



**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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»,
программа магистратуры «Управление информационной
безопасности в профессиональном образовании»**

Выполнил:

Магистрант группы ОФ-209/210-2-1
Александров Константин Юрьевич

Научный руководитель:

д.п.н., профессор

Уварина Наталья Викторовна


Проверка на объем заимствований:

74 % авторского текста

Работа рекомендована к защите

« 27 » _____ мая _____ 2020 г.

Заведующий кафедрой АТИТиМОТД

 В.В. Руднев

Челябинск, 2020

Аннотация

на магистерскую диссертацию

Александрова Константина Юрьевича

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

Магистерская диссертация содержит 74 страницы, 10 страниц, 2 рисунка, 61 источник литературы.

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

Объект исследования – применяемые защитные меры ИС, которые используются для обработки, хранения, создания данных, которым необходима защита их целостности, доступности и конфиденциальности.

Цель магистерской диссертации – проведение анализа инфраструктуры образовательного учреждения и выявление основных рисков информационной системы учреждения.

В процессе исследования изучена теория, виды угроз и их характеристики. Описаны международные стандарты управления информационной безопасностью, а также Методики ФСТЭК для определения современных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Результатом исследования является создание методических материалов для оценки рисков угроз, позволяющих повысить качество выбора защитных мер для информационных систем образовательных учреждений.

Магистрант Александров Константин Юрьевич _____

ОГЛАВЛЕНИЕ

Оглавление.....	3
Введение	4
Глава 1. угрозы информационной безопасности в образовательном учреждении.....	8
1.1 Виды угроз информационной безопасности в образовательном учреждении и их характеристика	8
1.2 Выявление угроз, уязвимостей и рисков в системе защиты информации образовательной организации.....	13
Выводы по первой главе.....	19
Глава 2. нормативная документация в области управления рисками информационной безопасности в образовательном учреждении.....	20
2.1. Международные стандарты управления информационной безопасностью	20
2.2. Методика ФСТЭК определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.....	22
Выводы по второй главе	30
ГЛАВА 3. РАЗРАБОТКА ОЦЕНКИ РИСКА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФГБОУ ВО «Южно-Уральский государственный гуманитарно-педагогический университет»	31
3.1. Методика оценивания риска угроз, ее концепция и основные этапы	31
3.2. Анализ информационно-телекоммуникационной системы ФГБОУ ВО «Южно-Уральский государственный гуманитарно-педагогический университет».....	38
Выводы по третьей главе.....	58
Заключение	59
Список использованной литературы	61

ВВЕДЕНИЕ

Актуальность исследования. В современном мире, где используется множество различных информационных систем, как никогда остро возникла проблема обеспечения информационной безопасности, так как полученную информацию можно использовать для совершения различных преступных действий. Информационные системы используются во всех сферах деятельности, в различных образовательных организациях, используют сеть Интернет для реализации их функционала, и поэтому они оказываются открытыми для реализации внутренних и внешних угроз, поэтому проблемы информационной безопасности становятся не менее важными для образовательного учреждения, чем экономическая или физическая безопасности.

Основное предназначение информационных систем заключается в увеличении эффективности деятельности образовательной организации, упрощения ее работы, а это означает, что меры защиты для информационной системы обязаны быть оптимальными с точки зрения выгоды и затрат на его создание.

Актуальность темы диссертации исходит из важности наилучшего выбора мер защиты для информационных систем, которые выбираются на основе оценки угроз.

Главные точки зрения на проблемы оценки рисков и подбора мер защиты информационных, автоматизированных систем 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.

Создано множество документов, регулирующих стороны мер оценивания и анализа защиты 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.

После анализа работ специалистов было выявлено, что несмотря на значимость исследований, проблема оценки и анализа угроз и систем безопасности изучена и проработана не полностью.

Для того чтобы увеличить качество выбора мер защиты, нужно разработать методику анализа и оценки угроз.

Анализ рисков состоит из мероприятий по обследованию организаций с целью определения ресурсов, которые нужно защищать, и видов угроз для образовательной организации. По результатам исследований организации необходимо определить факторы, которые влияют на реализацию угроз безопасности и их воздействия.

В данный момент нет стандартизированной методики для анализа и оценки угроз информационной безопасности для образовательных учреждений. Все разработанные методики оценки угроз являются всего лишь рекомендательными, но не обязательными для исполнения организациями.

Главная **проблема** исследования – создать методику оценки угроз информационной безопасности образовательного учреждения, приняв за основу существующие стандарты и методики управления рисками информационной безопасности.

Цель исследования – проведения анализа информационной структуры образовательной организации и оценивание рисков и угроз информационной системы и ресурсов образовательной организации.

Объект исследования – меры защиты информационных систем, которые хранят, создают информацию, которая важна со стороны обеспечения ее конфиденциальности, сохранения целостности и доступности.

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

Гипотеза исследования - создание методического аппарата, который позволяет делать разумный выбор защитных мер для информационных систем, применяя научно-обоснованной методики оценки рисков угроз.

Цель достигается путем разрешения установленной гипотезы, поэтому требуется разделить ее на подзадачи:

- Рассмотрение видов угроз и составление их характеристик;
- Определение угроз, рисков и уязвимостей в защитной системе образовательного учреждения;
- Анализ методик и методов оценки рисков информационной безопасности;
- Создание способов анализа и оценки рисков информационной безопасности, которые связаны с угрозами безопасности информационных ресурсов;
- Анализ информационных ресурсов университета, уязвимостей и источников угроз;
- Создать описание угроз информационной безопасности по ранее созданным способам анализа и оценки.

Методы исследования

Для создания понятий в диссертации применяются приемы логики, анализа, синтеза и определения. Так же применяется структурный и системный анализ для создания комплекса мер защиты. Еще используются методы математической статистики.

Научная новизна результатов исследования – создать методику которая улучшит выбор мер защиты информационных систем, различия которых разнятся использованием показателя затратоемкости.

Обоснованность полученных результатов возможна при использовании современного математического аппарата и должны быть

согласованы с современными практиками в области информационной безопасности.

Практическая значимость исследования – выбранная методика, которая позволяет увеличить качество подбора защитных мер для информационной системы образовательного учреждения и реализована в виде модуля управления рисками безопасности ИС.

База исследования: Федеральное государственное бюджетное образовательное учреждение высшего образования «Южно-Уральский государственный гуманитарно-педагогический университет», расположенный по адресу: г. Челябинск, пр. Ленина 61.

ГЛАВА 1. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

1.1 Виды угроз информационной безопасности в образовательном учреждении и их характеристика

Угрозы информационной безопасности – это условия и факты, которые создают возможную или реальную угрозу, которая связана незаконным воздействием на систему и похищением данных[34].

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

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

Под угрозами конфиденциальной информации понимаются вероятные действия к информационным системам и ее ресурсам. Они могут приводить к незаконному завладению данными сведениями.

Такие действия как:

- Знакомство с информацией без нарушения ее целостности;
- Значительное или незначительное изменение информации и ее состава;
- Нанесение урона информации вплоть до ее уничтожения в криминальных целях.

В итоге, незаконные действия с информацией нарушают ее тайну, правдивость и целостность, что может повлечь за собой к нарушению режима управления и качества.

Каждая угроза наносит ущерб – моральный или материальный, а меры защиты и предупреждения угрозе позволяет уменьшать его количество, в идеальном варианте – полностью уменьшить, в реальных

случаях – максимально снизить ущерб или в частичной мере. Но и это получается далеко не всегда [40].

С учетом этого, происходит систематизация угроз по следующим группам:

1. По величине принесенного ущерба:

- Предельный, после которого образовательное учреждение может прекратить свою деятельность;
- Значительный, но не приводящий прекращению деятельности;
- Незначительный, который не влияет на образовательное учреждение.

2.

По вероятности возникновения:

- Весьма вероятная угроза;
- Вероятная угроза;
- Маловероятная угроза.

3. По причинам появления:

- Стихийные бедствия;
- Преднамеренные действия.

4. По характеру нанесенного ущерба:

- Материальный;
- Моральный.

5. По характеру воздействия:

- Активные;
- Пассивные.

6. По отношению к объекту:

- Внутренние;
- Внешние.

Источники внешних угроз:

- Конкуренты;

- Преступные личности;
- Отдельные лица и организации административно-управленческого аппарата.

