрабатывающих информацию, важную с точки зрения обеспечения ее конфиденциальности, целостности и доступности.

Предмет исследования – методика оценки рисков угроз и выбора защитных мер для информационных систем.

Гипотеза исследования состоит в разработке методического аппарата, позволяющего осуществлять рациональный выбор защитных мер для информационных систем за счет применения научно-обоснованной методики оценки рисков угроз.

Достижение цели путем решения поставленной гипотезе потребовало ее разделения на следующие **задачи**:

- изучить виды угроз информационной безопасности в образовательной организации и их характеристику;

- выявить угрозы, уязвимости и риски в системе защиты информации образовательной организации;

- проанализировать существующие методики анализа и оценки рисков ИБ;

- разработать методику анализа и оценки рисков ИБ, связанных с угрозами безопасности информационных ресурсов;

- проанализировать информационные ресурсы колледжа, источники угроз и уязвимостей;

- описать оценку угроз ИБ по разработанной методике.

Методы исследования

Для формирования понятий в работе используются логические приемы, определения, анализ и синтез. Для разработки модели оценки рисков и методики формирования рационального комплекса защитных мер для информационной системы используются методы системного и структурного анализа. Для количественной оценки вероятности реализации угроз нарушителем применяются методы математической статистики.

Научная новизна результатов исследования заключается в разработке методики, позволяющей повысить качество выбора защитных мер для информационной системы, отличающаяся применением предложенного в работе показателя затратоемкости активов.

Обоснованность полученных результатов достигается использованием современного и апробированного математического аппарата, системно-структурным анализом описания объекта исследования, непротиворечивостью полученных выводов и их согласованностью с современными практиками в области информационной безопасности.

Практическую значимость исследования составляет предложенная методика, которая позволит повысить качество выбора защитных мер для информационной системы образовательной организации и может быть реализованы в виде модуля управления рисками безопасности информационной системы.

Базой исследования: Государственное бюджетное образовательное учреждение «Южно-Уральский государственный колледж», расположенный по адресу ул. Курчатова, 7, г. Челябинск.

Апробация исследования: результаты исследования были опубликованы на Международной научно-практической конференции «Технические системы и технологические процессы», 2018г.; Международной научно-практической конференции «Интеграция современных научных исследований в развитие общества», Всероссийской научно-практической конференции «Актуальные проблемы образования Позиция молодых 2017 года».

Структура работы: Магистерская диссертация состоит из введения, трех глав, заключения, библиографического списка, состоящего из 61 наименований. Работа содержит 2 рисунка, 11 таблиц. Общий объем работы составляет 79 страниц.

Глава 1. Современные угрозы информационной безопасности в образовательной организации

1.1 Виды угроз информационной безопасности в образовательной организации и их характеристика

Под угрозами безопасности информационной системы понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными, непреднамеренными воздействиями на нее [34].

Угроза – это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.

Угроза безопасности информации – потенциальная возможность нарушения основных качественных характеристик (свойств) информации при её обработке техническими средствами: конфиденциальности, целостности, доступности [40].

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.

Такими 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 [40].

С учётом этого угрозы могут быть классифицированы по следующим кластерам:

1) по величине принесённого ущерба:

- предельный, после которого образовательная организация может стать банкротом;

- значительный, но не приводящий к банкротству;

- незначительный, который образовательная организация может компенсировать и др.;

2) по вероятности возникновения:

- весьма вероятная угроза;

- вероятная угроза;

- маловероятная угроза;

3) по причинам появления:

- стихийные бедствия;

- преднамеренные действия;

4) по характеру нанесённого ущерба:

- материальный;

- моральный;

5) по характеру воздействия:

- активные;

- пассивные;

6) по отношению к объекту:

- внутренние;

- внешние.

Источниками внешних угроз являются:

- недобросовестные конкуренты;

- преступные группировки и формирования;

- отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:

- администрация организации;

- персонал;

- технические средства обеспечения производственной и трудовой деятельности [40].

Соотношение внешних и внутренних угроз на усреднённом уровне можно охарактеризовать так:

82% угроз совершается собственными сотрудниками образовательной организации либо при их прямом или опосредованном участии;

17% угроз совершается извне – внешние угрозы;

1% угроз совершается случайными лицами [40].

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность студентов, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус. Выделяются четыре группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

– компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;

– программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;

– данные, хранимые как на жестких дисках, так и на отдельных носителях;

– сам персонал, отвечающий за работоспособность IT-систем;

– обучающиеся, подверженные внешнему агрессивному информационному влиянию и способные создать в колледже криминальную ситуацию. В последнее время перечень таких ситуаций существенно расширился, что говорит о возможной целенаправленной психологической атаке на сознание детей и подростков.

Угрозы, направленные на повреждение любого из компонентов системы, могут носить как случайный, так и осознанный преднамеренный характер. Среди угроз, не зависящих от намерения персонала, обучающихся или третьих лиц, можно назвать:

– любые аварийные ситуации, например, отключение электроэнергии или затопление;

– ошибки персонала;

– сбои в работе программного обеспечения;

– выход техники из строя;

– проблемы в работе систем связи [55].

Все эти угрозы информационной безопасности носят временный характер, предсказуемы и легко устраняются действиями сотрудников и специальных служб.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев не могут быть предвидены. Их виновниками могут оказаться обучающиеся, служащие, конкуренты, третьи лица с намерением на совершение кибер-преступления. Для подрыва информационной безопасности такое лицо должно иметь высокую квалификацию в отношении принципов работы компьютерных систем и программ. Наибольшей опасности подвергаются компьютерные сети, компоненты которых расположены отдельно друг от друга в пространстве. Нарушение связи между компонентами системы может привести к полному подрыву ее работоспособности. Важной проблемой может стать нарушение авторских прав, намеренное хищение чужих разработок. Компьютерные сети редко подвергаются внешним атакам с целью воздействия на сознание

обучающихся, но и это не исключено. И самой серьезной опасностью станет использование оборудования в колледже для вовлечения студента в криминал и терроризм.

С точки зрения проникновения в периметр информационной безопасности и для совершения хищения информации или создания нарушения в работе систем необходим несанкционированный доступ.

Способы несанкционированного доступа

Можно выделить несколько видов несанкционированного доступа:

1. Человеческий. Информация может быть похищена путем копирования на временные носители, переправлена по электронной почте. Кроме того, при наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

2. Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.

3. Аппаратный. Он связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

Существует 5 принципов системы обеспечения информационной безопасности организации.

Принцип комплексности. При создании защитных систем необходимо предполагать вероятность возникновения всех возможных угроз для каждой организации, включая каналы закрытого доступа и используемые для них средства защиты. Применение средств защиты должно совпадать с вероятными видами угроз и функционировать как комплексная система защиты, технически дополняя друг друга. Комплексные методы и средства обеспечения информационной безопасности организации являются сложной системой взаимосвязанных между собой процессов.

Принцип эшелонирования представляет собой порядок обеспечения информационной безопасности организации, при котором все рубежи защитной системы будут состоять из последовательно расположенных зон безопасности, самая важная из которых будет находиться внутри всей системы.

Принцип надежности (равнопрочности). Стандарт организации обеспечения информационной безопасности должен касаться всех зон безопасности. Все они должны быть равнопрочными, то есть иметь одинаковую степень надежной защиты с вероятностью реальной угрозы.

Принцип разумной достаточности предполагает разумное применение защитных средств с приемлемым уровнем безопасности без фанатизма создания абсолютной защиты. Обеспечение организации высокоэффективной защитной системой предполагает большие материальные затраты, поэтому к выбору систем безопасности нужно подходить рационально. Стоимость защитной системы не должна превышать размер возможного ущерба и затраты на ее функционирование и обслуживание.

*Принцип непрерывности***.** Работа всех систем безопасности должна быть круглосуточной и непрерывной [55].

Как правило, защита от угроз, в основном регламентируется инструкциями, разработанными и утвержденными в образовательной организации с учетом особенностей эксплуатации информационных систем организации и действующей нормативной базой учреждения.

2.1 Выявление угроз, уязвимостей и рисков в системе защиты информации образовательной организации

Угроза безопасности ИС – это возможность нарушения безопасности ИС, ИС образовательной организации в частности. Наиболее часто угроза является следствием наличия в защите ИС уязвимых мест. Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании [15].

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

Источниками возможных угроз информации в образовательной организации являются:

- компьютеризированные учебные аудитории, в которых проходит учебный процесс;

- Интернет;

- рабочие станции неквалифицированных в сфере информационной безопасности работников образовательной организации.

Анализ информационных рисков можно разделить на следующие этапы:

- классификация объектов, подлежащих защите, по важности;

- определение привлекательности объектов защиты для взломщиков;

- определение возможных угроз и вероятных каналов доступа на объекты;

- оценка существующих мер безопасности;

- определение уязвимостей в обороне и способов их ликвидации;

- составление ранжированного списка угроз;

- оценка ущерба от несанкционированного доступа, атак в отказе обслуживании, сбоев в работе оборудования.

