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

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

Организация и управление службой информационной безопасности в образовательной организации

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
81,23% авторского текста

Работа рекомендована к защите
«17» января 2022 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Чубатюк Евгений Сергеевич

Научный руководитель:
к.т.н., доцент
Руднев Валерий Валентинович

Челябинск
2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность проблемы исследования. Отличительной особенностью современности является переход от индустриального общества к информационному, в котором главным ресурсом становится информация. В этой связи информационная сфера представляет собой специфическую составляющую деятельности образовательной организации, связанную с созданием, хранением, распространением, передачей, обработкой и использованием информации.

С учетом усиления роли информации на современном этапе, правовое регулирование общественных отношений, возникающих в информационной сфере, является приоритетным направлением в Российской Федерации, целью которого является обеспечение информационной безопасности.

Обеспечение, создание и управление службы безопасности образования является одним из основных направлений информатизации, поскольку информационная безопасность является обязательным условием и одним из критериев эффективности образовательной организации и безопасности образовательного процесса в целом.

Становление научного направления «информационная безопасность и защита информации» в РФ связано с именами таких отечественных ученых, как А.А. Грушко, В.Ю. Гайкович, В.А. Герасименко, В.И. Герасимов, Н.Н. Дмитриевский, Г.В. Емельянов, В.А. Минаев, П.Д. Зегжда, В.В. Кульба, А.Г. Мамиконов, А.П. Першин, С.П. Расторгуев, А.А. Стрельцов, Е.Е. Тимонина, Л.М. Ухлинов, Д.С. Черешкин, В.В. Шураков, А.Б. Шелков и др.

Общие вопросы информационной безопасности посвящены в работах таких ученых, как В.В. Домарев, В.А. Галатенко, С.М. Доценко, В.Ф. Шпак, В.И. Ярочкин, А. Володин, Б. Байбурин, А.В. Петраков, А.Ю. Щербаков, Е.Б. Белов, А.А. Малюк и др.

Правовые аспекты информационной безопасности нашли отражение в трудах Ю.М. Батурина, И.Л. Бачило, В.А. Копылова, В.Н. Лопатина, Ю.А.

Тихомирова, М.А. Федотова и др.

Технические стороны информационной безопасности отражены в работах А.П. Тимофеев, А.В. Соколов, Г. Н. Устинова, В.Г. Проскурин, С.А. Маркова, О.Ю. Макаров и другие.

Законодательство в области обеспечения информационной безопасности представлено различными нормативно-правовыми актами, включая Федеральные Законы, Постановления Правительства, Указы Президента, ведомственные приказы Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ).

Федеральный закон (ФЗ) «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации. В силу того, что образовательные организации в своей деятельности неизбежно сталкиваются с информацией в различных формах её представления, действие данного ФЗ распространяется и на них.

В статье 5 ФЗ «Об информации, информационных технологиях и о защите информации» говорится о том, что информация, в зависимости от категории доступа к ней, подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами. К информации ограниченного доступа относятся персональные данные. Отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами,

юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно- телекоммуникационных сетях, или без использования таких средств, регламентируются Федеральным законом «О персональных данных» от 27.07.2006 N 152-ФЗ. Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Все образовательные организации являются операторами персональных данных, так как при организации образовательного процесса сталкиваются с обработкой информации, в том числе и в первую очередь с обработкой персональных данных. Согласно нормативно-правовым актам в области обеспечения защиты персональных данных в обязанности оператора персональных данных входит обеспечение безопасности персональных данных, которое достигается путем определения актуальных угроз информационной безопасности, классификация ИСПДн, применение правовых, организационных и технических мер по защите информации.

Персональные данные являются наиболее значимым и наиболее уязвимым компонентом информационных ресурсов образовательной организации.

Лицам, нарушившим требования закона о персональных данных, в зависимости от конкретных обстоятельств и серьезности деяния может грозить не только административная и уголовная ответственность, но также гражданско-правовая и даже дисциплинарная. При этом административная ответственность с 1 июля 2017 года ужесточилась – вместо одного состава правонарушения ст. 13.11 КоАП РФ теперь предусматривает семь, а максимальный штраф составляет 75 тыс. руб. Ответственность за нарушение ФЗ «О персональных данных» не ограничивается административными штрафами, отдельные нормы Трудового, Гражданского и Уголовного кодексов РФ также предусматривают санкции для операторов-

правонарушителей.

Необходимость обеспечения нормативных требований и учета специфики организационно-правовых и программно-аппаратных мер защиты информационных ресурсов, и в частности, персональных данных в конкретной образовательной организации определяют актуальность темы диссертации.

Для большинства служб информационной безопасности образовательных организаций обеспечение достаточного уровня защиты информационных ресурсов согласованным набором различных мер является проблемой.

Цель исследования: теоретически обосновать, разработать рекомендации по повышению эффективности службы информационной безопасности в образовательной организации.

Объект исследования: информационная безопасность в образовательной организации.

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

В процессе разработки темы была выдвинута следующая **гипотеза:** достаточный уровень защищенности персональных данных будет обеспечен при условии реализации программы, содержащей меры по обеспечению рекомендаций, разработанных на основе анализа угроз в образовательной организации для службы информационной безопасности.

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.

Теоретическую и информационную базу исследования составляют основные положения по информационной безопасности, системный подход к исследуемому объекту и предмету, в качестве информационных источников использованы аналитические и статистические материалы по информационной безопасности, материалы научных конференций, средств массовой информации, отражающие аспекты информационной безопасности.

Научная новизна исследования состоит в том, что показана

возможность внедрения комплекса нововведений, позволяющих повысить эффективность системы управления службой информационной безопасности в условиях колледжа.

Практическая значимость работы заключается в разработке программы совершенствования службы информационной безопасности ГБПОУ «Южно-Уральский Государственный Технический Колледж», разработанной на основе анализа угроз названной организации.

Положения, выносимые на защиту:

1. 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. 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.

2. Анализ состояния информационной безопасности образовательной организации позволяет выявить следующие угрозы:

1. Каналы внесения вредоносного программного обеспечения при использовании различных съемных носителей информации, использовании сети Интернет и локальных сетей.

2. Случайные ошибки сотрудников учреждения, в том числе ввод неверных данных или их изменение.

3. Отказ внутренней инфраструктуры, в том числе отказ как информационных систем, так и программного и аппаратного обеспечения, физическое повреждение аппаратуры.

4. Угрозы технического характера.

5. Угрозы нетехнического характера – отсутствие парольного доступа, хранение конфиденциальной информации в доступных местах.

6. Несанкционированный доступ к информации (использование без разрешений). При этом могут быть выполнены следующие действия: чтение, изменение и удаление информации.

7. Хищение программно-аппаратных средств.

