МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

УПРАВЛЕНИЕ СЛУЖБОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Выпускная квалификационная работа
по направлению 44.04.04 «Профессиональное обучение»,
программа магистратуры «Управление информационной безопасности в профессиональном образовании»

Выполнил:
магистрант группы ОФ-209/210-2-1
Сибагатулин А. Н.
Научный руководитель:
д.п.н., профессор кафедры
АТ,ИТиМОТД Уварина Н. В.

Проверка на объем заимствований:
79.61 % авторского текста

Работа рекомендована к защите
« 27 » мая 2020г.

Заведующий кафедрой АТИТиМОТД
_____ В.В. Руднев

Челябинск 2020

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
Южно-Уральский государственный гуманитарно-педагогический университет
ПРОФЕССИОНАЛЬНО ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
Кафедра «Автомобильного транспорта, инновационных технологий и методики обучения техническим дисциплинам»

З А Д А Н И Е

на выпускную квалификационную работу

Магистранту группы ОФ-209-2-1 Сибагатулину Аскату Нафисовичу, обучающегося по направлению подготовки 44.04.04 «Профессиональное обучение (управление информационной безопасностью в профессиональном образовании)».

Научный руководитель квалификационной работы: д.п.н., профессор кафедры АТ,ИТиМОТД Уварина Наталья Викторовна

1. Тема выпускной квалификационной (магистерской) работы «Управление службой информационной безопасности в образовательной организации» утверждена приказом и.о. ректора Южно-Уральского государственного гуманитарно-педагогического университета №1463-с от 09.06.2018

2. Срок сдачи магистрантом законченной работы на кафедру: 24 июня 2020г.

3. Содержание и объем работы (пояснительной расчетной и экспериментальной частей, т.е. перечень подлежащих разработке вопросов):

4. Материалы для выполнения квалификационной работы:

1. Учебная, научно-техническая, педагогическая, методическая литература по теме квалификационной работы

2. Материалы преддипломной практики

5. Перечень графического материала (с точным указанием обязательных таблиц, чертежей или графиков, образцов и др.):

1. Уровни и проявления угрозы информационной безопасности

2. Классификация средств защиты

3. Схема взаимодействия системы контент фильтрации

6. Консультанты по специальным разделам ВКР:

Раздел	Консультант	Отметка о выполнении
Педагогика	Уварина Н. В.	
Экономика	Уварина Н. В.	
Охрана труда	Уварина Н. В.	

Дата выдачи задания: 11 июня 2019г.

Задание выдал: Уварина Н. В. _____

Задание принял: Сибагатулин А. Н.

_____

КАЛЕНДАРНЫЙ ПЛАН

№ и/и	Наименование этапов подготовки выпускной квалификационной работы	Срок выполнения этапов ВКР	Отметка о выполнении
1.	Предзащита ВКР	мая 2020	
2.	Доработка ВКР после предзащиты	июня 2020	
3.	Нормоконтроль	июня 2020	
4.	Подписание ВКР научным руководителем	июня 2020	
5.	Оформление пояснительной записки и презентации ВКР (сдача на кафедру)	июня 2020	
6.	Подписание рецензии на ВКР	июля 2020	
7.	Получение справки о проверке на объем заимствований	30 мая 2020	
8.	Защита ВКР на заседании Государственной экзаменационной комиссии	09 июля 2020	

Автор ВКР: Сибагатулин А. Н. _____

Научный
руководитель ВКР Уварина Н. В. _____

Заведующий
кафедрой, доц., к.т.н. Руднев В.В. _____

АННОТАЦИЯ

Сибагатулин А. Н. Управление службой информационной безопасности в образовательной организации - Челябинск: ЮУрГГПУ, 2020, 72 стр. машинописного текста, 8 таблиц, 9 рисунков, список использованной литературы 105 наименований, приложений – 4 (20 стр.)

Ключевые слова: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ.

Первая глава посвящена описанию теоретическим основам управления службой информационной безопасности в образовательной организации.

В главе рассмотрены понятийный аппарат исследования, основные составляющие информационной безопасности в образовательной организации; основные типичные угрозы, особенности и методы защиты информации в образовательной организации.

Во второй главе, посвященной описанию экспериментальной работы по совершенствованию управления службой информационной безопасности ГБПОУ «Южно-Уральский Государственный Технический Колледж», на основе анализа особенностей управления службой информационной безопасности и информационных рисков колледжа разработаны практические рекомендации по реализации нововведений управления данной службой с целью нивелирования описанных в первой главе и проанализированных в колледже информационных угроз и рисков.

Итоги выполнения второй главы имеют высокую практическую значимость, так как разработанные рекомендации носят типовой характер и могут быть применены в других образовательных организациях,

В заключении диссертационной работы сделаны основные выводы по результатам исследования.

Магистрант _____Сибагатулин А. Н.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность проблемы исследования. Информационная среда современного общества охватывает все сферы человеческой деятельности и включает в себя колоссальный объем информации. Вопросы информационной безопасности чаще всего рассматриваются в контексте национальной безопасности, однако следует учитывать, что одним из наиболее активных потребителей и генераторов информации является сфера образования, где формируется интеллектуальный и нравственный потенциал будущих поколений. Эффективность образовательной системы в значительной мере зависит от эффективности потребления и генерации информации, что позволяет ставить вопрос об ограждении обучаемых от информации, способной нанести ущерб личности обучаемого и спровоцировать деструктивные последствия.

Существующее в Российской Федерации законодательство об образовании позволяет образовательной организации осуществлять электронное обучение, в том числе использовать дистанционные технологии. Учащиеся, становятся активными пользователями сети Интернет, в том числе по вопросам, не связанным с образовательной деятельностью. Важным при этом становятся вопросы обеспечения информационной безопасности детей. Обеспечение информационной безопасности образовательной организации является одним из основных направлений информатизации и, в целом, функционирования образовательной организации. Информационная безопасность является условием и одним из критериев эффективности деятельности образовательной организации.

Цель исследования: теоретически обосновать, разработать и проверить эффективность информационной безопасности в образовательной организации.

Объект исследования: информационной безопасности в образовательной организации

Предметом исследования являются правовые средства и методы, с помощью которых достигается информационная безопасность в образовательной организации.

В процессе разработки темы была выдвинута следующая **гипотеза:** проведение мероприятий с родителями школьников в образовательных организациях позволяет повысить их компетентность вопросах обеспечения информационной безопасности детей, что в итоге повысит эффективность комплекса проводимых мер по ограничению доступа детей к информации, способной причинить вред здоровью и (или) развитию ребенка.

В соответствии с предметом исследования для достижения поставленной цели и проверки гипотезы необходимо решить следующие **задачи:**

1) рассмотреть понятие и основные составляющие информационной безопасности в образовательной организации;

2) изучить угрозы информационной безопасности образовательной организации;

3) определить особенности защиты информации в образовательном учреждении;

4) выявить особенности управления службой информационной безопасности в ГБПОУ «Южно-Уральский Государственный Технический Колледж»;

5) провести анализ информационных рисков образовательного учреждения;

6) разработать практические рекомендации по реализации нововведений управления службой информационной безопасности в образовательной организации.

Методологическая и информационная база исследования.

В ходе проведения диссертационной работы были использованы научные труды отечественных и зарубежных ученых, материалы периодической печати, законы Российской Федерации, материалы научно-

практических конференций по проблемам разработки и реализации информационной безопасности образовательных организаций.

Методы исследования:

- теоретические методы: теоретический анализ психолого-педагогической, управленческой, методической литературы по теме исследования;

- эмпирические методы: проведение в практической части тестовых исследований по методикам, количественного и качественный анализа;

- наблюдение, сравнительно-сопоставительный;

- статистический анализ.

Научная новизна исследования заключается в системном изучении всего массива нормативных правовых актов, раскрывающих сущность универсальных и специфических свойств информационной безопасности образовательной организации, выделении узловых проблем в системе информационной безопасности образовательной организации, требующих особого правового регулирования, определении концептуальных перспектив в области правового обеспечения информационной безопасности в образовательной организации.

Практическая значимость работы заключается в том, что она связана с актуальными проблемами управления службой информационной безопасности образовательных организаций, на примере ГБПОУ «Южно-Уральский Государственный Технический Колледж». Разработаны практические рекомендации по реализации нововведений управления службой информационной безопасности колледжа.

Достоверность и обоснованность научных результатов диссертационной работы обеспечиваются реализацией научной методологии, использованием личностно-деятельностного подхода к решению поставленной проблемы; анализом и синтезом теоретического и экспериментального материала; организацией опытно-экспериментальной работы с применением комплекса методов, адекватных объёму, предмету,

целям и задачам исследования; деятельностью эксперимента, многократной и всесторонней проверкой теоретических выводов и практической значимости.

База опытно-экспериментальной работы. Базой опытно-экспериментальной работы послужил ГБПОУ «Южно-Уральский Государственный Технический Колледж».

Этапы исследования:

1. Первый этап (1-2 семестр обучения) - изучение и анализ научной литературы по проблеме исследования, основными составляющими информационной безопасности в образовательной организации; основными типичными угрозами, особенностями и методами защиты информации в образовательной организации.

2. Второй этап (3-4 семестр обучения) - анализ особенностей управления службой информационной безопасности и информационных рисков ГБПОУ «Южно-Уральский Государственный Технический Колледж»; разработка практических рекомендаций по реализации нововведений управления службой ИБ колледжа с целью нивелирования информационных угроз и рисков.

3. Третий этап (4 семестр обучения) - осуществлены обобщение материалов исследования, их систематизация, обработка экспериментальных данных, формирование и уточнение выводов; оформление рукописи диссертации.

Структура работы состоит из введения, двух глав, заключения, библиографического списка и приложения.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ УПРАВЛЕНИЯ СЛУЖБОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1. Понятие и основные составляющие информационной безопасности в образовательной организации

В современном обществе информационная сфера представляет собой системообразующий фактор, определяющий все происходящие в жизни общества процессы и поведение членов общества как участников этих процессов. Информационная среда оказывает активное влияние на все составляющие безопасности государства – политическую, экономическую, оборонную и другие [99]. Она оказывает мощнейшее воздействие и на состояние образовательной системы. Растущая зависимость от информационно-коммуникационных технологий во всех областях человеческой жизни привела к уязвимости, которые необходимо надлежащим образом определить, тщательно проанализировать, устранить или уменьшить. Все соответствующие субъекты – государственные органы, частный сектор или отдельные граждане – должны признать эту общую ответственность, принять меры для защиты и при необходимости обеспечить скоординированные меры по укреплению безопасности в информационном пространстве.

Информация (лат. informatio — разъяснение, изложение), первоначально — сведения, передаваемые людьми устным, письменным или другим способом с помощью условных сигналов, технических средств и т.д. С середины 20-го века информация является общенаучным понятием, включающим в себя:

- сведения, передаваемые между людьми, человеком и автоматом, автоматом и автоматом;

- сигналы в животном и растительном мире;

- признаки, передаваемые от клетки к клетке, от организма к организму;

- и т.д.

Другими словами, информация носит фундаментальный и универсальный характер, являясь многозначным понятием. Эту мысль можно подкрепить словами Н. Винера (отца кибернетики): «Информация есть информация, а не материя и не энергия».

Согласно традиционной философской точке зрения, информация существует независимо от человека и является свойством материи. В рамках рассматриваемой дисциплины, под информацией понимаются сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах.

В Доктрине информационной безопасности Российской Федерации под термином информационная безопасность понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В более узком смысле, под информационной безопасностью понимается состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Сегодня, термин «информационная безопасность» часто можно встретить в сфере образования. В любом образовательном учреждении хранится, обрабатывается и используется огромное количество информации – это, и персональные данные учеников и сотрудников, и различная конфиденциальная информация по деятельности объекта, и сведения об обеспечении образовательного процесса, и другая информация, доступность к которой должна быть ограничена [3]. Ценность хранимой информации

указывает на то, что обеспечение информационной безопасности в образовательном учреждении должно быть одним из приоритетных направлений работы образовательной организации.

Под «информационной безопасностью образовательной организации» понимается состояние защищенности персональных данных субъектов образовательного процесса, обучающихся от информации, причиняющей вред их здоровью и развитию, информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Нормативно правовая база регламентирующая информационную безопасность образовательных учреждений включает в себя:

- Распоряжение правительства РФ от 2 декабря 2015 г. № 2471-р «Концепция информационной безопасности детей»;

- Федеральный закон РФ от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

- Письмо Минобразования РФ от 13.08.2012 № 01-51-088ин «Об организации использования информационных и коммуникационных ресурсов общеобразовательных учреждений»;

- Указ Президента России от 01.06.2012 № 761 «О национальной стратегии действий в интересах детей» на 2012-2017 годы;

- СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в образовательных учреждениях»;

- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (ред. от 28.07.2012);

- Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;

- Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Письмо Минобразования от 25.05.2001 № 753/23-16 «Об информатизации дошкольного образования в России»;

- Доктрина информационной безопасности РФ;

- Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

- ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;

- Конституция РФ;

- Конвенция о правах ребенка.

Для обеспечения функционирования системы информационной безопасности в образовательной организации, необходим пакет внутренних нормативных документов.

Для организации безопасного доступа в Интернет, в образовательной организации необходимо разработать следующий пакет документов:

- правила использования сети Интернет в ОО для всех субъектов образовательного процесса;

- документ ознакомления и согласия с Правилами использования сети Интернет в ОО, удостоверенное подписью в документе ознакомления и согласия с правилами. Регулярное (периодичное) заполнение документа ознакомления;

- инструкция для сотрудников ОО о порядке действий при осуществлении контроля за обучающимися, работниками организации, родителями при использовании ресурсов Интернета

- приказ, назначающий администратора точки доступа к сети Интернет;

- должностная инструкция администратора точки доступа к сети Интернет в ОО;

- положение о Совете образовательной организации по вопросам регламентации доступа к ресурсам сети Интернет. В положении указать

персональный состав Совета, поддерживать в актуальном состоянии персональный состав Совета;

- регламент работы обучающихся, родителей, учителей (преподавателей) и других сотрудников ОО;

- документ регистрации посетителей точки доступа к сети Интернет в образовательной организации;

- документ регистрации ресурсов, посещаемых с точки доступа к сети Интернет в образовательном учреждении. Регулярное (периодичное) заполнение документов регистрации;

- ответственный за антивирусную безопасность ОО;

- локальные акты, регламентирующие обязанности ответственных за антивирусную безопасность ОО;

- положение «О защите детей от информации, причиняющей вред их здоровью и развитию» в ОО, содержащее классификаторы информации, доступ к которой обучающимся запрещен и разрешен;

- лицензионное соглашение или договор на использование программных контент-фильтров, используемых в ОО;

На всех компьютерных устройствах, входящих в сеть ОО, необходимо установить лицензионное антивирусное программное обеспечение и регулярно обновлять антивирусные базы (сигнатуры), в том числе и на личных устройствах обучающихся и сотрудников.

Необходимо отметить, что сегодня учебно-воспитательный процесс в образовательных учреждениях различного типа происходит в рамках сетевого взаимодействия всех участников этого процесса в условиях информационно-образовательной среды.

Организация взаимодействия участников учебно-воспитательного процесса представлена на рисунке 1.

Очевидно, что при сетевом взаимодействии через отрытые каналы связи все участники взаимодействия могут стать как объектом, так и

источником угроз информационной безопасности образовательного учреждения и личности.

