МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

Кафедра Автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Организация режима защиты конфиденциальной информации в профессиональной образовательной организации

Магистерская диссертация
по направлению: 44.04.04 Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании
Форма обучения заочная

Проверка на объем заимствований:
87 % авторского текста

Работа рекомендована к защите
«18» 01 2021 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил(а):
Студент(ка) группы ЗФ-309-210-2-1
Гагарин Антон Владимирович

Научный руководитель:
Белевитин Владимир Анатольевич, д.т.н,
профессор

Челябинск
2021

СОДЕРЖАНИЕ

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 конфиденциальной информации.

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 конфиденциальной информации 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 защиты конфиденциальной информации в образовательной организации на основе существующих стандартов и методик управления рисками информационной безопасности.

Цель исследования – анализ информационно-телекоммуникационной инфраструктуры образовательной организации и оценка эффективности , 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.

Предмет исследования – методика защитных мер для конфиденциальной информации.

Гипотеза исследования состоит в разработке методического аппарата, позволяющего осуществлять рациональный выбор защитных мер конфиденциальной информации 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 в системе защиты конфиденциальной информации в образовательной организации;

- проанализировать существующие методики защиты конфиденциальной информации;

- разработать методику защиты конфиденциальной информации;

- проанализировать информационные ресурсы колледжа, источники угроз и уязвимостей;

- описать оценку эффективности защиты конфиденциальной информации 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 конфиденциальной информации, отличающаяся применением предложенного в работе показателя затрат ёмкости 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.

Теоретическая значимость заключается в том, что основные его положения и результаты повысили уровень защиты информационного пространства, а также снизили риски возникновения угроз информационной безопасности образовательной организации СПО.

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

Базой исследования является Государственное бюджетное образовательное учреждение «Миасский педагогический колледж», расположенный по адресу ул. Парковая, 2а, г. Миасс.

ГЛАВА 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

1.1 Понятие терминов «информационная безопасность» и «конфиденциальность»

Анализ состояния случаев информационной безопасности образовательных организаций приводит к выводу о том, что система мер по обеспечению защиты данных значительно снижает:

— вероятность утечки информации;

— несанкционированного доступа,

— разглашения или потери информации.

Профилактическая работа среди участников тренинга по обеспечению защиты образовательных организаций позволяет повысить уровень личной безопасности пользователей (обучающихся и других участников образовательного процесса) в виртуальном и реальном пространстве. Вместе с тем, информационная культура участников образовательного процесса не ограничивается информационными технологиями, а включает в себя идеологические, моральные, психологические и другие гуманитарные составляющие. Для успешного противодействия информационным угрозам необходима комплексная система информационной безопасности образовательной организации (далее КСИБ ОО).

Принципы КСИБ ОО

КСИБ ОО должна обеспечивать:

• конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);

• целостность (точность и полноту информации и компьютерных программ);

• доступность (способность пользователей получать информацию в пределах своей компетенции).

• безопасность (обеспечение информационной безопасности можно рассматривать как:

– совокупность деятельности по недопущению вреда сознанию и психике обучающегося;

– соблюдение прав участников образовательного процесса в соответствии с ФЗ № 152 от 27.07.2006 "О персональных данных" и ФЗ № 242 от 21.07.2014 «Закон о локализации Персональных данных россиян на территории РФ».

Соответственно проекта новой Доктрины информационной безопасности РФ с учетом зарубежного и отечественного опыта обеспечение информационной безопасности осуществляется по следующим направлениям:

1. Правовая защита – это конкретные правовые акты, правила, инструкции для процедуры, меры, обеспечивающие защиту информации и прав участников образовательного процесса на правовой основе;

2. Организационная защита – это регулирование деятельности исполнителя и отношений на нормативной и правовой основе, исключая или ослабляя любой ущерб;

3. Инженерно-техническая защита – это использование различных технических и программных средств, которые предотвращают ущерб, который способствует сохранению информации и обеспечивает защиту пользователям информации.

4. Психолого-педагогическая защита – обучение обучающихся адекватному восприятию и оценке информации, ее критическое отражение на основе нравственных и культурных ценностей. Проблема информационной безопасности обучающихся становится проблемой концепции системы образования, системы обучения педагогических кадров и повышения информационной культуры всех участников образовательного процесса.

Оценка нормативно-законодательной базы информационной безопасности образовательного процесса показала, что сайты информационной безопасности в Министерстве образования и науки в России, региональных

министерствах образования и муниципальных органах образования включают в себя:

• информацию, которая является государственной тайной, согласно выпискам из перечня информации, подлежащих классификации в министерствах, ведомствах и организациях;

• информационные ресурсы, содержащие документальную информацию в соответствии со списком конфиденциальной информации;

• информацию, защита которой предусмотрена в законодательных актах Российской Федерации, включая персональные данные;

• инструменты и системы для информатизации, программного обеспечения, автоматизированных систем управления, систем связи и передачи данных, которые получают, обрабатывают, хранят и передают информацию с ограниченным доступом.

В свою очередь, ст. 16 Федерального закона от 27.07.2006 № 149 "Об информации, информационных технологиях по защите информации" определяет порядок защиты информации. Согласно этой статье, защита информации – это принятие правовых, организационных и технических мер. Эти меры должны быть направлены на защиту информации от:

– несанкционированного доступа;

– уничтожения, модификации, блокировки, копирования, передачи, распространения и других незаконных действий в отношении информации.

Кроме того, этим Федеральным законом определяется и ответственность граждан за защиту информации. Так, п. 5 ст. 9 Закона № 149-ФЗ гласит: "Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению такой информации". Такая обязанность возлагается Трудовым кодексом РФ (далее - ТК РФ), гл. 14 которого определяет защиту персональных данных

работника. В соответствии со ст. 90 ТК РФ: "Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами".

Для развития вышеотмеченных положений в РФ 27.07.2006 принят Федеральный закон № 152-ФЗ "О персональных данных", который вступил в силу с 1 января 2008 г. Его основной целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в т. ч. защиты прав на неприкосновенность частной жизни, личную и семейную тайны. Статья 3 данного закона определяет: "Персональные данные – любая информация, относящаяся к определенному или неопределенному на основании такой информации лицу (субъекту персональных данных), в т. ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация".

В целях обеспечения безопасности информации и ее организации на основе законодательных документов соответствующее законодательство было разработано в старшей организации. Правовые нормы обеспечения информационной безопасности определяются в организационных и функциональных документах, определяющих порядок предоставления конфиденциальной информации, механизмы их защиты, а также механизмы защиты прав субъектов от образовательного процесса.

Организационные и функциональные документы включают:

• поручение директору назначить ответственного лица за информатизацию в организации;

• ответственность лиц, ответственных за обеспечение информационной безопасности;

• требования к обеспечению безопасности информации в коллективном договоре;

• требования к защите информации в контрактах для всех видов деятельности;

• инструкция, определяющая порядок предоставления информации внешним организациям по их просьбе, а также права доступа к сотрудникам образовательной базы и т. д.

Этот список документов не является исчерпывающим, его можно расширить дополнительно.

1.2 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 [10].

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[12].

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 [12].

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 [12].

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 [12].

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 [21].

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 [22].

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.

1.3 Угрозы и система защиты конфиденциальной информации

Под угрозой или опасностью утечки информации понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление неблагоприятных возможностей внешних или внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемые и охраняемые информационные ресурсы, в том числе и финансовые, включая документы и базы данных (101, с.36).

Информация является одним из важнейших видов продуктов и видов товара на рынке, в том числе на международном. Средства ее обработки, накопления, хранения и передачи постоянно совершенствуются. Информация как категория, имеющая действительную или потенциальную ценность, стоимость, как и любой другой вид ценности, - охраняется, защищается ее собственником или владельцем.

Защищают и охраняют, как правило, не всю или не всякую информацию, а наиболее важную, ценную для ее собственника, ограничение распространения которой приносит ему какую-то пользу или прибыль, возможность эффективно решать стоящие перед ним задачи.

Под защищаемой информацией понимают сведения, на использование и распространение которых введены ограничения их собственником [66, с.27].

Под общими признаками (концепциями) защиты любого вида охраняемой информации понимают следующее:

— защиту информации организует и проводит собственник, владелец / уполномоченное на это лицо;

— защитой информации собственник охраняет свои права на владение и распространение информации, стремится оградить ее от незаконного завладения и использования в ущерб его интересам;

— защита информации осуществляется путем проведения комплекса мер по ограничению доступа к защищаемой информации и созданию условий, исключающих или существенно затрудняющий несанкционированный доступ к засекреченной информации. Следовательно, защита информации - есть комплекс мероприятий, проводимых собственником информации по ограждению своих прав на владение и распоряжение прав на информацию, создание условий, ограничивающих и исключающих или существенно затрудняющих несанкционированный доступ к засекреченной информации и ее носителям [71, с.7].