8. Использование устаревших программных и аппаратных средств обработки информации.

3. Проанализировав актуальные угрозы информационной безопасности колледжа, можно сделать вывод, что все они устраняются посредством технических и организационных мер.

4. В ЮУрГТК предложено использовать разные программные средства защиты информации, а некоторые старые заменить на более сильные.

5. Разработанная стратегия информационной безопасности в условиях ГБПОУ «Южно-Уральский Государственный Технический Колледж» повысит эффективность работы службы информационной безопасности.

6. Обеспечение информационной безопасности достигается только при комплексном использовании всех средств защиты информации - организационные, физические, социально-психологические мероприятия и программном - технические средства защиты.

Апробация результатов исследования. Основные положения и результаты диссертационного исследования нашли отражение в опубликованных статьях и выступлении на международных научно-практических конференциях.

База исследования: ГБПОУ «Южно-Уральский Государственный Технический Колледж».

Структура магистерской диссертации состоит из введения, двух глав, заключения, библиографического списка, состоящего из 57 наименований, приложение. Работа содержит 9 рисунков. Общий объем работы составляет 70 страниц.

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, устранитьили 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.

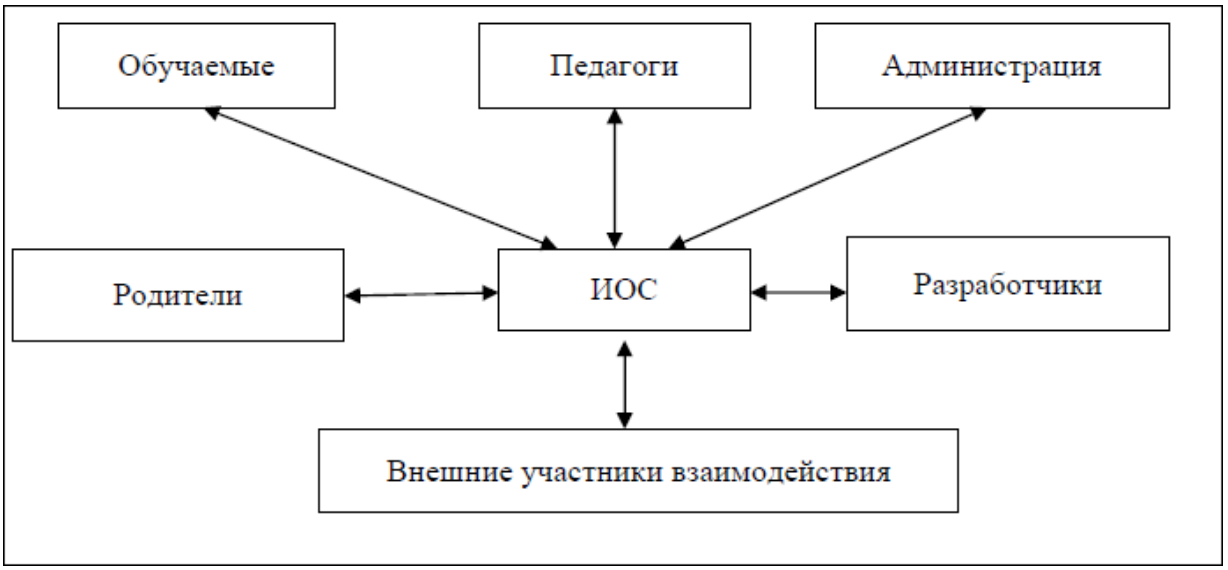

Рисунок 1 - Структура сетевого взаимодействия всех участников учебно-воспитательного процесса в условиях информационно-образовательной среды (ИОС)

Система информационной безопасности образовательной организации включает в себя следующие компоненты:

1. Правовой - это 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

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 за щиты детей от информации, наносящей вред их здоровью, нравственному и духовному развитию.

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

1. Компьютерное оборудование и другие аппаратные компоненты, которые могут быть повреждены или выведены из строя;

2. Программное обеспечение, используемое для корректной работы образовательной системы, могут пострадать от вредоносных программ;

3. Данные, содержащиеся на различных носителях, таких как жесткие

диски, флеш-накопители и др.

4. Персонал, обеспечивающий корректную работу информационных систем.

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

Аварийные ситуации, такие как перебои в подаче электроэнергии или возможность затопления;

Случайные ошибки персонала, основанные на усталости, рассеянности и других причинах;

Сбои в работе программного обеспечения, возникшие из-за недоработок этого ПО;

Проблемы в работе систем связи [55].

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

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

Способы несанкционированного доступа.

Существует несколько типов несанкционированного доступа:

Человеческий. Похищение информации происходит путем ее копирования на различные носители, отправлена по электронной почте. Так же возможен вариант внесение искаженной информации в базы данных при наличии доступа к серверам.

Программный. Используются специальные программы, обеспечивающие перехват информации и сетевого трафика, его дешифровку, внесение коллизий и изменений в работу программного обеспечения.

Аппаратный. Для выполнения этого способа используются специальные технические средства, обеспечивающие перехват информации с различных каналов связи, в том числе сетевой и телефонный.

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

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

Принцип эшелонирования. Он представляет собой порядок обеспечения информационной защиты организации, в котором все уровни защитной системы состоят из последовательно расположенных зон безопасности, самая важная из которых располагается внутри всей системы.

Принцип надежности. Стандарты информационной безопасности в области организации, должен использоваться во всех зонах безопасности. Они должны иметь одну и ту же степень надежной защиты с вероятностью реальной угрозы.

Принцип разумной достаточности подразумевает рациональное

применение защитных методов с приемлемым уровнем обеспечения безопасности. Создание высокоэффективной системы защиты подразумевает под собой большие материальные затраты, поэтому необходим рациональный подход к выбору системы безопасности. Защитная система не должна стоить больше возможного ущерба и затрат на ее функционирование и обслуживание.

Принцип непрерывности. Системы безопасности должны работать круглосуточно и непрерывно [55].

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

Анализ состояния информационной безопасности образовательной организации позволяет выявить следующие угрозы:

1. Каналы внесения вредоносного программного обеспечения при использовании различных съемных носителей информации, использовании сети Интернет и локальных сетей.

2. Случайные ошибки сотрудников учреждения, в том числе ввод неверных данных или их изменение.

3. Отказ внутренней инфраструктуры, в том числе отказ как информационных систем, так и программного и аппаратного обеспечения, физическое повреждение аппаратуры.

4. Угрозы технического характера.

5. Угрозы нетехнического характера – отсутствие парольного доступа, хранение конфиденциальной информации в доступных местах.

6. Несанкционированный доступ к информации (использование без разрешений). При этом могут быть выполнены следующие действия: чтение, изменение и удаление информации.