Необходимо уточнить, что необходимым условием для функционирования системы безопасности образовательной организации является проведение мероприятий для педагогов, обучающихся и родителей, с целью развития компетенций, связанных с работой на компьютерных устройствах, поиском и обработкой информации в Интернете, защитой от «вредной» информации.

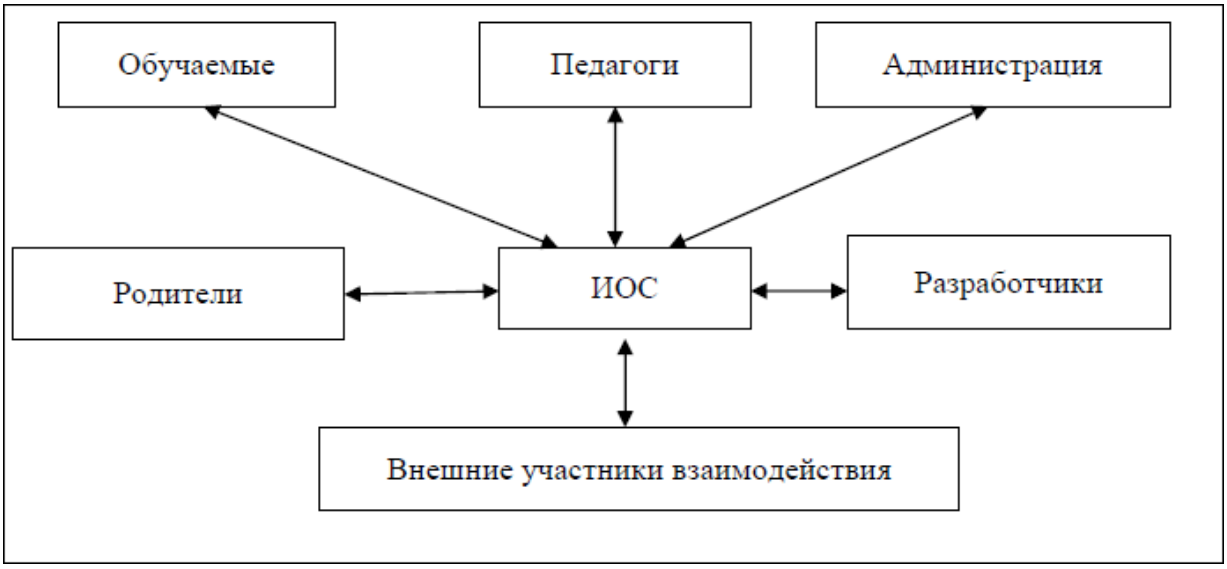

Рис. 1. Структура сетевого взаимодействия всех участников учебно-воспитательного процесса в условиях информационно-образовательной среды (ИОС)

Система информационной безопасности образовательной организации включает в себя следующие компоненты:

1. Правовой эго специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

2. Организационный - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какою-либо ущерба;

3. Программно-технический - это использование различных алгоритмических, программных и аппаратных средств, препятствующих нанесению ущерба.

В системе информационной безопасности образовательной организации можно выделить следующие направления:

- организация контентной фильтрации данных из Интернета на компьютерных устройствах, используемых учениками;

- обеспечение антивирусной защиты и других интернет-угроз компьютеров и мобильных устройств локальной сети организации;

- обеспечение защиты персональных данных субъектов образовательного процесса;

- организация правомерного использования объектов авторского права.

При создании системы информационной безопасности в образовательной организации необходимо учитывать ключевые характеристики информационной среды, в рамках которой реализуется сетевое взаимодействие. Такая среда обладает следующими свойствами:

- она создана и поддерживается для конкретных целей;

- она является динамичной;

- она является быстрой;

- она относительно безгранична;

- она имеет низкие входные барьеры;

- она быстро растет;

- ее можно рассматривать с позиций различных структур, которые неизбежно формируют представления о соответствующем поведении и ценностях [24].

1.2. Угрозы информационной безопасности образовательной организации

В сфере обеспечения информационной безопасности одним из ключевых понятий является понятие угрозы. Под угрозой в общем случае понимается возможное событие, явление, действие или процесс, которое потенциально способно нанести ущерб чьим-либо интересам. Угроза объекту информационной безопасности это совокупность факторов и условий, которые возникают в процессе взаимодействия различных объектов или их элементов и способны оказать негативное воздействие на конкретный объект информационной безопасности.

Информационная угроза – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации.

Угроза информационной безопасности – совокупность условий и факторов, которые создают опасность нарушения информационной безопасности.

Попытка реализации угрозы называется атакой, а предпринимающий такую попытку – злоумышленником.

Угрозы информационной безопасности могут быть классифицированы по различным признакам [91]:

а) По природе возникновения (естественные и искусственные).

- Естественные – это те угрозы, которые возникли в результате какого-либо природного катаклизма (землетрясения, наводнения и др.);

- Искусственные – результат деятельности человека.

б) По степени преднамеренности:

- Случайные – угрозы, вызванные ошибками или халатностью персонала;

- Преднамеренные – возникают в результате целенаправленной деятельности злоумышленников.

в) По аспекту информационной безопасности:

- Угрозы конфиденциальности, угрозы целостности, угрозы доступности.

г) По компонентам, на которые нацелена угроза:

Данные, программное обеспечение, аппаратное обеспечение.

Рассмотрим более подробно, какие угрозы информационной безопасности существуют непосредственно в образовательной организации [96]:

- Несанкционированный доступ к персональным данным, конфиденциальной информации, и программам, хранящим важные документы. Для образовательных учреждений возможна подмена исходных данных в электронных журналах, личных делах педагогов и учащихся;

- Отрицательное влияние на психику учащегося. Свободный доступ в школе/колледже/институте в интернет открывает для детей огромное количество информации, где помимо обучающих и развивающих ресурсов, также присутствуют и ресурсы с нежелательной информацией (материалы порнографического характера, насилия над людьми и животными, пропаганды наркотиков, экстремистской идеологии);

- Чрезмерное использование учащимися социальных сетей, следствием чего является разрушение нормального образовательного процесса обучения;

- Кибертерроризм, как новая форма терроризма, возможна и в образовательных учреждениях. Создание безопасной информационно-технологической среды существенно снизит риск кибератаки на объекты образования, которые могут привести к нарушению функционирования управляющих автоматически систем и последующему повреждению инфраструктуры.

Можно выделить четыре уровня опасности для субъектов образовательного процесса, связанной с угрозами информационной безопасности (таблица 1).

Таблица 1

Уровни и проявления угрозы информационной безопасности

Уровень угрозы	Возможные проявления реализации угрозы для субъектов образовательного процесса
низкий	незначительные негативные последствия
средний	негативные последствия
высокий	значительные негативные последствия
критический	потеря жизни или здоровья

Тип информационного опыта, получаемый учащимися в рамках сетевого взаимодействия, является важным фактором, определяющим типы рисков, которым они подвергаются, и, следовательно, типы защиты, которая может быть наиболее эффективной.

Информационным угрозам подвергаются не только субъекты ИОС как элементы этой системы, но и связи между ними. Учитывая, что в рамках ИОС происходит взаимодействие ее субъектов, можно рассматривать информационные воздействия с точки зрения угрозы учебному процессу, возможности его реализации и достижению его целей.

Методология управления рисками должна включают четыре основных шага оценки риска:

- инвентаризация сетевых ресурсов, включенных в сферу оценки;

- идентификация угроз, связанных с этими активами;

- категорирование вероятности и потенциальных результатов реализации угроз для субъектов ИОС и связей;

- определение средств контроля, необходимых для снижения выявленных рисков до приемлемого уровня.

Анализ угроз и рисков создает предпосылки для формирования компетентности педагогических работников и управленческих кадров в области информационной безопасности посредством освоения ряда дополнительных специальных компетенций. Содержание педагогических

воздействий на каждом этапе обучения должно определяться в зависимости от актуальных угроз информационной безопасности. Необходимо также разработать условия безопасного использования соответствующих образовательных информационных сервисов.

Особенность обучения информационной безопасности состоит в том то, что изучения только правового, организационного и технического обеспечения информационной безопасности недостаточно для эффективного противодействия угрозам сетевой информационной среды. Необходимо воспитать нравственность и ответственность за использование информации, которая может причинить ущерб не только личности, неумело с ней обращающейся, но и другим участникам информационных процессов [25]. Противодействием угрозам информационной безопасности должно стать обучение позитивным и ответственным формам онлайн-поведения.

Под информационной безопасностью личности следует понимать такое состояние и условия жизнедеятельности личности, при которых минимизирована или отсутствует угроза нанесения вреда личному информационному пространству и информации, которой обладает индивид [6].

Для эффективной организации мероприятий по обеспечению информационной безопасности обучающихся, существует ряд угроз, исходящих из сети Интернет, включая различные социальные сети.

Все угрозы могут быть использованы для дестабилизации обстановки в образовательной организации, а при наихудшем варианте развития событий – и для проведения террористического акта. Федеральный закон N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает правовые принципы, стандарты и механизмы правовой охраны и защиты детей от информации, наносящей вред их здоровью, нравственному и духовному развитию.

В основу данного закона положены нормы Конституции РФ, ратифицированные РФ принципы и нормы международного права,

гарантирующие свободу слова, творчества и массовой информации, свободы в выборе и доступе к информации взрослой аудитории при условии оптимальной защиты детей от деструктивного информационного воздействия.

Закон обозначает основные принципы государственной политики в сфере защиты детей от негативной информации:

- принцип приоритетности интересов детей, обеспечения государством особой их защиты;

- признание допустимости и правомерности ограничения в этих целях конституционных прав и свобод физических и юридических лиц в случаях, когда они вступают в противоречие с правами и законными интересами детей, нарушают их физическую, интеллектуальную, нравственную и психическую безопасность;

- признание права ребенка на информационную безопасность: наличие защиты со стороны общества и государства от тех видов информации, которые представляют опасность для жизни и здоровья детей, либо могут причинить вред их моральному нравственному, духовному, психическому и физическому развитию; признание правомерности установления в интересах защиты национальной безопасности и общественной нравственности абсолютного запрета на использованиесредств массовой информации, компьютерных сетей и других носителей информации в целях совершения уголовно наказуемых деяний, осуществления экстремистской деятельности, пропаганды порнографии, наркотических средств и психотропных веществ, культа насилия и жестокости, а также для распространение иной информации, оборот которой запрещен федеральными законами (например, злоупотреблениеизображением и голосом ребенка в эротических целях, распространениеконфиденциальных сведений о ребенке без его согласия и согласия его законных представителей);

- учет при формировании государственной информационной политики в целях защиты и гармоничного развития детей российских традиций и культурных ценностей;

- признание приоритета над запретительными мерами превентивных мер защиты детей от информации, наносящей вред их здоровью и развитию.

Ответственность образовательной организации по вопросу обеспечения информационной безопасности детей закреплена в Федеральном законе №273-ФЗ «Об образовании в Российской Федерации». В компетенции образовательной организации входит создание необходимых условий для охраны и укрепления здоровья обучающихся, на основании которых мы выделили задачи педагогического характера для организации мероприятий по информационной безопасности:

1. формирование у учащихся устойчивого убеждения в использовании информационных ресурсов;

2. формирования устойчивых поведенческих навыков в сфере информационной безопасности;

3. развитие у учащихся способности распознать и противостоять негативной информации в Интернет-пространстве и СМИ, через обучение способам защиты от вредной информации.

Решение этих задач должно выполняться комплексно и систематически на каждом этапе работы в системе образовательной организации, с возможностью дополнения и варьирования по мере необходимости, исходя из результативности каждого этапа. Безопасность доступа обучающихся к ресурсам сети Интернет и контроль за процессом работы в сети может достигаться путем применения комплекса аппаратно–технических и организационных мер.

Таким образом, обеспечение информационной безопасности образовательного учреждения на современном этапе становится одним из основных видов его деятельности. Как правило, в образовательной

организации не всегда работают специалисты, способные быстро решать вопросы обеспечения информационной безопасности учащихся, принимать решения по постоянно возникающим проблемам. Возникающие проблемы в каждой образовательной организации приходится устранять, вне зависимости от того, есть подготовленные специалисты или их нет. Если работа по информационной безопасности учащихся будет вестись целенаправленно, на протяжении всего периода обучения в образовательной организации, если в образовании будет большеспециалистов, знающих как справиться с возникающими сложностями в обеспечении информационной безопасности, то в образовательных организациях будет комфортно всем участникам образовательного процесса.

1.3 Особенности защиты информации в образовательной организации

Процесс информатизации полностью поглощает современный мир. Информация на сегодняшний день представляется главным атрибутом полноценной жизни человека, общества и государства в целом. Любую сферу деятельности человека сложно представить без информации, она присутствует везде и имеет при этом огромную ценность. Поэтому защита информации является одним из приоритетных направлений политики государства, и каждой отдельной организации. [97,98]

Защита информации – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессесбора, хранения, обработки и передачи информации в информационных системах.

Принято различать следующие средства защиты (рисунок 2).

Рис. 2. Классификация средств защиты

1. Формальные средства защиты – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.

2. Неформальные средства защиты – регламентируют деятельность человека.

Информационная безопасность в образовательной организации - понятие составное, включающее в себя информационно-технические, и правовые аспекты. Сейчас все работники образовательных организаций находятся наравне с учителями информатики, так как информационная безопасность вписывается во все виды деятельности образовательной организации.

В качестве целей создания системы информационной безопасности в образовательной организации следует привести:

1) защиту обучающихся, педагогов, их прав и интересов, а также имущества от опасных воздействий, генерируемых информационной средой;

2) обеспечение эффективного функционирования и развития образовательной организации;

3) снижение ущерба от негативных воздействий угроз информационной безопасности, снижение вероятности проявления угроз и последствий реализации рисков;

4) улучшение качества жизни, повышение благополучия учащихся и педагогов (за счет снижения психологических расстройств, смертности, повышения сохранности здоровья, снижения риска потери или хищения информации).

С учетом, как мирового, так и отечественного опыта обеспечение информационной безопасности осуществляется по следующим основным направлениям:

- правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

- организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

- инженерная и программно-техническая защита – это использование различных алгоритмических, программных и аппаратных средств, препятствующих нанесению ущерба.

Образовательные организации являются операторами персональных данных, поскольку занимаются обработкой персональных данных учащихся и педагогов. Следовательно, ответственными сотрудниками этих учреждений должен обеспечиваться ФЗ № 152 «О персональных данных».

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

В рамках образовательных организаций должен быть выполнен комплекс работ по сбору пакета документов (25 форм), предоставляемых на проверку регуляторам (контролирующим организациям).

При построении системы информационной безопасности образовательной организации решающую роль играет организационная защита. При этом в первую очередь необходимо учесть следующее.

Безопасность информации должна быть обеспечена только при комплексном использовании всех имеющихся средств защиты.

Безопасность доступа обучающихся к ресурсам сети Интернет и контроль за процессом работы в сети может достигаться путем применения комплекса аппаратно–технических и организационных мер.

С целью обеспечения реализации проведения мероприятий, направленных на ограничение доступа обучающихся к видам информации, распространяемой посредством сети «интернет» в образовательных организациях предлагаются использование современных систем контент фильтрации.