Защита информации - это деятельность собственника информации или уполномоченных им лиц по: обеспечению своих прав на владение, распоряжение и управление защищаемой информацией; предотвращению утечки и утраты информации; сохранению полноты достоверности, целостности защищаемой информации, ее массивов и программ обработки, сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами [74, с.18].

Сохранение сведений в тайне, владение секретами дает определенные преимущества той стороне, которая ими владеет. Защищаемая информация, как и любая другая информация, используется человеком или по его воле различными созданными искусственно или существующими естественно системами в интересах человека. Она носит семантический, то есть смысловой, содержательный характер. Это дает возможность использовать одну и ту же информацию разными людьми, народами независимо от языка ее представления и знаков, которыми она записана, формы ее выражения и т.д.

В то же время защищаемая информация имеет и отличительные признаки:

— засекречивать информацию, то есть ограничивать к ней доступ, может только ее собственник (владелец) или уполномоченные им на то лица;

— чем важнее для собственника информация, тем тщательнее он ее защищает. А для того чтобы все, кто сталкивается с этой защищаемой информацией, знали, что одну информацию необходимо оберегать более тщательно, чем другую, собственник определяет ей различную степень секретности;

— защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства.

Основной угрозой информационной безопасности является несанкционированный (незаконный, неразрешенный) доступ злоумышленника или постороннего лица к документированной информации с ограниченным доступом и, как результат, овладение информацией и незаконное, противоправное ее использование.

Разработка мер, и обеспечение защиты информации осуществляются подразделениями по защите информации (служба безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии Гостехкомиссии России и/или ФАПСИ на право оказания услуг в области защиты информации [69, с.63].

Под злоумышленником понимается лицо, действующее в интересах противника, конкурента или в личных корыстных интересах (на сегодняшний день - террористы любых мастей, промышленный и экономический

шпионаж, криминальные структуры, отдельные преступные элементы, лица, сотрудничающие со злоумышленником, психически больные лица и т.п.) [73, с.64].

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности фирмы (работники милиции, МЧС, коммунальных служб, медицинской помощи, прохожие и др.), посетители организации, работники других организаций, включая контролирующие органы, а также работники самого предприятия, не обладающие правом доступа в определенные здания и помещения, к конкретным документам, базам данных [70, с.2].

Каждое из указанных лиц может быть злоумышленником или его сообщником, агентом конкурента и т.п., но может и не быть им. [65, с.64]

Наиболее часто встречающимися угрозами (опасностями) конфиденциальных сведении в документопотоках могут быть:

1. Несанкционированный доступ постороннего лица к документам, делам и базам данных за счет его любопытства или обманных, провоцирующих действий, а также случайных или умышленных ошибок персонала фирмы.

2. Утрата документа или его отдельных частей (листов, приложений, схем, копий, экземпляров, фотографий и др.), носителя чернового варианта документа или рабочих записей за счет кражи, утери, уничтожения.

3. Утрата информацией конфиденциальности за счет ее разглашения персоналом или утечки по техническим каналам, считывания данных в чужих массивах, использования остаточной информации на копировальной ленте, бумаге, дисках и дискетах, ошибочных действий персонала.

4. Подмена документов, носителей и их отдельных частей с целью фальсификации, а также сокрытия факта утери, хищения.

5. Случайное или умышленное уничтожение ценных документов и баз данных, несанкционированная модификация и искажение текста, реквизитов, фальсификация документов.

6. Гибель документов в условиях экстремальных ситуаций [52, с.24].

Для электронных документов угрозы особенно реальны, т.к. факт кражи информации практически трудно обнаружить. В отношении конфиденциальной информации, обрабатываемой и хранящейся в компьютерах, условия возникновения угроз, по мнению ряда специалистов, классифицируются по степени риска следующим образом:

1. Непреднамеренные ошибки пользователей, референтов, операторов, референтов, управляющих делами, системных администраторов и других лиц, обслуживающих информационные системы.

2. Кражи и подлоги информации.

3. Стихийные ситуации внешней среды.

4. Заражение вирусами.

В соответствии с характером указанных выше угроз формируются задачи обеспечения защиты информации в документопотоках, направленные на предотвращение или ослабление этих угроз.

Следует внимательнее относиться к вопросам отнесения информации к различным грифам секретности и, соответственно, к обеспечению уровня ее защиты.

Защита информации представляет собой регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и секретности (конфиденциальности)

информационных ресурсов предприятия. Данный технологический процесс в конечном счете должен обеспечить надежную информационную безопасность организации в его управленческой и финансово-производственной деятельности.

Комплексная система защиты информации - рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее утечке и разглашению [62, с.9].

Правовой элемент системы защиты информации основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений предприятия и государства по поводу правомерности использования системы защиты информации (системы лицензирования в области защиты информации и сертификации средств защиты информации); на обязанности персонала: соблюдать установленные собственником информации ограничительные и технологические меры режимного характера защиты информационных ресурсов организации.

Правовое обеспечение системы защиты информации включает:

— Наличие в организационных документах, правилах внутреннего трудового распорядка, трудовых договорах, контрактах, заключаемых с персоналом, в должностных инструкциях (регламентах) положений и обязательств по защите информации;

— Формулирование и доведение до сведения всего персонала банка (в том числе не связанного с защищаемой и охраняемой информацией) положения о правовой ответственности за разглашение информации, несанкционированное уничтожение или фальсификацию документов;

— Разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите документированной информации [83, с.58].

Организационный элемент, как одна из основных частей системы защиты информации содержит меры управленческого, режимного (ограничительного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты информации фирмы. Эти меры связаны с установлением режима секретности (конфиденциальности) информации в организации.

Организационно-документационное обеспечение включает в себя документирование и регламентацию:

— Формирования и организации деятельности службы безопасности организации, службы кадров и службы закрытого (конфиденциального) документационного обеспечения управления (ДОУ) (или менеджера по безопасности, или помощника (референта) руководителя предприятия), обеспечения деятельности этих служб нормативно-методическими документами по организации и технологии защиты информации;

— Составления и регулярного обновления состава перечня защищаемой информации организации, составления и ведения перечня защищаемых бумажных и электронных документов организации;

— Разрешительной системы (иерархической схемы) разграничения доступа персонала к защищаемой и охраняемой информации предприятия;

— Методов отбора персонала для работы с защищаемой информацией, методики обучения и инструктирования работников;

— Направлений и методов воспитательной работы с персоналом, контроля соблюдения работниками порядка защиты информации;

— Технологии защиты, обработки и хранения бумажных и электронных документов, баз данных предприятия (делопроизводственной, электронной и смешанной технологий);

— Вне машинной технологии защиты электронных документов - защиты носителей информации;

— Порядка защиты ценной информации предприятия от случайных или умышленных несанкционированных действий работников банка;

— Порядка защиты информации при проведении совещаний, заседаний, переговоров, приеме посетителей, работе с представителями контрольных органов, средств СМИ, рекламных агентств и т.д.;

— Оборудования и аттестации зданий и помещений, рабочих зон, выделенных для работы с документированной информацией [62, с.23].

Инженерно-технический элемент предназначен для пассивного и активного противодействия средствами технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств. При защите информационных систем этот элемент имеет весьма важное значение, хотя стоимость средств технической защиты и охраны велика.

Элемент включает в себя:

— Сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здание и помещение (заборы, решетки, стальные двери, кодовые замки, идентификаторы, сейфы);

— Средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов и других приборов и офисного оборудования, проведении совещаний, заседаний, беседах с посетителями и сотрудниками, диктовке документов;

— Средства защиты помещений от визуальных способов технической разведки;

— Средства обеспечения охраны территории, здания и помещений (средств наблюдения, оповещения, сигнализация);

— Средства противопожарной охраны;

— Средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры);

— Технические средства контроля, предотвращающие вынос персоналом из помещения специально маркированных предметов, документов, дискет, книг [72, с.36].

Программно-математический элемент предназначен для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих станциях локальных сетей и различных информационных системах. Элемент включает в себя:

— Регламентацию доступа к базам данных, файлам, электронным документам персональными паролями, идентифицирующими командами и другими методами;

— Регламентацию специальных средств и продуктов программной защиты;

— Регламентацию криптографических методов защиты информации в ЭВМ и сетях, криптографирования (шифрования) текста документов при передаче их по каналам телеграфной и факсимильной связи, при пересылке почтой;

— Регламентацию доступа персонала в режимные (охраняемые) помещения с помощью идентифицирующих кодов, магнитных карт, биологических идентификаторов [72, с.37].

Криптографическое обеспечение включает в регламентацию:

1. Использования различных криптографических методов в компьютерах и серверах, корпоративных и локальных сетях, различных информационных системах.

2. Определение условий и методов криптографирования текста документа при передаче его по незащищенным каналам почтовой,

телеграфной, телетайпной, факсимильной и электронной связи; регламентацию использования средств криптографирования переговоров по незащищенным каналам телефонной, спутниковой и радиосвязи.