Основные объекты, нуждающиеся в защите от несанкционированного доступа:

- бухгалтерские ЛВС, данные планово-финансового отдела, а также статистические и архивные данные;

- серверы баз данных;

- консоль управления учетными записями;

- www/ftp-серверы;

- ЛВС и серверы исследовательских проектов.

Как правило, связь с Интернетом осуществляется сразу по нескольким линиям связи (оптоволоконная магистраль, спутниковые и радиоканалы). Отдельные каналы предоставляются для связи с другими образовательными каналами или для безопасного обмена данными.

Чтобы исключить риски, связанные с утечкой и порчей передаваемой информации, такие сети не должны подключаться к глобальным сетям и общей коллежской сети.

Критически важные узлы для обмена данными колледжа (например, бухгалтерская ЛВС) также должны существовать отдельно.

Угрозы информационной безопасности на автоматизированном рабочем месте сотрудника представлены в таблице 1.

Таблица 1

Автоматизированное рабочее место сотрудника

Угроза	Уязвимости
1. Физический доступ нарушителя к рабочему месту	1. Отсутствие системы контроля доступа сотрудников к чужим рабочим местам
	2. Отсутствие системы видеонаблюдения в колледже
2. Разглашение конфиденциальной информации, хранящейся на рабочем месте сотрудника организации	1. Отсутствие соглашения о неразглашении между работником и работодателем
	2. Нечеткая регламентация ответственности сотрудников колледжа
3. Разрушение (повреждение, утрата) конфиденциальной информации при помощи специализированных программ и вирусов	1. Отсутствие ограничения доступа пользователей к сети интернет и к внутренней корпоративной сети

Также в колледже существует угрозы доступности, угрозы целостности и угрозы конфиденциальности информации.

1. Угрозами доступности информации являются: разрушение (уничтожение) информации: вирус, повреждение оборудования.

Мерами предотвращения данных угрозы может являться следующее**:**

– Установка программы антивируса.

– Осуществление резервного копирования данных на съемные носители для быстрого восстановления утерянных данных во время системной ошибки.

– Установка аварийных источников бесперебойного питания.

– Подвод электроэнергии не менее от двух независимых линий электропередачи.

– Плановое обслуживание зданий и в целом всей поддерживающей инфраструктуры.

2. Угрозами целостности информации являются: нарушение целостности со стороны персонала: ввод неверных данных, несанкционированная модификация информации, кража информации, дублирование данных; потеря информации на жестких носителях; угрозы целостности баз данных; угрозы целостности программных механизмов работы организации.

Мерами предотвращения данной угрозы может являться следующее**:**

– Введение и частая смена паролей.

– Использование криптографических средств защиты информации.

3. Угрозами конфиденциальности являются: кражи оборудования; делегирование лишних или неиспользуемых полномочий на носитель с конфиденциальной информацией; открытие портов; установка нелицензионного ПО; злоупотребления полномочиями.

Анализ состояния информационной безопасности в колледже позволяет выявить следующие угрозы.

1. Заражение компьютерными вирусами через съёмные носители информации, компьютерную сеть, сеть Интернет.

2. Ошибки штатных сотрудников, т.е. неверный ввод данных или изменение данных.

3. Внутренний отказ информационной системы, т.е. отказ программного или аппаратного обеспечения, повреждение аппаратуры.

4. Угрозы технического характера.

5. Угрозы нетехнического или некомпьютерного характера - отсутствие паролей, конфиденциальная информация, связанная с информационными системами, хранится на бумажных носителях.

6. Несанкционированный доступ к информации (использование ресурсов без предварительно полученного разрешения). При этом могут совершаться следующие действия: несанкционированное чтение информации, несанкционированное изменение информации, а также несанкционированное уничтожение информации.

7. Кража программно-аппаратных средств.

8. Использование устаревших программных и аппаратных средства обработки информации.

Таким образом, наиболее существенными угрозами информационной безопасности в колледже являются следующие угрозы: хищение персональной информации студентов колледжа, несанкционированное внесение изменений в персональную информацию студентов и личные карточки студентов, ошибки сотрудников колледжа при внесении данных в личные дела и карточки студентов.

Выводы по первой главе

По итогам первой главы магистерской диссертации можно сделать следующие выводы.

Сформулированы и классифицированы угрозы, возникающие в информационных системах.

Угроза безопасности информации – потенциальная возможность нарушения основных качественных характеристик (свойств) информации при её обработке техническими средствами: конфиденциальности, целостности, доступности.

Все источники угроз безопасности информации можно разделить на три основные группы:

- обусловленные действиями субъекта (антропогенные источники угроз);

- обусловленные техническими средствами (техногенные источники угрозы);

- обусловленные стихийными источниками.

Как правило, защита от угроз, в основном регламентируется инструкциями, разработанными и утвержденными в образовательной организации с учетом особенностей эксплуатации информационных систем организации и действующей нормативной базой учреждения.

Также были выявлены угрозы, уязвимости и риски в системе защиты информации в образовательной организации. Предложены меры их устранения, в результате выполнения которых в образовательной организации позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Глава 2. Нормативно-правовая документация в области управления рисками информационной безопасности в образовательной организации

2.1. Семейство международных стандартов управления информационной безопасностью

Существуют многочисленные методики в сфере управления информационными рисками, предложенные десятками руководств, алгоритмов и методов. Основные из них описаны в международных и государственных стандартах в области ИБ, другие имеют автоматизированный подход, реализуемый программными продуктами.

Задача проанализировать существующие методики, дать им краткую характеристику и определить те, которые подойдут под специфику деятельности организации.

ГОСТ Р ИСО/МЭК 27005-2010

Данный стандарт, из серии стандартов ISO/IEC 27000, представляет руководство по менеджменту риска ИБ в организации, поддерживая, в частности, требования к системе управления информационной безопасности (СУИБ) в соответствии с ИСО/МЭК 27001. Руководство, содержащееся в этом стандарте, предназначено для применения в любых организациях, независимо от их типа, размера и характера бизнеса [19].

Данный стандарт был разработан в 2005 году и до сих пор ведётся его модификация, на данный момент актуальной является версия 2010 года [19]. Стандарт заменяет уже устаревшую серию стандартов ИТ безопасности ISO 13335, в связи с чем действие международных стандартов ISO 13335-3 и ISO 13335-4 было отменено.

Стандарт ISO 27005 не предоставляет какой-либо конкретной методологии по менеджменту риска ИБ, он определяет подход организации по управлению рисками и носит рекомендательный характер.

Данный стандарт будет использоваться как основной для анализа рисков ИТ инфраструктуры «Организации», т.к. он полностью применим для данной организации и описывает все этапы по управлению рисками: установление

контекста, принятие риска, оценка риска, обработка риска, мониторинг и пересмотр риска ИБ. Подробно с ними ознакомится можно в стандарте. [1]

Британский стандарт BS 7799-3

Семейство стандартов BS 7799 является первым международным стандартом в области управления информационной безопасностью. Первая часть стандарта – BS 7799-1 «Практические правила управления информационной безопасностью» - была разработана в 1995 г. и является практическим руководством по управлению ИБ в организации. Вторая часть стандарта – BS 7799-2 «Системы управления информационной безопасностью. Спецификация и руководство по применению» - появившаяся в 1998 г., определяет то, что должна представлять из себя СУИБ. В 2006 году Британским Институтом стандартов была выпущена третья часть стандарта – BS 7799-3 «Системы управления информационной безопасностью. Руководство по управлению рисками информационной безопасности» [2].

Стандарт BS 7799-3 является предшественником стандарта ISO 27005. Эти стандарты дополняют друг друга, а во многих вещах взаимно перекликаются. Эти стандарты служат фундаментом в методологии управления рисками и определяют все наиболее важные моменты, связанные с рисками. Дополнительно ознакомится с основными моментами можно в самом стандарте [2].

ГОСТ Р ИСО/МЭК 27001-2006

Данный стандарт принадлежит серии стандартов ISO/IEC 27000 и был принят в 2005 г. Он является заменой второй части британского стандарта BS 7799 [18].

Стандарт устанавливает требования к системе управления информационной безопасности для её создания, развития и поддержания. Так как стандарты ISO 27005 и BS 7799-3 представляют конкретное руководство и рекомендации по реализации требований ISO 27001, относящихся к процессам управления рисками и связанными с ними мероприятиями, то его так же необходимо учитывать в данной работе.

С требования, содержащиеся в ISO 27001, взаимосвязанные с ISO 27005 и BS 7799-3, можно подробно ознакомится в следующих пунктах стандарта [18]:

- создание СУИБ;
- внедрение и эксплуатация СУИБ;
- мониторинг и анализ СУИБ;
- сопровождение и совершенствование СУИБ;
- анализ СУИБ руководством;
- совершенствование СУИБ.

2.2. Методика ФСТЭК определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Методика разработана ФСТЭК в 2008 году и активно используется для определения актуальных угроз безопасности ПДн [38].

Методика определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) разработана ФСТЭК России на основании Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» и «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781, с учетом действующих нормативных документов ФСТЭК России по защите информации. Методика предназначена для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в следующих автоматизированных информационных системах персональных данных:

- государственных или муниципальных ИСПДн;
- ИСПДн, создаваемых и (или) эксплуатируемых предприятиями, организациями и учреждениями (далее – организациями) независимо от форм

собственности, необходимых для выполнения функций этих организаций в соответствии с их назначением;

– ИСПДн, создаваемых и используемых физическими лицами, за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд.