Основными задачи в ходе систем контент фильтрации являются:

- Автоматизация процессов обнаружения нежелательных, запрещенных Интернет-ресурсов, путем применения современных синтаксических, морфологических алгоритмов обработки запросов;

- Интеграция модернизированных системы контент фильтрации в уже существующую систему без потери временных издержек;

- Интеграцию с другими подразделениями образовательного процесса, деятельность которых направлена на повышения качества обучения и отслеживания нежелательных ресурсов.

Не стоит забывать, что обеспечить 100%-ную защиту от нежелательного контента в сети Интернет невозможно. При соблюдении всех правил в разработке современной СКФ возможно снижение риска до минимально допустимого значения.

Предлагаемая схема разработки современной СКФ представлена на рисунке 3.

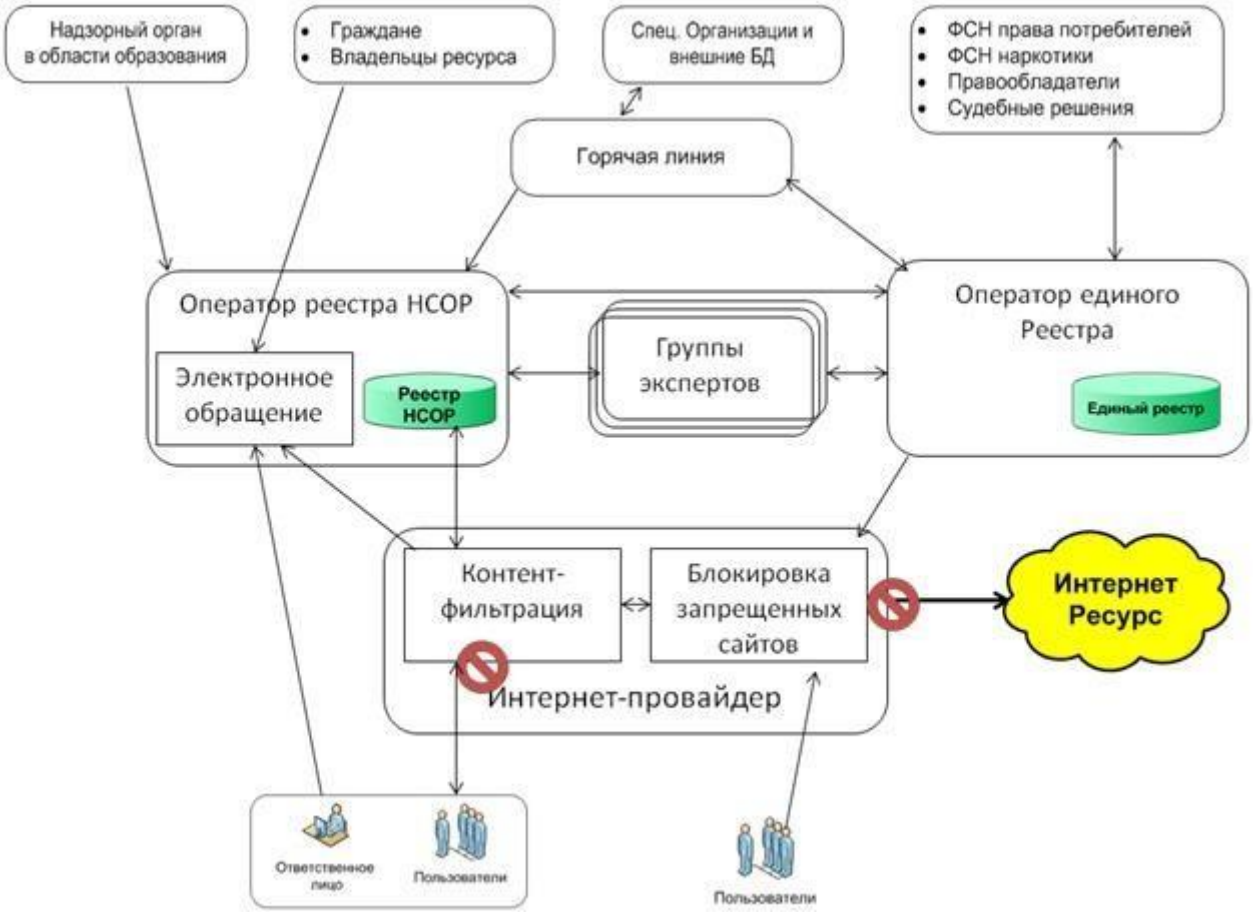

Рис. 3. Схема взаимодействия системы контент фильтрации со всеми структурами.

Подводя итоги анализа текущей ситуации по обеспечению информационной безопасности учащихся образовательных организаций были сделаны выводы по ряду факторов, которые необходимо улучшить для более качественного функционирования механизма по защите детей от нежелательного контента и информации причиняющей вред здоровью детей.

На данный момент известно, что только техническими средствами эту проблему не решить. На сегодняшний день нет компьютерных программ, способных полностью защитить пользователя от доступа к нежелательной информации. Самым эффективным механизмом информационной безопасности несовершеннолетних может стать работа по формированию

осознанного самостоятельного умения учащихся выбирать безопасную информацию.

Лучший фильтр, который может обеспечить безопасность ребенка в сети и решить многие другие проблемы, – в голове самого ребенка, [redacted]нужно только настроить этот фильтр.

Чтобы негативная информация в сети не позволила спровоцировать ребенка на деструктивные действия, особое внимание необходимо уделить профилактике наркомании и других видов зависимого поведения детей и подростков. Формирование у обучающегося навыков здорового и безопасного образа жизни, устойчивых антинаркотических установок можно осуществлять в рамках предметов естественно–биологического цикла, факультативных занятий, психологических тренингов, внеурочных мероприятий.

Умело спроектированное воспитательное пространство образовательной организации, организация занятости детей и подростков социально–значимой деятельностью является действенным способом обеспечения информационной безопасности. Повышению информационной компетентности подрастающего поколения способствует участие учащихся в областных конкурсах, конкурсе творческих работ по информатике и информационным технологиям, привлечение детей и подростков к изданию газет, работе телестудий, разработке сайтов. Проводимые мероприятия дадут больший результат, если образовательное учреждение будет привлекать родителей учащихся и повышать их компетенцию в вопросах информационной безопасности учащихся, через родительские собрания или ежемесячные родительские встречи.

Ответственность образовательной организации по вопросу обеспечения информационной безопасности детей закреплена в Федеральном законе № 273-ФЗ «Об образовании в Российской Федерации».

В компетенции образовательной организации входит создание необходимых условий для охраны и укрепления здоровья обучающихся, наосновании которых мы выделили задачи для организации мероприятий по информационной безопасности:

- формирование у учащихся устойчивого убеждения в использовании информационных ресурсов;

- формирования устойчивых поведенческих навыков в сфере информационной безопасности;

- развитие у учащихся способности распознать и противостоять негативной информации в Интернет-пространстве и СМИ, через обучение способам защиты от вредной информации.

Решение этих задач должно выполняться комплексно и систематически на каждом этапе работы в системе образовательного учреждения, с возможностью дополнения и варьирования по мере необходимости, исходя из результативности каждого этапа.

Таким образом, обеспечение информационной безопасности образовательного учреждения на современном этапе становится одним из основных видов его деятельности. Если работа по информационной безопасности учащихся будет вестись целенаправленно, на протяжении всего периода обучения в образовательных организациях, если в нашем образовании будет больше специалистов, знающих как справиться с возникающими сложностями в обеспечении информационной безопасности, то в наших образовательная организациях будет комфортно всем участникам образовательного процесса.

Выводы по первой главе

Информационная безопасность относится к механизмам, которые защищают ЭИОС от негативного воздействия, исходящего из сетевого пространства. Она не должна сводиться к простому техническому контролю аппаратных и программных средств и сетевых ресурсов, ее следует понимать как исследование и практику защиты субъектов ИОС во всех ееформах.

Проблема обеспечения информационной безопасности ЭИОС характеризуется острой необходимостью и неотложностью.

Социально-педагогическое решение проблемы информационной безопасности состоит, в обязательном включении в деятельность педагогических и управленческих кадров такого компонента профессиональной подготовки как компетентность в области информационной безопасности. Педагогическое воздействие должно быть направлено не только на привитие знаний, умений и навыков работы с информацией, но также на формирование опыта деятельности по защите от негативной информации в профессиональной и управленческой деятельности.

По результатам анализа информационной безопасности можно сделать вывод, что в настоящее время в российской образовательной системе отсутствует комплексный подход к формированию системы информационной безопасности. Отдельные организационно-педагогические мероприятия и действия, ориентированные на обеспечение информационной безопасности личности, можно рассматривать только как предпосылки к разработке и принятию педагогическим сообществом болееширокого комплекса мер.

Глава 2. Экспериментальная работа по совершенствованию управления службой информационной безопасности в ГБПОУ «Южно-Уральский Государственный Технический Колледж»

2.1. Особенности управления службой информационной безопасности в ГБПОУ «Южно-Уральский Государственный Технический Колледж»

ГБПОУ «Южно-Уральский Государственный Технический Колледж» – это динамично развивающееся образовательная организация с постоянно обновляющейся материально-технической базой.

Место нахождения Учреждения: 454071, г. Челябинск, ул. Гагарина, д7.

Организация осуществляет реализацию интегрированных образовательных программ начального и среднего профессионального образования.

Главной задачей техникума является создание необходимых условий для удовлетворения потребности личности в получении начального профессионального образования, конкретной профессии (специальности) соответствующего уровня квалификации с возможностью повышения общеобразовательного уровня обучающихся, не имеющих среднего (полного) общего образования, а также ускоренного приобретения трудовых навыков для выполнения определенной работы или группы работ.

Миссия ГБПОУ «Южно-Уральский Государственный Технический Колледж». Реализация основных и дополнительных профессиональных образовательных программ с целью формирования общих и профессиональных компетенций конкурентоспособного специалиста с развитыми социально-значимыми качествами, нацеленного на саморазвитие.

Стратегическая цель в области качества:

Обеспечение условий реализации основных и дополнительных профессиональных образовательных программ для удовлетворения потребностей всех категорий обучающихся, персонала техникума, заинтересованных социальных партнеров, государства и общества, в целом.

Цели ГБПОУ «Южно-Уральский Государственный Технический Колледж» в области качества:

- Удовлетворение всех категорий обучающихся, членов коллектива, работодателей, заинтересованных социальных партнеров, государства и общества в целом.

- Формирование специалиста, обладающего творческим мышлением, навыками в управлении и саморазвитии, социально-значимыми качествами личности.

- Совершенствование системы управления техникумом для повышения качества подготовки выпускников.

- Обеспечение положительной динамики развития техникума для успешного продвижения выпускников на рынке труда.

- Профессиональное и социальное развитие коллектива.

- Обеспечение комплексной безопасности образовательного процессав соответствии с ГОСТ Р 54934-2012/OHSAS 18001:2007.

Инженерно-педагогический коллектив техникума, используя компетентностный подход в профессиональном образовании обучающихся как основу профессиональной мобильности выпускника, мотивирует их на рабочих профессий высокого уровня и создает комфортную среду обучения и воспитания.

Специальности ГБПОУ «Южно-Уральский Государственный Технический Колледж» на 2019-2020 г. представлены в таблице 2.

Таблица 2

Специальности ГБПОУ «Южно-Уральский Государственный Технический Колледж» на 2019-2020 г.

Наименование специальности, профессии	код профессии и специальности	Формаоб учения	Итого
ТО и ремонт двигателей, систем и агрегатов автомобилей	08.01.08	очная (9)	25
Монтаж, ТО и ремонт промышленного оборудования	23.01.17	Очная (9)	25
Информационные системы и программирование	23.01.03	очная (9)	25
Сетевое и системное администрирование	29.01.08	Очная (9)	25
Инфокоммуникационные сети и системы связи	35.01.11	Очная (9)	25
Сварочное производство	35.01.13	Очная (9)	75
Технология металлообрабатывающего производства	35.02.16	Очная (9)	25
Литейное производство черных и цветных металлов	35.01.23	Очная (9)	50
Монтаж и техническая эксплуатация промышленного оборудования	35.01.24	Очная (9)	25
Автоматизация технологических процессов и производств	43.01.09	Очная (9)	25
ТО и ремонт автомобильного транспорта	43.02.01	Очная (9)	25
Экономика и бухгалтерский учет	36.01.15	Очная (9)	25
Земельно-имущественные отношения	08.01.05	Очная (11)	25
Всего СПО			400
Садо-парковое и ландшафтное строительство	18103	ОВЗ	24
Итого			424

Информационная безопасность является одним из составных элементов комплексной безопасности техникума. Под информационной безопасностью техникума понимается состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита - процедуры и мероприятия, обеспечивающиезащитуинформации на правовой основе;

- организационная защита – это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

-инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

Информационная безопасность включает:

- защиту интеллектуальной собственности техникума;

- защиту компьютеров, локальных сетей и сети подключения к системе Интернета;

- организацию защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся;

- учет всех носителей конфиденциальной информации.

К объектам информационной безопасности техникума относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. и персональные данные;

- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, - хранение и передачу информации с ограниченным доступом.

Правовую основу Положения составляют:

- Конституция Российской Федерации;

- Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ;

- Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ;

- Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;

- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 26.07.2006 № 149-ФЗ;

- Федеральный закон «О персональных данных» от 27.07.06 № 152-ФЗ (в ред. от 27.07.2011) - ГОСТ Р ИСО/МЭК 17799-2005.

- Информационная технология. Практические правила управления информационной безопасностью (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст)

- другие законодательные акты, руководящие и нормативно-методические документы Российской Федерации в области обеспечения информационной безопасности.

Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в техникуме;

- предотвращение нарушений прав личности обучающихся, работников техникума на сохранение конфиденциальности информации;

- предотвращение несанкционированных действий по блокированию информации;

Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам техникума, нарушению нормального функционирования и развития техникума;

- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в [illegible] отношений;

- эффективное пресечение незаконных посягательств [illegible] ресурсы, технические средства и информационные

технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

- координация деятельности структурных подразделений техникумапо обеспечению защиты информации;

- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий

- развитие и совершенствование защищенного юридически значимого электронного документооборота.

- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности

- создание механизмов управления системой информационной безопасности (СИБ).

Система обеспечения информационной безопасности распространяются на:

- автоматизированные системы техникума;

- средства телекоммуникаций;

- помещения;

- сотрудников техникума.

Организационное и техническое обеспечение рабочего процесса возлагается на сотрудников отдела по безопасности.

Организационная структура отдела по безопасности представлена в виде следующей схемы (рисунок 4).