7. Хищение программно-аппаратных средств.

8. Использование устаревших программных и аппаратных средств обработки информации.

Таким образом, наиболее возможными угрозами информационной

безопасности в колледже являются: кража персональной информации обучающихся, несанкционированное внесение изменений в нее, а также непреднамеренные ошибки сотрудников при внесении и редактировании данной информации.

Самым серьезным недостатком в организации информационной безопасности является отсутствие взаимопонимания между теми, кто обеспечивает информационную безопасность, и теми, кто пользуется данной информацией. Нередко пользователи информации нарушают порядок обращения с ней и не соблюдают требования нормативно-правовых документов, регламентирующих информационную безопасность. Решение данной проблемы возможно только при соблюдении принципов информационной безопасности, постоянной требовательности по соблюдению конфиденциальности со стороны руководителя ОО.

С учетом этих недостатков для обеспечения информационной безопасности в ОО требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности ОО;

- защита компьютеров, локальных сетей и сети подключения к системе Интернета в классе информатики ОО;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и учащихся ОО;

- учет всех носителей конфиденциальной информации.

Реализация данного комплекса мер вносит кардинальные изменения в организацию работы с информацией в ОО, а также делопроизводства, в т. ч. и по вопросам безопасности.

При таком подходе, основными составными задачами делопроизводства станут: документирование информации, учет документов, организация документооборота, обеспечение надежного хранения документов, своевременное их уничтожение, проверка наличия хранящихся документов, контроль за своевременным и правильным их исполнением. Необходимо помнить, что не на всяком документе имеется гриф "Для служебного

пользования" ("Ограниченного пользования"), однако это не означает, что такой документ не представляет никакой ценности. Не бывает важных или не очень важных документов. Самый малозначительный, на первый взгляд документ, при определенных обстоятельствах может оказаться чрезвычайно важным. Организация вышеперечисленных мероприятий позволит избежать непредвиденных ситуаций, путаницы и неразберихи. Следует отметить, что при организации делопроизводства необходимо выявить и учесть все возможные каналы утечки информации. Наиболее характерными каналами утечки информации для ОО могут стать разглашение, хищение и несанкционированный доступ. Учитывая эти аспекты, систему организации делопроизводства можно представить в следующем виде:

- учет всей документации ОО, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

- регистрация и учет всех входящих (исходящих) документов ОО в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);

- особый режим уничтожения документов. Уничтожать документы можно с помощью уничтожителя бумаг, или сжиганием. В обязательном порядке нужно составлять об этом акт, подписываемый комиссией, назначенной приказом руководителя ОО.

Для облегчения контроля все документы следует разделить на две группы: для общего пользования и для служебного пользования (ограниченного пользования). Документам каждой категории необходимо присвоить свой гриф. Это можно сделать при помощи штампов, специальных отметок или цветового выделения (для общего пользования – зеленый цвет, для служебного – красный). При присвоении соответствующего грифа соблюдаются определенные правила, которые необходимо учитывать в своей

работе: ответственность за присвоение соответствующего грифа несет исполнитель документа, а субъектом оценки его присвоения является руководитель ОУ; ценность информации определяется с помощью таких критериев, как полезность, своевременность, актуальность, достоверность, конфиденциальность; информация подлежит защите при условии, что доступ к ней закрыт на законном основании. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила: все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах.

Для создания безопасной информационной системы в ОО можно принять меры:

- Обеспечить защиту компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.)

- Установить строгий контроль за электронной почтой, обеспечить постоянный контроль за входящей и исходящей корреспонденции.

- Использовать контент-фильтры для фильтрации сайтов по их содержимому.

Одна сумма всех этих мероприятий, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Специалисты, которые имеют отношение к системе защиты, должны быть в полной мере представить себе принципы ее функционирования и в случае возникновения сложной ситуации адекватно реагировать. Под защитой должна находиться вся система обработки информации.

Лица, занимающиеся обеспечением информационной безопасности, должны нести ответственность.

Надежная система защиты должна быть полностью протестирована и совместима. Защита становится более эффективной и гибкой, если она

допускает изменение их параметров со стороны администратора.

Выводы по первой главе

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]

Анализ состояния информационной безопасности колледжа позволяет выявить следующие угрозы:

1. Каналы внесения вредоносного программного обеспечения при использовании различных съемных носителей информации, использовании сети Интернет и локальных сетей.

2. Случайные ошибки сотрудников учреждения, в том числе ввод неверных данных или их изменение.

3. Отказ внутренней инфраструктуры, в том числе отказ как информационных систем, так и программного и аппаратного обеспечения, физическое повреждение аппаратуры.

4. Угрозы технического характера.

5. Угрозы нетехнического характера – отсутствие парольного доступа, хранение конфиденциальной информации в доступных местах.

6. Несанкционированный доступ к информации (использование без

разрешений). При этом могут быть выполнены следующие действия: чтение, изменение и удаление информации.

7. Хищение программно-аппаратных средств.

8. Использование устаревших программных и аппаратных средств обработки информации.

.

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: 454071, г. Челябинск, ул. Гагарина, д 7.

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.

Инженерно-педагогический коллектив техникума, используя компетентностный подход в профессиональном образовании обучающихся как основу профессиональной мобильности выпускника, мотивирует их на приобретение 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 2020-2021 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 оборудывания	23.01.17	Очная (9)	25
Информационные системы и програмирование	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 оборудывания	35.01.24	Очная (9)	25
Автоматизация технических 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
Земально-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 защищенностиинформационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

К объектам информационной безопасности техникума относятся:

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

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

- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачиданных, 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 за кон «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;

- эффективное пресечение незаконных посягательств на ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер защиты информации;

- координация деятельности структурных подразделений техникума по обеспечению защиты информации.

Система обеспечения информационной безопасностираспространяются на:

- автоматизированные системы техникума;

- средства телекоммуникаций;

- помещения;

- сотрудников техникума.

Организационная структура отдела по безопасности представлена в

виде следующей схемы (рисунок 4).