3. Регламентацию доступа к базам данных, файлам, электронным документам персональными паролями, идентифицирующими командами и другими методами; регламентацию доступа персонала в выделенные помещения с помощью идентифицирующих кодов, шифров (например, на сегодняшний день вошло в практику использования, как идентифицирующий кодов системы паролей, отпечатков пальцев и сетчатки глаза человека) [72, с.39].

Составные части криптографической защиты, пароли и другие ее атрибуты разрабатываются и меняются специализированными организациями, входящими в структуру Федеральной службы по техническому и экспертному контролю России. Применение пользователями иных систем шифровки не допускается [49, с. 19].

Таким образом, наиболее часто встречающимися угрозами (опасностями) конфиденциальных документов являются:

1. Несанкционированный доступ постороннего лица к документам, делам и базам данных за счет его любопытства или обманных, провоцирующих действий, а также случайных или умышленных ошибок персонала фирмы.

2. Утрата документа или его отдельных частей (листов, приложений, схем, копий, экземпляров, фотографий и др.), носителя чернового варианта документа или рабочих записей за счет кражи, утери, уничтожения.

3. Утрата информацией конфиденциальности за счет ее разглашения персоналом или утечки по техническим каналам, считывания данных в чужих массивах, использования остаточной информации на

копировальной ленте, бумаге, дисках и дискетах, ошибочных действий персонала.

4. Подмена документов, носителей и их отдельных частей с целью фальсификации, а также сокрытия факта утери, хищения.

5. Случайное или умышленное уничтожение ценных документов и баз данных, несанкционированная модификация и искажение текста, реквизитов, фальсификация документов.

6. Гибель документов в условиях экстремальных ситуаций [52, с.24].

В отношении конфиденциальной информации, обрабатываемой и хранящейся в компьютерах, условия возникновения угроз, классифицируются по степени риска следующим образом:

1. Непреднамеренные ошибки пользователей, референтов, операторов, референтов, управляющих делами, системных администраторов и других лиц, обслуживающих информационные системы.

2. Кражи и подлоги информации.

3. Стихийные ситуации внешней среды.

4. Заражение вирусами.

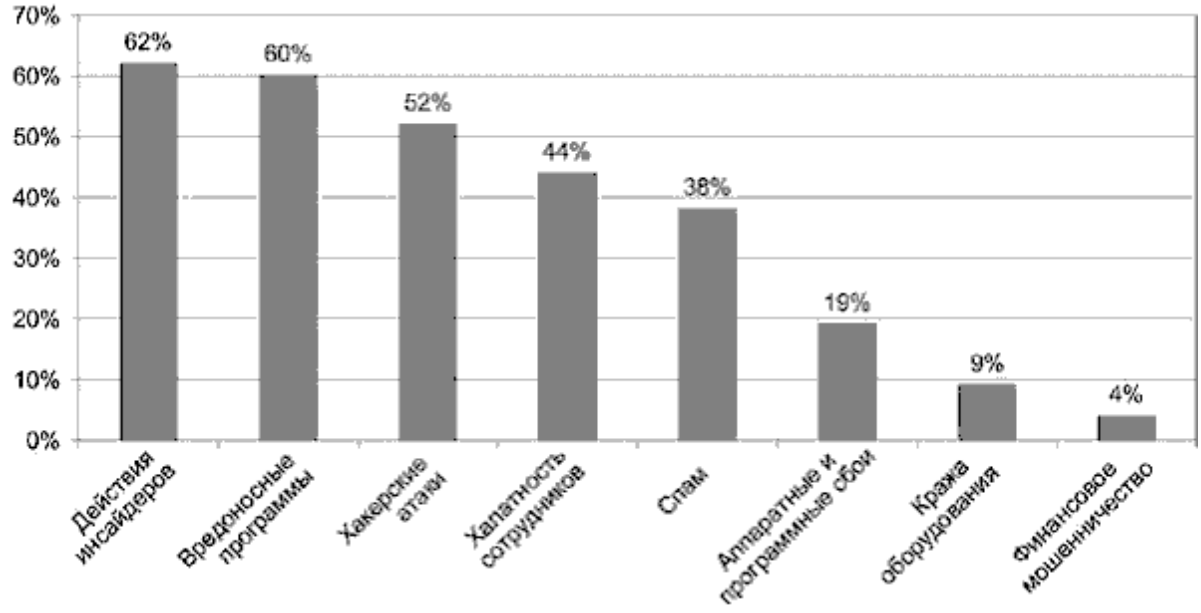

Рисунок 1 — Самые опасные ИТ-угрозы (исследование Infowatch, 2017)

Система защиты информационных ресурсов включает в себя следующие элементы:

— правовой;

— организационный;

— инженерно-технический;

— программно-аппаратный;

— криптографический [51, с.26].

В каждой вышеупомянутой части обеспечение системы защиты информации организации могут быть реализованы на практике только отдельно составные элементы, в зависимости от: поставленных задач защиты организации; величины фирмы.

Структура системы, состав и содержание комплекса частей обеспечения системы защиты информации фирмы, их взаимосвязь зависят от ценности защищаемой и охраняемой информации, характера возникающих угроз информационной безопасности предприятия, требуемой защиты и стоимости системы.

Одним из основных признаков защищаемой информации являются ограничения, вводимые собственником информации на ее распространение и использование.

В общем виде цели защиты информации сводятся к режимно-секретному информационному обеспечению деятельности государства, отрасли, предприятия, фирмы. Защита информации разбивается на решение двух основных групп задач:

1. Своевременное и полное удовлетворение информационных потребностей, возникающих в процессе управленческой, инженерно-технической, маркетинговой и иной деятельности, то есть обеспечение специалистов организаций, предприятий и фирм секретной или конфиденциальной информации.

2. Ограждение засекреченной информации от несанкционированного доступа к ней соперника, других субъектов в злонамеренных целях [13, с.52].

Риск угрозы утечки любых информационных ресурсов (открытых и с ограниченным доступом) создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий электроснабжения, связи, другие объективные обстоятельства, а также заинтересованные и не заинтересованные в возникновении угрозы лица. Пример тому - сбой электроснабжения в Москве в 2005 году, последствия которого до сих пор испытывают некоторые организации [60, с.145].

Главная задача защиты информации, по мнению большинства специалистов, - защитить доступ (физический или программный) к месту пребывания электронной конфиденциальной информации таким образом, чтобы максимально удорожить процесс несанкционированного доступа к защищаемым данным [15, с.220].

Выводы по первой главе

Анализ состояния случаев информационной безопасности образовательных организаций приводит к выводу о том, что система мер по обеспечению защиты данных значительно снижает: а) вероятность утечки информации; б) несанкционированного доступа; в) разглашения или потери информации.

Для успешного противодействия информационным угрозам необходима комплексная система информационной безопасности образовательной организации (далее КСИБ ОО), которая должна обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (способность пользователей получать информацию в пределах своей компетенции).
- безопасность.

Обеспечение информационной безопасности можно рассматривать как: а) совокупность деятельности по недопущению вреда сознанию и психике обучающегося; б) соблюдение прав участников образовательного процесса в соответствии с ФЗ № 152 от 27.07.2006 "О персональных данных" и ФЗ № 242 от 21.07.2014 «Закон о локализации Персональных данных россиян на территории РФ».

На первом этапе построения КСИБ ОО, в обеспечение информационной безопасности ОО, определяется, что подлежит защите, а на втором этапе – выявляются возможные каналы утечки информации, определяются потенциальные и реальные криминальные и техногенные угрозы безопасности: а) педагогическому коллективу, обучающимся; б) финансам собственным, заемным и находящимся на хранении в организации,

документальной и компьютерной информации, информации передаваемой по всем средствам связи; в) имуществу организации (персональных компьютеров, программного обеспечения и средств обеспечения передачи информации) при их нахождении в организации; г) техническим системам и средствам обеспечения информационной безопасности колледже; д) информационным системам. Кроме того, разрабатываются гарантии для защиты информационных и технологических систем с целью предотвращения (ограничения) осуществления угроз или предотвращения распространения угрозы и ограничения ее распространения.

Угрозы информационной безопасности корпоративной сети ГБПОУ «Миасский педагогический колледж» разделены по их характеру (технологические, организационные), виду (физические, логические, воздействия на персонал и действия персонала), источнику (человеку, форс-мажор и др.) и объекту (на ресурс, на канал связи, на ОС и ПО, на сетевое обслуживание и др.).

Как показывает практика, проверка организации КСИБ образовательной организации (ОО) обычно имеет следующие недостатки:

- Отсутствует список информации, составляющей конфиденциальную информацию;
- Лицо, ответственное за обеспечение информационной безопасности, не имеет официальных обязательств;
- Процедура записи носителей информации с конфиденциальной информацией не соблюдается;
- нарушен порядок ведения бизнеса;
- Отсутствует взаимопонимание между теми, кто обеспечивает безопасность информации, и теми, кто использует эту информацию.