Документ предназначен для специалистов по обеспечению безопасности информации, руководителей организаций и предприятий, организующих и проводящих работы по обработке ПДн в ИСПДн.

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

В соответствии со статьей 19 Федерального закона N152-ФЗ от 27 июля 2006 г. «О персональных данных» ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и(или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз [43].

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы

утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

Детальное описание угроз, связанных с утечкой ПДн по техническим каналам, приведено в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Выявление технических каналов утечки ПДн осуществляется на основе нормативных и методических документов ФСТЭК России.

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в ИСПДн правила разграничения доступа к информации. Этими субъектами могут быть:

- нарушитель;
- носитель вредоносной программы;
- аппаратная закладка.

Под нарушителем здесь и далее понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в информационных системах. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПДн, нарушители подразделяются на два типа:

– нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;

– нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, – внутренние нарушители.

Для ИСПДн, предоставляющих информационные услуги удаленным пользователям, внешними нарушителями могут являться лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий, алгоритмических или программных закладок через автоматизированные рабочие места, терминальные устройства ИСПДн, подключенные к сетям общего пользования.

Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационным ресурсам ИСПДн и мер по контролю порядка проведения работ.

Угрозы несанкционированного доступа от внешних нарушителей реализуются с использованием протоколов межсетевого взаимодействия.

Детальное описание угроз, связанных с несанкционированным доступом в ИСПДн персональных данных, приведено в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Выявление угроз НСД к ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов, персонала ИСПДн, должностных лиц, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса составляются специальные опросные листы.

Наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии данной угрозы. Формируя на основе опроса перечень источников угроз ПДн, на основе опроса и сетевого сканирования перечень уязвимых звеньев ИСПДн, а также по данным обследования ИСПДн – перечень технических каналов утечки информации, определяются условия существования в ИСПДн угроз безопасности информации и составляется их полный перечень. На основании

этого перечня в соответствии с описанным ниже порядком формируется перечень актуальных угроз безопасности ПДн.

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 2.

Таблица 2

Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4.По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если , то возможность реализации угрозы признается низкой;

если , то возможность реализации угрозы признается средней;

если , то возможность реализации угрозы признается высокой;

если , то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 3.

Таблица 3

Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

С использованием данных о классе ИСПДн и составленного перечня актуальных угроз, на основе «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и

технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

Таким образом, данная методика оценки является классическим подходом к оценке рисков ИБ и включает следующие основные этапы:

- оценка исходного уровня защищённости;
- оценка частоты (вероятности) реализации угроз;
- оценка опасности каждой угрозы;
- оценка актуальности угроз;
- формирование требований по обеспечению безопасности.

Оценка отдельных параметров проводится по определённой в документе шкале. Подсчёт итогового результата осуществляется по формуле, по результатам которой выводится качественная и количественная оценка исследуемой угрозы [48].

Выводы по второй главе

В второй главе магистерской диссертации были проанализированы основные стандарты в области управления рисками ИБ. Определены те, которые удовлетворяют целям оценки рисков в специфике деятельности образовательной организации.

Основным стандартом по оценке рисков выбран ГОСТ Р ИСО/МЭК 27005-2010, так как он описывает все основные этапы управления рисками и подходит под специфику образовательной организации.

Второстепенные стандарты, так же рассмотренные в данной главе, необходимы в качестве дополнения к основному стандарту при разработке общей методики оценки рисков.

Глава 3. Разработка методики оценки риска угроз информационной безопасности ГБПОУ «Южно-Уральский государственный колледж

3.1. Методика оценки риска угроз, концепция, основные этапы

В качестве базового стандарта для определения методики оценки риска информационной безопасности взят стандарт ISO 27005-2010. Данный стандарт предлагает следующий этапы оценки риска:

– анализа риска, куда входит идентификация риска (включая идентификацию активов, угроз, существующих средств контроля, уязвимостей, последствий);

– измерение риска;

– оценивание риска.

На рисунке 1 схематично изображен процесс оценки рисков информационной безопасности [9].

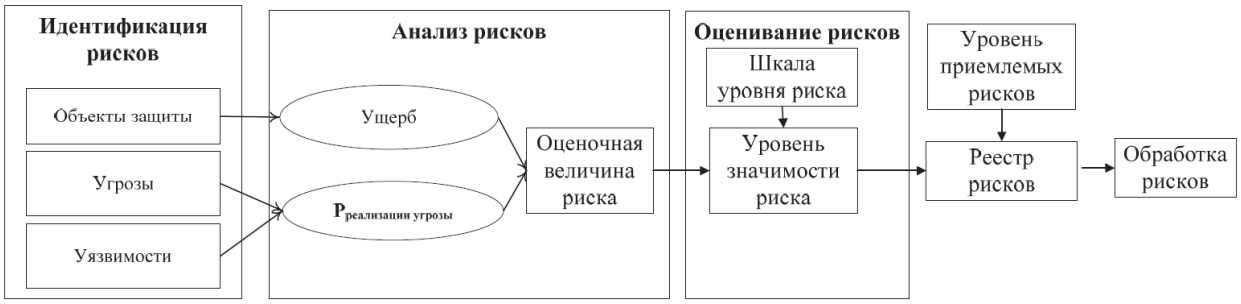

Рис. 1. - Процесс оценки рисков информационной безопасности

Существует множество методик анализа рисков. Некоторые из них основаны на достаточно простых табличных методах и не предполагают применения специализированного программного инструментария, другие наоборот, активно его используют. Несмотря на повышение интереса к управлению рисками, используемые в настоящее время методики относительно неэффективны, поскольку этот процесс во многих организациях осуществляется каждым подразделением независимо. Централизованный контроль над их действиями зачастую отсутствует, что исключает возможность реализации единого и целостного подхода к управлению рисками во всей организации.

Для решения задачи оценки рисков информационной безопасности в настоящее время наиболее часто используются следующие программные комплексы: CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), ГРИФ, CORAS и ряд других [9].

Все известные методики можно разделить на:

- методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»), к таким методикам, в частности, относится *FRAP*;

- количественные методики (риск оценивается через числовое значение, например, размер ожидаемых годовых потерь), к этому классу относится методика *RiskWatch*;

- методики, использующие смешанные оценки (такой подход используется в *CRAMM,* методике *MSAT*) [10].

Определим основные этапы, необходимые для целей оценки риска.

1. Идентификация активов. Необходимо идентифицировать и описать все активы образовательной организации и определить их ценность. Идентификация активов проводится в ходе аудита ИБ, определяются основные структуры, АИС и ИСПДн, которые обрабатывают различные типы данных. Данные заносятся в перечень в виде таблицы.

2. Идентификация угроз. Необходимо составить перечень угроз с идентификацией вида и источника. Выявление угроз проводится так же в ходе аудита ИБ, с учётом угроз безопасности информации, представленных в банке данных угроз безопасности информации ФСТЭК России [8].

3. Идентификация уязвимостей. Необходимо составить перечень уязвимостей, связанных с активами, угрозами и средствами контроля; перечень уязвимостей, которые не связаны с подлежащей к рассмотрению идентифицированной угрозой.

4. Измерение риска. Выбор методологии (из представленных далее) измерения риска, включающая качественную либо количественную оценку риска. На данном этапе проводится оценка угроз и уязвимостей по

количественной либо качественной шкале экспертным путём. Данные заносятся в общую таблицу, где проводится оценка риска на основании ценности актива.

5. Измерение уровня риска. Необходимо составить перечень рисков с присвоенными уровнями значений.

6. Оценивание риска. На этом этапе сравниваются измеренные риски с критериями оценивания риска. В результате составляется перечень рисков, с назначенными приоритетами в соответствии с критериями оценивания риска в отношении сценариев инцидентов, которые приводят к этим рискам.

В процессе оценивания риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, которые существуют или могут существовать, определяются существующие меры и средства контроля и управления, их воздействие на идентифицированные риски, определяются возможные последствия и, наконец, назначаются приоритеты установленным рискам, а также осуществляется их ранжирование по критериям оценки риска, зафиксированными при установлении контекста.

Данный стандарт [19] предлагает два подхода в оценке рисков ИБ:

- оценка рисков информационной безопасности высокого уровня;
- детальная оценка риска информационной безопасности.

Первый подход необходим для первоначального простого подхода, с возможностью построения стратегической картины при небольших затратах ресурсов и денежных средств. Данный подход предполагает более глобальное рассмотрение организации и её информационных систем, рассматривается более ограниченный перечень угроз и уязвимостей, а риски являются более общими.

Второй подход в общем использует матричный метод, используя таблицы. В стандарте предлагается на рассмотрение три метода оценки рисков. Данный подход включает в себя тщательную идентификацию и

определение ценности активов, оценку угроз этим активам и оценку уязвимостей.

Первый метод – матрица с предопределёнными значениями.

Здесь мера риска определяется исходя из предложенной стандартом таблицы (таблица 4) на основе шкалы от 0 до 8.