Источники внутренних угроз:

- Администрация;
- Персонал;
- Технические средства обеспечения производственной и трудовой деятельности [40].

Внешние и внутренние угрозы соотносятся таким образом:

- 82% - внутренние. Совершены как при участии сотрудников, так и ими самими;
- 17% - внешние угрозы;
- 1% - случайные[40].

Главная особенность угроз – это не только вероятность хищения данных или их повреждение и изменение, но и возможность повреждения студентами, как самого оборудования, так и внесение различных вредоносных программ. Всего выделяется четыре группы объектов, которые могут быть подвержены случайному либо намеренному повреждению:

- Компьютерное оборудование и другие аппаратные компоненты, которые могут быть повреждены или выведены из строя;
- Программное обеспечение, используемое для корректной работы образовательной системы, могут пострадать от вредоносных программ;
- Данные, содержащиеся на различных носителях, таких как жесткие диски, флеш-накопители и др.
- Персонал, обеспечивающий корректную работу информационных систем;

- Обучающиеся, подверженные психологическим атакам и информационному влиянию.

Угрозы, направленные на выведение из строя различных компонентов системы, могут быть как случайными, так и преднамеренными. Среду угроз, которые не зависят от действий персонала, обучающихся и третьих лиц, можно выделить следующие:

- Аварийные ситуации, такие как перебои в подаче электроэнергии или возможность затопления;
- Случайные ошибки персонала, основанные на усталости, рассеянности и других причинах;
- Сбои в работе программного обеспечения, возникшие из-за недоработок этого ПО;
- Проблемы в работе систем связи [55];

Данные угрозы временные, прогнозируемы и устранимы действиями обслуживающего персонала и сотрудниками специальных служб.

Преднамеренные угрозы информационной безопасности имеют опасный характер и непредсказуемы. Виновными в данных угрозах могут быть обучающиеся, персонал учреждения, конкуренты и другие лица, заинтересованные в совершении преступления. Для того чтобы внедриться и помешать работе информационных систем данное лицо должно обладать достаточными знаниями в отношении принципов работы программного и аппаратного обеспечения. Наибольшей опасности могут быть подвержены сетевые компоненты, ведь они расположены отдельно друг от друга в пространстве. Нарушив связь между несколькими компонентами, можно вывести ее из строя полностью. Так же возможны варианты похищения интеллектуальной собственности, для присвоения чужих наработок и идей. Конечно, не стоит исключать воздействие на сознание обучающихся, ведь данные методики атак могут привести к вовлечению студентов в криминальные или террористические действия.

С точки зрения проникновения в информационную систему и выполнения нужных атак, необходим несанкционированный доступ.

Способы несанкционированного доступа.

Существует несколько типов несанкционированного доступа:

1. Человеческий. Похищение информации происходит путем ее копирования на различные носители, отправлена по электронной почте. Так же возможен вариант внесение искаженной информации в базы данных при наличии доступа к серверам.
2. Программный. Используются специальные программы, обеспечивающие перехват информации и сетевого трафика, его дешифровку, внесение коллизий и изменений в работу программного обеспечения.
3. Аппаратный. Для выполнения этого способа используются специальные технические средства, обеспечивающие перехват информации с различных каналов связи, в том числе сетевой и телефонный.

Так же существуют 5 принципов системы обеспечения информационной безопасности, которые обеспечивают снижение рисков несанкционированного доступа:

1. Принцип комплексности. При создании систем защиты нужно просчитывать вероятности возникновения всех угроз безопасности для учреждения по всем каналам доступа, в том числе и закрытым. Применение защитных средств должно совпадать вероятными видами угроз и функционировать не только по отдельности, но и осуществлять комплексную защиту, дополняя и закрывая уязвимые стороны друг друга. Комплексные методы и средства защиты представляет собой сложную систему взаимосвязанных между собой процессов.

2. Принцип эшелонирования. Он представляет собой порядок обеспечения информационной защиты организации, в котором все уровни защитной системы состоят из последовательно расположенных зон безопасности, самая важная из которых располагается внутри всей системы.
3. Принцип надежности. Стандарты информационной безопасности в области организации, должен использоваться во всех зонах безопасности. Они должны иметь одну и ту же степень надежной защиты с вероятностью реальной угрозы.
4. Принцип разумной достаточности подразумевает рациональное применение защитных методов с приемлемым уровнем обеспечения безопасности. Создание высокоэффективной системы защиты подразумевает под собой большие материальные затраты, поэтому необходим рациональный подход к выбору системы безопасности. Защитная система не должна стоить больше возможного ущерба и затрат на ее функционирование и обслуживание.
5. Принцип непрерывности. Системы безопасности должны работать круглосуточно и непрерывно [55].

Обычно, защитные системы регламентируются инструкциями, которые разрабатывает и утверждает образовательная организация, принимая во внимание особенности информационной системы, и действующей нормативной базой учреждения.

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

Угроза безопасности ИС – возможное нарушение безопасности информационной системы образовательного учреждения. Наиболее часто угроза является следствием наличия в защите ИС уязвимых мест.

Базовыми угрозами информационной безопасности являются нарушение конфиденциальности, целостности и отказ в обслуживании [15].

Угроза безопасности информации – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность, которая связана с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Возможные источники угроз в образовательном учреждении:

- Учебные аудитории, оснащенные компьютерами, в которых происходит процесс обучения;
- Сеть Интернет;
- Рабочие станции сотрудников, не имеющих квалификации в сфере информационной безопасности.

Анализ информационных рисков разделяют на следующие этапы:

- Классификация объектов, подлежащих защите, по важности;
- Определение привлекательности объектов защиты для нарушителей информационной безопасности;
- Определение вероятных угроз и возможных каналов доступа к объектам;
- Оценка существующих мер обеспечения информационной безопасности;
- Составление списка уязвимостей в защите информационной системы и способов их устранения;
- Составление ранжированного списка угроз;
- Оценка возможного ущерба от несанкционированного доступа и атак, перебоев в работе оборудования и программного обеспечения.

Основные объекты, защищаемые от несанкционированного доступа:

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

- Серверы баз данных;
- Сервер управления учетными записями;
- Различные ftp и www-серверы;
- Внутренние и внешние ЛВС.

Связь с сетью Интернет в большинстве случаев выполняется по различным линиям связи, таким как оптоволоконные магистрали, каналы спутниковой и радиосвязи. Так же есть отдельные каналы для передачи определенных типов данных и созданных для обеспечения их безопасности.

Для предупреждения рисков, связанных с утечкой и искажением передаваемой информации, такие каналы не должны иметь общие точки с глобальными сетями и ЛВС университета.

Критически важные узлы для обмена данными университета также должны быть изолированы от остальных сетей.

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

Таблица 1

Автоматизированное рабочее место сотрудника

Угроза	Уязвимости
1. Физический доступ нарушителя к рабочему месту	1. Отсутствие систем контроля и управления доступом сотрудников к чужим рабочим местам 2. Отсутствие систем видеонаблюдения в учебном заведении
2. Разглашение конфиденциальной информации, используемой и хранящейся на рабочем месте	1. Не заключение договора о неразглашении информации между работником и

сотрудника учреждения	работодателем
3. Искажение, повреждение и потеря конфиденциальной информации, используя вредоносное программное обеспечение и физическое воздействие на носители информации	1. Отсутствие разделения на внутреннюю и внешнюю сети (локальную и Интернет)

Еще в университете могут возникнуть угрозы целостности, конфиденциальности и доступности.

1. Угрозами доступности являются: уничтожение информации вследствие деятельности вредоносного программного обеспечения или физического повреждения оборудования.

Мерами предотвращения данных угроз могут быть следующие варианты:

- Установка антивирусного программного обеспечения;
- Резервирование данных, как и на съемные носители, так и в облачные хранилища для быстрого восстановления данных вследствие каких-либо системных ошибок или повреждения данных;
- Установка источников бесперебойного питания для корректной работы информационных систем при отсутствии подачи электроэнергии;
- Резервирование линий электроэнергии из независимых друг от друга источников;
- Проведение процедур обслуживания, как и самого оборудования, так и инфраструктуры и самого здания в котором располагается инфраструктура.