Учитывая эти недостатки, для обеспечения безопасности информации необходимы следующие приоритетные действия:

— защита интеллектуальной собственности образовательной организации, компьютеров, локальных сетей и сети интернет-подключения;

— организация защиты конфиденциальной информации, включая личные данные сотрудников и обучающихся;

— организация служебной деятельности, в том числе с учетом вопросов безопасности сотрудников и обучающихся.

При таком подходе основными составными задачами обеспечения безопасности информации ОО станут: документирование информации, учет документов, организация документооборота, обеспечение надежного хранения документов, своевременное их уничтожение, проверка наличия хранящихся документов, контроль за своевременным и правильным их исполнением.

Соответственно проекта новой Доктрины информационной безопасности РФ с учетом зарубежного и отечественного опыта обеспечение информационной безопасности осуществляется по следующим направлениям: а) Правовая защита – это конкретные правовые акты, правила, инструкции для процедуры, меры, обеспечивающие защиту информации и прав участников образовательного процесса на правовой основе; б) Организационная защита – это регулирование деятельности исполнителя и отношений на нормативной и правовой основе, исключая или ослабляя любой ущерб; в) Инженерно-техническая защита – это использование различных технических и программных средств, которые предотвращают ущерб, который способствует сохранению информации и обеспечивает защиту пользователям информации; в) Психолого-педагогическая защита – обучение обучающихся адекватному восприятию и оценке информации, ее критическое отражение на основе нравственных и культурных ценностей.

Проблема информационной безопасности обучающихся становится проблемой концепции системы образования, системы обучения педагогических кадров и повышения информационной культуры всех участников образовательного процесса.

ГЛАВА 2. НОРМАТИВНО-ПРАВОВАЯ ДОКУМЕНТАЦИЯ В ОБЛАСТИ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Международные стандарты 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.

Данный стандарт был разработан в 2005 году и до сих пор ведётся его модификация, на данный момент актуальной является версия 2010 года. 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»

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.

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 [3]:

- 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.

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 2007г.

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.

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 1.

Таблица 1— 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;	–	+	–

Продолжение таблицы 1

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;	+	–	–
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;	–	+	–

Продолжение таблицы 1

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.

— 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).

— 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.

— 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 2.

Таблица 2 — 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. [4]

Выводы по второй главе

В данной главе 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 И ВНЕДРЕНИЕ МЕТОДИКИ ЗАЩИТЫ КОНФЕДИЦИАЛЬНОЙ ИНФОРМАЦИИ В ГБПОУ «МИАССКИЙ ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»

3.1 Методика защиты конфиденциальной информации

Для решения проблемной ситуации (создания системы защиты конфиденциальной информации) в организации необходимо:

1. Выделить, объединив участников документооборота, самостоятельное структурное подразделение (службу конфиденциального делопроизводства). Разработать положение о подразделении, должностные инструкции работников подразделения;
2. Разработать новую инструкцию о конфиденциальном делопроизводстве, устанавливающую порядок составления, оформления конфиденциальных документов, конфиденциального документооборота, контроль исполнения конфиденциальных документов, согласования документов, ведения делопроизводства. Ознакомить всех сотрудников организации.
3. Необходимо обучить сотрудников, правилам работы с конфиденциальными документами.
4. Выделить помещение для службы конфиденциального делопроизводства. В нем должно быть помещение для хранения конфиденциальных документов, помещение для работы с конфиденциальными документами. Это помещение должно быть оборудовано соответствующим образом:

— перед входом в помещение должна быть установлена камера видеонаблюдения;

— на дверях должен стоять кодовый замок или идентификатор;

— должен стоять сейф или металлические шкафы для хранения документов;

— рабочие места в помещениях для работы сотрудников должны быть огорожены специальными перегородками;

— на окнах необходимо повесить жалюзи или светонепроницаемые шторы.

5. Ввести пропускной режим в здание ГБПОУ «Миасский педагогический колледж».

6. Все конфиденциальные документы должны быть сосредоточены в службе конфиденциального делопроизводства.

7. Выделить специальное помещение и оборудовать соответствующим образом для проведения конфиденциальных совещаний и переговоров.

8. Необходимо разработать положение о конфиденциальной информации, правила работы с конфиденциальными документами.

9. В целях обеспечения информационной безопасности внутренняя сеть и Интернет должны быть разделены. В идеале, компьютер для выхода в Интернет должен быть обособлен и, не иметь никакой прямой связи с другими рабочими станциями.

10. Удобнее всего (для постоянного использования) хранить архивы на оптических носителях, которые в конце рабочего дня должны сдаваться в службу конфиденциального делопроизводства.

11. Исходя из ситуации, и в целях совершенствования системы защита информации, нужно, чтобы на предприятии функционировала служба безопасности.

Функции, которой будут следующими:

— организует и обеспечивает пропускной и внутри объектовый режим в зданиях и помещениях, порядок несения службы охраны,

контролирует соблюдение требований режима сотрудниками, арендаторами, партнерами и посетителями;

— разрабатывает основополагающие документы с целью закрепления в них требований обеспечения безопасности и защиты государственной тайны и конфиденциальной информации, в частности устава, правил внутреннего трудового распорядка, положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;

— разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся информацией ограниченного доступа, при всех видах работ организует и контролирует выполнение требований инструкции по защите конфиденциальной информации;

— изучает все стороны производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций в отношении деятельности организации и е клиентов, партнеров, смежников;

— организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности организации;

— разрабатывает, ведет, обновляет и пополняет перечень сведений, составляющих конфиденциальную информацию и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиту информации;

— обеспечивает строгое выполнение требований нормативных документов по защите конфиденциальной информации;

— осуществляет руководство службами и подразделениями безопасности предприятий организации в части оговоренных в договорах условий по защите конфиденциальной информации

— организует и регулярно проводит учебу сотрудников фирмы и службы безопасности по всем направлениям защиты конфиденциальной информации, добиваясь, чтобы к охране коммерческих секретов был глубоко осознанный подход;

— ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальной информации;

— ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;

Служба безопасности должна быть самостоятельной организационной единицей, подчиняющейся непосредственно генеральному директору организации. Возглавлять службу безопасности должен начальник службы в должности заместителя генерального директора по безопасности.

Особое внимание следует обратить на обучение сотрудников, занимающихся сбытом продукции и услуг компании. Эти люди часто находятся в ситуациях, благоприятных для утечки информации. Они должны быть четко проинструктированы, что можно говорить, что нельзя. Нередки анонимные запросы от "потенциальных клиентов" с просьбой сообщить информацию об изделии для понимания того, как его применить наилучшим образом. Конкурент может выяснить существенные вещи, проанализировав эту, незначительную, на первый взгляд, информацию. Лучше всего, чтобы люди, занимающиеся сбытом, не обладали информацией о новых разработках, еще не поступивших в производство. Надо быть предельно осторожным при проведении различных ярмарок, выставок, торговых

показов. Весь персонал, работающий на них, должен быть самым тщательным образом проинструктирован.

Альтернативный путь организации - формирование совета по безопасности. Для совета выбирается один представитель от каждого отдела.

Это позволит службе безопасности иметь как бы своего делегата в каждом отделе, который будет пояснять программу безопасности и сам иногда проводить тренинги. Созданный таким образом совет обучает работников и выявляет возникающие проблемы по защите коммерческой тайны. Такая система имеет следующие преимущества:

— укрепляются связи между сотрудниками службы безопасности и сотрудниками производства;

— растет понимание требований защиты информации сотрудниками;

— развиваются и совершенствуются стратегии обеспечения защиты информации в каждом отделе, получается поддержка правил и норм, установленных администрацией;

— рассмотрение существующих проблем безопасности с позиций отделов;

— сокращение штата службы безопасности;

— экономия средств на тренинги.

Важно уделить внимание поддержанию и совершенствованию нововведении, чтобы не вернуться к прежним методам работы. Итогом данного исследования является принятие руководством анализируемого предприятия решения о необходимости совершенствования конфиденциального делопроизводства с учетом всех описанных рекомендаций и факторов по их внедрению.

3.2 Анализ информационно-телекоммуникационной системы ГБПОУ «Миасский педагогический колледж»

Объектом исследования является ГБПОУ «Миасский педагогический колледж», распложенный по адресу: г. Миасс, ул. Парковая 2а.

Учредителем колледжа является Министерство образования и науки Челябинской области.

ГБПОУ «Миасский педагогический колледж» старым регионе государственным средним профессиональным образовательным учреждением повышенного типа. Главная цель и направление деятельности ГБПОУ «Миасский педагогический 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.

Колледж сегодня специализируется на подготовке учителей начальных классов, воспитателей детей дошкольного возраста, педагогов дополнительного образования в области физкультурно-оздоровительной деятельности.

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

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.

Организационная структура колледжа представлена на рисунке 2.