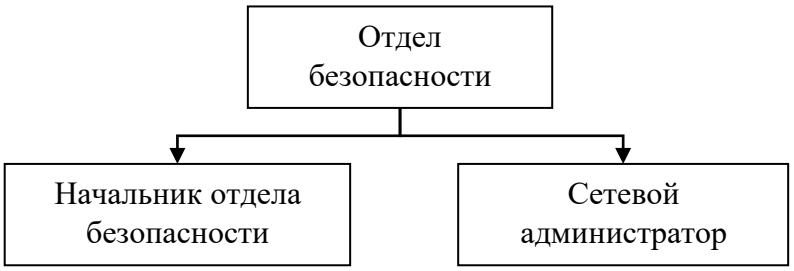

Рисунок 2 - Организационная структура отдела безопасности ГБПОУ «Южно-Уральский Государственный Технический Колледж»

Учебный процесс в колледже сопровождается значительной информационной базой, развитием компьютерного парка и внедрением в образовательный процесс модернизированных информационных систем. Для обеспечения учебного процесса все кафедры и отделы оснащены персональными компьютерами и необходимой техникой. Для решения задач в области применения современных информационных технологий в колледже оборудовано 5 компьютерных классов. Целесообразно ввести несколько уровней конфиденциальности информации:

Информация ограниченного доступа:

Служебная тайна - информация, содержащая сведения о финансах, производстве, управлении и других видах деятельности субъекта, разглашение которой может нанести экономический ущерб;

Профессиональная тайна - сведения, содержащие организацию учебной деятельности и процессов.

Персональные данные – любая информация, содержащая сведения о конкретном лице (сведения о студентах, преподавателях и др.);

Информация общего доступа:

Постановления, указы, распоряжения;

Информация, содержащая статистические сведения об образовательной деятельности;

Информация, доступ к которой не ограничен законом и уставом;

На территории учреждения ведется круглосуточное наблюдение через

пост охраны.

Посетители имеют право прибывать на территории только в сопровождении сотрудника учреждения. В колледже осуществлена пожарно–охранная сигнализация и установлены соответствующие датчики. Аппаратные средства хранения информации (сервера) располагаются в отдельном помещении. Мониторинг объекта осуществляется через систему видеонаблюдения.

К основным объектам защиты можно отнести:

- серверы баз данных;
- станция управления учетными записями;
- ftp и www – серверы;
- ЛВС бухгалтерии и др.;
- данные архивов, финансового, статистического и учебного отделов;
-внешние и внутренние информационные ресурсы.

На рисунке 5 приведено категорирование информационных активов по видам тайны, из которого следует, что организация защиты.

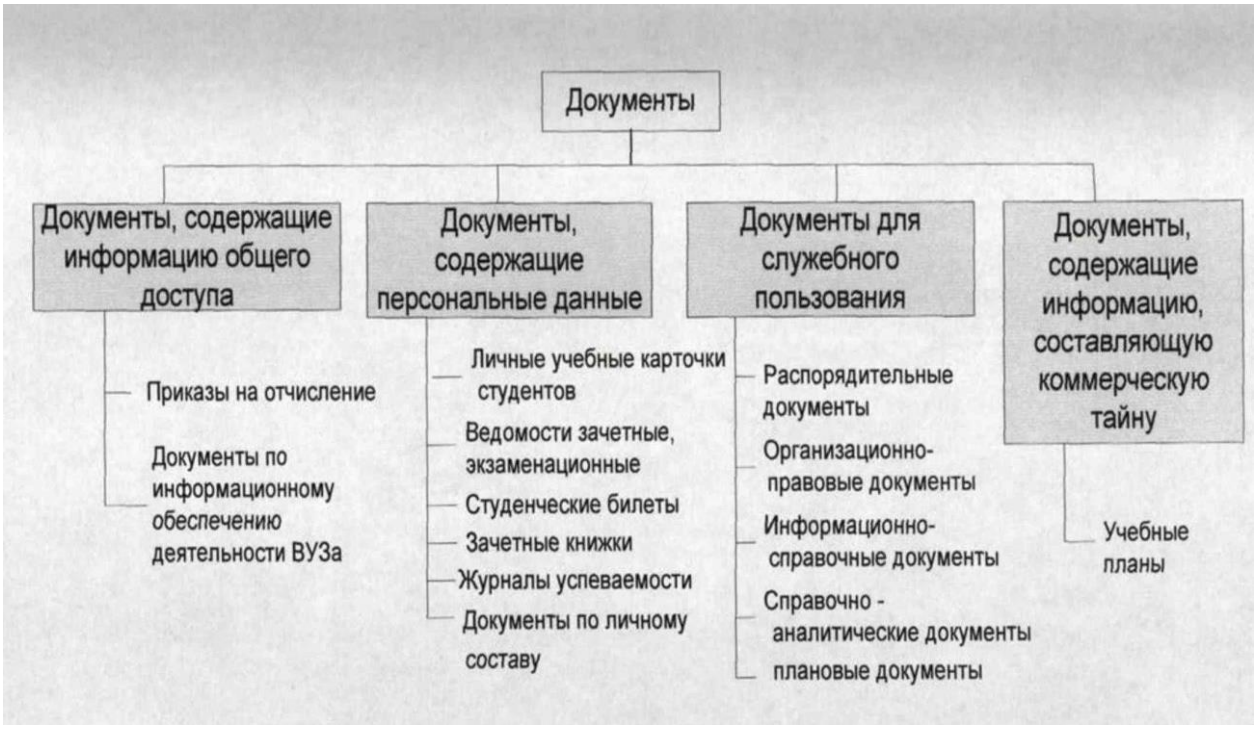

Рисунок 3 - Категорирование информационных активов деканата

Обеспечение защиты информационных активов колледжа специфично, так как это учреждение с непостоянной аудиторией. По причине того, что атаки могут исходить от любых субъектов, целесообразно разделить на две категории: внешние нарушители и внутренние нарушители. Внешним нарушителем является лицо, которое не является сотрудником и не имеет доступа к информационной системе. В эту категорию входят:

- **хакеры** (субъекты, создающие и реализующие атаки, с целью нанесения ущерба и овладения информацией ограниченного доступа): посредством несанкционированного доступа к информационным системам может уничтожить или изменить информацию; внедрение вредоносных программ и вирусов, аппаратных и программных закладок с последующим осуществлением несанкционированного доступа);

- провайдеры, и поставщики технического и программного обеспечения (осуществление несанкционированного доступа через рабочие станции к информационным ресурсам и к каналам связи);

Все остальные субъекты – **внутренние нарушители**. В соответствии с руководящим документом ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» внутренние нарушители подразделяются на восемь категорий:

Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн.

Применительно к данному учреждению такими правами обладает руководство, управление информатизации. В соответствии с правами эти лица могут: иметь доступ к некоторым частям ПДн, которые циркулирует по внутренним каналам; знать информацию о топологии ИСПДн, коммуникационных протоколах и сервисах; выявлять имена и пароли зарегистрированных пользователей; изменять конфигурацию аппаратных и программных средств.

Зарегистрированные пользователи ИСПДн, осуществляющие

ограниченный доступ к ресурсам ИСПДн с рабочего места.

К этой категории можно отнести сотрудников управлений, преподавателей и студентов учреждения. Лица данной категории: имеют один идентификатор и пароль; располагают конфиденциальными данными, к которым имеют санкционированный доступ.

Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.