Таблица 4

Матрица оценки риска

Ценность актива	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8
Обозначение: Н - низкий, С - средний, В - высокий.									

Ценность актива определяется с точки зрения стоимости его замены, приобретения или восстановления, если это физический или программный актив, либо, если это информационный актив, его оценка определяется из опросов отдельных представителей владельцев информации. Все оценки приводятся к единой числовой шкале от 0 до 4. Далее проводится идентификация каждого вида угроз для каждой группы активов, с которыми связан данный вид угроз, чтобы провести последующую оценку. Уровень угрозы определяется как вероятность её возникновения, а уровень уязвимости как простота использования угрозы, чтобы вызвать неблагоприятные последствия. Оценка проводится по качественной шкале от высокий до низкий. На основании полученных оценок по таблице 4 определяется мера риска:

- низкий риск: 0-2;

- средний риск: 3-5;

- высокий риск: 6-8.

Второй метод – метод ранжирования мер угроз риска.

Данный метод связывает ценность активов с вероятностью возникновения угрозы (таблица 5).

Первый шаг – оценивание последствий по шкале от 1 до 5 (пример из стандарта [19]) для каждого находящегося под угрозой актива (b). Второй шаг – оценивание вероятности возникновения угрозы по шкале от 1 до 5 (c). Третий шаг – вычисление меры риска путём умножения (bxc), после чего проводится ранжирование.

Таблица 5

Ранжирование угроз посредством мер риска

Идентификатор угрозы (a)	Последствия (ценность актива) (b)	Степень вероятности возникновения угрозы (c)	Мера риска (d)	Ранжирование угроз (e)
Угроза A	5	2	10	2
Угроза B	2	4	18	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Эта процедура позволяет сопоставить и ранжировать в порядке приоритетов различные угрозы с разными последствиями и вероятностью возникновения.

Третий метод – оценка ценности для вероятности и возможных последствий рисков.

Основывается так же на оценке двух значений – для каждого актива и риска, комбинация которых будет определять баллы для каждого актива. Данный метод, помимо оценки риска, определяет то, каким системам следует отдавать предпочтение при обработке риска. Метод основывается на тех же таблицах, что и первый метод, с небольшими изменениями.

Сначала каждому активу присваивается ценность. Потом оценивается значение вероятности угрозы исходя из комбинации степени вероятности возникновения угрозы и простоты использования уязвимости по таблице 6.

Таблица 6

Оценка ценности для степени вероятности и возможных последствий рисков

Уровни угрозы	Низкая			Средняя			Высокая		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Значение степени вероятности	0	1	2	1	2	3	2	3	4

Затем, находя пересечение линий значения ценности актива и значения степени вероятности в таблице 7, присваиваются баллы активу/угрозе. Баллы актива/угрозы подсчитываются, чтобы получить итоговые баллы для актива. Эта цифра может использоваться для проведения различий между активами, составляющими часть системы.

Таблица 7

Ценность актива и значения степени вероятности

Значение степени вероятности	Ценность актива				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Окончательный шаг заключается в подсчете всех итоговых баллов активов системы, чтобы получить баллы системы. Эта цифра может использоваться для проведения различий между системами и определения того, защите какой системы следует отдавать предпочтение [19].

Результаты этапа оценки рисков

Перечень оценённых рисков, расставленных в соответствии с приоритетами согласно критериям оценивания риска.

В данной работе, для оценки рисков ИБ в колледже мы будем использовать третий метод, т.к. идёт оценка не только отдельных активов, но и системы в целом.

Уровень угрозы будем определять по методике ФСТЭК определения актуальных угроз [38] т.к. в информационной системе колледжа основная информация, подлежащая защите – персональные данные. Согласно данной методики, необходимо определить исходный уровень защищённости системы (Y_1) и частоту (вероятность) реализации угрозы (Y_2). Данные параметры определяются экспертами, после чего определяется коэффициент реализуемости угрозы Y, который является нашим уровнем. Он вычисляется по следующей формуле:

$$Y = (Y_1 + Y_2)/20.$$

где Y_1 определяется следующей шкалой:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Y_2 - показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной системы в складывающихся условиях обстановки, и имеет следующие параметры (с числовым коэффициентом в соответствии):

Таблица 8

Описание параметров показателя Y_2

Y2	Описание
Маловероятно 0	отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся).

низкая вероятность 2	объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации).
средняя вероятность 5	объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны.
высокая вероятность 10	объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Тогда по итогу уровень угрозы Y определяется следующей шкалой:

если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признается низкой;

если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней;

если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признается высокой;

если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

Уровень уязвимости определяет возможность получения доступа к системе и простоты её использования экспертным путём по следующей шкале:

Таблица 9

Описание показателей уровня уязвимости

Уровень риска (уязвимости)	Описание
Высокий	• Уязвимость позволяет получить полный контроль над критичной системой (бизнес-приложение или критичный компонент ИТ-инфраструктуры), запускать произвольный код. • Средства для использования уязвимости доступны.

Средний	• Уязвимость позволяет получить полный контроль над критичной системой (бизнес-приложение или критичный компонент ИТ-инфраструктуры), запускать произвольный код. • Доступные средства для использования уязвимости пока недоступны.
Низкий	• Уязвимость позволяет получить некритичную информацию. • Уязвимость обнаружена в системе, не содержащей критичную информацию.

Завершающим этапом анализа рисков является их оценивание и обработка. Оценивание риска проводится согласно заданным критериям. По стан-арту ISO 27005 критерии оценивания риска следующие:

0 - 2 – низкий риск;

3 - 5 – средний риск;

6 - 8 – высокий риск.

По результатам анализа рисков, оценки рисков будут приводится относительно выявленных угроз. Тогда границы для критериев риска будут определяться следующим образом:

[0; 2x +x/2] – низкий риск;

(3x-x/2; 5x+x/2] – средний риск;

(6x-x/2; 8] – высокий риск.

Где x – количество выявленных угроз.

3.2. Анализ информационно-телекоммуникационной системы ГБПОУ «Южно-Уральский государственный колледж

Объектом исследования является Южно-Уральский государственный колледж, распложенный по адресу: г. Челябинск, ул. Курчатова, 7.

Учредителем колледжа является Министерство образования и науки Челябинской области.

ГБПОУ «Южно-Уральский государственный колледж» является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа. Главная цель и направление деятельности ГБПОУ «Южно-Уральский государственный колледж» – повышение качества знаний и уровня профессиональных компетенций выпускников колледжа за счет разработки, создания и внедрения инновационных образовательных технологий, основанных на E-Learning, электронных учебно-методических комплексах, компетентностном подходе. Данные технологии и формы обучения позволили реально повысить качество профессиональной подготовки, прежде всего практического обучения, и сделали выпускников колледжа востребованными на рынке труда [47].

Колледж сегодня специализируется на подготовке бухгалтеров, финансистов, коммерсантов, менеджеров, маркетологов, юристов, техников автоматизированных систем обработки информации и управления, дизайнеров.

Педагоги колледжа имеют опыт практической работы по соответствующей специальности и глубокую теоретическую подготовку, необходимую для успешной реализации программ подготовки специалистов среднего звена. Среди них — кандидаты наук, заслуженные работники образования РФ, преподаватели высшей категории.

Для эффективного взаимодействия с учетом большого контингента обучающихся и месторасположением учебных зданий после реорганизации были присоединены два колледжа ГБОУ СПО (ССУЗ) «Челябинский колледж промышленной автоматики» (создан в 1953 г.) и ГБОУ СПО (ССУЗ) «Челябинский колледж промышленной автоматики» (создан в 1953 г.), которые в дальнейшем определили три образовательных комплекса (по территориальному признаку и направлениям подготовки):

- Информационных технологий и экономики (ул. Курчатова, д.7);
- Промышленной автоматики (ул. Доватора, д.38);

- Промышленного дизайна и торговли (ул. Блюхера, ул.1А).

Непосредственное управление деятельностью колледжа осуществляет директор.

Руководство и педагогический состав

Управление Колледжем осуществляется в соответствие с законодательством Российской Федерации и Уставом учебного заведения. Общее руководство Колледжа осуществляет выборный представительный орган – Совет колледжа, в состав которого входят представители всех категорий работников, студенты. Председателем Совета по должности является директор колледжа. Решение Совета колледжа проводится в жизнь приказом директора. Срок полномочия Совета колледжа составляет 5 лет.

Организационная структура колледжа представлена на рисунке 2.