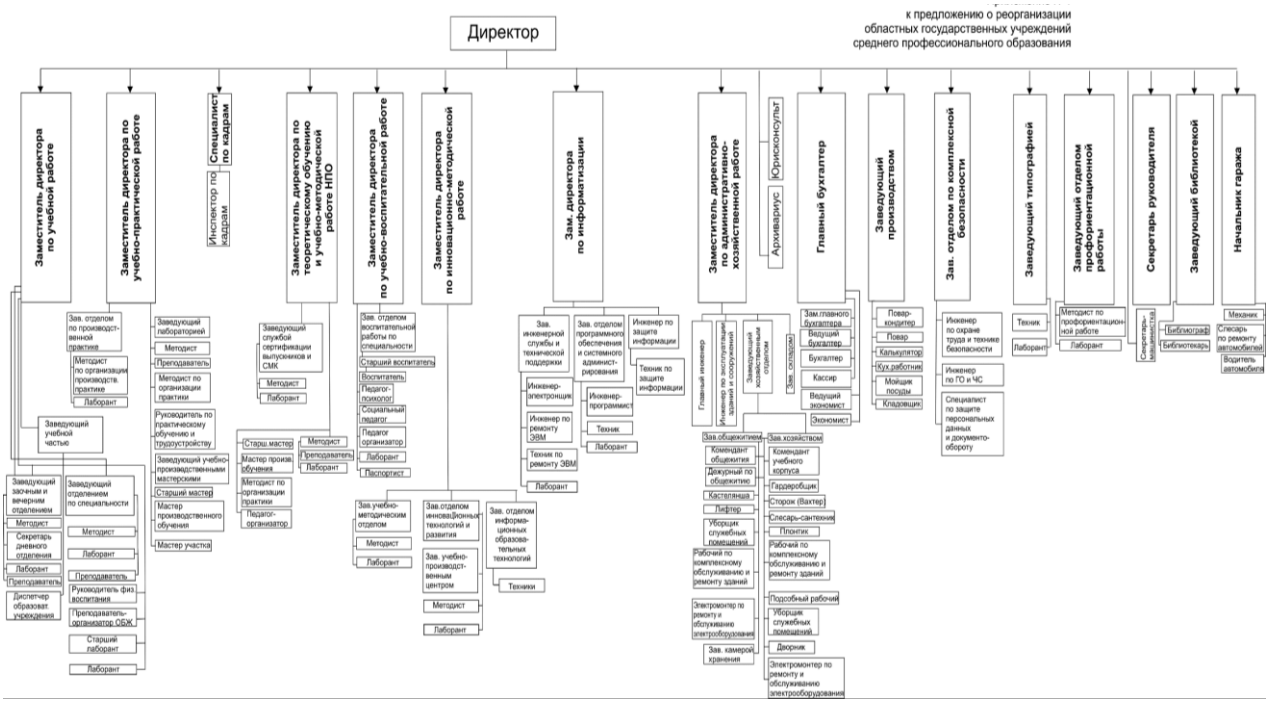

Рисунок 2 — Структура колледжа ГБПОУ «Миасский педагогический колледж»

Непосредственное управление деятельностью колледжа осуществляет директор. Директор назначается Учредителем.

Каменкова Наталья Владимировна - директор колледжа.

Неустроева Наталия Владимировна - заместитель директора по учебной работе.

Коростина Наталья Викторовна – заведующая отделением.

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

Сысолятин Дмитрий Евгеньевич - заместитель директора по административно-хозяйственной работе.

Сибгатулина Анжела Левонковна - 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.

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.

Исследуемая организация 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 http://miasspk.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 включают в себя:

- локальную сеть на одновременную работу 56 компьютеров. (Высокоскоростная глобальная сеть (пакет 20 000 Мб в месяц). 70% учебных площадей оснащено компьютерной и коммуникационной техникой)
- 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;
- систему 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;
- систему 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 3 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 3 — Перечень АИС и ИСПДн, обрабатывающих КИ, КТ и ПДн

№	Название АИС и ИСПДн
1	АС «Абитуриент»
2	1С Колледж

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 к 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 [9] .

3.3 Оценка эффективности выполненных разработок

Важным условием для внедрения проекта по созданию комплексной системы защиты информации (КСЗИ), является расчёт рисков. Для расчётов уровня рисков воспользуемся формулой: $CTh = 1 - \prod_{i=1}^{n} (1 - Th)$

где величина Th означает уровень угрозы, рассчитывается по следующей формуле:

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}$$

где ER - критичность реализации угрозы (%); P(V) - вероятность реализации угрозы (%).

Таблица 4 — Потоки защищаемой информации

Риски / пути их реализации	Крити-чность ER	Вероят-ность P(V)	Th	CTh
1	2	3	4	5
1. Риски изменений в стране, обществе				
1.1. Изменение политических и экономических характеристик и факторов:				0,054
- политические и экономические изменения	25	10	0,025	
- изменение законодательства	30	10	0,03	
1.2. Влияние непредвиденных ситуаций:				0,00007
- стихийные бедствия и природные катаклизмы	7	1	0,0007	
2. Риски окружения проекта в составе организации				
2.1. Изменение финансовой обстановки проекта:				0,636
- приостановка финансирования	90	20	0,018	
- отсутствие резервных средств для реагирования на события рисков (в т.ч. для ликвидации отставания от графика)	90	70	0,63	
2.2. Низкая организованность работ				0,116
- отставание от графика работ, срыв сроков	20	10	0,02	
- недостаток рабочей силы	40	20	0,08	

- преуменьшение стоимости работ и расход финансовых средств для других задач	40	5	0,02	
2.3. Риски персонала				0,151
- влияние индивидуальных личностных качеств сотрудников (переоценка собственных возможностей, преувеличение роли технологической стороны в ущерб менеджменту)	30	10	0,03	
- риск отсутствия персонала, которому сложно подобрать замену (болезнь, увольнение, отпуск и другие непредвиденные обстоятельства)	50	25	0,125	

В данном пункте были рассчитаны риски проекта. Максимальный риск связан с изменением финансовой обстановки проекта. Минимальный риск связан с влиянием непредвиденных обстоятельств.

В таблице 5 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 5 — Оценка рисков ИБ

Активы	Оценка	Угрозы	Значение степени вероятности	Мера риска	Итоговый бал для актива
	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	

Продолжение таблицы 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	

Продолжение таблицы 5

		Угроза перехвата одноразовых паролей в режиме реального времени	1	3	
		Угроза использования уязвимых версий программного обеспечения	4	6	
	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	

Продолжение таблицы 5

		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	
	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	

Продолжение таблицы 5

		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	
	3	Угроза внедрения вредоносного кода в BIOS	0	3	110
		Угроза доступа к защищаемым файлам с использованием обходного пути	2	5	

Продолжение таблицы 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	

Продолжение таблицы 5

		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	
	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	

Продолжение таблицы 5

		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	
	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	

Продолжение таблицы 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	

Продолжение таблицы 5

	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	

Продолжение таблицы 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	
	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	

Продолжение таблицы 5

		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.

Структура разбиения работ представляет собой детальное описание каждого этапа по созданию КСЗИ, и помогает оптимизировать план проекта и требования заказчика. Структура разбиения работ представлена на рисунке 2.

Структура декомпозиции работ по совершенствованию КСЗИ:

КСЗИ 1. Проектирование

КСЗИ 1.1. Определение главных показателей имеющихся бизнес-процессов с точки зрения информационной безопасности;

КСЗИ 1.2. Выявление и анализ проблем, слабых мест имеющихся бизнес-процессов;

КСЗИ 1.3. Разработка значений главных показателей новых бизнес - процессов;

КСЗИ 1.4. Анализ и отбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;

КСЗИ 1.5. Разработка и согласование структуры новых бизнес - процессов.

КСЗИ 2. Создание новой организационно - распорядительной документации

КСЗИ 2.1. Положение «О коммерческой тайне»;

КСЗИ 2.2. Перечень сведений, составляющих коммерческую тайну;

КСЗИ 2.3. Приказы об утверждении положения режима коммерческой тайны и перечня сведений, составляющих коммерческую тайну;

КСЗИ 2.4. Внесение изменений в должностные инструкции;

КСЗИ 2.5. Согласование и утверждение организационно - распорядительных документов.

КСЗИ 3. Подготовка реализации проекта созданию КСЗИ

КСЗИ 3.1. Определение ответственных лиц и исполнителей проекта;

КСЗИ 3.2. Приобретение программно - аппаратного средства защиты от НСД; КСЗИ 3.3. Приобретение средства контроля и управления доступом;

КСЗИ 3.4. Приобретение средств видеонаблюдения;

КСЗИ 4. Внедрение

КСЗИ 4.1. Установка и настройка программно - аппаратного средства защиты от НСД;

КСЗИ 4.2. Установка средства контроля и управления доступом;

КСЗИ 4.3. Установка средств видеонаблюдения;

КСЗИ 4.4. Контроль защищенности;

КСЗИ 4.5. Обучение персонала.