Лица данной категории: знают топологию ИСПДн и о составе технических средств; имеют физический доступ к некоторым техническим средствам ИСПДн.

Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента ИСПДн.

Лица этой категории: располагают информацией о программном обеспечении, технических средствах, используемых в данном сегменте; имеет доступ к средствам защиты и протоколирования и к аппаратным средствам ИСПДн.

Зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Лица этой категории: знает информацию о программном и аппаратном обеспечении полной ИСПДн; имеет физический доступ ко всем аппаратным средствам; имеет право конфигурировать аппаратное обеспечение.

Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Лица этой категории: располагает всей информацией об ИСПДн; имеет доступ к средствам защиты и протоколирования данных.

Программисты – разработчики программного обеспечения и лица, сопровождающие его на данном объекте.

Лица данной категории: знают информацию о процедурах и программах обработки данных на ИСПДн; может вносить ошибки, программные закладки

и вредоносный код на стадии разработки; может знать информацию о топологии и аппаратных средствах ИСПДн.

Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт аппаратных средств на ИСПДн.

Лица данной категории: может внедрять аппаратные закладки на стадии разработки и сопровождения; может знать информацию о топологии и аппаратных средствах ИСПДн.

Применительно к данному учреждению к внутренним нарушителям можно отнести:

- пользователи информационных ресурсов (персонал управлений, отделов и других подразделений, преподаватели, студенты) (непреднамеренная модификация или уничтожение данных; установка вредоносного и несертифицированного программного обеспечения; передача индивидуального пароля посторонним лицам);

- лица, обслуживающие и поддерживающие информационную систему (случайное или преднамеренное неправильное конфигурирование технических или сетевых средств);

- другие лица, имеющие доступ к объектам обработки информации (технический и обслуживающий персонал) (непреднамеренное нарушение работоспособности средств электрообеспечения и инженерных сооружений);

Особая и наиболее значительная категория нарушителей – студенты. На сегодняшний день многие из них достаточно хорошо подготовлены и разбираются в киберпространстве. Путем некоторых манипуляций студенты в состоянии произвести ряд нарушений безопасности и нанести ущерб.

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

Проанализировав актуальные угрозы, можно сделать вывод, что все они устраняемые посредством технических и организационных мер. В таблице 3 представлены меры борьбы с актуальными угрозами, которые могут быть использованы в колледже для защиты данных.

Таблица 3- Методы борьбы с актуальными угрозами

Актуальная угроза	Технические меры борьбы с угрозой	Организационные меры борьбы с угрозой
Несанкционированный доступ к аппаратным объектам с возможностью хищения или порчи оборудования.	-Охранная сигнализация и видеонаблюдение; - кодовый замок – блокиратор на вход в помещение с серверами.	- Охранно – пропускной режим; - контроль средств обработки информации.
Неумышленное уничтожение или модификация информации сотрудниками.	- Использование средств защиты и резервного копирования данных.	-Инструктаж сотрудников.
Непреднамеренное превышение прав использования оборудования по причине отсутствия соответствующих знаний.	- Использование средств защиты от несанкционированного доступа.	- Инструктаж сотрудников; - разграничение прав доступа.
Перехват сетевого трафика.	- Шифрование данных; - использование межсетевого экрана.	- Инструктаж администратора безопасности; - учет средств защиты данных.
Установка вредоносного ПО и изменение конфигурации ПО.	- Использование средств антивирусной защиты.	- Инструктаж сотрудников; -инструктаж администратора безопасности.
Непреднамеренное раскрытие конфиденциальной		-Инструктаж сотрудников;

информации сотрудниками.		- составление акта о неразглашении.
Отказ и сбой сетевого оборудования с последующим уничтожением информации	-Использование источников бесперебойного писания; -использование сертифицированного аппаратного и программного обеспечения; -резервное копирование данных.	-Инструктаж системного администратора.
Программные закладки	-Использование сертифицированного ПО; - использование средств антивирусной защиты.	-Инструктаж сотрудников; -инструктаж администратора.
Использование чужих регистрационных данных для входа в информационные службы		-Инструктаж сотрудников; -инструктаж администратора безопасности;

Методы борьбы с угрозами, указанные в таблице, будут учтены и использованы при разработке политики безопасности колледжа.

Отправной точкой при разработке комплексной системы защиты информации ЮУрГТК, является ясное понимание роли и места системы защиты информации в деятельности ОО и в сфере обеспечения безопасности в целом. В ЮУрГТК используются большой объем информации.

Безопасность ОО представляет собой своеобразную многоуровневую систему барьеров, включающих в себя такие меры, как установка различных типов сигнализации, организация наблюдения и другие охранные процедуры. Кроме того, нельзя забывать, что при построении систем безопасности не должно оставаться «тонких» мест, и все компоненты системы должны быть сбалансированы, взаимосвязаны и согласованы. Ни одна современная система сигнализации, ни сверхчувствительные датчики не являются эффективными, если будет место человеческому фактору - не дисциплинированность, неумение, безответственность сотрудников. Можно утверждать, что ни одна

система безопасности не застрахована от влияния человеческого фактора полностью. Но современная интеллектуальная система безопасности должна сводить это влияние к минимуму. Чем меньше возможность человека влиять на систему, тем ниже роль ошибок в безопасности информации.

С каждым годом технические возможности злоумышленников расширяются. Соответственно, системы безопасности должны всегда быть в развитии на шаг вперед. Следовательно, необходимо стремиться сразу, строить такую систему безопасности, которая со временем не устареет, и с возможностью при необходимости её модернизировать, «нарастить» до более совершенного уровня. Система также должна сохранять целостность данных даже при форс мажорных обстоятельствах, включая природные катаклизмы, пожары, саботаж, прочие действия потенциальных злоумышленников и другие факторы, так или иначе нарушающие работу системы. Защита будет прочной, если будет комплексной.

Поэтому в ЮУрГТК было предложено использовать разные программные средства защиты информации, а некоторые старые заменить на более сильные.

- Средства шифрования - аппаратные, программные ипрограммно-аппаратные шифровальные (криптографические) средства, реализующие алго ритмыкриптографического преобразования информации для ограничения дос тупа к ней, в том числе при ее хранении, обработке и передаче.

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств - универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

- *Фильтр SkyDNS для учебных заведений (Рис.4)*.