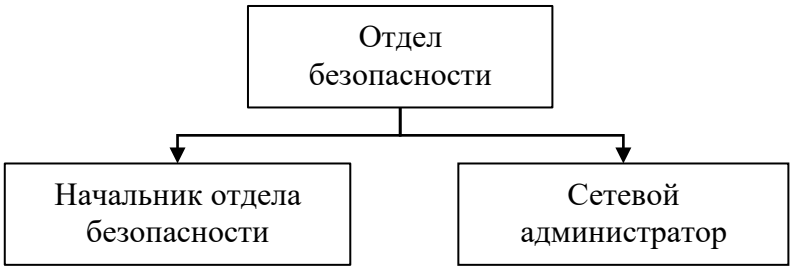

Рис. 4. Организационная структура отдела безопасности ГБПОУ «Южно-Уральский Государственный Технический Колледж»

Функции начальника отдела по безопасности:

- организует и руководит всей деятельностью по реализации Правил информационной безопасности;

- обеспечивает свободный и равный доступ обучающихся к Сетям в соответствии с учебной программой и возможностями техникума;

- организует и руководит всей деятельностью по реализации Правил информационной безопасности;

- обеспечивает свободный и равный доступ обучающихся к Сетям в соответствии с учебной программой и возможностями техникума;

- отвечает за организацию мер, включая сотрудничество с провайдером, по ограничению доступа обучающихся к ресурсам вредного или незаконного содержания в Сетях в соответствии с действующим законодательством;

- обеспечивает контроль за соблюдением правил работы обучающихся в сетях;

- организует поддержку и обновление сайта.

- размещает на сайте только материалы, утвержденные директором;

- незамедлительно сообщает директору о выявлении нарушений и принимает меры по устранению нарушений.

Функциями сетевого администратора являются:

- обеспечение общей безопасности и эффективности работы в Сетях;

- предлагать и осуществлять меры по ограничению доступа обучающихся к вредным или незаконного содержания ресурсам в Сетях в соответствии с законодательством;

- периодически просматривать содержимое Сети техникума с целью предотвращения любых возможных угроз и рисков безопасности для обучающихся;

- немедленно сообщать начальнику отдела по безопасности или директору о нарушении Правил или о создании незаконного контента в сети техникума.

С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику учреждения, допущенному к работе с конкретной подсистемой АС, составляется персональное уникальное имя - учетная запись пользователя и пароль, под которым он регистрируется, и работать в системе.

Правила работы сотрудников техникума и обучающихся в компьютерных сетях приведены в Приложении 1.

Для исполнения задач, связанных с производственной деятельностью сотрудникам техникума предоставляется доступ к ресурсам Интернет. Правила работы с ресурсами Интернет приведены в приложении 2.

Для служебного использования сотрудниками отдела по безопасности при настройке системы предназначены Локальные учетные записи компьютеров (Administrator, Guest).

2.2. Анализ информационных рисков образовательной организации

Деканат является важным структурным подразделением техникума, которое осуществляет координацию учебного процесса нескольких родственных кафедр и специальностей (факультет). В деканате ведется обработка и хранение данных, отражающих промежуточную успеваемость студентов, обучающихся на соответствующих кафедрах.

В деканате ГБПОУ «Южно-Уральский Государственный Технический Колледж» используется традиционная технологическая схема обработки, хранения, защиты и классификации документов (бумажный документооборот). При такой схеме используются в основном ручные методы работы с документами. Преобладающая часть документов представлена на бумажных носителях и только некоторые из них в процессе хранения дублируются в электронном виде. Перемещаются

только документы на бумажных носителях. При создании некоторых документов используются их шаблоны в электронном виде. Недостатки такой схемы заключаются в перегруженности персонала деканата во время сдачи зачетных и экзаменационных сессий, связанной с выпиской и фиксацией индивидуальных и групповых ведомостей, неэффективностью поиска и контроля документов. Отсюда длинные очереди, нервозность сотрудников деканата и студентов, что создает благоприятную обстановку для реализации различных угроз.

На рисунке 5 приведено категорирование информационных активов по видам тайны, из которого следует, что организация защиты (соблюдения требований ИБ) требуют три последних вида документов, содержащие персональные данные, служебную и коммерческую тайну.

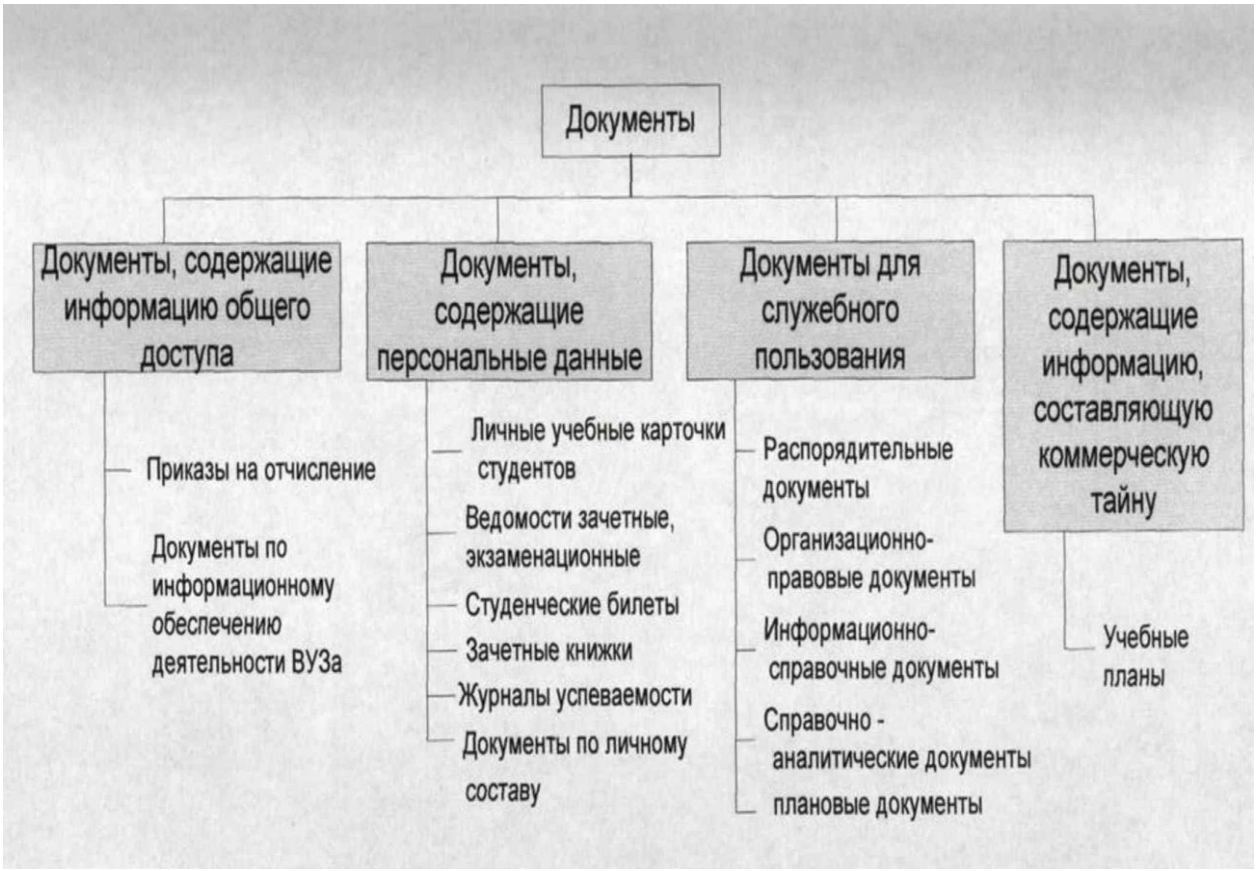

Рис. 5. Категорированние информационных активов деканата

В таблице 3 перечислены основные угрозы информационным активам деканата.

Таблица 3

Угрозы информационным активам деканата

Информационные активы	Угрозы
Ведомости	Кража, подделка, уничтожениеКража,
Журнал успеваемости	уничтожениеКража,
Зачетные книжки	уничтожение, ознакомлениеКража,
Студенческие билеты	подделка, уничтожение, ознакомление
Личные учебные карточки студентов	Подделка, уничтожение,
Учебные планы	ознакомлениеПодделка, ознакомление
Приказы	ПодделкаКража,
Организационно-распорядительная документация	подделка

На рисунке 6 представлена общая схема бумажного документооборота в виде информационных потоков, реализующих основные бизнес-процессы деканата. Так, индивидуальная экзаменационная ведомость создается студентом на бланке, выданном ему заместителем декана, далее заместитель декана подписывает ее и отдает студенты. Студент приходит на экзамен и отдает ее преподавателю, преподаватель заполняет ее и возвращает в деканат.

Источниками возможных угроз информации являются:

– компьютеризированные учебные аудитории, в которых происходит учебный процесс;

– Интернет;

– рабочие станции неквалифицированных в сфере ИБ работников техникума.

Анализ информационных рисков можно разделить на следующиеэтапы:

–классификация объектов, подлежащих защите, по важности;

–определение привлекательности объектов защиты для взломщиков;

–определение возможных угроз и вероятных каналов доступа

–оценка существующих мер безопасности;

–определение уязвимостей в обороне и способов их ликвидации;

–составление ранжированного списка угроз;

–оценка ущерба от НСД, атак в отказе обслуживании, сбоев в

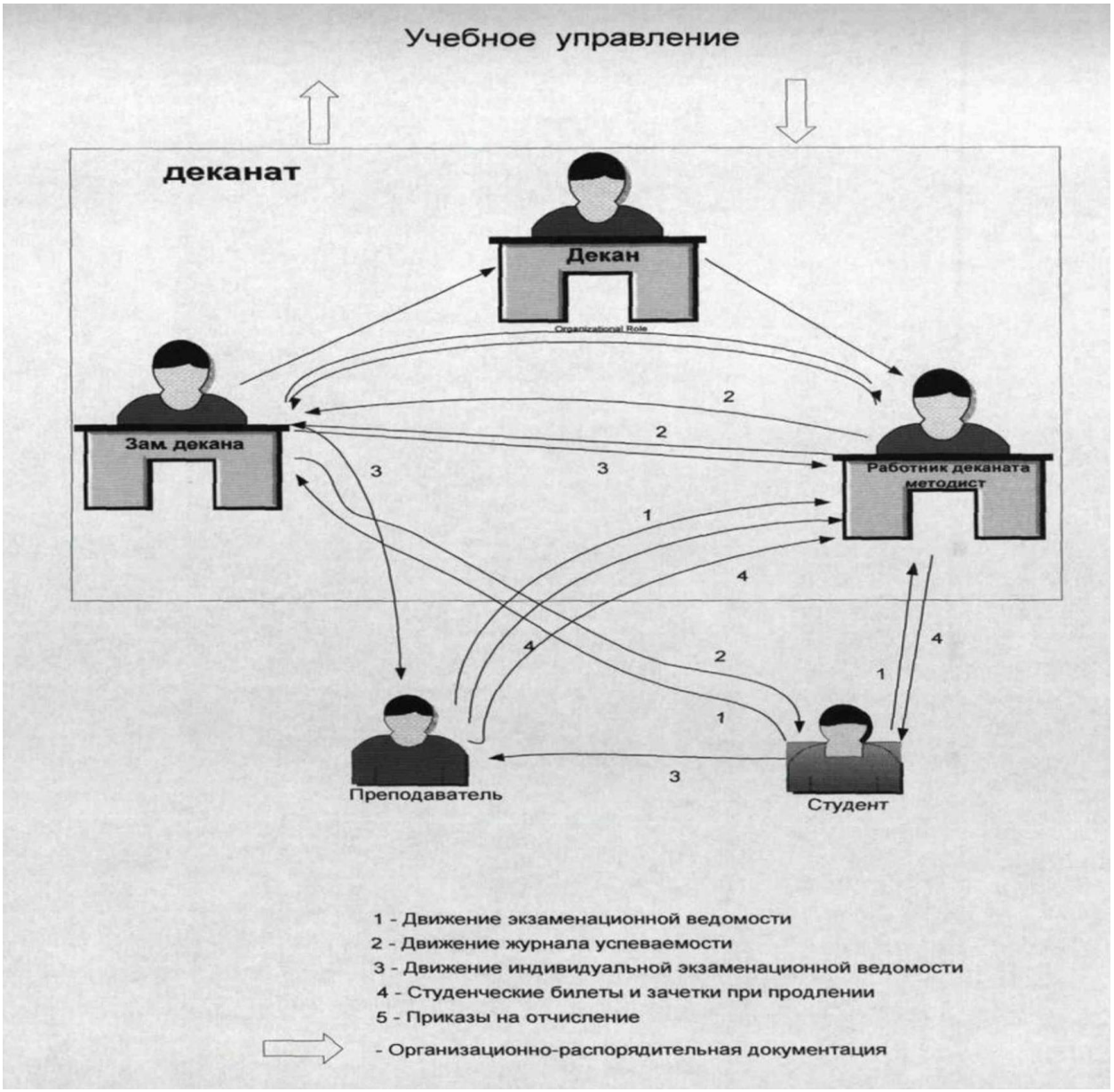

Рис. 6. Схема документооборота

Основные объекты, нуждающиеся в защите от НСД:

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

–серверы баз данных;

–консоль управления учетными записями;

–www/ftp сервера;

–ЛВС и серверы исследовательских проектов.

Специфика защиты информации в образовательной организации заключается в том, что техникум - публичное заведение с непостоянной аудиторией, а также место повышенной активности «начинающих кибер-преступников».

Анализ информационных рисков является предпосылкой для эффективного управления информационной безопасностью в ГБПОУ «Южно-Уральский Государственный Технический Колледж». Основную группу потенциальных нарушителей в техникума составляют студенты, некоторые из них имеют достаточно высокий уровень знания компьютеров, сетей. Возраст - от 18 до 23 лет - и юношеский максимализм побуждает таких людей блеснуть знаниями перед сокурсниками: устроить вирусную эпидемию, получить административный доступ и «наказать» преподавателя, заблокировав выход в Интернет. Студенты имеют доступ только в компьютерные учебные аудитории, от них и исходит внутренняя угроза. Модель злоумышленник в ГБПОУ «Южно-Уральский Государственный Технический Колледж» представлена в таблице 4.

Таблица 4

Модель злоумышленника в ГБПОУ «Южно-Уральский Государственный Технический Колледж»

Категория	Квалификация	Мотив	Ущерб
Студент	Имеет представление о том, как в деканате обрабатывается нужный ему документ. Знает механизм работы деканата. Пытается найти сообщника в лице преподавателя или работника деканата	Исправление оценки, подрыв репутации, месть	Выпуск неквалифицированного специалиста, подрыв репутации

Сотрудник деканата(м	Работает с документами, имеет досним, создает их. Может скрыть неправомерную деятельность	Получениеличной выгоды	Выпуск неквалифицированного специалиста

Продолжение таблицы 4

Категория	Квалификация	Мотив	Ущерб
Зам.декана	Несет ответственность за создание документов. Неправомер- ное действие никем не будет заме- чено	Личныепросьбы друзей, знакомых Получениеличной выгоды	Выпуск неквалифицированного специалиста, подрыв
Посетитель	О системе защиты и о деятельности деканата знает понаслышке. Ему ничего не угрожает в том случае, если его поймают на	Срыв работы системы	Пострадает репутация деканата
Хакер	Знает, как работает система, действует скрытно, обладает типовыми знаниями о методах построения вычислительных систем.		Простои в работе, нервирование сотрудников

Для снижения полученных рисков (возможных потерь) необходимо ввести управляющие факторы, соответствующие определенным организационным и техническим мероприятиям по защите информационных ресурсов деканата. Управляющие факторы на рисунке 7 изображены в виде защитного барьера, уменьшающего силу связи между соответствующими концепциями.