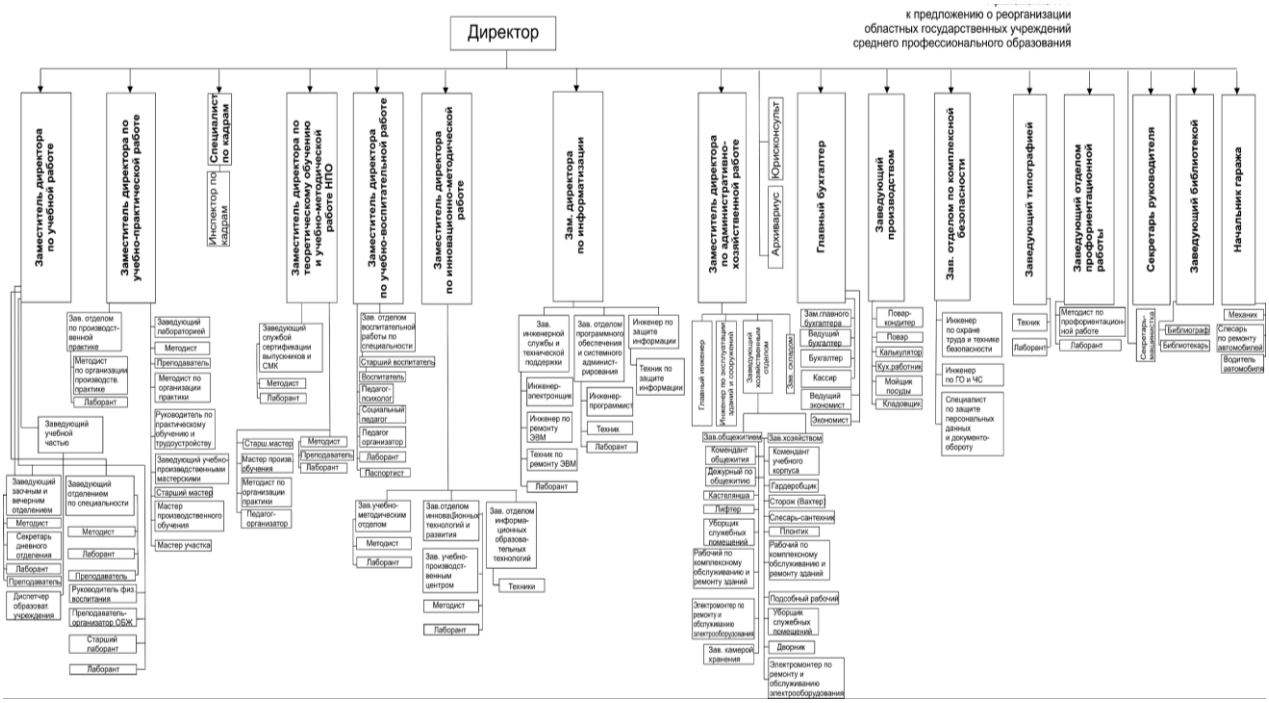

Рис.2. – Структура колледжа ГБПОУ «Южно-Уральский государственный колледж [47]

Непосредственное управление деятельностью колледжа осуществляет директор. Директор назначается Учредителем.

Лапин Владимир Геннадьевич - директор колледжа.

Калиновская Татьяна Сергеевна - заместитель директора по учебной работе.

Милюков Иван Васильевич - заместитель директора по производственному обучению.

Торопов Андрей Алексеевич - заместитель директора по учебно-практической работе.

Фадеев Виталий Олегович - заместитель директора по административно-хозяйственной работе.

Абзалова Алла Геннадьевна - главный бухгалтер.

Рассмотрим информационные ресурсы данного колледжа и порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности.

Пользование информационными ресурсами ГБПОУ «Южно-Уральский государственный колледж» регламентируется в соответствии с Федеральным законом «Об образовании в Российской Федерации» от 29 декабря 2012 г. № 273-ФЗ.

Доступ педагогических работников и обучающихся к информационным ресурсам обеспечивается в целях качественного осуществления образовательной и иной деятельности, предусмотренной Уставом колледжа [47].

Педагогические работники бесплатно пользуются образовательными, методическими и научными услугами колледжа. Пользование образовательными, методическими и научными услугами колледжа осуществляется через сайт и локальную сеть колледжа, а также методические кабинеты, учебную часть.

Исследуемое предприятие содержит следующие информационные ресурсы:

информация, относящаяся к коммерческой тайне:

– заработная плата,

– договоры с поставщиками и арендаторами.

защищаемая информация:

– личные дела работников и обучающихся;

– трудовые договора;

– личные карты работников;

– содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности;

– прочие разработки и документы для внутреннего пользования.

открытая информация:

– буклеты,

– информация на web-сайте **www.ecol.edu.ru**,

– учредительный документ,

– устав,

– перечень образовательных программ и т.д.

Доступ к информационно-телекоммуникационным сетям: доступ педагогических работников к информационно-телекоммуникационной сети Интернет в колледже осуществляется с персональных компьютеров (ноутбуков и т.п.), подключенных к сети Интернет. Для доступа к информационно-телекоммуникационным сетям в колледже педагогическому работнику предоставляются идентификационные данные (логин и пароль / учётная запись). Предоставление доступа осуществляется системным администратором колледжа.

Доступ к базам данных: педагогическим работникам обеспечивается доступ к следующим электронным базам данных:

– профессиональные базы данных;

– информационные справочные системы;

– поисковые системы.

Доступ к электронным базам данных осуществляется на условиях, указанных в договорах, заключенных колледжем с правообладателем электронных ресурсов (внешние базы данных).

Информация об образовательных, методических, научных, нормативных и других электронных ресурсах, доступных к пользованию, размещена на сайте колледжа.

Электронные образовательные ресурсы

– локальная сеть на одновременную работу 768 компьютеров. (Высокоскоростная глобальная сеть (пакет 20 000 Мб в месяц). 70% учебных площадей оснащено компьютерной и коммуникационной техникой (в т.ч. 450 рабочих мест электронной библиотеки) 150 мест Internet в общежитии);

– образовательный портал;

– Web-страница преподавателя;

– программные оболочки Moodle;

– учебно-методический комплекс на основе кейс-технологий (на бумажных носителях);

– учебно-методический электронный комплекс по специальности:

– более 50 электронных учебников по дисциплинам;

– система организации самостоятельной работы студентов в электронной библиотеке;

– междисциплинарный учебно-методический электронный комплекс по компетенциям:

– электронные учебники по компетенциям;

– практическое обучение в корпоративных учебно-производственных центрах;

– система сертификации;

– мониторинг (система оценки знаний, умений, навыков) [47].

Программное обеспечение, используемое в учебном процессе, позволяет в полном объеме реализовывать все образовательные программы. Применяются:

– операционные системы: Windows XP, 8, 10;

– прикладные пакеты: MS Office, «1-С бухгалтерия 7», «1 — С - Предприятие», 1С-Колледж;

– справочная юридическая система, «Консультант-Плюс»;

– автоматизированные рабочие места (АРМ) конструктора КОМПАС;

– рабочие станции защищены средствами антивирусной защиты: антивирусом Касперского. Вирусные базы регулярно обновляются.

В колледже ведется целенаправленная работа по созданию и развитию современных технологий обучения с привлечением системы электронного обучения E-Learning, формированию новых программ подготовки выпускников различных уровней в соответствии с требованиями рынка, открытию новых специальностей и специализаций по направлениям в соответствии с требованиями промышленности, сферы торговли и услуг, разработки и осуществления систем дополнительного, дистанционного и непрерывного образования, внедрения системы трудоустройства выпускников на базе длительного взаимодействия колледжа и потребителей (предприятий, фирм и организаций) при подготовке специалистов различного уровня и профиля [47].

Внедрение в колледже электронной системы обучения в помощь педагогу и студенту позволило полностью перейти к индивидуально-массовым формам обучения, а мощная электронная библиотека создала возможность преподавателям большую часть рутинной работы переложить на технику, студентам самостоятельно овладевать и обновлять знания. Выросла эффективность труда педагогов и студентов, повысилась доступность образования [47].

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

– информационное сопровождение и контроль учебного процесса, деятельности структурных подразделений колледжа;

– организация и проведение учебных занятий, организация внеаудиторной самостоятельной работы обучающихся;

– сопровождение дополнительных образовательных услуг;

– мониторинг результатов освоения учебной программы обучающимися.

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

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

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

В колледже на настоящий момент действует информационная система «Абитуриент» созданная для автоматизации приёма документов у абитуриентов очного и заочного отделений, составления проходных списков, приказов о зачислении студентов в колледж. АС «Абитуриент» существенно упрощает работу приёмной комиссии колледжа. АС «Абитуриент» хранит и работает со следующими данными об абитуриентах: ФИО, паспортные данные, дата рождения, сведения о регистрации по месту жительства, место работы, телефон, результаты сдачи экзаменов, сведения о родных абитуриента. Эти данные являются персональной информацией и охраняются законом «О защите персональных данных».

Данные об абитуриентах хранятся на сервере баз данных. Доступ к данным осуществляется с помощью специально разработанного пользовательского интерфейса АС «Абитуриент». Каждый пользователь

системы имеет свой логин и пароль. Все изменения, вносимые в данные конкретными пользователями, фиксируются. Сервер установлен в отделе «Информационные технологии», физический доступ к нему имеют только сотрудники данного отдела.

Анализ и оценка риска проводится согласно методике, разработанной во второй главе данной работы.

Идентификация активов

В таблице 10 представлен перечень информационных систем, полученный в ходе проведения аудита ИБ колледжа. Оценка ценности информационных активов, обрабатываемых в АИС и ИСПДн, была определена экспертным путем.