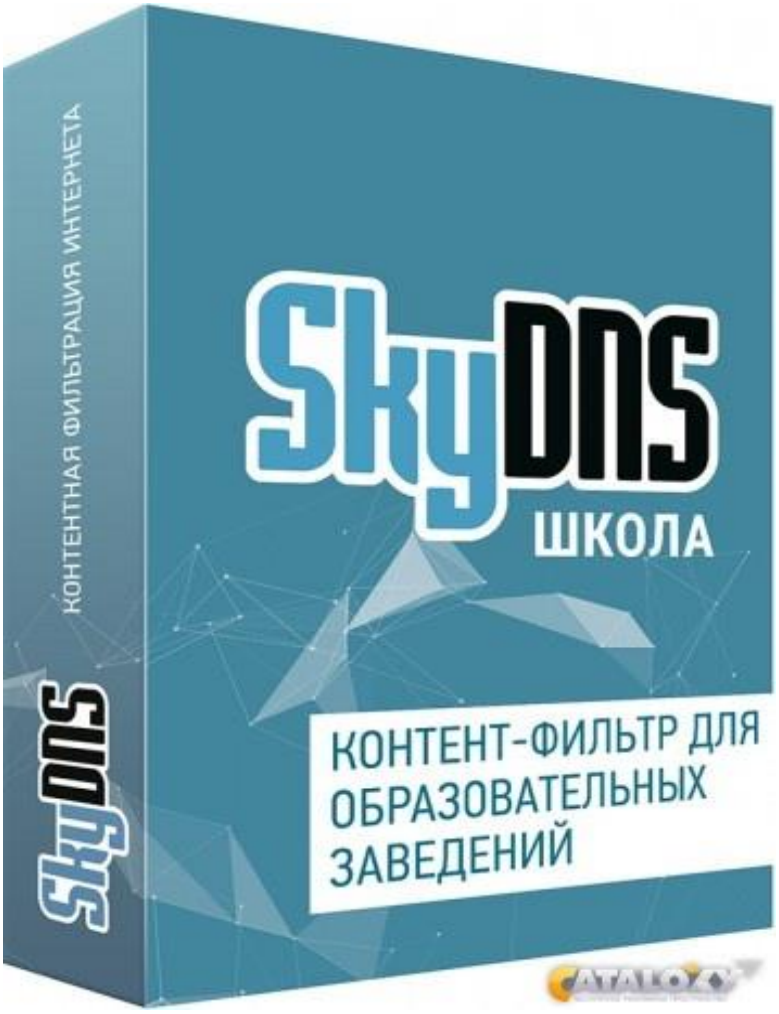

Рисунок 4- Фильтр SkyDNS

Аппаратная версия контент-фильтра на базе роутеров ZyXEL Keenetic. Совместно с компанией ZyXEL создан инновационный продукт для администраторов сетей учебных заведений и библиотек — аппаратный контент-фильтр SkyDNS Z. В него входят специальный тариф контент-фильтра SkyDNS Школа Z с расширенными возможностями и интернет-шлюз ZyXEL Keenetic со встроенным модулем контент-фильтрации. Преимущества SkyDNS Z очевидны — с приобретением этого комплекта значительно упрощается внедрение интернет-фильтрации и управление ее настройками.

- Антивирусная программа Kaspersky CRYSTAL 3.0(Рис.5)

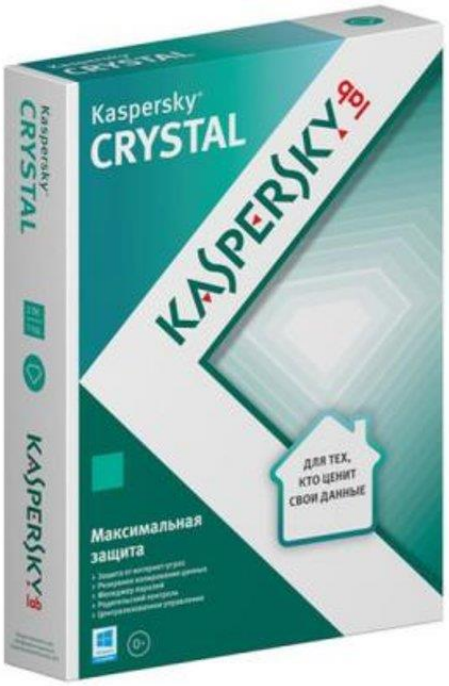

Рисунок 5 - Kaspersky CRYSTAL 3.0

Пакет Kaspersky Crystal включает в себя как самый полный набор антивирусных функций, так и возможность осуществлять контентную фильтрацию.

- VPN (виртуальная частная сеть) (Рис.6) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

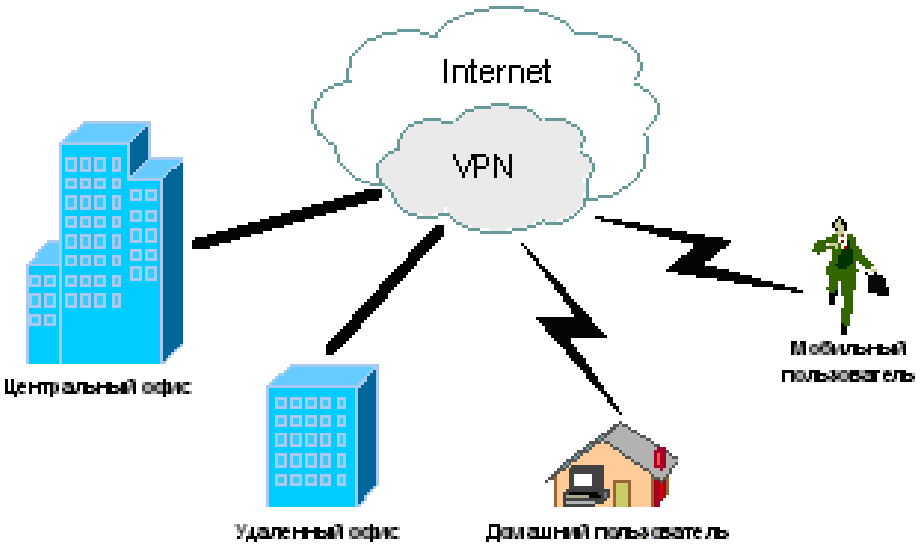

Рисунок 6 - VPN

Лицензионные версии операционных систем Microsoft Windows XP (Рис.5) и

Microsoft Windows Vista.(Рис.6)

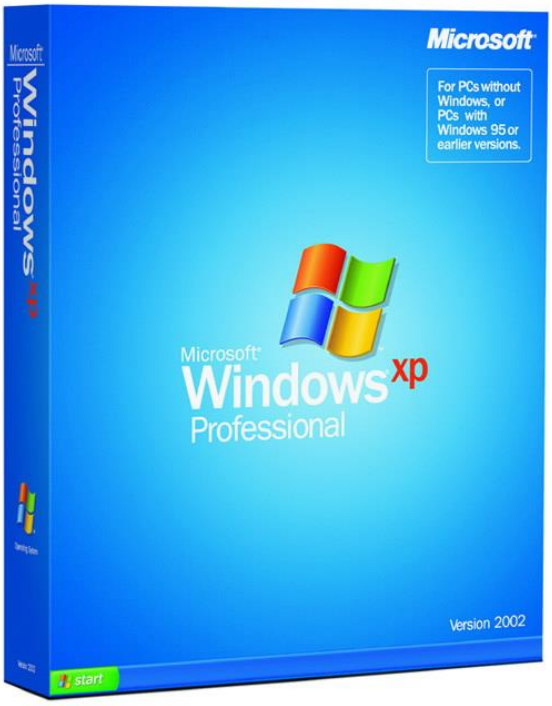

Рисунок 7 - Microsoft Windows XP

Microsoft Windows XP (рис.7) - операционная система семейства Windows NT корпорации Microsoft. Была выпущена 25 октября 2001 года и является развитием Windows 2000 Professional. Название XP происходит от англ. experience (опыт). Название вошло в практику использования, как профессиональная версия.