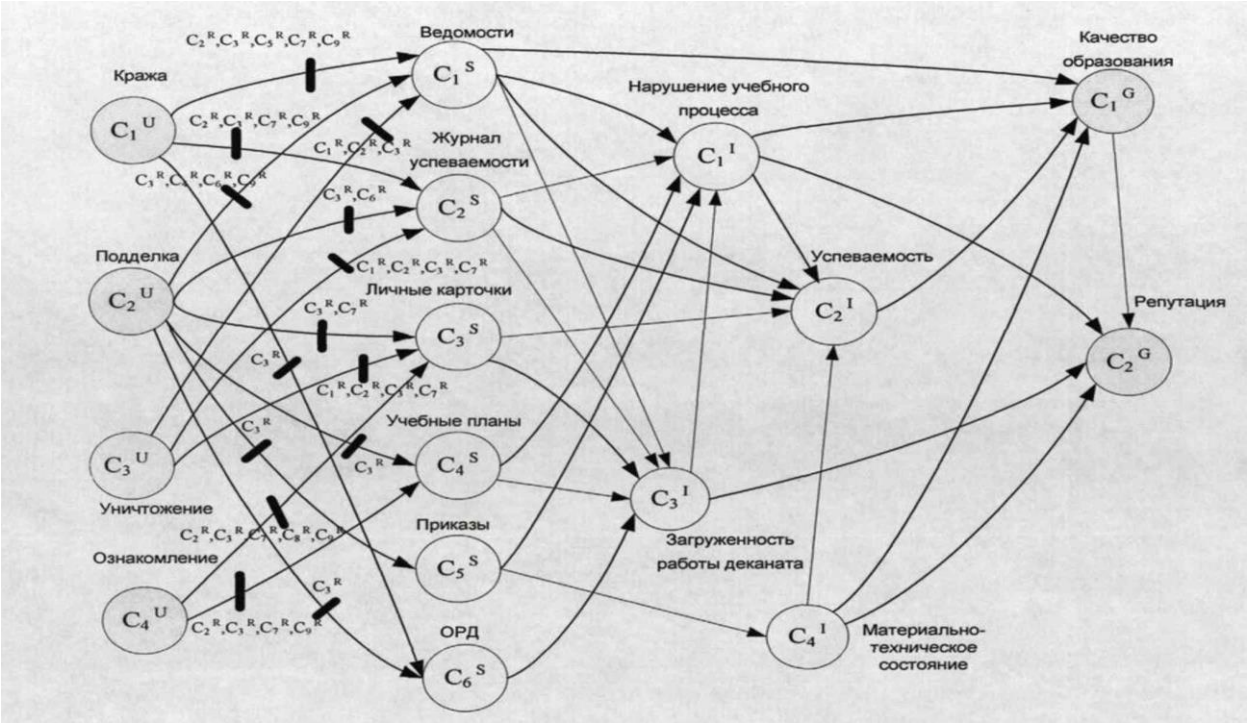

Рис. 7. Управляющие факторы для оценки рисков деканатаВозможный

перечень управляющих факторов приведен в таблице 5.

Таблица 5

Управляющие воздействия ГБПОУ «Южно-Уральский Государственный Технический Колледж»

Концепт	Наименование концептаC_1^R
C_2^R	Дублирование информации (резервное копирование) Регламентация хранения информационных ресурсов с соответствующим уровнем защиты
C_3^R	Разграничение доступа к информационным ресурсам. Определение прав доступа к информационным ресурсам
C_4^R	Разработка процедуры реагирования на инциденты
C_5^R	Регулярный инструктаж и обучение персонала
C_6^R	Внешний аудит делопроизводстваC_7^R
	Регламентация доступа в помещение

Разработанные контрмеры (управляющие воздействия) должны быть отражены на все уровнях политики информационной безопасности деканата (организационном, процедурном и техническом).

Проведенный анализ позывает, что при существующем бумажном документообороте для того, чтобы уменьшить уязвимость, необходимо уменьшить количество точек соприкосновения защищаемой информации с потенциальными злоумышленниками. Обеспечение этого возможно двумя способами. Первый из них вязан с введеним мер по ужесточению контроля за прохождением бумажного документооборота, в том числе мер по повышению личной ответственности преподавателей и работников деканата, что не всегда бывает эффективным, так как «любые защитные меры в силу ряда объективных причин со временем имеют тенденцию к ослаблению своей эффективности, в результате чего общий уровень ИБ может снижаться». Это касается в первую очередь человека и человеческих отношений. Второй способ - переход (полный или частичный) от бумажного документооборота к электронному, что более эффективно, так как, помимо повышения защищенности, позволяет также сократить время на обработку документации и уменьшить число работников деканата при сохранении высокого качества работы с документами.

2.3. Практические рекомендации по реализации нововведений управления службой информационной безопасности в образовательной организации

Для совершенствования управления информационной безопасности в ГБПОУ «Южно-Уральский Государственный Технический Колледж» предлагается методика анализа и управления информационными рисками техникума с использованием нечетких когнитивных карт (НКК).

Предложенный в работе метод анализа рисков, основанный на теории когнитивной модели информационных процессов, обеспечивающих различные аспекты деятельности техникума, позволит предложить рациональные механизмы управления этими процессами исходя из заданного уровня ИБ.

Специфика когнитивного моделирования предполагает описание поведения во времени для всех концептов, на которые оказывается влияние другими концептами. При формализации этого описания разделяют абсолютные уровни значений концептов, определяющих их состояния (уровни) и приращения (изменения этих уровней). В течение одного такта модельного времени состояния предполагаются неизменными.

Предлагаемая методика оценки рисков техникума, состоит из следующих основных шагов:

1. Определение целей и задачи моделирования. Анализ рисков производится исходя из непосредственных целей и задач, стоящих перед руководством техникума или службой, ответственной за безопасность информационных активов (ресурсов) техникума. Цель и задачи моделирования при анализе информационных рисков связаны с оценкой потенциального ущерба при нарушении основных свойств информационных активов техникума, таких как конфиденциальность, целостность, доступность информации, используемой при реализации бизнес-процессов.

2. Исходные данные о предметной области. Построение НКК предполагает когнитивный анализ информационных процессов в техникуме, влияющих на его ИБ. Для построения НКК задается список концептов, характеризующих состояние ИБ исследуемого объекта, определяются направления (знаки) влияния концептов друг на друга и силы этого влияния (веса связей). Исходными данными для решения этой задачи являются функциональные и информационные модели бизнес-процессов техникума и его подразделений, на основании которых осуществляются:

– идентификация информационных активов техникума, включая категорирование различных видов информации;

– определение потенциальных угроз этим активам;

– определение возможных видов ущерба.

Для оценки весов связей используются результаты анализа угроз, действующих на конкретный актив (концепт); уязвимостей, через которые эти угрозы могут быть реализованы, и модель злоумышленника (нарушителя) информационной системы объекта.

3.Построение нечеткой когнитивной модели. Составление списка факторов (концептов), определяющих ИБ исследуемого объекта и отношения причинности (причинно-следственные связи) между каждой парой концептов, производится путем опроса и обработки мнений экспертов, на основе чего строится искомая нечеткая когнитивная карта.

4.Анализ рисков. На основе построенной НКК формируется когнитивная матрица смежности (весов связей) концептов.

На рисунке 4.2 (Приложение 3) приведена классификация мероприятий по защите информационной системы техникума.

5. Управление рисками. К числу таких мероприятий относятся контрмеры:

- на уровне поддерживающей инфраструктуры;
- на организационном уровне;
- на кадровом уровне;
- на уровне программного обеспечения и вычислительной техники;
- на уровне инфотелекоммуникаций;
- на уровне обеспечения непрерывности бизнеса.

Построение НКК позволит ввести эффективное управление информационной безопасностью техникума. Так, оценивая степень влия- ния вводимых управляющих воздействий на целевые факторы, можно выбрать наиболее подходящие контрмеры в зависимости от постановки задачи снижения информационных рисков.

На основании проведенного анализа основных бизнес-процессов, угроз, информационных активов, рисков деканата был выбран список концептов НКК и их переменных состояния. Построенная НКК для оценки информационных рисков показана на рисунке 8.

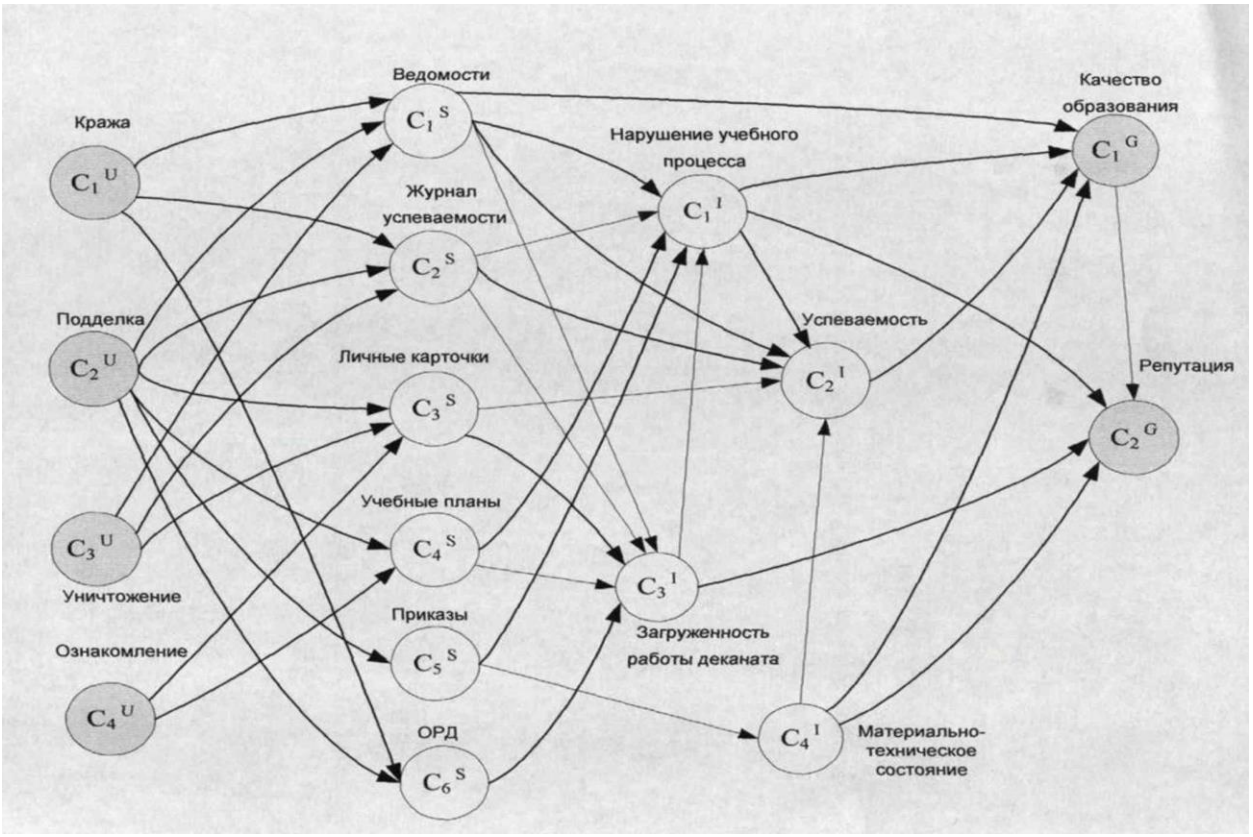

Рис.8. Нечеткая когнитивная карта для оценки рисков деканата

В таблице 6 приведен перечень указанных концептов и их переменных состояния.

Таблица 6

Перечень концептов НКК и их переменных состояния

№ п/п	Концепт	Вид концепта	Наименование концепта	Переменная состояния концента
1.	C_1^U	Дестабилизирующий фактор	Кража	Число краж документов / ед. времени
2.	C_2^U	Дестабилизирующий фактор	Подделка	Число подделанных документов / ед. времени
3.	C_3^U	Дестабилизирующий фактор	Уничтожение	Число уничтоженных документов / ед. времени
4.	C_4^U	Дестабилизирующий фактор	Ознакомление	Число нарушений конфиденциальности / ед. времени
5.	C_1^S	Информационный актив	Ведомости	Количество обработанных ведомостей / ед. времени
6.	C_2^S	Информационный актив	Журналы успеваемости	Количество журналов успеваемости, ед.
7.	C_3^S	Информационный актив	Личные учебные карточки	Количество студентов на факультете, ед.

8.	C_4^S	Информационный актив	Учебные планы	Количество учебных планов, созданных или претерпевших изменение / ед. времени
9.	C_5^S	Информационный актив	Приказы	Количество созданных приказов на отчисление / ед. времени
10.	C_6^S	Информационный актив	Организационно-распорядительн	Количество ОРД, прошедших через деканат / ед. времени
11.	C_1^I	Базисный фактор	Нарушения учебного	Количество срывов занятий за год
12.	C_2^I	Базисный фактор	Успеваемость	Средний балл успеваемости, в 5-ти балльной системеКоличество
13.	C_3^I	Базисный фактор	Загруженность деканатаМате	обходящихдокументов /ед. времени Денежные средства, руб.
14.	C_4^I	Базисный фактор	риально-техническоесо стояниеКачест	Число выпускников,
15.	C_1^G	Целевой фактор	во образования	работающих по специальности, в% Количество абитуриентов (кон-
16.	C_2^G	Целевой фактор	Репутация	курс) при поступлении, ед. / ме-сто

Для средств антивирусной защиты в ГБПОУ «Южно-Уральский Государственный Технический Колледж» предлагается внедрить следующие инструментальные средства (пакеты программ), позволяющие автоматизировать процессы построения НКК, анализа и управления рисками:

CognitiveRiskAnalizer - программа для расчета и анализа информационных рисков с применением нечетких когнитивных технологий;

RiskManagement - программа управления информационными рисками;

Fuzzy Cognitive Maps Builder — универсальное решение для автоматизации анализа и управления рисками с использованием нечетких когнитивных карт.

В таблице 7 приведен пример выбора средств антивирусной защиты (АВЗ), межсетевых экранов (МЭ) и средств резервного копирования с учетом их влияния на целевой фактор «Материально-техническоесостояние».

Таблица 7

Выбор средств антивирусной защиты

Контрмеры	Решения	Стомость, руб.	Влияние на НКК	Эффективность
Внедрение	KAV Work Space Security	8732	сильно	22,9
	Dr.Web for Workstation	990	среднесред	8,9
	Norton Internet Security 2008	1 735.41	не	5,1
Внедрение	KAV Work Space Security	8732	сильно	22,9
	VipNet 3.1 Personal Firewall	472	средне	18,8
	Norton Internet Security 2008	1 735.41	средне	5Д
Резервное	Norton Ghost 14	1 369.80	средне	6,5
	Acronis True Image 9.1 Workstation	2255	сильно	88,5
	Системные средства резервного копирования	-	средне	0

Таким образом, расчет эффективности введения тех или иных управляющих воздействий (в данном случае выбора средств антивирусной защиты) показывает, что лучшее решение снижения степени влияния вирусов на концепт «Материально-техническое состояние» дает выбор KAV Work Space Security и Acronis True Image 9Л Workstation.

Для управления информационными рисками необходимо задать управляющие факторы, их стоимость и базу правил для них. Программа вводит в НКК управляющие факторы в виде барьеров и после пересчета «Полный эффект» и «Общий риск», и строится вторая диаграмма оценки информационных рисков «После внедрения контрмер», позволяющая визуально сравнить информационные риски до внедрения и после внедрения контрмер.