Таблица 10

Перечень АИС и ИСПДн, обрабатывающих КИ, КТ и ПДн

№ п/п	**Наименование информационной системы**	**Описание информационной системы**	**Перечень содержания информационной системы**
1	«1С Колледж проф»	Программный продукт представляет собой комплексное решение для управления деятельностью учреждений начального и среднего профессионального образования и охватывает все уровни управленческой деятельности основных подразделений колледжа.	- Паспортные данные студента - Паспортные данные родителей (родственников) студента - СНИЛС студента - СНИЛС (родственников) студента - Данные аттестата студента - Контактный телефон - Электронная почта - Достижения - Группы здоровья - Специальность - Приказы о зачислении, отчислении, академических отпусках - Паспортные данные, СНИЛС, ИНН, контактный телефон, стаж работы сотрудников образовательной организации - Образовательные программы, рабочие

			программы, КТП, расписание занятий, успеваемость студентов
2	Региональная АИС «Сетевой город образования»	Автоматизированная информационная система «Сетевой Город. Образование», модуль «Профессиональная образовательная организация Модуль для профессиональных образовательных организаций АИС ПОО позволяет решать административные задачи профессиональных образовательных организаций и проводить мониторинг текущего учебного процесса.	- Паспортные данные студента - Паспортные данные родителей (родственников) студента - СНИЛС студента - СНИЛС (родственников) студента - Данные аттестата - Контактный телефон - Электронная почта - Достижения - Группы здоровья - Специальность - Приказы о зачислении, отчислении, академических отпусках - Паспортные данные, СНИЛС, ИНН, телефон, стаж работы сотрудников образовательной организации - Образовательные программы, рабочие программы, КТП, расписание занятий, успеваемость студентов
3	ФИС ГИА и Приема	Федеральная информационная система обеспечения проведения единого государственного экзамена и приема граждан в образовательные учреждения среднего профессионального образования и образовательные учреждения высшего образования	-Паспортные данные студента - Данные аттестата - Направление подготовки - Специальность - Приказ о зачислении
4	Сайт образовательной организации		- ФИО преподавателей - Фотографии преподавателей - Краткая биография преподавателей - Все документы об образовательной организации

			- Фото с мероприятий, в том числе массовые фото студентов
5	СТЭК Документооборот	Программный продукт "СТЭК – Документооборот" помогает структурировать и автоматизировать движение документов в организации с момента их создания или получения до завершения исполнения или отправления.	ФИО сотрудника, его должность, подразделение
6	ПП «Комплексная бухгалтерская система» СТЭК	ПП «Комплексная Бухгалтерская Система» СТЭК версия для государственных(муниципальных) учреждений предназначена для автоматизации бухгалтерского учета государственных учреждений любого типа: казенных, бюджетных и автономных, состоящих на самостоятельном балансе, финансируемых из федерального, регионального (субъекта РФ) или местного бюджетов, а также из бюджета государственного внебюджетного фонда, ведущих учет согласно приведенным выше Планам счетов и инструкциям по их применению.	*Подсистема: «СТЭК – Бухгалтерия»* ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников - должность - банковские реквизиты *Подсистема: «СТЭК – Склад»* ФИО сотрудников - Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников

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

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

			- Паспортные данные сотрудников: (Серия, номер, когда, кем выдан) - дата рождения сотрудников - СНИЛС сотрудников - ИНН сотрудников - Адрес по прописке сотрудников - Место рождения студентов - Контактный телефон сотрудников ФИО студентов - Паспортные данные студентов: (Серия, номер, когда, кем выдан) - дата рождения студентов - СНИЛС студентов - ИНН студентов - Адрес по прописке студентов - Место рождения студентов - Контактный телефон студентов - лицевой счет *Подсистема:* ***«СТЭК – Расчёты со студентами»*** ФИО студентов - Паспортные данные студентов: (Серия, номер, когда, кем выдан) - дата рождения студентов - СНИЛС студентов - ИНН студентов - Адрес по прописке студентов - Место рождения студентов - Контактный телефон студентов - лицевой счет ФИО родителей - Паспортные данные родителей: (Серия, номер, когда, кем выдан)

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

Идентификация уязвимостей

В ходе проведения аудита ИБ Организации уязвимости были выявлены следующих областях:

- персонал;
- помещения и оборудование;
- нормативно-методическая база;
- системы связи;
- программные средства и операционные системы.

Персонал, может привести ко множествам угроз. Неквалифицированные и невнимательные сотрудники могут нанести непреднамеренный вред организации. Излишняя болтливость, стремление отомстить руководству или коллеге по работе, подверженность манипуляциям (воздействие со стороны злоумышленника) может раскрыть конфиденциальные данные организации, нанести финансовый или репутационный ущерб. Наличие вредных привычек может привести к физическому ущербу, например, пожар из-за оставленного окурка.

Помещения и оборудование имеют множество возможностей реализации различных угроз. Отсутствие пожарной сигнализации в помещении, отсутствие системы контроля доступа в помещение, несоответствие помещения требованиям безопасности могут приводит к ряду различных угроз. Со стороны оборудования могут возникать такие уязвимости, как неисправность оборудования, износ и старение элементов оборудования, зависимость от физической среды эксплуатации, необходимость физической защиты от НСД и т.п.

Нормативно-методическая база, использует несовершенства организации в области разработки нормативно-методических документов, регламентов, актов и т.д.

Программные средства и операционные системы имеют множество уязвимостей, обусловленные ошибками кода, недостатком или отсутствием необходимых средств защиты (аутентификации, проверки целостности), внедрением вредоносных программ и т.п., которые могут привести к реализации различных угроз, таких как например отказ в обслуживании, НСД.

Подробный перечень организационных и программно-аппаратных уязвимостей предоставлен в отчёте, который был составлен в ходе проведения аудита колледжа.

Оценка риска

В таблице 11 предоставлена оценка рисков ИБ по активам и соответствующим им угрозам, оценка которых была проведена ранее. Оценка

проводилась по методике, разработанной в параграфе 3.1 магистерской диссертации.

Таблица 11

Оценка рисков ИБ

Активы	Оценка	Угрозы	Значение степени вероятности	Мера риска	Итоговый бал для актива
«1С Колледж проф»	2	Угроза внедрения вредоносного кода в BIOS	0	2	87
		Угроза доступа к защищаемым файлам с использованием обходного пути	2	4	
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	2	4	
		Угроза исследования механизмов работы программы	1	3	
		Угроза неправомерного ознакомления с защищаемой информацией	3	5	
		Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	2	4	
		Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	2	4	
		Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	3	5	
		Угроза несанкционированного удаления защищаемой информации	3	5	
		Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	3	5	
		Угроза определения топологии вычислительной сети	2	4	
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	1	3	

		Угроза перехвата данных, передаваемых по вычислительной сети	3	5	
		Угроза подбора пароля BIOS	0	2	
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	0	2	
		Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	3	5	
		Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	2	4	
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	1	3	
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	2	4	
		Угроза несанкционированной модификации защищаемой информации	3	5	
		Угроза перехвата одноразовых паролей в режиме реального времени	1	3	
		Угроза использования уязвимых версий программного обеспечения	4	6	
ФИС ГИА и Приема	1	Угроза внедрения вредоносного кода в BIOS	0	1	65
		Угроза доступа к защищаемым файлам с использованием обходного пути	2	3	
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	2	3	
		Угроза исследования механизмов работы программы	1	2	
		Угроза неправомерного ознакомления с защищаемой информацией	3	4	

		Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	2	3
		Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	2	3
		Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	3	4
		Угроза несанкционированного удаления защищаемой информации	3	4
		Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	3	4
		Угроза определения топологии вычислительной сети	2	3
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	1	2
		Угроза перехвата данных, передаваемых по вычислительной сети	3	4
		Угроза подбора пароля BIOS	0	1
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	0	1
		Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	3	4
		Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	2	3
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	1	2

		Угроза заражения компьютера при посещении неблагонадёжных сайтов	2	3	
		Угроза несанкционированной модификации защищаемой информации	3	4	
		Угроза перехвата одноразовых паролей в режиме реального времени	1	2	
		Угроза использования уязвимых версий программного обеспечения	4	5	
СТЭК Документооборот	3	Угроза внедрения вредоносного кода в BIOS	0	3	110
		Угроза доступа к защищаемым файлам с использованием обходного пути	2	5	
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	2	5	
		Угроза исследования механизмов работы программы	1	4	
		Угроза неправомерного ознакомления с защищаемой информацией	3	6	
		Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	2	5	
		Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	2	5	
		Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	3	6	
		Угроза несанкционированного удаления защищаемой информации	3	6	
		Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	3	6	
		Угроза определения топологии вычислительной сети	2	5	

		Угроза перехвата вводимой и выводимой на периферийные устройства информации	1	4	
		Угроза перехвата данных, передаваемых по вычислительной сети	3	6	
		Угроза подбора пароля BIOS	0	3	
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	0	3	
		Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	3	6	
		Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	2	5	
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	1	4	
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	2	5	
		Угроза несанкционированной модификации защищаемой информации	3	6	
		Угроза перехвата одноразовых паролей в режиме реального времени	1	4	
		Угроза использования уязвимых версий программного обеспечения	4	7	
ПП «Комплексная бухгалтерская система» СТЭК	3	Угроза внедрения вредоносного кода в BIOS	0	3	110
		Угроза доступа к защищаемым файлам с использованием обходного пути	2	5	
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	2	5	
		Угроза исследования механизмов работы программы	1	4	
		Угроза неправомерного ознакомления с защищаемой информацией	3	6	

		Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	2	5
		Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	2	5
		Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	3	6
		Угроза несанкционированного удаления защищаемой информации	3	6
		Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	3	6
		Угроза определения топологии вычислительной сети	2	5
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	1	4
		Угроза перехвата данных, передаваемых по вычислительной сети	3	6
		Угроза подбора пароля BIOS	0	3
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	0	3
		Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	3	6
		Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	2	5
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	1	4

		Угроза заражения компьютера при посещении неблагонадёжных сайтов	2	5	
		Угроза несанкционированной модификации защищаемой информации	3	6	
		Угроза перехвата одноразовых паролей в режиме реального времени	1	4	
		Угроза использования уязвимых версий программного обеспечения	4	7	
«Контур-Экстерн» — отчётность через интернет	3	Угроза внедрения вредоносного кода в BIOS	0	3	110
		Угроза доступа к защищаемым файлам с использованием обходного пути	2	5	
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	2	5	
		Угроза исследования механизмов работы программы	1	4	
		Угроза неправомерного ознакомления с защищаемой информацией	3	6	
		Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	2	5	
		Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	2	5	
		Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	3	6	
		Угроза несанкционированного удаления защищаемой информации	3	6	
		Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	3	6	
		Угроза определения топологии вычислительной сети	2	5	

		Угроза перехвата вводимой и выводимой на периферийные устройства информации	1	4	
		Угроза перехвата данных, передаваемых по вычислительной сети	3	6	
		Угроза подбора пароля BIOS	0	3	
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	0	3	
		Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	3	6	
		Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	2	5	
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	1	4	
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	2	5	
		Угроза несанкционированной модификации защищаемой информации	3	6	
		Угроза перехвата одноразовых паролей в режиме реального времени	1	4	
		Угроза использования уязвимых версий программного обеспечения	4	7	
	2	Угроза внедрения вредоносного кода в BIOS	0	2	87
		Угроза доступа к защищаемым файлам с использованием обходного пути	2	4	
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	2	4	
		Угроза исследования механизмов работы программы	1	3	
		Угроза неправомерного ознакомления с защищаемой информацией	3	5	

Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	2	4
Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	2	4
Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	3	5
Угроза несанкционированного удаления защищаемой информации	3	5
Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	3	5
Угроза определения топологии вычислительной сети	2	4
Угроза перехвата вводимой и выводимой на периферийные устройства информации	1	3
Угроза перехвата данных, передаваемых по вычислительной сети	3	5
Угроза подбора пароля BIOS	0	2
Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	0	2
Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	3	5
Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	2	4
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	1	3
Угроза заражения компьютера при посещении неблагонадёжных сайтов	2	4

		Угроза несанкционированной модификации защищаемой информации	3	5	
		Угроза перехвата одноразовых паролей в режиме реального времени	1	3	
		Угроза использования уязвимых версий программного обеспечения	4	6	
Региональная АИС «Сетевой город образования»	4	Угроза внедрения вредоносного кода в BIOS	0	4	132
		Угроза доступа к защищаемым файлам с использованием обходного пути	2	6	
		Угроза использования информации идентификации/аутентификации, заданной по умолчанию	2	6	
		Угроза исследования механизмов работы программы	1	5	
		Угроза неправомерного ознакомления с защищаемой информацией	3	7	
		Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	2	6	
		Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	2	6	
		Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	3	7	
		Угроза несанкционированного удаления защищаемой информации	3	7	
		Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	3	7	
		Угроза определения топологии вычислительной сети	2	6	
		Угроза перехвата вводимой и выводимой на периферийные устройства информации	1	5	

		Угроза перехвата данных, передаваемых по вычислительной сети	3	7	
		Угроза подбора пароля BIOS	0	4	
		Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	0	4	
		Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	3	7	
		Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	2	6	
		Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	1	5	
		Угроза заражения компьютера при посещении неблагонадёжных сайтов	2	6	
		Угроза несанкционированной модификации защищаемой информации	3	7	
		Угроза перехвата одноразовых паролей в режиме реального времени	1	5	
		Угроза использования уязвимых версий программного обеспечения	4	8	

Обработка результата оценки риска

Завершающим этапом оценки рисков ИБ является их оценивание. Необходимо сравнить измеренные риски с критериями оценивания рисков и назначить приоритеты для дальнейшей обработки рисков.

Исходя из результатов оценки рисков, шкала критерия оценивания рисков следующая:

0 - 55 – риски являются низкими;

56 - 121 – риски являются средними;

122 - 176 – риски являются высокими.

Информационным системам с высоким риском требуется незамедлительное планирование и реализация корректирующих действий, направленных на снижение риска. Так как ИСПДн, которая связана с финансовой деятельностью колледжа, имеет высокий риск финансовых потерь, что является неприемлемым и необходимо в первую очередь принять все меры по устранению, либо уменьшению рисков, связанных с данной ИСПДн. А именно:

- обеспечить полноту нормативно правовой базы; пересмотреть и усилить ведение контрольно-пропускного режима;

- пересмотреть и модернизировать серверные помещения, серверное и телекоммуникационное оборудование, АРМ;

- улучшить сопровождение IT инфраструктуры, объединив в единое подразделение структурные подразделения, занимающиеся техническим сопровождением инфраструктуры колледжа;

- повысить квалификацию и осведомлённость персонала по вопросам информационной безопасности;

- обеспечить ответственности за сохранность сведений конфиденциального характера;

- обеспечить антивирусную защиту на всех серверах и АРМ.

Информационным системам со средним риском так же необходимо реализовать вышеперечисленные меры для уменьшения рисков, в частности для ИСПДн, которые обрабатывают ПДн, КИ и КТ, имеющие более высокий приоритет.

Информационные системы с низким приоритетом обрабатываются в последнюю очередь, т.к. риски, связанные с данными АИС, могут нанести меньший ущерб, а реализация некоторых защитных мер может быть не оправдана.

При низком риске следует решить, нужны ли какие-то корректирующие действия, или можно принять риск.

Выводы по третьей главе

В третьей главе были подробно рассмотрены этапы оценивания риска стандарта ГОСТ Р ИСО/МЭК 27005-2010 и на его основе разработана методика оценки риска, включающая идентификацию активов, угроз, уязвимостей, а также их последующую оценку.

Оценка угроз в разработанной методике определяется из методики определения актуальных угроз ФСТЭК.

Данная методика даёт качественную и количественную оценку, с последующей приоритезацией рисков, согласно заданным критериям, что позволяет выявить наиболее важные системы для дальнейшей обработки рисков.

Проведён анализ ИТС колледжа на предмет оценки рисков ИБ. Были определены информационные активы колледжа и их оценка. Выявлены угрозы и уязвимости для АИС образовательной организации, проведена их оценка.

Далее была проведена оценка рисков, исходя из полученных ранее результатов.

ЗАКЛЮЧЕНИЕ

Магистерское диссертационное исследование решает проблему разработки методики оценки угроз информационной безопасности образовательной организации на основе существующих стандартов и методик управления рисками информационной безопасности. Результаты проведенного исследования позволили сделать следующие общие выводы:

1. Проблема выбора защитных мер для ИС образовательной организации СПО.

Угроза безопасности ИС – потенциальная возможность нарушения основных качественных характеристик (свойств) ИС при её обработке техническими средствами: конфиденциальности, целостности, доступности.

Все источники угроз безопасности ИС можно разделить на три основные группы:

- обусловленные действиями субъекта (антропогенные источники угроз);

- обусловленные техническими средствами (техногенные источники угрозы);

- обусловленные стихийными источниками.

Как правило, защита от угроз, в основном регламентируется инструкциями, разработанными и утвержденными в образовательной организации с учетом особенностей эксплуатации информационных систем организации и действующей нормативной базой учреждения.

2. Нормативно-правовая документация в области управления рисками информационной безопасности в образовательной организации.

Описаны международные стандарты управления информационной безопасностью, а также Методика ФСТЭК определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Основным стандартом по оценке рисков выбран ГОСТ Р ИСО/МЭК 27005-2010, так как он описывает все основные этапы управления рисками и подходит под специфику образовательной организации.

3. Проведённый анализ и оценка рисков, связанные с угрозами безопасности информационных ресурсов ГБПОУ «Южно-Уральский государственный колледж» выявил риски информационной безопасности для их последующей обработки.

Для достижения поставленных целей были реализованы следующие задачи:

- разработана методика оценки рисков ИБ для образовательной организации на основе проанализированных стандартов в области управления рисками ИБ;

- проанализирована информационно-телекоммуникационная инфраструктура колледжа с целью выявления информационных активов, угроз и уязвимостей;

- проведена оценка информационных активов, угроз и уязвимостей и по результатам выведена общая оценка рисков в виде сводной таблицы.

Проведенное исследование не исчерпывает всей полноты рассмотренной проблемы и обусловливает появление новых вопросов, которые требуют своего решения.