2. Угрозы нарушения целостности информации: ее нарушение со стороны сотрудников, обслуживающих систему, внесение неверных данных, несанкционированное изменение информации, кража информации, утрата информации с носителей, изменения в базах данных, программных механизмах работы организации.

Можно использовать следующие меры для пресечения данных угроз:

- Введение системы паролей и смена их в течение определенных периодов;
- Разграничение и ограничение прав пользователей в операционных системах;
- Использование криптографических средств защиты информации.

3. Угрозы конфиденциальности: хищение оборудования, внесение лишних или неиспользуемых полномочий на носитель с важной информацией, открытие неиспользуемых портов, установка нелегального программного обеспечения.

Анализ состояния информационной безопасности университета позволяет выявить следующие угрозы:

1. Каналы внесения вредоносного программного обеспечения при использовании различных съемных носителей информации, использовании сети Интернет и локальных сетей.
2. Случайные ошибки сотрудников учреждения, в том числе ввод неверных данных или их изменение.
3. Отказ внутренней инфраструктуры, в том числе отказ как информационных систем, так и программного и аппаратного обеспечения, физическое повреждение аппаратуры.
4. Угрозы технического характера.
5. Угрозы нетехнического характера – отсутствие парольного доступа, хранение конфиденциальной информации в доступных местах.

6. Несанкционированный доступ к информации (использование без разрешений). При этом могут быть выполнены следующие действия: чтение, изменение и удаление информации.
7. Хищение программно-аппаратных средств.
8. Использование устаревших программных и аппаратных средств обработки информации.

Таким образом, наиболее возможными угрозами информационной безопасности в университете являются: кража персональной информации обучающихся, несанкционированное внесение изменений в нее, а так же непреднамеренные ошибки сотрудников при внесении и редактировании данной информации.

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

По итогам первой главы магистерской диссертации можно сделать следующие выводы.

Сформулированы и классифицированы угрозы, которые возникают в информационных системах.

Угроза безопасности информации – возможное изменение основных характеристик информации при ее использовании и обработке. Угрозы информационной безопасности делятся на три группы:

- Вызванные действиями субъекта (антропогенные источники угроз);
- Вызванные техническими средствами (техногенные источники угрозы);
- Вызванные стихийными источниками.

Как правило, защита от угроз определяется действующими инструкциями образовательного учреждения.

В конце, была проведено ранжирование уязвимостей, угроз в защите информации. Предложены меры их устранения, итогом будет повышенная эффективность методов защиты и уменьшение процента потери и изменения информации.

ГЛАВА 2. НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ В ОБЛАСТИ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

2.1. Международные стандарты управления информационной безопасностью

В мире есть огромное количество различных методик в области управления информационными рисками, которые основаны на различных руководствах, методиках и алгоритмах. Большинство из них использованы в государственных и международных стандартах в области информационной безопасности. Они полностью автоматизированы и используются в программных продуктах. Задача заключается в анализе всех ныне существующих методик, определение их характеристик и составление списка подходящих для образовательного учреждения.

ГОСТ Р ИСО/МЭК 27005-2010

Он является стандартом из серии ISO/IEC 27000 и мануалом по управлению рисками информационной безопасности (ИБ) в учреждении, которая поддерживает стандарты к системе управления информационной безопасности согласно стандарту ISO/IEC 27001. Данный стандарт используется в любых организациях и учреждениях, не принимая во внимание их тип, характер и размер [19].

Данный стандарт разработан в 2005 году и до сих пор модифицируется и улучшается, на данный момент актуальна версия 2010 года [19]. Актуальная версия производит замену неактуальных стандартов серии ISO 13335, и в соответствии с этим, стандарты 13335-3 и 13335-4 были отменены (их действие).

Рассмотренный стандарт не предоставляет конкретной методологии по управлению рисками ИБ и является рекомендательным.

Этот стандарт будет основным для анализа учреждения, потому что он описывает все этапы управления рисками и его применение возможно для анализа данной организации[1].

Британский стандарт BS 7799-3

Эти стандарты появились раньше всех, и по праву занимают первое место и звание международного стандарта в сфере управления информационной безопасностью. Первая часть - стандарт BS 7799-1 «Практические правила управления информационной безопасностью». Он разработан в 1995 году и является практическим руководством по управлению ИБ в учреждении.

Второй частью стандарта является BS 7799-2 «Системы управления информационной безопасностью. Спецификация и руководство по применению» - появившаяся в 1998 г., определяет представление СУИБ. Третья часть стандарта – BS 7799-3 «Системы управления информационной безопасностью. Руководство по управлению рисками информационной безопасности» появилась в 2006 году [2].

Данный стандарт предшествует стандарту ISO 27005. Эти стандарты дополняют друг друга, имеют общие черты, а также являются основными в методологии управления рисками, определяют все важные моменты, связанные с рисками. Дополнительно ознакомиться с основными моментами можно в самом стандарте [2].

ГОСТ Р ИСО/МЭК 27001-2006

Данный стандарт является определяющим для систем управления информационной безопасностью, так как он определяет требования к ней.. Стандарты ISO 27005 и BS 7799-3 так же обязаны применяться и использоваться в магистерской работе, так как они взаимосвязаны со стандартом ISO 27001.

С взаимосвязанными требованиями стандартов ISO 27001, ISO 27005 и BS 7799-3, возможно ознакомление в данных пунктах стандарта[18]:

- Создание СУИБ;

- Внедрение и эксплуатация СУИБ;
- Мониторинг и анализ СУИБ;
- Сопровождение и совершенствование СУИБ;
- Анализ СУИБ руководством;
- Улучшение СУИБ.

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

Данная методика разработана Федеральной службой по техническому и экспортному контролю (ФСТЭК) в 2008 году и используется для определения актуальных угроз безопасности персональных данных [38].

Методика выявления современных угроз защищенности персональных данных при их обработке в информационных системах персональных данных создана ФСТЭК России и основана на Федеральном законе от 27 июля 2006 г. N 152-ФЗ «О персональных данных» и «Положении об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», которое утверждено постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781, принимая во внимание нормативные документы ФСТЭК России по обеспечению защиты информации. Данная методика применяется при создании работ по защите персональных данных при их обработке в данных информационных системах:

- Государственных или муниципальных информационных систем персональных данных;
- Информационных системы персональных данных, которые созданы или используются организациями и учреждениями независимо от форм собственности, которые нужны для

реализации этих функций в организациях в соответствии с их назначением;

- Информационные системы персональных данных, которые создаются или используются физическими лицами, не включая в себя случаи использования систем для некоммерческих целей.

Документ используется специалистами по обеспечению безопасности информации, руководителей учреждений и предприятий, организующих и проводящих работы по обработке персональных данных в информационных системах персональных данных.

Под угрозами безопасности персональных данных при их обработке в информационных системах персональных данных 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» данные обязательно должны быть под защитой от незаконного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных незаконных действий. Угрозы безопасности данных могут возникать как со случайными действиями персонала, так и с действиями потребителей данных. Еще существует возможность угрозы за счет незаконных действий других источников угроз [43].

Возможна реализация угроз персональных данных за счет утечки по различным техническим каналам, а также при неправомерном доступе. Подробное описание угроз находится в «Базовой модели угроз безопасности персональных данных при их обработке в информационных

системах персональных данных». Определение каналов утечки персональных данных основан на нормативных и методических документах ФСТЭК России. Источники угроз, которые реализуются с помощью неправомерного доступа к базам данных с применением стандартного или разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в информационных системах персональных данных правила разграничения доступа к информации. Этими субъектами могут быть:

- Нарушитель;
- Вредоносное программное обеспечение;
- 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, которые представляют информационные услуги удаленным пользователям, внешними нарушителями могут быть лица, имеющие возможность несанкционированного доступа к информации с использованием специальных программных воздействий, алгоритмических или программных закладок через автоматизированные рабочие места,

терминальные устройства ИСПДн, подключенные к сетям общего пользования.

Полномочия внутреннего нарушителя в большей степени зависят от установленных разграничений по допуску физических лиц к информационным ресурсам ИСПДн и мер по контролю порядка проведения работ.