Внедрение данных программ позволит быстро и наглядно построить НКК, произвести расчеты по оценке и переоценке рисков, выявить наибольшие риски в исследуемой информационной системе, в наглядной форме представить эффективность внедренных мероприятий. Программы

могут работать как в комплексе, так и отдельно, в зависимости от решаемых задач.

Разработанная методика анализа и управления информационной безопасностью техникума с использованием нечетких когнитивных карт позволит:

– оценить текущее состояние ИБ техникума и достаточность организационных, процедурных и технических средств защиты по заданию допустимого уровня рисков;

– выявить наиболее опасные угрозы и уязвимости, влияющие на информационную (бизнес-процессы) систему техникума;

– оценить возможный ущерб от действия угроз на его информационную систему;

– дать экономическую оценку необходимых затрат на организацию мероприятий по обеспечению ИБ техникума, обосновать перед руководством размер необходимых вложений;

– быстро адаптироваться к новым внешним и внутренним угрозам и информационным технологиям;

– дать эффективный и простой механизм принятия решений для службы, занимающейся обеспечением ИБ техникума.

Как уже отмечалось, обеспечение ИБ, основанное на методологии анализа и управления ИБ с использованием НКК, состоит из процедур оценки риска и выбора комплекса мер по достижению приемлемого (заданного) уровня. Управление рисками позволяет найти разумный баланс между стоимостью средств/мер защиты и требованиями непрерывности бизнеса.

Структура перспективной системы поддержки принятия решений (СППР) по обеспечению безопасности информационной системы техникума (рисунок 9) состоит их трех основных подсистем: информационной базы СППР, блока моделирования и анализа рисков и блока управления рисками.

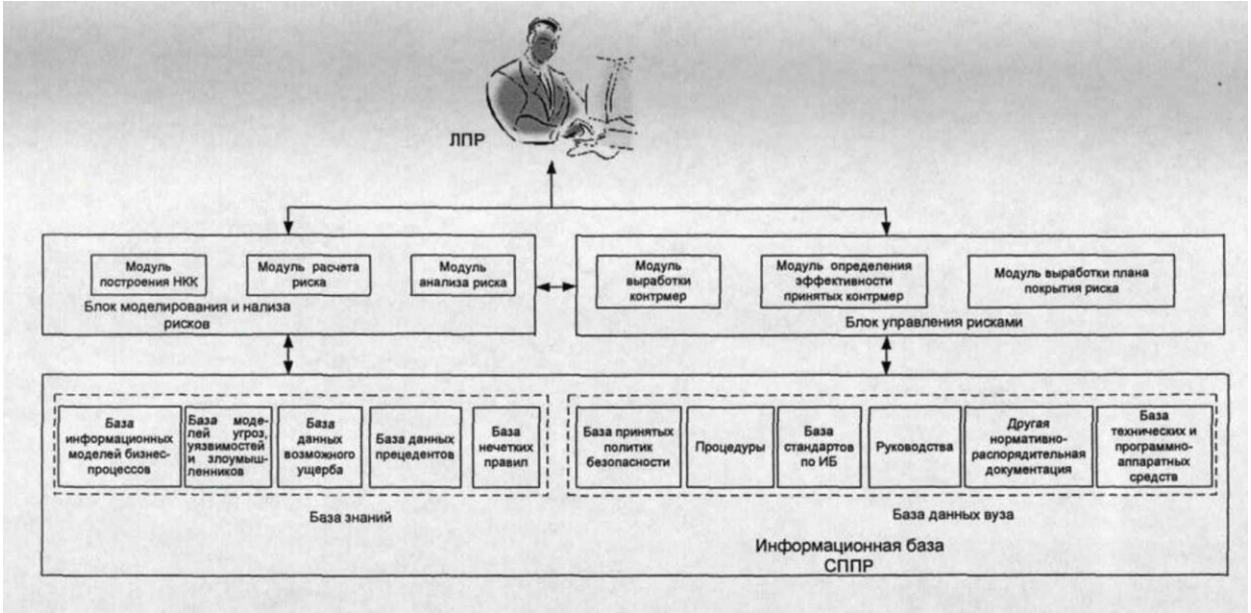

Рис.9. Структура СППР по анализу и управлению рисками

Информационная база СППР состоит из базы данных и базы знаний. В базу данных техникума будут входить:

– типовые требования к ИБ и база принятых политик безопасности;

– база стандартов в области ИБ;

– база правил и процедур ИБ (реагирование на инциденты, резервное копирование, предоставление доступа, оформление новых сотрудников и т.д.)

– инструкции и руководства (инструкции пользователям, по антивирусной защите, по работе в сети Интернет, по защищенному удаленному доступу, по резервному копированию, по действиям в чрезвычайных ситуациях и т.д.)

– база данных (характеристик) существующих технических механизмов и программно-аппаратных средств защиты;

– нормативно-распорядительные документы в области ИБ. База знаний должна содержать:

– базу информационных потоков основных бизнес-процессов техникума;

– базу моделей угроз, уязвимостей и злоумышленников;

– базу данных возможного ущерба от действий злоумышленников;

– базу описания всех прецедентов нарушения ИБ техникума;

– базу нечетких правил принятия решений в условиях действия угроз.

База знаний обеспечивает информационную поддержку экспертам на всех этапах построения и анализа нечеткой когнитивной карты.

Блок моделирования и анализа рисков включает в себя следующие подсистемы:

– модуль построения НКК;

– модуль расчета риска;

– модуль анализа риска.

Модуль построения НКК непосредственно выполняет функцию построения нечеткой когнитивной карты на основе данных представленными экспертами.

Затем модуль расчета риска дает оценку зависимостей всех исследуемых факторов от угроз ИБ и в модуль анализа рисков представляет в графическом и табличном виде оценку риска.

Блок управления рисками представляет собой подсистему принятия решений по выработке мероприятий, связанных с управлением рисками и состоит из следующих модулей:

– модуль выработки контрмер;

– модуль определения эффективности выбранных контрмер;

– модуль выработки плана покрытия риска.

Модуль выработки контрмер генерирует список необходимых мероприятий по управлению рисками, которые вводятся в когнитивную карту в виде барьеров, снижающих силу влияния между концептами. Затем модуль определения эффективности принятых контрмер оценивает допустимый уровень риска по критерию «стоимость-эффективность», на основании чего формируется план управления рисками для всех уровней политики безопасности техникума.

В качестве блока моделирования и анализа рисков используется ПО CognitiveRiskAnalizer и FCM Builder, в качестве блока управления рисками - ПО RiskManagement и FCM Builder.

Отчет о результатах оценки риска и необходимых мероприятий по управлению рисками дает возможность лицу, отвечающему за безопасность техникума в нашем случае это будет начальник службы безопасности принимать обоснованные решения по изменению политики, процедур и регуляторов безопасности.

В заключение рассмотрим распределение обязанностей по поддержанию ИБ техникума.

Управление рисками рассматривается на административном уровне ИБ.

Руководитель организации (ректор) несет ответственность за выполнение миссии, возложенной на ГБПОУ «Южно-Уральский Государственный Технический Колледж», и обеспечивает выделение ресурсов, необходимых для выполнения этой миссии на основе результатов оценки рисков.

Разработкой и реализацией эффективной программы управления рисками будет заниматься руководитель службы безопасности.

В функции сотрудников службы безопасности будут входить также сбор данных о расходах на поддержание ИБ и статистика прецедентов по нарушению ИБ техникума.

В соответствии с организационной структурой техникума, руководители структурных подразделений несут ответственность за бесперебойное функционирование своих информационных систем и за применение и эксплуатацию соответствующих средств защиты (регуляторов безопасности) и назначают в своем подразделении администраторабезопасности, который тесно взаимодействует со службой ИБ ГБПОУ
«Южно-Уральский Государственный Технический Колледж».

Системный администратор будет отвечать за эксплуатацию регуляторов безопасности подведомственной им сети.

Служба ИБ техникума должна будет обеспечить обучение сотрудников организации и пользователей информационных систем вопросам информационной безопасности в соответствии с политикой безопасности техникума. Процесс оценки и управления информационными рисками будет проводиться во всех структурных подразделениях и на всех этапах эксплуатации информационной системы для выявления новых потенциальных угроз и принятия соответствующих контрмер.

Прямые затраты труда на установку программного обеспечения составляют 34 дня, с учетом обновления программного обеспечения у всех пользователей затраты труда составят 63 дня. Значение коэффициента, учитывающего уровень сложности программного обеспечения, в зависимости от дополнительных характеристик составляет 1,34.

Общая трудоемкость разработки программного обеспечения с учетом коэффициента сложности составляет:

То=63*1,34=84,4 чел-дни.

Для выполнения работ по доработке программного обеспечения потребуется 4 человека

Стоимость трудозатрат составит: Зт=84,4*4*128,9*1,3=56 571 рубль.

Стоимость KAV Work Space Security и Acronis True Image 9Л Workstation составляет 120 000 рублей.

Кроме того, необходимо провести обучение сотрудников по использованию дополнительного функционала программного обеспечения.

Расчет стоимости обучения производится по формуле (1):

$$Зо=С*К*Ц*Ксв, \quad (1)$$

где С – срок обучения, час;

К – количество обучаемых, чел;

Ц – оплата труда за обучение, руб.

Зо= 8*218*130*1,3=294 736 руб.

Кроме определенных затрат потребуется обновление инструкций пользователя программы, которые составляются как в печатном, так и в электронном виде. На разработку инструкции потребуется 20 часов, что в стоимостном эквиваленте составит 3 380 рублей.

Расходы на печать инструкций составят:

Рп = 50шт*10л*2,5 руб = 1 250 руб.

Расчет экономического эффекта представлен в таблице 8.

Таблица 8

Расчет экономического эффекта по установке нового программного обеспечения

Показатель	Значение, руб.
Расходы всего	439 937
В том числе	
Стоимость модуля	84 000
Трудозатраты	56 571
Обучение	294 736
Разработка инструкции	3 380
Печать инструкции	1 250
Экономия стоимости трудозатрат	1 742 510
Экономический эффект	1 302 573

Таким образов в результате внедрения KAV Work Space Security и Acronis True Image 9Л Workstation в ГБПОУ «Южно-Уральский Государственный Технический Колледж» будет получен эффект в сумме 1 302,6 тыс. руб. Теперь рассчитаем срок окупаемости затрат на внедрениепроекта (Ток) по формуле (5):

$$Ток = КП / П, \quad (2)$$

где КП - затраты на реализацию проекта,

П – прибыль по проекту, в нашем случае это экономия по ФОТ.

Ток = 439,9/ 1742,5 = 0,25 года

Таким образом, окупаемость затрат на реализацию проекта составит 0,25 года.

Таким, образом, результаты расчета показывают, что при условиях внедрения программного обеспечения KAV Work Space Security и Acronis True Image 9Л Workstation и его доработке в ГБПОУ «Южно-Уральский Государственный Технический Колледж» снижаются не только трудозатраты с 2596 человеко-часа в месяц, но и стоимостные на 1742,5 тыс.руб./год.

Итак, реализация проекта является экономически целесообразной.

Вывод по второй главе

Предложен подход к оценке защищенности информационных активов техникума, основанный на построении нечеткой когнитивной карты, которая позволяет в наглядной форме представить влияние угроз на жизненные процессы техникума и оценить степень влияния этих угроз на факторы, определяющие состояние техникума на рынкеобразовательных услуг.

Разработан список концептов, определяющих состояние информационной безопасности техникума, необходимый для построения нечеткой когнитивной карты.

Предложен алгоритм анализа нечеткой когнитивной карты для оценки информационных рисков техникума, который позволяет выявить состояние информационной безопасности техникума, определить факторы, влияющие в наибольшей степени на ИБ техникума и выработать рекомендации по снижению и управлению рисками техникума.

Приведены примеры построения нечеткой когнитивной карты для оценки рисков техникума и отдельных его структурных подразделений. Проведена оценка степени влияния угроз на заданные целевые факторы с последующими рекомендациями по снижению этого влияния. Показано, что введение электронного документооборота (на примере деканата) позволяет снизить уязвимость информационной системы за счет исключения «человеческого фактора» и уменьшения точек соприкосновения защищаемой информации с потенциальными злоумышленниками.

ЗАКЛЮЧЕНИЕ

Проблема обеспечения информационной безопасности ИОС характеризуется острой необходимостью и неотложностью.

Социально-педагогическое решение проблемы информационной безопасности состоит, в обязательном включении в деятельность педагогических и управленческих кадров такого компонента профессиональной подготовки как компетентность в области информационной безопасности. Педагогическое воздействие должно быть направлено не только на привитие знаний, умений и навыков работы с информацией, но также на формирование опыта деятельности по защите от негативной информации в профессиональной и управленческой деятельности.

По результатам анализа информационной безопасности можно сделать вывод, что в настоящее время в российской образовательной системе отсутствует комплексный подход к формированию системы информационной безопасности. Отдельные организационно-педагогические мероприятия и действия, ориентированные на обеспечение информационной безопасности личности, можно рассматривать только как предпосылки к разработке и принятию педагогическим сообществом болееширокого комплекса мер.

ГБПОУ «Южно-Уральский Государственный Технический Колледж» – это динамично развивающееся образовательное учреждение с постоянно обновляющейся материально-технической базой, с учебным хозяйством, на полях которого ведутся сельскохозяйственные работы.

Система обеспечения информационной безопасности распространяются на:

- автоматизированные системы техникума;
- средства телекоммуникаций;
- помещения;

- сотрудников техникума.

Организационное и техническое обеспечение рабочего процесса возлагается на сотрудников отдела по безопасности.

Источниками возможных угроз информации являются:

– компьютеризированные учебные аудитории, в которых происходит учебный процесс;

– Интернет;

– рабочие станции неквалифицированных в сфере ИБ работников техникума.

Основные объекты, нуждающиеся в защите от НСД:

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

–серверы баз данных;

–консоль управления учетными записями;

–www/ftp сервера;

–ЛВС и серверы исследовательских проектов.

В деканате ГБПОУ «Южно-Уральский Государственный Технический Колледж» используется традиционная технологическая схема обработки, хранения, защиты и классификации документов (бумажный документооборот). При такой схеме используются в основном ручные методы работы с документами. Отсюда длинные очереди, нервозность сотрудников деканата и студентов, что создает благоприятную обстановку для реализации различных угроз.

При существующем бумажном документообороте для того, чтобы уменьшить уязвимость, необходимо уменьшить количество точек соприкосновения защищаемой информации с потенциальными злоумышленниками. Обеспечение этого возможно двумя способами. Первый из них вязан с введеним мер по ужесточению контроля доступа в систему бумажного документооборота, в том числе мер по повышению личной ответственности преподавателей и работников

деканата, что не всегда бывает эффективным, так как «любые защитные меры в силу ряда объективных причин со временем имеют тенденцию к ослаблению своей эффективности, в результате чего общий уровень ИБ может снижаться». Это касается в первую очередь человека и человеческих отношений. Второй способ - переход (полный или частичный) от бумажного документооборота к электронному, что более эффективно, так как, помимо повышения защищенности, позволяет также сократить время на обработку документации и уменьшить число работников деканата при сохранении высокого качества работы с документами.