Рисунок 8 - Microsoft Windows Vista

Microsoft Windows Vista (рис.8) операционная система семейства Microsoft Windows NT, линейки операционных систем, используемых на пользовательских персональных компьютерах. В линейке продуктов Windows NT Windows Vista носит номер версии 6.0. Для обозначения «Windows Vista» иногда используют аббревиатуру «WinVI», которая объединяет название «Vista» и номер версии, записанный римскими цифрами.

- Интернет-браузеры «Opera 10.62» и «Internet Explorer 6.0».

Веб-браузер и программный пакет для работы в Интернете, выпускаемый компанией Opera Software. Разработан в 1994 году группой исследователей из норвежской компании Telenor. С 1995 года продукт компании Opera Software, образованной авторами первой версии браузера.

Браузер написан на языке программирования C++, обладает высокой скоростью работы и совместим с основными веб-технологиями.

Отличительными особенностями Opera долгое время являлись многостраничный интерфейс (система вкладок в окне программы) и возможность масштабирования отображаемых документов целиком, вместе с графикой; впоследствии эти функции появились и в других браузерах. В Opera расширены функциональные возможности использования мыши: кроме стандартных способов навигации предусмотрены так называемые «жесты мышью».

Internet Explorer 6.0 - наиболее распространенный веб-браузер в мире, созданный для удобной и комфортной работы пользователей Интернета. Считается самым простым, безопасным и быстрым в работе. Браузер способен оптимизировать возможности пользователей и разработчиков во время работы с веб-службами. Обозреватель Internet Explorer обладает новыми функциональными возможностями, благодаря которым навигация по веб-страницам стала более быстрой, простой и безопасной. Internet Explorer имеет простой и лаконичный интерфейс, позволяющий пользователям освоить программу за максимально короткое время.

- *Программное обеспечение защиты информации «Secret net 6»(Рис.9)*

Рисунок 9 - Secret Net 6.5-C

Система защиты информации Secret Net 6.5-C (сетевой вариант) интегрируется с доменом Microsoft Active Directory и дополняет своими защитными механизмами стандартные средства обеспечения информационной безопасности операционных систем семейства Microsoft Windows.

Реализация предложенных мероприятий и средств позволит:

- Разграничить права доступа в систему.

- Повысить уровень защищенности информации каждого пользователя в отдельности и системы в целом.

- Уменьшить количество спама.

- Ограничить доступ к ресурсам информационно - телекоммуникационной сети «Интернет», не совместимых с образовательным процессом и способным причинить вред здоровью и развитию студентов.

- Отражать вредоносные атаки через сеть.

- Повысить уровень защиты ПД.

Также нами разработана стратегия информационной безопасности в условиях ГБПОУ «Южно- Уральский Государственный Технический Колледж».

1. Общие сведения

1.1 Наименование

Система информационной безопасности ГБПОУ «Южно- Уральский Государственный Технический Колледж»

2. Цели и назначение проектирования системы

2.1 Цели проектирования системы

- Обеспечение защиты субъектов информационной системы колледжа от несанкционированного доступа внешних нарушителей;

- разделение пользователей информационной системы колледжа и присвоение им соответствующих прав доступа и действий;

- обеспечение защиты от модификации и уничтожения конфиденциальной информации соответствующих управлений;

- расширение теоретических знаний сотрудников колледжа в области информационной безопасности с целью минимизации антропогенных угроз;

-своевременное определение угроз безопасности объектам и субъектам информационной системы колледжа, их ликвидация и реализация плана действий при возникновении последующих угроз;

-обеспечение постоянного контроля режима безопасности информационной системы, с целью предоставления непрерывного доступа к информационной службе колледжа для поддержания деятельности;

-реализация мер защиты от вирусных атак;

-разработка и последующие сохранение условий для минимизации нарушений и ущерба системе информационной безопасности колледжа.

2.2 Назначение проектируемой системы

Проектируемая система информационной безопасности разрабатывается с целью обеспечения комплексной защиты объектов информационной системы колледжа, посредством усовершенствования исходной системы. Проектируемая стратегия соответствует нормативным актам и требованиям.

3. Характеристики объекта защиты

ГБПОУ «Южно- Уральский Государственный Технический Колледж»

является государственным учреждением с распределенной многопользовательской структурой с разграничением доступа к информационным службам.

4. Требования к системе

Система должна соответствовать стандартам и нормативным документам в области информационной безопасности и обеспечивать защиту на:

- Организационном уровне;
- Программном уровне;
- Техническом уровне.

5. Объекты защиты

5.1 Перечень информационных порталов

Данный перечень разрабатывается на основании обследования информационной системы колледжа.

5.2 Перечень физических объектов защиты:

- Рабочая станция администратора системы;
- Серверы баз данных;
- Обрабатываемые данные управлений колледжа, не подлежащие для публичного доступа;
- Программные и аппаратные средства обработки информации;
- Действующая система защиты;
- Каналы обмена данными;
- Локальные вычислительные сети.

6. Классификация пользователей системы информационной безопасности

Пользователь – лицо, использующее информационную систему и результаты её работы. Все выделенные пользователи имеют доступ к ресурсам информационной системы в соответствии с определенными правилами и обязанностями. Пользователей учреждения можно разделить на:

- Руководство – сотрудники колледжа, обеспечивающие выполнение правил и принципов существующей стратегии информационной безопасности;

- Администратор информационной системы – сотрудники колледжа, конфигурирующие, внедряющие дополнительные модули и контролирующие информационную систему;
- Администратор информационной безопасности – сотрудники колледжа, обеспечивающие целостность ресурсов, циркулирующих в информационной системе;
- Пользователи информационной системы – лица колледжа (персонал управлений, преподаватели и сотрудники), эксплуатирующие информационную систему и имеющие идентификационные данные для доступа к разрешенным данным.