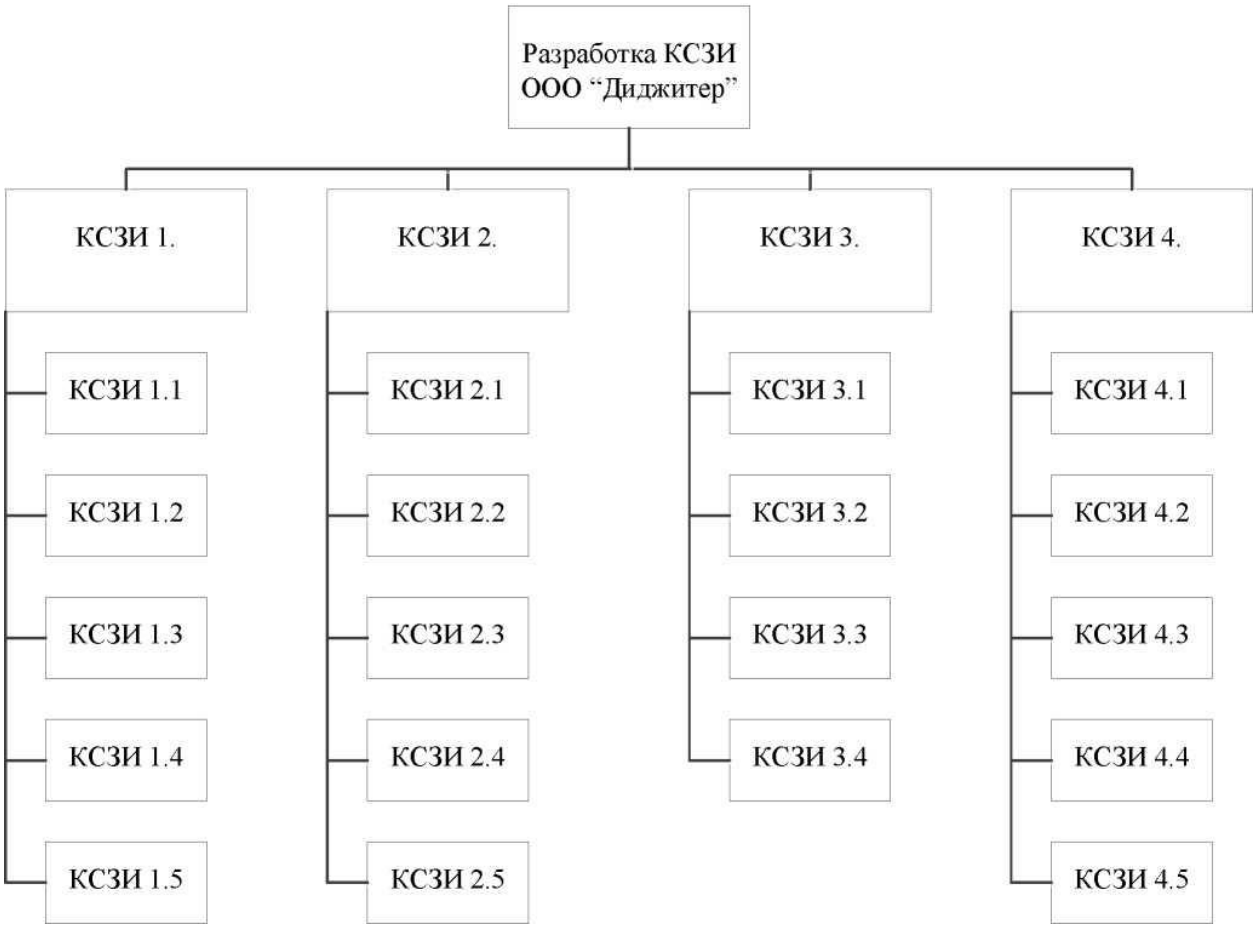

Рисунок 2— Структурная схема разбиения работ

В результате предпроектного обследования были выявлены уязвимости, которые подлежат устранению. Данные проблемы возможно устранить с помощью создания комплексной системы защиты информации. Для этого необходимо произвести расчёт экономической эффективности проекта, который ответит на вопрос о целесообразности реализации мер по

созданию комплексной системы защиты информации. Стоимость программных и технических средств представлена в таблице 6. Стоимость услуг по реализации проекта представлена в таблице 7. Поток денежных платежей представлен в таблице 8.

Таблица 6- Стоимость обеспечения

№ п/п	Наименование	Количество	Цена за шт. (руб.)	Сумма (руб.)
1	СЗИ НСД «Аура 1.2.4»	6	4000	24000
2	Комплект видеонаблюдения «ЭкоЛайн Dome-204»	1	13880	13880
3	Считыватель карт Matrix-II	1	1585	1585
4	Карта Optimus EM-marine	10	23	230
5	Кнопка выхода Optimus	1	99	99
6	Автономный контроллер Z - 5R	1	580	580
7	Электромагнитный замок Optimus EM - 180	1	1700	1700
Итог				42074

Таблица 7- Стоимость услуг по обеспечению проекта

№ п/п	Наименование	Стоимость (руб.)
1	Разработка и описание бизнес-процессов компании с точки зрения ИБ	9600
2	Разработка организационно-распорядительной документации	4600
3	Установка и настройка средства защиты от НСД «Аура 1.2.4»	8000
4	Установка и настройка комплекта видеонаблюдения «ЭкоЛайн Dome-204»	7000
5	Установка средства контроля управления доступом	5000
6	Обучение пользователей	2400
Итог		36600

Стоимость внедрения КСЗИ составляет 78674 рублей.

Таблица 8- Поток денежных платежей по проекту

Периоды	0	1	2	3
Первоначальные инвестиции (руб.)	-78674			
Выгоды (размеры риска) (руб.)		3000000	3000000	3000000
Стоимость годовой поддержки (руб.)		-5000	-5000	-5000
Затраты на администрирование и инфраструктуру (руб.)		-10000	-10000	-10000
Итого	-78674	2985000	2985000	2985000

Денежные вложения в реализацию проекта комплексной системы защиты информации составляют 78605 рублей. Ежегодно для поддержания системы необходимо выделять по 15000 рублей, на протяжении трех лет.

Для наглядного показа отличия вложений средств в проект от дохода хранения денег в банке воспользуемся методом Net Present Value (NPV). Рассчитаем NPV по формуле:

$$NPV = \sum_{t=1} \frac{CF_t}{(1+r)^t} - \sum_{t=0} \frac{I_t}{(1+r)^t}$$

где CF - денежный поток;

I — сумма инвестиционных вложений в проект в t-ом периоде; r — ставка дисконтирования; n — количество периодов.

Значение финансовых поступлений будем считать равным размеру ставки Центробанка России. Ставка центрального банка составляет 9,25 %

$$NPV = -78674 + 2985000/1{,}0925 + 2985000/(1{,}0925)^2 + 2985000/(1{,}0925)^3 =$$

$$= -78674 + 2732265 + 2500929 + 2289180 = 7443700$$

Из произведенного расчета видно, что значение NPV больше 0. Таким образом, в данной организации будет целесообразным проект внедрения КСЗИ. На основании вышесказанного можно сделать вывод, что создание КСЗИ в данной организации будет эффективным, так как величина потерь при отсутствии реализованных мер будет превышать затраты на ее реализацию и обслуживание.

Итогом выполненных работ служит проект по созданию комплексной системы защиты информации. В рамках разработки проекта КСЗИ были выявлены потоки защищаемой информации. Составлено резюме проекта.

Целью создания КСЗИ является: предотвращение разглашения, копирования, хищения, уничтожения, модификации, искажения информации ограниченного доступа; защита информации составляющей коммерческую тайну в соответствии с законодательством. Были определены необходимые организационно - распорядительные документы, программно - аппаратные и инженерно - технические меры. Рассчитаны риски реализации проекта. Выполняемые работы были разделены и упорядоченно структурированы. Представлены структурные схемы разбиения работ и реализации проекта. Для каждого вида работ был назначен ответственный, в связи с этим была разработана матрица ответственности. Разработаны графики которые наглядно показывают сроки и объемы выполнения работ.

Результатом выполнения проекта, является исполнение разработанных мер по комплексной защите информации.

По результатам расчета стоимости создания КСЗИ и ее обслуживания была произведена оценка эффективности. По данным оценки суммарные затраты на реализацию проекта составляют 78674 рублей, проект займёт 26 дней. С точки зрения экономической целесообразности проект признан эффективным, о чем свидетельствуют результаты расчета по методу Net Present Value. Реализация данного проекта позволит сэкономить колледжу, ликвидировать угрозы и тем самым предприятие получит дополнительную выгоду.

Выводы по третьей главе

В данной главе были подробно рассмотрены этапы оценивания риска стандарта ГОСТ Р ИСО/МЭК 27005-2010 и на его основе разработана методика защиты конфиденциальной информации, 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 последующим приоритетом рисков, согласно заданным критериям, что позволяет выявить наиболее важные системы для дальнейшей защиты информации.