Угрозы неправомерного доступа от нарушителей извне могут выполняться с помощью межсетевых протоколов. Подробное описание угроз, которые связаны с незаконным доступом в информационные системы персональных данных, подробно описано в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Выявляются угрозы несанкционированного доступа, которые реализуются с помощью программно-аппаратных средств, с помощью опросов специалистов, сотрудников, используя различные инструментальные средства. Для проведения опроса составляются специальные опросные листы.

Если выявлен источник угрозы, который может использоваться для выполнения угрозы, то это показывает, что данная угрозы есть. На основе опросов происходит составление списка угроз персональных данных. После проведения аудита сетевых источников, составляется список каналов утечки. На основании этого перечня в связи с описанным ниже порядком создается список актуальных угроз безопасности персональных данных. Угроза имеет актуальность, если она опасна для персональных данных и при этом выполняется в информационной системе персональных данных. Составление списка актуальных угроз происходит при использовании показателей исходной защищенности системы и вероятность выполнения угрозы.

Уровень исходной защищенности – это общий показатель, зависит он от технических и эксплуатационных характеристик информационных систем персональных данных, которые представлены в таблице 2.

**Показатели исходной защищенности информационных систем
персональных данных**

Технические и эксплуатационные характеристики информационных систем персональных данных	Уровень защищенности		
	Высокий	Средний	Низкий
<i>1. По территориальному размещению:</i>			
Охватывающая области, края, округа или страну;	-	-	+
Охватывающая город, село, поселок;	-	-	+
Охватывающая отделы и подразделения компании;	-	+	-
Локальная, охватывает рядом расположенные здания;	-	+	-
Локальная, охватывает здание;	+	-	-
<i>2. По наличию соединения с сетями общего пользования:</i>			
Имеет множество выходов в общую сеть;	-	-	+
Имеет единственный выход в общую сеть;	-	+	-
Не имеет выходов в общую сеть;	+	-	-
<i>3. По встроенным (легальным) операциям с записями баз персональных данных:</i>			
Имеет разрешение на операции поиска и чтения;	+	-	-
Имеет разрешение на операции записи, сортировки и удаления данных;	-	+	-
Имеет разрешение на операции передачи и модификации;	-	-	+
<i>4. По разграничению доступа к персональным данным:</i>			
Имеют доступ владельцы персональных данных или владельцы информационной системы;	-	+	-
Имеет доступ весь персонал владельца информационной системы;	-	-	+
Имеет открытый доступ;	-	-	+
<i>5. По наличию соединений с другими базами ПДн иных ИСПДн:</i>			
Использует другие информационные базы и не владеет ими;	-	-	+
Использует единственную базу и является ее владельцем;	+	-	-
<i>6. По уровню обобщения (обезличивания) ПДн:</i>			
Имеет обезличенные данные;	-	+	-
Обезличивание происходит при передаче в другие организации;	-	+	-
Не имеют обезличивание;	-	-	+
<i>7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:</i>			
Предоставляет всю базу данных;	-	-	+
Предоставляет часть базы данных;	-	+	-
Не предоставляет информацию.	+	-	-

Исходная степень защищенности должна определяться 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 положительных 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 создании перечня угроз персональных данных каждому уровню возможность появления угрозы соответствует свой коэффициент:

0 – степень защищенности высокая;

5 – степень защищенности средняя;

10 – степень защищенности низкая.

Вероятность выполнения угрозы – показатель, характеризующий какова возможность выполнения угроз безопасности. Существует четыре степени данного показателя:

- маловероятно – нет вероятности для исполнения угрозы;

- низкая вероятность – вероятность исполнения угрозы есть, но меры защиты практически не позволяют ее выполнить;

- средняя вероятность - вероятность исполнения угрозы есть, но есть уязвимости в мерах защиты, позволяющие ее реализовать;

- высокая вероятность - вероятность исполнения угрозы есть, меры защиты не выполняются.

Затем происходит оценка каждой угрозы. При определении уровня опасности, также вычисляется устный показатель опасности для

информационной системы персональных данных. Этот показатель имеет три значения:

низкая опасность – выполнение угрозы приводит незначительные последствия;

средняя опасность – выполнение угрозы приводит к негативным последствиям;

высокая опасность – выполнение угрозы приводит к значительным последствиям.

В дальнейшем, выбираются угрозы безопасности из общего списка угроз, которые актуальны для данной информационной системы, в соответствии с правилами, приведенными в таблице 3.

Таблица 3

Правила отнесения угрозы безопасности персональных данных к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Высокая	Средняя	Низкая
Очень высокая	Актуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Средняя	Актуальная	Актуальная	Неактуальная
Низкая	Актуальная	Неактуальная	Неактуальная

С применением данных о классе информационных систем персональных данных и созданного 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» утверждаются конкретные технические требования по защите информационных систем персональных данных от утечки информации по техническим каналам, от неправомерного доступа и выполняется выбор программных и аппаратных средств защиты

информации, используемые при создании и дальнейшей эксплуатации информационных систем персональных данных.

Поэтому, методика оценки включает в себя следующие этапы:

- Оценивание изначального уровня защиты системы;
- Оценивание вероятности выполнения угроз;
- Оценивание опасности угроз по отдельности;
- Оценивание их актуальности;
- Формирование требований по обеспечению безопасности.

Оценивание отдельных параметров производится по определённой в документе шкале. Расчет итогов происходит по формуле, в результатах которой показывается качественная и количественная оценка исследуемой угрозы [48].

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

Во второй главе магистерской диссертации были рассмотрены и проведен анализ основных стандартов в области управления рисками информационной безопасности. Были определены стандарты, удовлетворяющие целям оценки рисков в специфике деятельности образовательного учреждения.

В качестве главного стандарта выбран ГОСТ Р ИСО/МЭК 27005-2010. Он показывает все этапы управления рисками и полностью подходит для образовательного учреждения и его специфики.

Другие стандарты, которые были рассмотрены в данной главе, тоже будут использоваться как дополнения к главному стандарту.

ГЛАВА 3. РАЗРАБОТКА ОЦЕНКИ РИСКА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФГБОУ ВО «ЮЖНО- УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО- ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

3.1. Методика оценивания риска угроз, ее концепция и основные этапы

Основным стандартом выбран стандарт ISO 27005-2010, который предлагает следующие этапы оценки рисков:

- Анализ риска, в него входят идентификация рисков, включая в себя определение активов, угроз, существующих средств контроля, уязвимостей, последствий;
- Измерение рисков;
- Оценивание рисков.

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

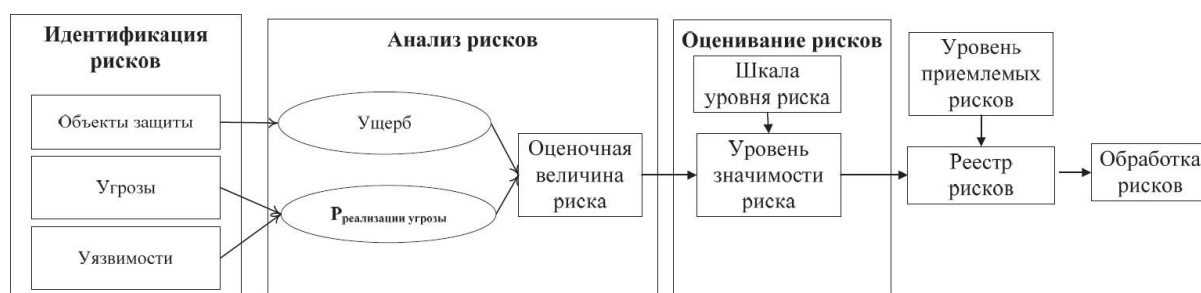


Рис.1. Процесс оценки рисков информационной безопасности

В современном мире есть множество методик анализа рисков. Часть из них создана на табличных методах и не предполагают применения специализированного программного обеспечения, другая часть используют его активно. Несмотря на то, что постоянно повышается интерес к управлению рисками, методики, которые используют в настоящее время, довольно неэффективны, так как данный процесс во многих организациях производится каждым подразделением независимо.

Централизованный контроль над действиями подразделений в большинстве случаев отсутствует, что исключает, что ставит крест на возможности реализации единого и целостного подхода к управлению рисками во всей организации.

Для решения задачи оценки рисков информационной безопасности в большинстве случаев используют 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].