7. Требования к функционалу в соответствии с классом защищенности

7.1 Подсистема управления доступом

- Должны быть реализованы механизмы аутентификации пользователя при попытке входа в информационные службы;
- Основные атрибуты пользователя: идентификатор, профиль и управление/отдел/подразделение;
- Основные права доступа: чтение, запись, выполнение;
- Атрибуты пользователя не должны распространяться;
- Права доступа имеют только авторизованные пользователи;
- Пользователи имеют доступ к рабочим станциям в соответствии с регламентом учреждения;
- Управление потоками данных осуществляется в соответствии с грифом конфиденциальности данных.

7.2 Подсистема обеспечения целостности

Должно обеспечиваться состояние неизменности серверов, системного и программного обеспечения. В качестве средств обеспечения целостности данных можно выделить:

- Авторизация и аутентификация пользователей информационной системы с целью обеспечения безопасности данных;

- Шифрование (повышает уровень защиты данных, но усложняет процесс разграничения доступа);
- Проведение аудита позволяет постоянно контролировать объекты информационной системы;
- Средства резервного копирования позволяют восстановить данные в результате сбоя или отказа технических средств;
- Фильтрация входных данных с целью выявления SQL – инъекции с шифрованием паролей;
- Физическая безопасность (контроль территории, пропускной режим, контроль помещений с техническими средствами системы);

Все меры безопасности должны проводиться под руководством администратора безопасности.

7.3 Подсистема регистрации и учета

Обеспечивает регистрацию входа/выхода субъектов доступа в систему/из системы; Осуществление контроля над исполняемыми программами и процессами, функционирующими с защищенными данными; регистрация попыток доступа к программным средствам. Основными параметрами являются:

- Дата и время;
- Наименование программы, к который запрашивается доступ;
- Результат действия (успешный/неуспешный);
- Ключ, идентифицирующий субъект во время доступа.

8. Требования к организационному обеспечению

8.1 В соответствии с выявленными угрозами, необходимо провести ряд организационных мер, направленных на расширение знаний персонала в области информационных технологий. Работа с сотрудниками:

– при получении прав для доступа к информационной системе персонал должен получить от администратора информацию о методах и средствах защиты;
– если сотрудник колледжа не обладает знаниями принципов и средств защиты информации, он не имеет доступа к системе;
– инструкция доступа к объектам и допуска к ресурсам информационной системы колледжа;
– введение средств дистанционного обучения персонала;
– изучение угроз, связанных с действиями сотрудников;
– информирование сотрудников управлений/отделов о запрете разглашения конфиденциальной информации, циркулирующей в соответствующем управлении/отделе;
– информирование сотрудников о запрете разглашения и передачи идентификационных данных пользователя для доступа к служебным системам другим лицам;
– соблюдение пользователем правил доступа к информационной системе колледжа;
– определение ответственность за нарушение политики информационной безопасности колледжа.

8.2 Фиксирование происшествий:
– программными или иными способами оперативное выявление происшествия;
– устранение источника угрозы;
– определение контрмер и их последующая реализация при согласовании с системным администратором и администратором информационной безопасности колледжа;
– анализ ущерба, причиненного реализованной угрозой;
– анализ угрозы и создание плана действий, которые в последующем позволят избежать данной угрозы.

Настоящая политика разработана в соответствии с Руководящим документом 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».[1]

Вывод по главе 2

Основные выводы о способах использования рассмотренных выше средств, методов и мероприятий защиты, сводится к следующему:

1. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации.

2. Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.

3. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.

4. Необходимо осуществлять постоянный контроль функционирования механизма защиты.

[1] Руководящий документ 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»

ЗАКЛЮЧЕНИЕ

ГБПОУ «Южно-Уральский Государственный Технический Колледж» - это динамично развивающееся образовательное учреждение с постоянно обновляющейся материально-технической базой, с учебным хозяйством.

Использование современных технологий управления информацией на основе связанных между собой систем управления базами данных, позволяет осуществлять подобные операции в автоматическом режиме. Вмешательство человека требуется только на этапах ввода исходной информации и формирования запроса на предоставление информации. В то же время, невозможно построить универсальную систему, которая вмещала бы в себя все существующие на сегодняшний день возможности и функции управления информацией. Одним из вариантов решения данной проблемы является организация единого операционного пространства с помощью специализированной электронной оболочки, способной интегрировать различные программные компоненты и виды данных. К рассматриваемым видам данных следует отнести: бумажные документы, файлы данных различных форматов, электронные документы, аудио и видео материалы, базы данных, приложения для работы с электронными документами, информационные ресурсы Интернет и другие. В частности, всякая информационная система, для которой определены механизмы автоматического входа-выхода, также может рассматриваться как информационный ресурс. Каждое учебное заведение имеет свои особенности и механизмы управления, которые необходимо учитывать при создании системы.

В ходе данной работы рассмотрены основные нормативные документы, регулирующие правовые отношения в области защиты информации, приведены сведения о возможных угрозах безопасности информационной системе, в том числе подробно приведена и рассмотрена характеристика угроз несанкционированного доступа. При рассмотрении угроз, особое внимание уделялось классификации нарушителей безопасности, поскольку они выполняют

доминирующую роль в нарушении безопасности информационной системе.

Особое внимание уделено основным компонентам для построения защищённой информационной системы. Подробно рассмотрены организация хранения информации в базе данных, классификация программного обеспечения и основные средства защиты локальной сети, приведены организационные меры защиты.

Единого рецепта, обеспечивающего 100% гарантии сохранности данных и надёжной работы сети, не существует. Однако создание комплексной, продуманной концепции безопасности, учитывающей специфику задач конкретной организации, поможет свести риск потери ценнейшей информации к минимуму.

Практически любую информацию можно защитить, если пользователь пожелает это сделать, сохранив ее таким образом. В скором будущем компьютеры заменят многие привычные сейчас вещи, следовательно, нам придется доверить компьютеру самое сокровенное, которое человек никогда в жизни не доверит другому человеку, поэтому потребуется более надежная защита информации, такая, что тайны человека смогут лишь узнать, в крайнем случае, после его смерти. Человечество надеется, что компьютер станет другом, которому можно будет сказать все, зная, что он никогда сам не раскроет их тайны.

Обеспечение информационной безопасности достигается только при комплексном использовании всех средств защиты информации - организационные, физические, социально-психологические мероприятия и программном - технические средства защиты. Исходя из проделанной работы можно сделать вывод, что программные средства защиты информации играют большую роль в обеспечении информационной безопасности образовательной организации.

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 инаправления 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 техническойкомиссии 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 [электронныйресурс] / 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 - Высшаяшкола 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 справилами 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 установленнымантивирусным 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 колледж.