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

Организация режима защиты конфиденциальной информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации любой организации, в частности образовательной. Конфиденциальная информация – любые сведения, составляющие служебную, коммерческую тайну, включая персональные данные сотрудников и студентов. Обладатель конфиденциальной информации – лицо, которое владеет конфиденциальной информацией на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальности [1]. Обладателем информации, составляющей конфиденциальность, является образовательная организация. Роль и место организации режима защиты информации в общей системе мер, направленных на защиту конфиденциальной информации образовательной организации, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учётом имеющихся в его распоряжении сил, средств, методов и способов защиты информации, а также на основе действующего нормативно-методического аппарата. Среди основных направлений режима защиты информации выделяют организационную, правовую и инженерно-техническую защиту информации. Организационной защите информации среди этих направлений отводится особое место. Организационная защита информации призвана посредством выбора конкретных сил и средств (включающих в себя правовые, инженерно-технические и инженерно-геологические) реализовать на практике спланированные руководством образовательной организации меры по защите конфиденциальной информации. Эти меры принимаются в зависимости от конкретной обстановки в образовательной организации, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к её утечке. Под угрозой безопасности информации понимается потенциальная возможность нарушения основных качественных

характеристик (свойств) информации при её обработке техническими средствами: конфиденциальности, целостности, доступности. Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями [3]. 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 [2]. Для организации режима защиты конфиденциальной информации в образовательной организации используются следующие методы.

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

Управление доступом. Метод, который основан на использовании регулирующих ресурсов автоматизированной системы, предотвращающих доступ к информационным носителям. Управление доступом осуществляется с помощью таких функций, как идентификация личности пользователя, работающего персонала и систем информационных ресурсов мерами:

присвоение каждому пользователю и объекту личного идентификатора; аутентификация, которая устанавливает принадлежность субъекта или объекта к заявленному им идентификатору; проверка соответствия полномочий, которая заключается в установлении точного времени суток, дня недели и ресурсов для проведения запланированных регламентом процедур; доступ для проведения работ установленных регламентом и создание необходимых условий для их проведения; реагирование на попытку несанкционированных действий в виде шумовой сигнализации, отключения, отказа в запросе и в задержке работ [1].

Маскировка. Метод криптографического закрытия, защищающий доступ к информации в автоматизированной системе. Регламентация – метод информационной защиты, при котором доступ к хранению и передаче данных при несанкционированном запросе сводится к минимуму. Принуждение – метод, который вынуждает пользователей при доступе к закрытой информации соблюдать определенные правила. Нарушение установленного протокола приводит к штрафным санкциям, административной и уголовной ответственности.

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

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

1. Физические средства защиты – используются в качестве внешней охраны для наблюдения за территорией объекта и защиты

автоматизированной информационной системы в виде специальных устройств.

2. Аппаратные средства защиты – это все виды электронных и электромеханических устройств, встроенных в блоки информационной автоматизированной системы, которые представлены как самостоятельные устройства, соединенные с этими блоками. Обеспечение режима защиты конфиденциальной информации с помощью аппаратных средств включает: – обеспечение запрета неавторизированного доступа удаленных пользователей и АИС (автоматизированная информационная система); – обеспечение надежной защиты файловых систем архивов и баз данных при отключениях или некорректной работе АИС; – обеспечение защиты программ и приложений. Вышеперечисленные задачи обеспечения организации режима защиты конфиденциальной информации обеспечивают аппаратные средства и технологии контроля доступа (идентификация, регистрация, определение полномочий пользователя).

3. Программные средства защиты входят в состав программного обеспечения или являются элементами аппаратных систем защиты. Такие средства осуществляют режим защиты конфиденциальной информации путем реализации логических и интеллектуальных защитных функций и относятся к наиболее популярным инструментам защиты. Это объясняется их доступной ценой, универсальностью, простотой внедрения и возможностью доработки под конкретную организацию или отдельного пользователя. В то же время, обеспечение режима защиты конфиденциальной информации с помощью программного обеспечения является наиболее уязвимым местом автоматизированной информационной системы образовательной организации [3]. Большинство современных операционных систем содержат программные решения для обеспечения блокировки повторного доступа к информации. При отсутствии таких средств могут использоваться различные

коммерческие программные обеспечения. Для режима защиты особо важной информации используется метод хранения данных с использованием системы сигнатур. В качестве сигнатуры может применяться система, включающая сочетание защитного байта с его размером, временем изменения и именем. При любом обращении к этому файлу система анализирует сочетание информации с оригиналом. Необходимо уточнить, что надежное обеспечение безопасности информации возможно только при использовании шифрования данных. Таким образом, организация защиты конфиденциальной информации представляет в настоящее время одно из ведущих направлений обеспечения безопасности государства, общества и отдельной личности. Проблемы различных аспектов безопасности становятся всё более актуальными с дальнейшим развитием информационно-коммуникационных технологий. Динамика развития законодательства в области информационной безопасности предполагает постоянное изменение методов и форм обеспечения режима защиты конфиденциальной информации, в том числе непрерывно развиваются и методы организации защиты информации в соответствии с вновь принимаемыми законами РФ, указами Президента РФ, постановлениями Правительства РФ.

Таким образом, цель исследования достигнута, поставленные задачи решены.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Азарова, Р.Н. Разработка паспорта компетенции: методические рекомендации для организаторов проектных работ и профессорско-преподавательских коллективов вузов / Р.Н. Азарова, Н.М. Золотарева. – М.: Исследовательский центр проблем качества подготовки специалистов, 2014. – 52 с.
2. Байденко, В.И. Выявление состава компетенций выпускников вузов как необходимый этап проектирования ГОС ВПО нового поколения: методич. пособие / В.И. Байденко. – М.: Исследовательский центр проблем качества подготовки специалистов, 2016. – 72 с.
3. Белевитин, В.А. Магистерская диссертация: рекомендации по подготовке и защите: учебно-методич. пособие / В.А. Белевитин, Е.А. Гнатышина, И.Г. Черновол. – Челябинск, 2016.
4. Вербицкий, А.А. Компетентностный подход и теория контекстного обучения: материалы к четвертому заседанию методологического семинара 16 ноября 2004 г. / А.А. Вербицкий. – М.: Исследовательский центр проблем качества подготовки специалистов, 2018. – 84 с.
5. Вербицкий, А.А. Инварианты профессионализма: проблемы формирования / А.А. Вербицкий. – М.: Логос, 2011. – 287 с.
6. Воронкин, А.С. Управление качеством дистанционного образования / А.С. Воронкин // Современные техника и технологии: сб-к трудов XVI Междун. научно-практической конф. студентов, аспирантов и молодых ученых (Томск, 12–16 апреля 2018 г.). – Томск, 2018. – Т. III. – С. 83–84.
7. Гладышева Ю.А. Особенности применения информационных техноло¬гий в образовательном процессе вуза / Ю.А. Гладышева [Электронный ресурс]. – Режим доступа: conference.osu.ru/.../conf_reports/conf8/467.doc

8. Годин, В.В. Управление информационными ресурсами / В.В. Годин, И.К. Корнеев. М.: ИН- ФРА-М, 2015.
9. Дистанционная форма обучения [Электронный ресурс]. – Режим доступа: http://ito.edu.ru/2008/Kursk/II/II-0-25.html.
10. Дуракова, И.Б. Теория управления персоналом / И.Б. Дуракова, О.А. Родин, С.М. Талтынов. – Воронеж: ВГУ, 2014. – 83 с.
11. Дятлова В.С. Информационно-коммуникационные технологии в системе образования / В.С. Дятлова [Электронный ресурс]. – Режим доступа: https://infourok.ru/statya-informacionnokommunikacionnie-tehnologii-v-sisteme-obrazovaniya-916893.html.
12. Дятлова В.С. Информационно-коммуникационные технологии в системе образования / В.С. Дятлова [Электронный ресурс]. – Режим доступа: https://infourok.ru/statya-informacionnokommunikacionnie-tehnologii-v-sisteme-obrazovaniya-916893.html.
13. Зеер, Э.Ф. Компетентностный подход к образованию // Образование и наука / Э.Ф. Зеер // Известия Уральского отделения Российской академии образования. – 2017. – № 3. – С. 27–40.
14. Зимняя И.А. Ключевые компетенции – новая парадигма результата образования / И.А. Зимняя. // Высшее образование сегодня. – 2018. – № 5. – С. 34–42.
15. Ибрагимов, Г.И. Компетентностный подход в профессиональном образовании / Г.И. Ибрагимов // Educational Technology & Society. – 2017. – 10(3). – С. 361–365.
16. Исаев, И.Ф. Колледж как инновационное образовательное учреждение / И.Ф. Исаев, Н.Л. Шеховская.– Белгород, 2018. – С. 5–24.
17. Исаев, И.Ф. Профессионально-педагогическая культура преподавателя / И.Ф. Исаев. – М.: Издат. центр «Академия», 2012. – 208 с.
18. Казанская, О.В. От дистанционного обучения к электронному / О.В. Казанская // Информационные технологии в образовании. Новосибирск: Изд-во НГТУ, 2019. – № 1 (17). – С. 4–5.