Определяем основные этапы, необходимые для целей оценки риска:

1. Идентификация активов. Нужно определить и описать все активы образовательного учреждения и оценить их. Определение активов происходит во время проверки информационной безопасности, рассматривается структура организации. Выявляются основные системы обработки данных и эти данные переносятся в перечень в виде таблицы.
2. Идентификация угроз. Нужно определить перечень угроз с описанием вида и источника. Определение угроз происходит во время аудита информационной безопасности, учитывая угрозы безопасности данных, которые предоставлены банком угроз безопасности ФСТЭК России [8].

3. Определение уязвимостей. Нужно создать перечень уязвимостей, которые связаны с активами, угрозами и средствами контроля; перечень уязвимостей, которые не связаны с подлежащей к рассмотрению определенной угрозой.
4. Измерение риска. Выбор методологии (из представленных далее) определения риска, которая включает в себя качественную или количественную оценку риска. Во время этого этапа происходит оценивание угроз и уязвимостей, по различным шкалам экспертным путем. Происходит занесение данных в общую таблицу, где проводится оценка риска на основании ценности актива.
5. Измерение уровня риска. Происходит составление перечня рисков с присвоенными уровнями значений.
6. Оценивание риска. На этом этапе происходит сравнение измеренных рисков с критериями оценивания риска. В итоге происходит составление список рисков, с приоритизацией с критериями оценивания риска касательно сценариев инцидентов, приводящих к этим рискам.

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

Данный стандарт [19] предполагает следующие подходы в оценке рисков:

- Оценивание рисков высокого уровня;
- Подробное оценивание рисков.

Первый подход используется для первоначальной оценки, с построением стратегической картины при малых затратах ресурсов и денежных средств. Этот метод более глобально рассматривает организацию и её информационные системы, определяется более малый перечень угроз и уязвимостей, а риски - более общие.

Второй подход использует матричный метод, с помощью таблицы. В стандарте используется три метода оценки рисков. Данный подход заключается в определении ценности активов, оценивании угроз данных активов и оценивании уязвимостей.

Первый метод – матрица с predetermined значениями.

Мера риска определяется с помощью стандарта. Оценка приведена в таблице 4, рассчитываясь 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 рассчитывается со стороны цены его замены, покупки или восстановления (для физического актива или программного). Все оценки приводятся к единой шкале от 0 до 8. Затем происходит распознавание каждого вида угроз для каждой группы активов, связанных с видами угроз, для проведения дальнейшей оценки. Уровень угрозы равен возможности ее возникновения. Уровень уязвимости равен простоте

использования угрозы для вызова неблагоприятных воздействий. Оценка производится от высокого до низкого уровня.

На основании данных из таблицы 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).

Началом будет оценка последствий от 1 до 5 для активов, которые под угрозой (b). Второй шаг – оценка вероятности появления угрозы от 1 до 5 (c). Третий шаг – вычисление меры риска путем умножения (bxc), после чего происходит распределение угроз.

Таблица 5

Распределение угроз через меры риска

Идентификатор угрозы (a)	Последствия (ценность актива) (b)	Степень вероятности возникновения угрозы (c)	Мера риска (d)	Ранжирование угроз (e)
Угроза А	5	2	10	2
Угроза В	2	4	18	3
Угроза С	3	5	15	1
Угроза D	1	3	3	5
Угроза Е	4	1	4	4
Угроза F	2	4	8	3

Данный порядок распределяет приоритет угроз по видам последствий и вероятностям появления.

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

Метод выведен на оценке двух значений – комбинация будет определять количество баллов для каждого актива. Данный метод, помимо

оценки риска, определяет то, какие системы будут получать приоритет при обработке риска. Метод основан на тех же таблицах, что и первый метод, только внесены небольшие изменения.

Для начала, происходит присвоение для каждого актива ценности. В дальнейшем, идет оценивание вероятностей угрозы, которая равна соотношению степени вероятности возникновения угрозы и простоты использования уязвимости по таблице 6.

Таблица 6

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

Последний шаг – расчёт всех баллов активов для подведения итогов и вычисления баллов системы. Эти итоговые баллы используются для ранжирования предпочтений защиты систем[19].

Итоги оценивания рисков

Список оцененных рисков, ранжированных в связи с приоритетами и критериями оценивания риска.

В данной работе оценка рисков будет выполняться по последнему методу, потому что он оценивает полностью систему, а это как раз нам и нужно.

Уровень угрозы определятся по руководству ФСТЭК определения актуальных угроз [38] так как в информационной системе университета главная информация, которая должна быть защищена – персональные данные. Применительно используемой методики, нужен расчет начального уровня защищенности системы (Y1) и вероятность ее выполнения (Y2).

Затем происходит оценка данных параметров экспертами и в конечном итоге будет рассчитан коэффициент реализуемости угрозы Y , который и есть наш уровень. Его вычисление делается по данной формуле:

$$Y = (Y1 + Y2)/20.$$

где $Y1$ равен следующим значениям:

0 – степень защищенности высокая;

5 – степень защищенности средняя;

10 – степень защищенности низкая.

$Y2$ - показатель, который показывает насколько возможно выполнение угрозы персональных данных в данных условиях. Показатель обладает следующими параметрами:

Таблица 7

Описание параметров показателя $Y2$

$Y2$	Описание
Маловероятно (0)	Нет показателей для реализации угрозы.
Низкая вероятность (2)	Показатели для реализации угрозы есть, но она мало реализуема.
Средняя вероятность (5)	Показатели для реализации угрозы есть, но меры по защите персональных данных недостаточны.
Высокая вероятность (10)	Показатели для реализации угрозы есть, мер по защите персональных данных нет.

Тогда по итогу уровень угрозы Y вычисляется следующей шкалой:

если $0 \leq Y \leq 0,3$ - возможность реализации угрозы низкая;

если $0,3 < Y \leq 0,6$ - возможность реализации угрозы средняя;

если $0,6 < Y \leq 0,8$ - возможность реализации угрозы высокая;

если $Y > 0,8$ - возможность реализации угрозы очень высокая.

Уровень уязвимости – вероятность реализации незаконного доступа к системе и определяется по шкале в таблице 8:

Таблица 8

Показания уровня уязвимости

Уровень уязвимости	Описание
Высокий	Возможность полного контроля над системой;

Средний	Возможность полного контроля над системой существует, но нет средств для ее реализации;
Низкий	Возможность получения информации, потеря которой не критична.

Последним этапом анализа рисков является их оценивание и обработка. Оценивание риска производится по заданным критериям. По стандарту ISO 27005 критерии оценивания будут следующие:

- 0 – 2 – малый риск;
- 3 – 5 – средний риск;
- 6 – 8 – огромный риск;

По результатам анализа рисков, оценки будут производиться относительно выявленных угроз. Затем границы критериев будут такими:

- $[0; 2x + x/2]$ – малый риск;
- $[3x - x/2; 5x + x/2]$ – средний риск;
- $[6x - x/2; 8]$ – огромный риск.

Где x – количество выявленных угроз.

3.2. Анализ информационно-телекоммуникационной системы ФГБОУ ВО «Южно-Уральский государственный гуманитарно-педагогический университет»

Объектом исследования является Федеральное государственное бюджетное образовательное учреждение высшего образования «Южно-Уральский государственный гуманитарно-педагогический университет», расположенный по адресу: 454080, Российская Федерация, Уральский федеральный округ, Челябинская область, г. Челябинск, пр. Ленина, 69.

Учредителем университета является Министерство науки и высшего образования Российской Федерации.

Челябинский государственный педагогический институт был основан в 1934 году (Постановление Оргкомитета советов от 22 июля 1934 г. № 949-а «Об организации с нового учебного года в городах

Магнитогорске и Челябинске двухгодичных институтов по подготовке преподавателей неполной средней школы»).

В предвоенные годы институт сыграл исключительно важную роль в становлении и развитии общеобразовательной школы и высшего педагогического образования в Уральском регионе. В первые дни Великой Отечественной войны вслед за директором института Д.А. Клюкиным в ряды Красной Армии ушли более 500 человек. Пали смертью храбрых декан географического факультета С.З. Калинин, преподаватели Г.В. Жикол, Н.А. Крискевич, выпускник филологического факультета, Герой Советского Союза А.И. Невзгодков, студенты института Ю. Ичева, М. Уваров, И. Волков и многие др.