Для совершенствования управления информационной безопасности в ГБПОУ «Южно-Уральский Государственный Технический Колледж» предлагается методика анализа и управления информационными рисками колледжа с использованием нечетких когнитивных карт (НКК).

Для средств антивирусной защиты в ГБПОУ «Южно-Уральский Государственный Технический Колледж» предлагается внедрить следующие инструментальные средства (пакеты программ), позволяющие автоматизировать процессы построения НКК, анализа и управления рисками: KAV Work Space Security и Acronis True Image 9Л Workstation.

Внедрение данных программ позволит быстро и наглядно построить НКК, произвести расчеты по оценке и переоценке рисков, выявить наибольшие риски в исследуемой информационной системе, в наглядной форме представить эффективность внедренных мероприятий.

Был разработан список концептов, определяющих состояние информационной безопасности колледжа, необходимый для построения нечеткой когнитивной карты.

Далее, был предложен алгоритм анализа нечеткой когнитивной карты для оценки информационных рисков колледжа, который позволяет выявить состояние информационной безопасности колледжа, определить факторы, влияющие в наибольшей степени на ИБ колледжа и выработаны рекомендации по снижению и управлению рисками колледжа.

Приведены примеры построения нечеткой когнитивной карты для оценки рисков колледжа и отдельных его структурных подразделений. Проведена оценка степени влияния угроз на заданные целевые факторы с последующими рекомендациями по снижению этого влияния. Показано, что введение электронного документооборота (на примере деканата) позволяет снизить уязвимость информационной системы за счет исключения «человеческого фактора» и уменьшения точек соприкосновения защищаемой информации с потенциальными злоумышленниками.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992г //СПС Консультант Плюс.

2. Андреев А.А. Некоторые проблемы педагогики в современных информационно-образовательных средах // Инновации в образовании., 2014. No6. С. 98 – 113.

3. Андреев Л.Ю. Законодательное и нормативно-правовое обеспечение функционирования закона «О защите детей от информации, причиняющей вред их здоровью и развитию» в сети Интернет // Молодой ученый. — 2016. — №6.1. — С. 4-7.

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утв. Федеральной службой по техническому и экспортному контролю 15 февраля 2008г //СПС Консультант Плюс.

5. Баймакова, И.А. Обеспечение защиты персональных данных. Методическое пособие / И.А. Баймакова, А.В. Новиков, А.И. Рогачев – М.:1С-Паблишинг, 2014. – 214 с.

6. Белкин, П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учеб. пособие для колледжов/ П.Ю. Белкин, О.О. Михальский, А.С. Першаков. – М.: Радио связь, 2015.- 215 с

7. Белов, Е.Б. Основы информационной безопасности [Текст]. Учебное пособие для вузов / Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2016. – 544 с.

8. Вараменко, Я.А. Информатизация образования: итоги и направления дальнейшей работы // Педагогическая информатика. 2017. - №1. -С. 41 -51.

9. Галатенко В.А. Стандарты информационной безопасности: курс лекций: учебное пособие/В.А. Глатенко.- ИНТУИТ, 2016.-264 с.

10. Гафнер В.В. Информационная безопасность: учебное пособие / В.В. Гафнер://: ГОУ ВПО «Уральский государственный педагогический университет. - Екатеринбург, 2009. — Режим доступа: http://www.iprbookshop.ru/9715.— ЭБС «IPRbooks», по паролю

11. Гнатышина, Е.А. Инновационные процессы в образовании: коллективная монография / Е.А. Гнатышина, Д.Н. Корнеев, Н.Ю. Корнеева и др.- Челябинск: Цицеро, 2016. – 210с.

12. Гнатышина, Е.А. Компетентностно ориентированное управление подготовкой педагогов профессионального обучения : монография / Е.А. Гнатышина; ГОУ ВПО «ЧГПУ» - Челябинск.: «ЧГПУ», 2008. – 410с.

13. Гнатышина, Е.А. Магистерская диссертация: рекомендации по подготовке и защите: учебно-методическое пособие/ Е.А. Гнатышина, В.А, Белевитин, И.Г. Черновол.- Челябинск: ЧГПУ, 2016. – 158с.

14. Гнатышина, Е.А. Научно-исследовательская работа магистранта: теория и практика организации и проведения: учебно-методическое пособие: / Е.А. Гнатышина, В.А, Белевитин, И.Г. Черновол.- Челябинск: ЮУрГГПУ, 2017. – 128с.

15. ГОСТ 12.0.003-74 ССБТ. Опасные и вредные производственные факторы. Классификация [Электронный ресурс]. – Введ. 1976–01–01. //СПС Консультант Плюс.

16. ГОСТ 7.1-2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления [Электронный ресурс]. – Введ. 2004–07–01. //СПС Консультант Плюс.

17. ГОСТ 7.32-2001. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления [Электронный ресурс]. – Введ. 2002–07–01. //СПС Консультант Плюс.

18. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. – Введ. 2006–12–27. //СПС Консультант Плюс.

19. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения[Электронный ресурс]. – Введ. 2000–06–30. //СПС Консультант Плюс.

20. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс]. – Введ. 2007–01–01. //СПС Консультант Плюс.

21. Гражданский кодекс Российской Федерации [Электронный ресурс]: офиц. текст. – М. : Экзамен, 2001. – 304 с.

22. Григорьев, С.Г. Информатизация образования. Фундаментальные основы. / С.Г. Григорьев, В.В. Гриншкун. - Москва, 2013.- 231 с.

23. Джонс К.Д., Шема М., Джонсон Б.С., Инструментальные средства обеспечения безопасности/К.Д. Джонс, М. Шема, Б.С. Джонсон.- ИНТУИТ, 2017.-1028 с.

24. Ермолаева, О.Я. Международный опыт обеспечения информационной безопасности детей / О. Я. Ермолаева // Безопасность детей в информационном пространстве. – М.: Российская гос. детская б-ка, 2014. - С. 25-33.

25. Есипова А. А., Ребко Э. М. Основные структурные компоненты культуры безопасности жизнедеятельности // Молодой ученый. — 2014. — №18.1. — С. 36-38.

26. Есипова А. А., Степанова И. А. Использование мультимедийных средств обучения в практике преподавания курса «Основы безопасности жизнедеятельности» // Молодой ученый. — 2016. — №6.1. — С. 48-51.

27. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт [Электронный ресурс]: монография/ Ефимова Л.Л., Кочерга С.А.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.—

239 с.— Режим доступа: http://www.iprbookshop.ru/52672.— ЭБС «IPRbooks», по паролю.

28. Жарникова Ю. С. Угрозы информационной безопасности образовательного учреждения // Молодой ученый. — 2017. — №11.2. — С. 60-63. — URL https://moluch.ru/archive/145/40613/ (дата обращения: 19.02.2019).

29. Завьялова, Н.Б. Методология разработки интегрированной информационной образовательной среды / Н.Б. Завьялова, Л.П. Дьяконова // Материалы: XI конференция-выставка «Информационные технологии в образовании». – М.: МИФИ, 2011. – 200 с.

30. Зайцев А.П. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 616 с.— Режим доступа: http://www.iprbookshop.ru/12054.— ЭБС «IPRbooks», по паролю.

31. Зайцев А.П. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 616 с.— Режим доступа: http://www.iprbookshop.ru/12054.— ЭБС «IPRbooks», по паролю.

32. Зайцева, Ж.Н. Генезис виртуальной образовательной среды на основе интенсификации информационных процессов современного общества / Ж.Н. Зайцева, В.И. Солдаткин // Информационные технологии, №3, 2010. - С. 44-50.

33. Захарова, И.Г. Информационные технологии в образовании: учеб.пособие для студ. высш. пед. учеб. Заведений / И.Г. Захарова. – М: ИЦ «Академия», 2013. -192 с.

34. Захарова, И.Г. Формирование информационной образовательной среды высшего учебного заведения // Автореферат дис. ... доктора пед. наук. Тюмень, 2013. - 46 с.

35. Защита от несанкционированного доступа к информации. Термины и определения [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г //СПС Консультант Плюс.

36. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей [Электронный ресурс]: утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г. N114 //СПС Консультант Плюс.

37. Информационные и коммуникационные технологии в образовании: учебное пособие / И.В. Роберт, С.В. Панюкова, А.А. Кузнецов, А.Ю. Кравцова. – М.: Дрофа, 2011. – 320 с.

38. Информационные технологии для новой школы// материалы конференции, т.3 – СПб.: ГБОУ ДПО ЦПКС СПб «Региональный центр оценки качества образования и информационных технологий», 2013. – 199 с.

39. К вопросу проектирования онтологий предметной области при подготовке магистров по направлению информационная безопасность [Текст] / Е.А. Гафарова, Ф.В. Синицын // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы : сборник научных трудов. — Челябинск: Челябинский филиал РАНХиГС, 2016. — С. 56–59. — 200 с.

40. Комментарий к Кодексу Российской Федерации об административных правонарушениях" (постатейный):[Электронный ресурс]/ под ред. Н.Г. Салищевой; 6-е издание, переработанное и дополненное – Проспект, 2009 // СПС Консультант Плюс.

41. Концепция долгосрочного социально-экономического развития РФ на период до 2020г., утв. Распоряжением Правительства РФ от 17.11.2008 N 1662-р (ред. от 10.02.2017) Режим доступа: // СПС Консультант Плюс.

42. Концепция создания и развития информационно-образовательной среды Открытого Образования системы образования РФ [электронный ресурс] / Концепции информационно-образовательной среды. — Саратов, 2012. – URL: http://do.sgu.ru/conc.html. (дата обращения 27.02.12)

43. Концепция электронных изданий и ресурсов / РМЦ; Руководитель А.В.Осин – М., 2012. Режим доступа: http://eir.ru/concept.php

44. Копылов В.А. Информационное право Российской Федерации М.:Инфра-М, 2016 – 400с. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации.-М.: Изд.дом «Академия»2006.-256 с.

45. Красильникова, В.А. Информатизация образования: понятийный аппарат / В.А. Красильникова // Информатика и образования, № 4, 2013. - С. 21 – 27.

46. Красильникова, В.А. Электронные компоненты информационно-образовательной среды/ В.А. Красильникова, П.В. Веденеев, А.С. Заварихин, Т.Н. Казарина // Открытое и дистанционное образование. Выпуск 4(8), 2012. С. 54 – 56

47. Крысин, Л.П. Толковый словарь иноязычных слов / Л.П. Крысин. – М.:Инфокнига, 2012.-564с.

48. Курова, Н.Н. Информационная среда образовательного учреждения как управленческий ресурс современного руководителя школы [электронный ресурс] / Н.Н. Курова // Конференция «Информационные технологии в образовании».– М., 2012. –URL: http://www.ito.su/main.php?pid=26&fid=5434&PHPSESSID=00a0f682fb916586aca80c70e80f2ab0. .(дата обращения 27.02.12)

49. Лобачев, С.Л. Региональная информационно-образовательная среда - основа федеральной среды системы открытого образования // Телематика-2011. -СПб.: СПб ГТУ, 2011- 98с..

50. Лобачев, С.Л. Универсальная инструментальная информационно-образовательная среда системы открытого образования Российской Федерации / С.Л. Лобачев, А.А. Поляков. М.: ИЦПКПС, 2011. - 40 с.

51. Лодатко, Е.А. Моделирование педагогических систем и процессов [Текст] : монография / Е. А. Лодатко. — Славянск : СГПУ, 2010. — 148 с.

52. Лучинкина, А.И. Информационно-психологическая безопасность детей и подростков в интернет-пространстве. [Электронный ресурс] / А.И. Лучинки на, Т.В. Юдеева. — Электрон. дан. // Ученые записки Крымского инженерно педагогического университета. Серия: Педагогика. Психология. — 2015. — № 1. — С. 19-24. — Режим доступа: http://e.lanbook.com/journal/issue/297694 — по паролю (Дата обращения: 16.12.2016).

53. Майорова-Щеглова, С.Н. Социологические концепты детства и проблемы информационной безопасности детей / С. Н. Майорова-Щеглова // Без опасность детей в информационном пространстве. - Москва : Российская гос. детская б-ка, 2014. - С. 43-49. 21. Методические рекомендации по проведению образовательными организациями самообследования на предмет наличия комплекса мер, защиты детей от информации, причиняющей вред здоровью и развитию детей. – КГБУО «Алтайский краевой информационно-аналитический центр». – Барнаул, 2016 г.- 7 л.

54. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]. Учеб. пособие для вузов / А.А. Малюк. – М.: Горячая линия-Телеком, 2014. – 280 с.

55. Матрос, Д.Ш. Имитационное моделирование в управлении школой: пособие для директора школы. / Под ред. М.М.Поташника. М.: Новая школа, 1992. – 312с.

56. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утв. Федеральной службой по техническому и экспортному контролю 14 февраля 2008г //СПС Консультант Плюс.

57. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в

информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: утв. ФСБ РФ 21 февраля 2008г. N149/54-144 //СПС Консультант Плюс.

58. Моисеев, В.Б. Информационные технологии в системе высшего образования. / В.Б. Моисеев. Пенза: Изд-во Пенз. технол. ин-та, 2014. – 100с.

59. Моисеев, В.Б. Элементы информационно-образовательной среды высшего учебного, заведения. / В.Б. Моисеев. - Ульяновск: Изд-во Ул. ГТУ, 2012. – 122с.

60. Молодцова Е. Ю., Склямина М. Ю. К вопросу организации мероприятий по информационной безопасности учащихся в образовательном учреждении // Молодой ученый. — 2014. — №18.1. — С. 65-68. Партыка Т.Л., Попов И.И. Информационная безопасность.- 2-е изд., М.: ФОРУМ:ИНФРА-М, 2007.-368 с.

61. Морев, И. А. Проблемы компьютерного представления образовательной информации: метод. пособие / И.А. Морев. – Владивосток: Изд-во Дальневосточного университета, 2014. – 15 с.

62. Нежурина, М.И. Принципы организации и разработка специализированной информационно-образовательной среды для дистанционного обучения. автореф. дис. канд. техн. наук. М. 2014.

63. Новейший философский словарь /сост. А.А. Грицанов. — Минск.: Изд-во им. В.М. Скакун, 1998. - 896 с.

64. Новиков, А.М. Организация опытно-экспериментальной работы на базе образовательного учреждения [Текст] /А.М. Новиков// Дополнительное образование. – 2012. – № 4. С.51 – 53.

65. Новые педагогические и информационные технологии в системе образования /Е.С. Полат, М.Ю. Бухаркина и др. - М.: ИД «Академия», 2002. – 272с.

66. Новый подход к инженерному образованию: теория и практика открытого доступа к распределенным информационным и техническим

ресурсам. / Ю.В.Арбузов, В.Н.Леньшин, С.И.Маслов, А.А.Поляков, В.Г.Свиридов; под ред. А.А.Полякова. – М.: Центр-Пресс, 2010 – 186с..

67. О персональных данных [Электронный ресурс]: Федеральный закон N 152-ФЗ: [принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 года]// СПС Консультант Плюс.

68. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федер. закон: [принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 г.] //СПС Консультант Плюс.

69. Об образовании в Российской федерации (ред. От 29.07.2017) [Электронный ресурс]: федер. закон: [принят Гос. Думой 21.12. 2012 г.] //СПС Консультант Плюс.

70. Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 17 ноября 2007 г. N 781. //СПС Консультант Плюс.

71. Общая и профессиональная педагогика: учеб. пособие /под ред. Г.Д. Бухарова – Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2013. – 296 с.

72. Общая повестка дня России и АСЕАН в киберпространстве: противодействие глобальным угрозам, укрепление кибербезопасности и развитие сотрудничества // Индекс безопасности № 4 (111), том 20 – С. 77-92 [электронный ресурс] http://www.pircenter.org/media/content/files/17/14219241510.pdf. Дата обращения 10.10.2017

73. Основные направления научных исследований в области обеспечения информационной безопасности российской федерации (одобрены секцией по информационной безопасности Научного совета при Совете Безопасности Российской Федерации, протокол от 28 марта 2015г. №1) [электронный ресурс] http://www.scrf.gov.ru/security/information/document94/. Дата обращения: 12.09.2016

74. Основы общей теории и методики обучения информатике / под общей редакцией А.А.Кузнецова. – М.: Бином, 2013. – 154с

75. Основы открытого образования // Отв. Ред. В.И.Солдаткин. – Т. 1. – Российский государственный институт открытого образования. – М.: НИИЦ РАО, 2012. – 680 с.

76. Полат, Е.С. Дистанционное обучение: организационные и педагогические аспекты / Полат Е.С.– М.: Академия, 2006. –143с.

77. Полат, Е.С. Новые педагогические и информационные технологии в системе образования / Полат Е.С.– М.: Академия, 2006. – 272 с.

78. Полат, Е.С. Современные педагогические и информационные технологии в системе образования: учебное пособие для студентов высших учебных заведений / Е.С. Полат, М.Ю. Бухаркина. – 3-е изд., стер. – М.:Издательский центр «Академия», 2010 г. – 368 с.

79. Полат, Е.С. Теория и практика дистанционного обучения: учеб. пособие для студентов высш. пед. учеб. заведений / Е.С. Полат, М.Ю. Бухаркина, М.В. Моисеева; под ред. Е.С. Полат. - М.: Академия, 2014. - 416с.

80. Положение о сертификации средств защиты информации по требованиям безопасности информации [Электронный ресурс]: приказ Гостехкомиссии РФ от 27.10.1995 N 199 //СПС Консультант Плюс.

81. Порядок проведения классификации информационных систем персональных данных [Электронный ресурс]: приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008г.N55/86/20 //СПС Консультант Плюс.

82. Послание Президента Российской Федерации Федеральному собранию от 04.10.2014 [Электронный ресурс]: Послание Президента РФ // СПС Консультант Плюс.

83. Поташник, М.М. Управление в образовании. / М.М. Поташник, А.В. Лоренсов, О.Т. Хомерики. - М.:ИЦ «Академия», 2010 г. – 212 с.

84. Пурим, М. Другой интернет — какие нововведения ждут российских пользователей? [Электронный ресурс] / М. Пурим // Аргументы и факты: еженедельник. – 17/03/2014. - Режим доступа: http://www.aif.ru/techno/pc/1125738 – Загл. с экрана. (Дата обращения: 15.11.2019).

85. Пурим, М. Закрыть навсегда: «черные» и «белые» списки интернета [Электронный ресурс] / М. Пурим // Аргументы и факты: еженедельник. – 15/02/2013. - Режим доступа: http://www.aif.ru/society/web/40597– Загл. с экрана. (Дата обращения: 15.11.2016)

86. Российская педагогическая энциклопедия. [электронный ресурс]- URL: http://www.gumer.info/bibliotek_Buks/Pedagog/russpenc/15.php. Дата обращения 23.11.2016.

87. Рыжко, А.Л. Экономика информационных систем: учебное пособие. / А.Л. Рыжко, Н.М. Лобанова, Н.А. Рыжко, Е.О. Кучинская – М.: Финансовый университет, 2014. – 204 с.

88. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. - СПб.: Питер, 2015. - 320 с.

89. Скляров Д.В. Искусство защиты и взлома информации. - СПб.: БХВ-Петербург, 2014. - 288 с.

90. Современный энциклопедический словарь /под ред. А.М. Прохорова. - М.Просвещение, 1991-1112с.

91. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. - М.: ДМК Пресс, 2015. - 656 с.

92. Соколова О.И. Основы разработки информационной среды педагогического вуза. // Материалы: XI конференция-выставка «Информационные технологии в образовании» – М.: МИФИ, 2011 – 200 с.

93. Сотов А.И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации [Электронный ресурс]: монография/ Сотов А.И.— Электрон. текстовые

данные.— М.: Русайнс, 2015.— 128 с.— Режим доступа: http://www.iprbookshop.ru/48904.— ЭБС «IPRbooks», по паролю.

94. Титаренко, Е.С. Защита детей от негативной информации как средство нравственного воспитания. [Электронный ресурс] — Электрон. дан. // Концепт. — 2013. — № 6. — С. 1-6. — Режим доступа: http://e.lanbook.com/journal/issue/293447 - по паролю (Дата обращения: 16.12.2016).

95. Трудовой кодекс Российской Федерации [Электронный ресурс]: фед. закон: [принят Гос. Думой 21 дек. 2001 г.; одобр. Советом Федерации 26 дек. 2001 г.: по сост. на 1 марта 2009 г.] //СПС Консультант Плюс.

96. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]: // Собрание законодательства РФ. -2016. -№ 50. Ст. 7074. - Режим доступа: http://government.ru/docs/all/109306/. - Загл. с экрана (дата обращения: 15.12.2019).

97. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [электронный ресурс] - Режим доступа http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 09.03.2019)

98. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ [электронный ресурс] - Режим доступа http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 09.03.2019)

99. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» [Электронный ресурс]. - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_43224/. - Загл. с экрана (дата обращения: 15.12.2019).

100. Филин С.А. Информационная безопасность: Учебное пособие. - М.: Издательство «Альфа-Пресс», 2016. - 412 с.

101. Шоломицкий А.Г. Теория риска. Выбор при неопределенности и моделирование риска: Учеб. пособие для колледжов. Гос. ун-т - Высшая школа экономики. - М.: Изд. дом ГУ ВШЭ, 2015. - 400 с.

102. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: учеб. пособие. - М.: Гелиос АРВ, 2015. - 224 с.

103. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - СПб: Наука и техника, 2014. - 384 с.

104. Ямалов И.У. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций. - М.: Лаборатория Базовых Знаний, 2017.-288 с.

105. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. – М.: Академический Проект, 2014. – 544 с.

Приложение 1

Правила работы персонала и обучающихся колледжа в компьютерных сетях

1. Данные правила регулируют права и обязанности обучающихся, связанные с работой в компьютерной сети колледжа и сети Интернет (далее Сетей), а также основные правила работы и полномочия преподавателей и сотрудников колледжа. Правила призваны обеспечить и организовать использование образовательного потенциала Сетей в сочетании с системой мер по обеспечению охраны и безопасности студентов.

2. Основными принципами политики колледжа для работы в Сетях являются:

- равный доступ для всех обучающихся;

- использование Сетей обучающимися только для образовательных целей.

- защита обучающихся от вредной или незаконной информации, содержащей: порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр и т.п.

3. Полномочия преподавателей и сотрудников.

3.1 Начальник отдела по безопасности:

- организует и руководит всей деятельностью по реализации настоящих Правил;

- обеспечивает свободный и равный доступ обучающихся к Сетям в соответствии с учебной программой и возможностями колледжа;

- организует и руководит всей деятельностью по реализации настоящих Правил;

- обеспечивает свободный и равный доступ обучающихся к Сетям в соответствии с учебной программой и возможностями колледжа;

- отвечает за организацию мер, включая сотрудничество с провайдером, по ограничению доступа обучающихся к ресурсам вредного или незаконного содержания в Сетях в соответствии с действующим законодательством;

- обеспечивает контроль за соблюдением правил работы обучающихся в сетях;

- организует поддержку и обновление сайта.

Размещает на сайте только материалы, утвержденные директором;

- незамедлительно сообщает директору о выявлении нарушений и принимает меры по устранению нарушений;

3.2 Преподаватели компьютерных классов обязаны:

- объяснять обучающимся правила безопасного и ответственного поведения при работе в Сетях;

- использовать возможности Интернет в целях обогащения и расширения образовательной деятельности, для чего обучающимся назначать конкретные задания;

- осуществлять непрерывный контроль работы обучающихся в Сетях в учебное время;

- принимать незамедлительные меры для прекращения доступа обучающихся к ресурсам запрещенного содержания в Сетях;

- немедленно сообщать начальнику отдела по безопасности или директору о нарушении правил или о создании незаконного контента в сети колледжа; - не покидать учебный кабинет во время пары, и не допускать обучающихся во время перемены к работе в Сетях;

Преподаватели несут ответственность за целостность оборудования колледжа, закрепленного за учебным кабинетом, в котором проводят занятия.

3.3 Сетевой администратор обязан:

- обеспечивать общую безопасность и эффективность работы в Сетях;

- предлагать и осуществлять меры по ограничению доступа обучающихся к вредным или незаконного содержания ресурсам в Сетях в соответствии с законодательством;

- периодически просматривать содержимое Сети колледжа с целью предотвращения любых возможных угроз и рисков безопасности для обучающихся;

- немедленно сообщать начальнику отдела по безопасности или директору о нарушении Правил или о создании незаконного контента в сети колледжа.

4. Права и обязанности обучающихся

4.1. Обучающиеся имеют право:

- на равный доступ к Сетям с учетом политики информатизации колледжа;

- на получение доступа к сети Интернет (только под наблюдением преподавателя);

- на грамотное и ответственное обучение работе в Сетях;

- быть информированным о правилах работы в Сетях.

4.2. Обучающиеся обязаны соблюдать следующие правила:

- использовать Сети только для образовательных целей;

- запрещается выход на сайты, не включенные в перечень преподавателем для данного занятия;

- немедленно сообщить преподавателю при обнаружении материалов, содержащих порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр, и т.п.;

- запрещается проводить любую деятельность, которая угрожает целостности компьютерной сети колледжа или атаки на другие системы;

- запрещено использование нелицензионного программного обеспечения, защищенных авторским правом материалов без разрешения, и любой другой деятельности, которая нарушает авторские права.

5. Ответственность

5.1. Обучающиеся за нарушение положений настоящих Правил привлекаются к дисциплинарной ответственности в соответствии с правилами внутреннего распорядка колледжа.

5.2. Преподаватели и сотрудники за нарушение положений настоящих Правил несут ответственность в соответствии с Трудовым кодексом и привлекаются к дисциплинарной ответственности.

5.3. За нарушения, которые являются преступлениями, административными нарушениями или причиняют ущерб собственности, виновные несут ответственность в соответствии с законодательством РФ и РБ.

Приложение 2

Правила работы с ресурсами сети Интернет

1.1. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности.

Отдел по безопасности колледжа имеет право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

1.2. При работе с ресурсами сети Интернет недопустимо:

1.2.1. разглашение коммерческой и служебной информации колледжа, ставшей известной сотруднику колледжа по служебной необходимости либо иным путем;

1.2.2. распространение защищаемых авторскими правами материалов, затрагивающих какой- либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

1.2.3. публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам

и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

1.3. При работе с ресурсами Интернет запрещается:

1.3.1. загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

1.3.2. использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой компании.

1.4. Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политикой колледжа.

Приложение 3

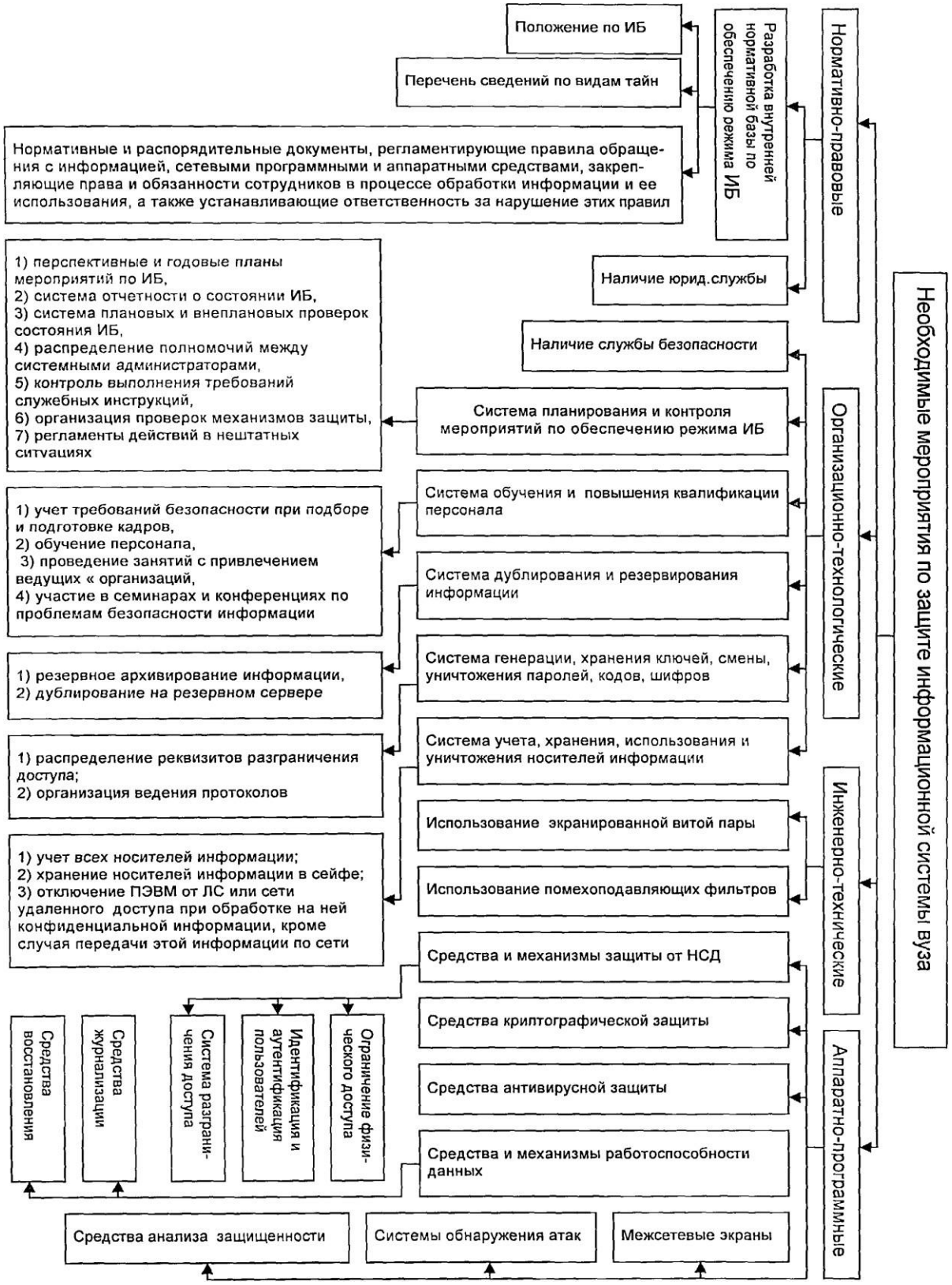

Рис.4. – Рекомендации по использованию контрмер по защиту информационной безопасности ГБПОУ «Южно-Уральский Государственный Технический Колледж»