19. Ковальчук, М.В. Конвергенция наук и технологий [Электронный ресурс] // Российские нанотехнологии. – 2015. – Т. 6. – № 1–2. – С. 13–23. – Режим доступа: http://www.nrcki.ru/files/nbik01.pdf (дата обращения: 17.10.20).
20. Комелина, Е.В. Использование технологий web2.0 в учебном процессе вуза / Е.В. Комелина, Т.М. Гусакова // Преподавание Информационных технологий в России: Всеросс. конф-я [Электронный ресурс]. – Режим доступа: http://www.iteducation.ru/2019/reports/Komelina_Gusakova. htm (17.09.2020).
21. Концепция Федерального закона «Об индустрии электронного обучения (e-Learning)» (проект) [Электронный ресурс]. – Режим доступа: http:// mmc1012. unn. ru/News/ExpertSovet.php.
22. Кораблёв, А.А. Информационно-телекоммуникационные технологии в образовательном процессе / А.А. Кораблёв // СПОа. – 2016. – № 2.
23. Краснова, Г.А. Технологии создания электронных обучающих средств / Г.А. Краснова, М.И, Беляев, А.В. Соловов. – М. : МГИУ, 2018. – 224 с. – ISBN 5-276-00203-7.
24. Критерии **оценки** эффективности применения информационных технологий [Электронный ресурс]. – Режим доступа: http://lifeprog.ru/1_5313-_chastnie-kriterii-effektivnosti-primeneniya-informatsionnih-tehnologiy. html.
25. Кузьмина, Н.В. Диагностика продуктивности деятельности преподавателя и мастера производственного обучения как фактор повышения профессионализма / Н.В. Кузьмина // Проблемы диагностики факторов продуктивной деятельности педагогического коллектива. – М., 2016. – 152 с.
26. Кузьмина, Н.В. Профессионализм личности преподавателя / Н.В. Кузьмина. – М.: АПН., 2017. – 149 с.
27. Ласточкин, Ю.В. Анализ соответствия цены и качества продукции в информационной экономике / Ю.В. Ласточкин, И.И. Ицкович // Экономика и производство, – 2018. – № 4. – С. 54–62.

28. Манако, А.Ф. КТ в обучении: взгляд сквозь призму трансформаций / А.Ф Манако // Образовательные технологии и общество (Educational Technology & Society). – 2015. – Т. 15. – № 3. – С. 392–413.
29. Методы системного педагогического исследования [Текст] : учеб. пособие / под ред. Н. В. Кузьминой. Л. : Изд-во ЛГУ, 2016. 172 с.
30. Можаева, Г.В. Электронное обучение в вузе: современные тенденции развития / Г.В. Можаева // Гуманитарная информатика. 2013. Вып. 7. – С. 126–138.
31. Мизинцев, В.П. Проблема аналитической оценки качества и эффективности учебного процесса в СПОе. – Куйбышев: Изд-во КГПИ, 2014. – 107 с.
32. Мизинцев В.П. Количественная оценка эффективности и качества учебного процесса: автореферат дис. ... д-ра пед. наук : 13.00.01 / Моск. гос. ин-т им. В. И. Ленина, – М., 2016. – 32 с.
33. Макарова, Л.В. Преподаватель: модель деятельности и аттестация / Л.В. Макарова. – М.: Исследовательский центр проблем качества подготовки специалистов, 2017. – 148 с.
34. Маркова, А.К. Психология профессионализма / А.К. Маркова. – М.: Знание, 2019. – 308 с.
35. Маврина, И.А. Проектирование системы критериальных оценок эффективности деятельности профессиональных объединений педагогов как субъектов развития образовательного учреждения / И.А. Маврина, А.А. Мотышева // Прикладная психология и психоанализ. – № 3. – 2016. – С. 30–31.
36. Петухова, Е.И. Информационные технологии в образовании / Е.И. Петухова // Успехи современного естествознания. – 2013. – № 10.
37. Планирование развития ИТ на базе методологии Balanced Scorecard // Корпоративный менеджмент. Информационные технологии в управлении, 1998-2003.

38. Подолякин, О.В. Оценка эффективности инвестиций в информационную систему управления вузом – Дисс. … канд. экон. наук. – Вологда, 2018.

39. Позднеев, Б.М. Развитие индустрии электронного обучения: гармонизация подходов и стандартов / Б.М. Позднеев [Электронный ресурс]. – Режим доступа: elobuch1.pdf.

40. Подчалимова Г.Н. Проектирование содержания дополнительного профессионального образования руководителей СПО: теория и практика. – М. Курск, 2020. – 494 с.

41. Позднеев, Б.М. Стандартизация метаданных электронных образовательных ресурсов / Б.М. Позднеев, В.Д. Тихомирова // Открытое образование. 2015, – № 1(108). – С. 55–59.

42. Полат, Е.С. К проблеме определения эффективности дистанционной формы обучения / Е.С. Полат // Открытое образование. – 2020. – № 3. – С. 71–77.

43. Пугачев, В.М. Роль информационных технологий в науке и образовании / В.М. Пугачев, Е.Г. Газенаур // Вестник КемГУ Информатика, – 2019. – №3 – С. 31–34.

44. Роберт, И.В. Теория и методика информатизации образования (психолого-педагогический и технологический аспекты): монография / И.В. Роберт. – М.: ИИО РАО, 2017. – 236 с.

45. Роберт, И.В. Современные информационные технологии в образовании: дидактические проблемы; перспективы использования / И.В. Роберт. – М.: ИИО РАО, 2015. – 140 с.

46. Скворцов, А.А. Педагогические условия дистанционного обучения студента в наукоемкой образовательной среде: автореф-т дис... д-ра пед. наук: 13.00.01 / Тамбовский гос. ун-т им. Г.Р. Державина, – Тамбов – 2015. – 32 с.

47. Субетто, А.И. Онтология и эпистемология компетентностного подхода, классификация и квалиметрия компетенций / А.И. Субетто. – СПб.; М: Исследоват. центр проблем кач-ва под-ки спец-ов, 2016. – 72 с.

48. Татур, Ю.Г. Компетентность в структуре модели качества подготовки специалиста / Ю.Г. Татур // Высшее образование сегодня. – 2014. – № 3. – С. 20–26.

49. Таурбаева, А.А Экономическая эффективность информационных технологий / А.А. Таурбаева [Электронный ресурс]. – Режим доступа: http:// www.konspekt.biz/index.php?text=2549.

50. Тевс, Д.П. Использование современных информационных и коммуникационных технологий в учебном процессе: учеб.-методич. пособие / Д.П. Тевс, В.Н. Подковырова, Е.И. Апольских, М.В, Афонина. – Барнаул: БГПУ, 2015.

51. ТСО или как управлять IT-затратами / Интернет-портал для управленцев [Электронный ресурс]. – Режим доступа: http://www.management.com.ua/ ims/ims023.html.

52. Тыщенко, О.Б. Границы возможностей компьютера в обучении / О.Б. Тыщенко, М.В. Уткес // Образование. – 2013. – № 4. – С. 85–91.

53. Федеральный закон от 28.02.2012 № 11-ФЗ «О внесении изменений в Закон РФ «Об образовании» в части применения электронного обучения и дистанционных образовательных технологий» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2012/03/02/elektronnoe-obuchenie-dok.html.

54. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www. zakonrf. info/zakon-obobrazovanii/.

55. Фещенко, А.В. Социальные сети в образовании: анализ опыта и перспективы развития / А.В. Фещенко // Открытое дистанционное образование. 2017. – № 3 (43). – С. 44–49.

56. Чванова, М.С. Методология информатизации системы непрерывной подготовки специалистов: монография / М.С. Чванова, И.А. Липский // М.: Тамбов, 2015. – С. 260.

57. Шилова, М.И. Учителю о воспитанности СПОьников / М.И. Шилова // М.: Педагогика, 2014. – С. 12.

58. Якимова, О.Ю. Методы оценки эффективности корпоративных информационных систем управления / О.Ю. Якимова [Электронный ресурс]. – Режим доступа: http://www.top-technologies.ru/ru/article/view?id=22603.

59. Яковлев, А.И. Критерии эффективности идейно-воспитательной работы / А.И. Яковлев // Эффективность идейно-воспитательной работы. – М.: Мысль, 2015. – С. 85.

60. Voxmintsev, A. V. Problems of construction of conceptual models of the virtual world / A.V. Voxmintsev, A.V. Melnikov // XI International Workshop on Computer science and information technologies CSIT’2009: Crete, Greece, 2019. – С. 128–130.