Уже в 1966 году институт обладал мощным научно-педагогическим потенциалом и был причислен к вузам 1-й категории.

Имена многочисленных выпускников: Е.М. Тяжелникова, Л.П. Скобликовой, В.А. Караковского и других – знала вся страна. ЧГПИ был инициатором создания первого в стране Научного общества учащихся (НОУ) и стал вместе с Дворцом пионеров и школьников имени Н.К. Крупской лауреатом премии Ленинского комсомола (1971). В 1971 при ЧГПИ был организован первый в стране педагогический отряд «Луч».

Указом от 11 сентября 1984 года Президиума Верховного Совета Союза Советских Социалистических Республик Челябинский государственный педагогический институт был награжден орденом «Знак Почета», что и отражалось в наименовании вуза.

Коллектив института в течение многих лет был участником ВДНХ СССР, удостоен диплома 1-й степени, получил 5 медалей.

В 1980-е годы вуз неоднократно получал переходящее Красное знамя Министерства просвещения СССР, РСФСР и ЦК профсоюза работников просвещения, высшей школы и научных учреждений.

С 1993 года государственная награда бывшего СССР в официальном наименовании вуза не указывается (Типовое положение об образовательном учреждении высшего профессионального образования (высшем учебном заведении) Российской Федерации, утвержденное постановлением Совета Министров - Правительства Российской Федерации от 26 июня 1993 г. № 597).

В 1995 году Челябинский орден «Знак Почета» государственный педагогический институт был переименован в Челябинский государственный педагогический университет согласно приказу от 31.10.1995 г. № 1229 (приказ Госкомитета по Высшей школе от 17.10.1995 г. № 1445 «Об изменении статуса Челябинского ордена «Знак Почета» государственного педагогического института»).

18 декабря 2002 года Челябинский государственный педагогический университет зарегистрирован в организационно-правовой форме: государственное образовательное учреждение высшего профессионального образования «Челябинский государственный педагогический университет» (Свидетельство о внесении записи в «Единый государственный реестр юридических лиц о юридическом лице», серия 74 № 002183039 от 18 декабря 2002г.)

В 2011 году государственное образовательное учреждение высшего профессионального образования «Челябинский государственный педагогический университет» переименовано в федеральное государственное

бюджетное образовательное учреждение высшего профессионального образования «Челябинский государственный педагогический университет» согласно приказу от 27.05.2011 г. № 1840 (приказ Министерства образования и науки Российской Федерации «О государственном образовательном учреждении высшего профессионального образования «Челябинский государственный педагогический университет»).

21 июля 2011 г. Государственное образовательное учреждение высшего профессионального образования «Челябинский государственный педагогический университет» зарегистрирован в организационно-правовой форме: федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Челябинский государственный педагогический университет» (Свидетельство о внесении записи в «Единый государственный реестр юридических лиц о юридическом лице», серия 74 № 005360157 от 21 июля 2011 г.).

В 2016 г. федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Челябинский государственный педагогический университет» переименовано в федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный педагогический университет» согласно приказу от 11.03.2016 г. № 203 (Приказ Министерства образования и науки Российской Федерации «О федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Челябинский государственный педагогический университет»).

В 2016 г. федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный педагогический университет» переименовано в федеральное

государственное бюджетное образовательное учреждение высшего образования «Южно-Уральский государственный гуманитарно-педагогический университет» согласно приказу от 05.07.2016 г. № 811 (Приказ Министерства образования и науки Российской Федерации «О переименовании федерального государственного бюджетного образовательного учреждения высшего образования «Челябинский государственный педагогический университет» и его филиала и о внесении изменений в устав федерального государственного бюджетного образовательного учреждения высшего образования «Челябинский государственный педагогический университет»)[47].

Руководство Университета и его педагогический коллектив Управление Университетом производится согласно законодательству Российской Федерации и Уставу учебного учреждения.

Органами управления Университета являются конференция работников и обучающихся Университета, ученый совет Университета, ректор Университета, попечительский совет Университета.

Организационная структура Университета представлена на рисунке 2.

Доступ сотрудников и обучающихся к информационным ресурсам регламентируется посредством Положения об электронной информационно-образовательной среде ФГБОУ ВО ЮУрГГПУ [47]

Сотрудники Университета имеют бесплатный доступ к образовательными, методическими и научными услугами Университета. Пользование образовательными, методическими и научными услугами Университета осуществляется через сайт и локальную вычислительную сеть Университета, а также личные кабинеты Студента и внутренний облачный Портал ФГБОУ ВО «ЮУрГГПУ».

Учреждение, которое мы проверяем, имеет данные виды информационных ресурсов:

Коммерческая тайна:

- Трудовые договора сотрудников;
- Контракты, заключенные с различными поставщиками и арендаторами;

Информация, находящаяся под защитой:

- Личные дела сотрудников и обучающихся;
- Содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности;
- Информация для внутреннего использования.

Открытая информация:

- Информация на web-сайте www.cspu.ru;
- Учредительные документы;
- Устав Университета;
- Лицензия на осуществление образовательной деятельности (с приложениями);
- Перечни образовательных программ, коллективные договоры и прочая информация.

Доступ к информационным ресурсам осуществляется с помощью персональных компьютеров, подключенных к сети Интернет. Для доступа используются идентификационные данные (Логин и Пароль либо Учетная запись), выдача которых осуществляется системным администратором Университета.

Электронная информационно-образовательная среда обеспечивает возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), как на территории Университета, так и вне ее. Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам и электронным библиотекам, содержащим издания по основным изучаемым дисциплинам и сформированным по согласованию с правообладателями учебной, учебно-методической и научной литературы.

Сведения об различных документах, размещены на сайте Университета.

Электронные ресурсы Университета представлены следующими позициями:

- Университетская сеть рассчитана на 1300 персональных компьютеров, в учебных целях используются 431 компьютер, так же доступно 425 ПК для использования обучающимися в свободное от основных занятий время.
- Локальная вычислительная сеть обеспечивает доступ к информационным ресурсам Университета на скорости 100 Мбит/с, оптические магистрали между корпусами до 1Гбит/с. Так же используются 22 точки беспроводного доступа.
- Внутренний облачный Портал ФГБОУ ВО «ЮУрГГПУ» www.cspu.sharepoint.com;
- Официальный сайт ФГБОУ ВО «ЮУрГГПУ» www.cspu.ru;

- Официальная группа «Студенческое сообщество ЮУрГГПУ» ВКонтakte <https://vk.com/id172953539>;
- Каталог образовательных информационных ресурсов Образовательный Портал ЮУрГГПУ- <https://cspu.sharepoint.com/sites/education/>;
- Электронная библиотечная система ЮУрГГПУ <http://elib.cspu.ru/xmlui/>;
- Электронный каталог ЮУрГГПУ - система “Элекат” <http://elecat.cspu.ru/>;
- Периодические издания (электронные версии журналов ФГБОУ ВО «ЮУрГГПУ») (<http://www.cspu.ru/nauka/vestnik-chgpu/>);
- Электронные библиотечные системы и электронные библиотеки, доступ к которым осуществляется на договорной основе - ЭБС IPRbooks: <http://iprbookshop.ru/>;
- Программные оболочки Moodle;
- Корпоративная служба электронной почты mail.cspu.ru;
- Автоматизированная система управления 1С:Университет;
- 1С:Бухгалтерия;
- Справочно-правовая система «Консультант»;
- Система «Антиплагиат»;
- Система с применением асинхронного и синхронного электронного обучения <https://cspu.sharepoint.com/sites/edudistance/>[47].

Используется программное обеспечение, позволяющее полностью реализовывать образовательные программы.

Применяются:

- Операционная система Windows 10 Enterprise 2016 LTSC (Договор №16-1726 от 13.12.2016);

- Microsoft Office Professional Plus 2016 (Договор №16-251 от 05.04.2018);
- Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition (Договор №16-17 от 18.01.2018);
- Справочная правовая система Консультант плюс (Договор №16-81 от 14.02.2018);
- Электронная библиотечная система ЮУрГГПУ на платформе DSpace (Открытая лицензия BSD);
- Научная электронная библиотека eLIBRARY (Лицензионное соглашение №1678 от 01.08.14);

Таким образом, в Университете одним из приоритетных направлений в деятельности вуза является информатизация образовательного процесса, которая рассматривается как процесс, направленный на повышение эффективности и качества учебных занятий и администрирования посредством применения ИКТ. Кроме этого в вузе организовано 50 мультимедийных аудиторий, оснащенных проекторами, экранами и интерактивными досками.