Список использованной литературы

1. Bjorn A.G. CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security, 2002.
2. BS 7799-3:2006. Системы управления информационной безопасностью - Часть 3: Руководство по управлению рисками информационной безопасности. – Введ. Март.2006
3. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. Berlin: ISO/IEC JTC 1/SC 27. 2013. 23 p.
4. Аверченков В.И. Организационная защита информации: учеб. пособие / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2014. – 184 с.
5. Ажмухамедов И.М., Ханжина Т.Б. Определение оптимального комплекса мер по обеспечению информационной безопасности / 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.
6. Андреева Н.В. Функциональная модель системы управления информационной безопасностью как средство внедрения стандартов линейки ISO/IEC 2700x (BS 7799) // Научно-технический вестник информационных технологий, механики и оптики. 2007. № 39. С. 40–44.
7. Банк данных угроз безопасности информации / ФСТЭК России // Threat List/ Список угроз – 2017. – URL: http://bdu.fstec.ru/threat. Дата обращения: 04.12.18.
8. Банк данных угроз безопасности информации // Федеральная служба по техническому и экспортному контролю. - URL: https://bdu.fstec. Ru. Дата обращения: 01.02.2018.
9. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии. – 2015. – № 1 (9). – С. 73-79.

10. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности / Е.К. Баранова // Управление риском. 2009. № 1(49). С. 15–26.

11. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации / Е.К. Баранова, А.В. Бабаш. – М.: ИНФРА-М_РИОР, 2014.

12. Бойцев О. Многофакторный анализ рисков информационной безопасности. Подходы и методы / О. Бойцев. - URL: http://www.nestor.minsk.by/kg/2008/44/kg84403.html. Дата обращения: 01.02.2019.

13. Велигура А. О выборе методики оценки рисков информационной безопасности / А. Велигура. – URL: http://itsec.ru/articles2/pravo/o_vybore_metodiki_ocenki_riskov_informac_bezop/. Дата обращения: 20.01.2019.

14. Виды и источники угроз информационной безопасности. – URL: http://infoprotect.net/note/vidyi_i_istochniki_ugroz_informacionnoy_bezopasnosti/ Дата обращения: 15.11.2018.

15. Вихорев С.В. Классификация угроз информационной безопасности / С.В. Вихров. - URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml/. Дата обращения: 22.11.2018.

16. Глушенко С.А. Применение системы Matlab для оценки рисков информационной безопасности организации // Бизнес-информатика. 2013. № 4 (26). С. 35–42.

17. ГОСТ 12.0.003-2015. Система стандартов безопасности труда. Опасные и вредные производственные факторы. Классификация. – Введ. 2015-12-10. – М.: Межгосударственный совет по стандартизации, метрологии и сертификации, 2015. – 16 с.

18. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента

информационной безопасности требования. – Введ. 2008-02-01 – М.: ФСТЭК России, 2006.

19. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/ МЭК ТО 13335-4-2007; Введ. с 30.11.2010. Москва: Изд-во Стандартинформ, 2011.

20. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска; Введ. с 01.12.2012. Москва: Изд-во Стандартинформ; 2012.

21. Губарева О.Ю. Оценка рисков информационной безопасности в телекоммуникационных сетях. // Вестник Волжского университета им. В.Н. Татищева. 2013. № 2 (21). С. 76–81.

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

23. Ильченко Л.М. Анализ системы менеджмента информационной безопасности на базе стандарта ISO 27001:2013. // Материалы 5 научно-практической конференции студентов, аспирантов и курсантов «IT вчера, сегодня, завтра». 2017. С. 51–61.

24. Ильченко Л.М. Расчет рисков информационной безопасности телекоммуникационного предприятия / Л.М. Ильченко, Е.К. Брагина, И.Э. Егоров, С.И. Зайцев // Открытое образование, №22. № 2. 2018.

25. Информационная безопасность образовательных учреждений. – URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/. Дата обращения: 01.12.2018.

26. Киселева И.А., Искаджян С.О. Информационные риски: методы оценки и анализа / И.А. Киселева, С.О. Искаджян // ИТпортал, 2017. №2 (14). URL: http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/. Дата обращения: 01.02.2019.

27. Королев В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории риска: учеб. пособие / В.Ю. Королев, В.Е. Бенинг, С.Я. Шоргин. - М.: ФИЗМАТЛИТ, 2011. 620 с.

28. Коротнев К. Методики управления рисками информационной безопасности и их оценки (часть 2) / К. Коротнев. – URL: https://safe-surf.ru/specialists/article/5194/587935/. Дата обращения: 01.02.2019.

29. Красникова Т.В., Невежин В.П. Моделирование оценки при аудите безопасности информационных систем / Т.В. Красникова, В.П. Невежин // VII Международная студенческая электронная научная конференция «Студенческий научный форум 2015».

30. Кудрявцева Р.Т. Управление информационными рисками с использованием технологий когнитивного моделирования: автореф. дис. … канд. техн. наук. – Уфа, 2008. – 17 с.

31. Куканова Н. Современные методы и средства анализа и управление рисками информационных систем компаний / Н. Куканова // www.dsec.ru, Digital Security. Дата обращения: 20.01.2019.

32. Левченко В.Н. Этапы анализа рисков / В.Н. Левченко. - URL: http://masters.donntu.org/2016/fknt/levchenko/library/article6.htm. Дата обращения: 12.01.2019.

33. Лютова И.И. Моделирование уровня приемлемого риска информационной безопасности // Вестник Адыгейского государственного университета. Серия 5: Экономика. 2014. №2 (141). URL: https://cyberleninka.ru/article/n/modelirovanie-urovnya-priemlemogo-riska-informatsionnoy-bezopasnosti. Дата обращения: 02.02.2019.

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

35. Медведовский И. Современные методы и средства анализа и контроля рисков информационных систем компаний / И. Медведовский //, www.dsec.ru, Digital Security. Дата обращения: 20.01.2019.

36. Международный стандарт ISO/IEC 27005:2008. Информационная технология – Методы защиты – Менеджмент рисков информационной безопасности BS ISO/IEC 27005:2008.

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

38. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.

39. Методики и программные продукты для оценки рисков. - URL: https://www.intuit.ru/studies/courses/531/387/lecture/8996?page=2/. Дата обращения: 01.02.2019.

40. Методы организации защиты информации: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю.Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с.

41. Милютина О.В. Особенности защиты информации в образовательном учреждении / О.В. Милютина. – URL: http://www.fcoit.ru/internet_conference/information_security_training_process/features_information_security_in_an_educational_institution.php. Дата обращения: 15.12.2018.

42. 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: 28.11.2018.

43. 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: 28.11.2018.

44. 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: 28.11.2018.

45. Обеспечение информационной безопасности организации. – URL: http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/. Дата обращения: 01.12.2018.

46. Организационное обеспечение информационной безопасности [Электронный ресурс]. - Режим доступа: www.starik2222.narod.ru. Дата обращения: 22.11.2018.

47. Официальный сайт ГБПОУ «Южно-Уральский государственный колледж». – URL: www.ecol.edu.ru. Дата обращения: 22.12.2018.

48. Оценка информационной безопасности в деятельности организаций. Способы оценки информационной безопасности. – URL: http://www.pvsm.ru/informatsionnaya-bezopasnost/19741. Дата обращения: 05.12.2018.

49. Пащенко И.Н., Васильев В.И. Разработка требований к системе защиты информации в интеллектуальной сети Smart Grid на основе стандартов ISO/IEC 27001 и 27005 // Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 117–126.

50. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. М.: Компания АйТи; ДМК Пресс, 2014.

51. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса / П.В. Плетнев, В.М. Белов. - URL: http://old.tusur.ru/filearchive/reports-magazine/2012-25-2/083.pdf**.** Дата обращения: 25.01.2019.

52. Пугин В.В., Губарева О.Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия / В.В. Пугин, О.Ю. Губарева. – URL: https://rus.neicon.ru/xmlui/bitstream/handle/123456789/12956/9_st-13.pdf?sequence=1. Дата обращения: 12.12.2018.

53. Садердинов А.А. Информационная безопасность предприятия: учеб. пособие / А.А. Садердинов, В.А. Трайнев, А.А. Федулов. – М.: Дашков и К, 2013. – 336 с.

54. Симонов С. Технологии и инструментарий для управления рисками / С. Симонов. JetInfo № 2, 2013.

55. Система обеспечения информационной безопасности. – URL: http://www.ec-leasing.ru/products/sistemy-obespechiniya-informacionnoi-bezopasnosti/. Дата обращения: 01.12.2018.

56. Средство оценки безопасности Microsoft Security Assessment Tool (MSAT). - URL: http://technet.microsoft.com/ru-ru/security/cc185712.aspx. Дата обращения: 12.01.2019.

57. Стандарты информационной безопасности. – URL: https://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html. Дата обращения: 20.11.2018.

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

59. Шарафутдинова А.Р., Пядышев В.С. Защита информации в образовательных учреждениях / А.Р. Шарафутдинова, В.С. Пядышева. – URL: http://www.rusnauka.com/17_APSN_2013/Matemathics/2_140911.doc.htm. Дата обращения: 25.12.2018.

60. Ярочкин, В. И. Информационная безопасность / В.И. Ярочкин. – М. Академический проект, 2012. – 640 с.

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