Студенты имеют возможность работать на компьютерах и в сети Интернет в рамках плановых занятий, а также в свободном доступе, если аудитория не занята по расписанию.

В свободное от занятий время каждый желающий (преподаватель или студент) может воспользоваться техническими и сетевыми ресурсами для выполнения учебных задач [47].

Отдел управления информационными технологиями выполняет комплекс работ, связанных с выработкой и реализацией единой корпоративной политики в вопросах внедрения информационных коммуникационных технологий во все сферы деятельности подразделений университета - управленческую, образовательную, воспитательную, научную и обеспечения ресурсами.

Занимается информатизацией управленческой и научно-исследовательской деятельностью, а также информатизацией учебно-воспитательного процесса.

В локальной сети университета есть Внутренний облачный Портал ФГБОУ ВО «ЮУрГГПУ» (Доступен по адресу www.cspu.sharepoint.com), который позволяет сотрудникам и обучающимся вести учебную деятельность удаленно, из дома. Сотрудники имеют возможность добавлять, редактировать и изменять документы, папки, в зависимости от статуса сотрудника. При этом, для изменения необходимо выполнить вход в Внутренний облачный Портал с помощью учетной записи Университета.

Так же сотрудники и обучающиеся имеют личные почтовые ящики, имеют доменный адрес Университета (@cspu.ru), и обсуживаются на почтовом сервисе mail.ru.

В университете имеется система 1С:Университет ПРОФ, с помощью которого осуществляется автоматизация основных процессов высшего образования, таких как:

- Приемная комиссия;
- Учебно-методический отдел;
- Научно-исследовательская часть;
- Управление аспирантуры и докторантуры;
- Диссертационные советы;
- Студенческий отдел кадров;
- Управление довузовского и дополнительного образования;
- Профсоюзный комитет.

Для автоматизации приема документов в Университете работает система 1С-Университет, которая позволяет автоматизировать прием документов у абитуриентов и хранит следующие персональные данные: личная информация абитуриента;

- контактная информация абитуриента;

- данные о ранее полученном образовании;
- данные о результатах ЕГЭ (не обязательно для заполнения, реализована возможность автоматизированной массовой загрузки этой информации);
- о направлениях подготовки (специальностях), на которые подает заявление абитуриент;
- перечень вступительных испытаний, сдаваемых абитуриентом (автоматическое заполнение на основании выбранного набора вступительных испытаний);
- отметка о согласии на зачисление на одно из направлений подготовки (установка данной отметки не обязательна);
- информация о льготах, отличительных признаках, результатах олимпиад абитуриента;
- информация о здоровье (группа здоровья, физкультурная группа, отметки о потребности в адаптированной программе и длительном лечении);
- информация об индивидуальных достижениях абитуриента;
- перечень документов, поданных абитуриентом при поступлении;
- сведения о родителях абитуриента[6].

Эти данные охраняются законом «О защите персональных данных».

Эти данные хранятся на серверах баз данных в университете с помощью пользовательского интерфейса программного обеспечения 1С-Университет. Каждый пользователь системы имеют доступ с помощью индивидуального набора логин/пароль, каждое изменение данных фиксируется.

Анализ и оценки рисков осуществляется по методике, разработанной во второй главе данной работы.

Определение активов

3) Список информационных систем, которые мы получили в результате исследования систем информационной безопасности университета, представлен в таблице 10. Ценность активов, была определена опытным путем.

Таблица 9

Перечень АИС и ИСПДн, обрабатывающих КИ, КТ и ПДн

№ П/П	Наименование информационной системы	Описание информационной системы	Перечень содержания информационной системы
1	ИС: Университет ПРОФ	Комплексное решение позволяет автоматизировать учет, хранение, обработку и анализ информации об основных процессах высшего учебного заведения: поступление в вуз, обучение, оплата за обучение, выпуск и трудоустройство выпускников, расчет и распределение нагрузки профессорско-преподавательского состава, деятельность учебно-методических отделов и деканатов, поддержка ГОС, ФГОС ВПО, ФГОС ВО и уровневой системы подготовки (бакалавр, специалист, магистр) на уровне учебных планов и документов государственного образца об окончании вуза, формирование отчетности, а также управление научной работой и	контактная информация абитуриента; данные о ранее полученном образовании; данные о результатах ЕГЭ (не обязательно для заполнения, реализована возможность автоматизированной массовой загрузки этой информации); о направлениях подготовки (специальностях), на которые подает заявление абитуриент; перечень вступительных испытаний, сдаваемых абитуриентом (автоматическое заполнение на основании выбранного набора вступительных испытаний); отметка о согласии на зачисление на одно из направлений подготовки (установка данной отметки не обязательна);

		инновациями, дополнительным и послевузовским образованием, аттестацией научных кадров, кампусом вуза, личные кабинеты (поступающий, студент, преподаватель).	информация о льготах, отличительных признаках, результатах олимпиад абитуриента; информация о здоровье (группа здоровья, физкультурная группа, отметки о потребности в адаптированной программе и длительном лечении); информация об индивидуальных достижениях абитуриента; перечень документов, поданных абитуриентом при поступлении; сведения о родителях абитуриента
2	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
3	Сайт образовательной организации (www.cspu.ru)		Персональные данные преподавателей (ФИО, контактные данные, краткая биография, информация о стаже и др.) Сведения об образовательном учреждении (в

			соответствии с Приказом Рособрнадзора №785 от 29.05.2014 "Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети "Интернет" и формату представления на нем информации" (с изменениями от 27.11.2017 приказ №1968 и 14.05.2019 приказ №631))
4	1С:Бухгалтерия	1С:Бухгалтерия — это профессиональный инструмент бухгалтера, с помощью которого можно вести бухгалтерский и налоговый учет, готовить и сдавать обязательную отчетность. Программа объединила в себе все достижения предыдущих версий и новые решения, основанные на опыте практической работы бухгалтеров сотен тысяч предприятий и организаций.	<p>ФИО сотрудников</p> <ul style="list-style-type: none"> - 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

Определение уязвимостей

В ходе проведения аудита информационной безопасности образовательного учреждения были выявлены уязвимости в следующих областях:

- Сотрудники Университета;

- Внутренние помещения и оборудование;
- Нормативно-методическая база;
- Системы связи;
- Программное обеспечение и операционные системы.

Сотрудники Университета могут создать множество угроз. По неосторожности и невнимательности персонал может нанести непреднамеренный вред организации. Несоблюдение договора о нераскрытии персональных данных может повлечь за собой раскрытие конфиденциальных информации организации, что приведет к репутационному и (или) финансовому ущербу. Несоблюдение техники безопасности может привести к физическому ущербу, такому как пожар, затопление и др.

Внутренние помещения и оборудование подразумевают под собой множество различных вариантов реализации угроз. Пренебрежение системами пожарной безопасности, контроля доступа и помещения, не отвечающие требованиям пожарной безопасности, могут привести к ряду различных угроз. Со стороны оборудования могут возникать неисправности оборудования из-за его морального и физического устаревания. Такое оборудование очень чувствительно к параметрам окружающей среды, необходимость защиты от несанкционированного доступа.

Программное обеспечение и операционные системы имеют множество уязвимостей, возникающих из-за ошибок в программном коде продукта во время разработки, несовершенством или отсутствием средств защиты, внедрением различного вредоносного ПО, которые могут привести реализации внешних атак.

Оценивание рисков

В таблице 10 представлено оценивание рисков информационной безопасности по активам и применимым к ним угрозам, оценивание которых было проведено до этого. Оценка проводилась по методике, разработанной в параграфе 3.1 магистерской диссертации.

Оценка рисков Информационной Безопасности

Активы	Оценка	Угрозы	Значение степени вероятности	Мера риска	Итоговый балл для актива
ИС: Университет ПРОФ	2	Внесение вредоносных изменений в BIOS	0	2	87
		Использование обходного пути для перехвата данных	2	4	
		Использование информации для аутентификации	2	4	
		Исследование принципов работы программного обеспечения	1	3	
		Незаконное ознакомление с данными	3	5	
		Незаконный доступ к оборудованию из внутренней сети	2	4	
		Незаконный доступ к виртуальным устройствам из виртуальной и (или) физической сети	2	4	
		Несанкционированный доступ к данным, хранящимся на виртуальном носителе	3	5	
		Несанкционированное удаление данных	3	5	
		Обнаружение открытых портов и определение служб, использующих данные порты	3	5	
		Определение топологии сети	2	4	
		Перехват данных, выводимых на периферийные устройства	1	3	
		Перехват информации, идущей по локальным сетям	3	5	
		Подбор пароля BIOS	0	2	
		Потеря данных из-за сбоев в работе подсистемы данных	0	2	
		Программное выведение из строя хранилищ данных	3	5	
		Физическое выведение из строя хранилищ данных	2	4	
		Хищение средств хранения данных	1	3	
		Внесение вредоносного ПО при посещении сайтов	2	4	
		Незаконная модификация данных	3	5	
				Перехват одноразовых паролей	
Использование версий ПО с уязвимостями	4			6	
ФИС ГИА и Приема		Внесение вредоносных изменений в BIOS	0	1	65
		Использование обходного пути для перехвата данных	2	3	
		Использование информации для аутентификации	2	3	

		Исследование принципов работы программного обеспечения	1	2	
		Незаконное ознакомление с данными	3	4	
		Незаконный доступ к оборудованию из внутренней сети	2	3	
		Незаконный доступ к виртуальным устройствам из виртуальной и (или) физической сети	2	3	
		Несанкционированный доступ к данным, хранящимся на виртуальном носителе	3	4	
		Несанкционированное удаление данных	3	4	
		Обнаружение открытых портов и определение служб, использующих данные порты	3	4	
		Определение топологии сети	2	3	
		Перехват данных, выводимых на периферийные устройства	1	2	
		Перехват информации, идущей по локальным сетям	3	4	
		Подбор пароля BIOS	0	1	
		Потеря данных из-за сбоев в работе подсистемы данных	0	1	
		Программное выведение из строя хранилищ данных	3	4	
		Физическое выведение из строя хранилищ данных	2	3	
		Хищение средств хранения данных	1	2	
		Внесение вредоносного ПО при посещении сайтов	2	3	
		Незаконная модификация данных	3	4	
		Перехват одноразовых паролей	1	2	
		Использование версий ПО с уязвимостями	4	5	
1С:Бухгалтерия	3	Внесение вредоносных изменений в BIOS	0	3	110
		Использование обходного пути для перехвата данных	2	5	
		Использование информации для аутентификации	2	5	
		Исследование принципов работы программного обеспечения	1	4	
		Незаконное ознакомление с данными	3	6	
		Незаконный доступ к оборудованию из внутренней сети	2	5	
		Незаконный доступ к виртуальным устройствам из виртуальной и (или) физической сети	3	6	
		Несанкционированный доступ к данным, хранящимся на виртуальном носителе	3	6	
		Несанкционированное удаление данных	3	6	
		Обнаружение открытых портов и определение служб, использующих данные порты	3	6	

	Определение топологии сети	2	5
	Перехват данных, выводимых на периферийные устройства	1	4
	Перехват информации, идущей по локальным сетям	3	6
	Подбор пароля BIOS	0	3
	Потеря данных из-за сбоев в работе подсистемы данных	0	3
	Программное выведение из строя хранилищ данных	3	6
	Физическое выведение из строя хранилищ данных	2	5
	Хищение средств хранения данных	1	4
	Внесение вредоносного ПО при посещении сайтов	2	5
	Незаконная модификация данных	3	6
	Перехват одноразовых паролей	1	4
	Использование версий ПО с уязвимостями	4	7

Подведение итогов оценки рисков

Последний этап оценки рисков – оценивание. Нужно сравнить риски с критериями и приоритетами.

Вводится следующая шкала оценки критериев:

- 0-55 – риски минимальны;
- 56-95 - риски средние;
- 96-130 – риски высокие.

Если риски высокие, то необходимо незамедлительно приступить к устранению рисков. Так как информационные системы персональных данных связаны с финансами, то существует огромная вероятность финансовых потерь и нужно закрывать риски:

- Обеспечение полноты нормативно-правовой базы. Ввести пропускной режим;
- Модернизация серверных помещений и его оборудования;

- Улучшение сопровождения ИТ инфраструктуры, объединение подразделений, занимающихся сопровождением инфраструктуры университета;
- Повышение осведомленности и квалификации сотрудников в области информационной безопасности;
- Введение ответственности за сохранность сведений конфиденциального характера;
- Обеспечение антивирусной защиты на всех серверах и рабочих машинах.

Информационные системы со средним уровнем риска так же должны защищаться с помощью вышеперечисленных мер для уменьшения рисков.

Информационные системы, имеющие низкий риск, обрабатываются в последнюю очередь, так как нанесенный ущерб может быть меньше чем затраты на введение мер информационной защиты. Также необходимо решить – стоит ли вводить корректирующие действия или принимать риски.

ВЫВОДЫ ПО ТРЕТЬЕЙ ГЛАВЕ

В этой главе проведен обзор этапов оценки рисков по ГОСТ Р ИСО/МЭК 27005-2010 и, основываясь на нем, выведена способ оценки риска, которая включает в себя определение активов, угроз, уязвимостей, и дальнейшее их оценивание.

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

Данный метод позволяет качественно оценить и ранжировать риски по заданным критериям.

Проведен анализ информационно технического сопровождения университета на предмет оценки рисков информационной безопасности. Определены и оценены информационные активы университета. Выявлены угрозы для автоматизированных информационных систем образовательного учреждения и проведена их оценка.

В дальнейшем проведена оценка рисков.

ЗАКЛЮЧЕНИЕ

Магистерская диссертация разрешает проблему создания методики оценки угроз информационной безопасности, основываясь на современных стандартах и методиках. Результаты проведенного исследования позволили мне сделать следующие общие выводы:

1. Проблема выбора мер защиты для информационных систем образовательного учреждения

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

Угрозы информационной безопасности делятся на три группы:

- Вызванные действиями субъекта (антропогенные источники угроз);
- Вызванные техническими средствами (техногенные источники угрозы);
- Вызванные стихийными источниками.

Как правило, защита от угроз определяется действующими инструкциями образовательного учреждения.

2. Документация в сфере управления рисками информационной безопасности в образовательном учреждении.

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

Стандартом, который будет использоваться, выбран ГОСТ Р ИСО/МЭК 27005-2010, потому что он полностью применим под особенности образовательного учреждения.

3. Проведены анализ, оценивание рисков, которые связаны с угрозами безопасности информационных ресурсов ФГБОУ «Южно-Уральский государственный гуманитарно-педагогический университет» которые обнаружили риски для их обработки в дальнейшем.

Для того, чтобы достичь установленные цели, были выполнены следующие задачи:

- создана методика оценивания рисков информационной безопасности для образовательного учреждения. Основа для методики – стандарты в области информационной безопасности;
- проведен анализ информационной-телекоммуникационной структуры университета. Цель анализа – выявление угроз, уязвимостей и информационных активов;
- оценены информационные активы, угрозы и уязвимости. На их основе создана общая оценка рисков.

Исследование не полностью раскрывают существующую проблему. Обязательно появятся новые вопросы, которые тоже в дальнейшем потребует 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.

74

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

76

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.

77

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. Милютин О.В. Особенности защиты информации в образовательном учреждении / О.В. Милютин. – URL: http://www.fcoit.ru/internet_conference/information_security_training_process/f

eatures_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.

78

№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 ФГБОУ ВО «Южно-Уральский государственный гуманитарно-педагогический университет». – URL: www.csru.ru. Дата обращения: 22.12.2019.

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: 25.12.2019.

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: 12.12.2019.

79

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-obespecheniya-informacionnoi-bezopasnosti/>. Дата обращения: 01.12.2019.

56. Средство оценки безопасности Microsoft Security Assessment Tool (MSAT). - URL: <http://technet.microsoft.com/ru-ru/security/cc185712.aspx>.
Дата обращения: 12.05.2020.

57. Стандарты информационной безопасности. – URL: <https://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html>. Дата обращения: 20.05.2020.

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: 20.05.2020.

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.