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

Анализ системы обеспечения информационной безопасности в образовательной организации и разработка рекомендаций по ее совершенствованию

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

Проверка на объем заимствований:
84,93 % авторского текста
Работа рекомендована к защите
«1» сентября 2022 г.
зав. кафедрой АТИТ и МОТД
_____ В.В. Руднев

Выполнила:
Студентка группы ОФ-209-210-2-1
Череева Ольга Александровна
Научный руководитель:
Зав. каф. АТИТ и МОТД, к.т.н.
Руднев Валерий Валентинович

Челябинск, 2022

Содержание

ВВЕДЕНИЕ

Актуальность

Сегодня одной из основных функций образовательной организации становится обеспечение информационной безопасности (ИБ), направленное на сохранение триады ИБ: конфиденциальность, целостность, и доступность.

Обеспечение информационной безопасности представляет собой деятельность по созданию препятствий и предотвращению реализации угроз информационных ресурсов организации.

Отсутствие правильно выстроенной системы обеспечения безопасности в образовательной организации, может привести к потере информации, что приведет к большим издержкам материального характера, потере персональных данных сотрудников и обучающихся, ущерб для имиджа образовательной организации.

В отечественной и зарубежной литературе в настоящее время немалое внимание уделяется проблемам информационной безопасности [1]

Более подробно во второй половине XX века проблему исследования информационной политики, развития информационного пространства в Российской Федерации были рассмотрены в работах: Е.К. Грошевой, С.Г. Зайцева, А.В. Нагирной, В.П. Макаровой, Т.А. Меркуловой, П. В. Ревенкова, Т.Е. Телятник.

Особый вклад в исследование информационной безопасности в различных сферах общества, культуры, науки и техники, внесли такие ученые и исследователи, как А.Г. Баданов, А.В. Баранова, Е.Г. Белякова, В.К. Новиков, Е.Б. Маринкин, Ю.А. Павленко, Е.В. Слепцова, В.П. Шерстюк А.М., Яновский, и другие. В работах этих ученых сформулированы концептуальные положения о сущности и содержании категорий информационной безопасности, исследованы их взаимосвязи, обоснованы приемы и способы исследования информационной безопасности и различных составляющих системного подхода.

Важное значение с точки зрения объекта и предмета настоящего исследования имеют также работы А.В. Кульбы, А.С. Рябцева, К.В. Станиславчика, А.Б. Табакова, В.П. Шерстюка, В.Н. Ясенева.

В настоящее время, несмотря на большое количество работ по проблематике, следует отметить, что ее теоретическая изученность явно недостаточна, практические методики по формированию оптимального механизма информационной безопасности в образовательных организациях не соответствуют условиям реального времени. В работах отечественных и западных авторов превалирует односторонний подход в исследовании проблем информационной безопасности, рассматривается какая-то одна сторона из всего механизма информационной безопасности в организациях вообще.

Для того чтобы отразить подход организации к защите своих информационных активов необходимо разработать политику информационной безопасности, каждая организация должна осознать необходимость поддержания соответствующего режима безопасности и выделения на эти цели значительных ресурсов.

Политика информационной безопасности - свод документов, в которых рассматриваются вопросы организации, стратегии, методов и процедур в отношении конфиденциальности, целостности и доступности информационных ресурсов организации. Политика безопасности строится на основе *анализа рисков* - процесса определения угроз безопасности системы и отдельным ее компонентам, определение их характеристик и потенциального ущерба.

Конечная цель разработки политики информационной безопасности - обеспечить целостность, доступность и конфиденциальность для каждого информационного ресурса.

Таким образом, потребность в создании оптимальной системы обеспечения информационной безопасности, а также проработка вопроса использования более совершенных методов обеспечения информационной

безопасности образовательных организаций определили объект, предмет, цель и основные задачи исследования.

Цель исследования заключается в анализе существующей системы обеспечения информационной безопасности образовательной организации и совершенствовании системы для обеспечения и повышения информационной безопасности образовательной организаций.

Объектом исследования является система обеспечения информационной безопасности образовательной организации.

Предмет исследования: направления совершенствования системы обеспечения информационной безопасности образовательной организации - в ГБПОУ «Южно-Уральский государственный колледж».

Гипотеза исследования состоит в предположении о повышении эффективности системы обеспечения информационной безопасности образовательной организации при реализации программы рекомендаций по совершенствованию названной системы.

Реализация поставленной цели и проверка выдвинутой гипотезы в магистерской диссертации потребовала постановки и последовательного решения следующих взаимосвязанных задач:

1. Раскрыть сущность и содержание системы обеспечения информационной безопасности в образовательной организации.
2. Изучить объект защиты - ГБПОУ «Южно-Уральский государственный колледж», его структуру, информационные ресурсы и информационные потоки колледжа; проанализировать систему обеспечения информационной безопасности в ГБПОУ ЮУГК; выявить уязвимости в системе защиты информации.
3. Разработать рекомендации по совершенствованию системы информационной безопасности колледжа ГБПОУ «Южно-Уральский государственный колледж».
4. Привести экономическое обоснование эффективности предложенных мер совершенствования системы обеспечения

информационной безопасности колледжа ГБПОУ «Южно-Уральский государственный колледж».

Научная новизна проведенных исследований и полученных в работе результатов заключается в том, что показана возможность необходимого обновления существующей системы обеспечения информационной безопасности образовательного процесса в образовательной организации среднего профессионального образования путем реализации комплексной программы мер.

Практическая значимость: разработаны рекомендации по совершенствованию системы обеспечения информационной безопасности информационной безопасности колледжа ГБПОУ «Южно-Уральский государственный колледж», приведено экономическое обоснование предложенных мер.

Методологическую основу исследования составили законодательные и нормативно-правовые документы РФ, разработки в области обеспечения информационной безопасности, методы и способы построения процессов управления информационной безопасностью в целях повышения информационной безопасности в организациях, системный 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.

Структура магистерской диссертации: введение, три главы, выводы по главам, заключение, библиографический список, приложения.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

1.1 Сущность системы обеспечения информационной безопасности образовательной организации

Пересмотр и изменение содержания образования на всех уровнях, были обусловлены стремительным развитием процесса информатизации общества. Эти изменения ориентируются на профессиональную подготовку, выработку качественно новой модели подготовки обучающихся к жизни и деятельности в условиях информационного общества, а также формирования необходимых для этих условий личных качеств и навыков [43].

Информатизация образования является неотъемлемой составляющей формирования информационного общества в Российской Федерации и важным направлением развития всей системы российского образования на сегодняшний день [11].

К числу системообразующих направлений информатизации образования, следует отнести:

— расширение применения электронного обучения и дистанционных образовательных технологий при реализации образовательными организациями всех своих образовательных программ;

— расширение применения средств автоматизации деловых процессов, баз данных, информационно-коммуникационных технологий в практике управления образованием на всех уровнях управления, в том числе в каждой образовательной организации;

— создание цифрового учебного и просветительского контента, электронных учебников и учебных пособий, электронных информационно-образовательных сред и платформ, электронных учебных курсов,

обеспечивающих гражданам возможности получения образования в течение всей жизни вне зависимости от места их проживания;

— развитие методов и форм обучения и воспитания с применением электронного обучения и дистанционных образовательных технологий, включая расширение возможностей реализации образовательных программ исключительно средствами электронного обучения и дистанционных образовательных технологий, ориентированных на развитие интеллектуального потенциала обучающихся, на формирование умений самостоятельного приобретения необходимых знаний.

Оснащение образовательных организаций современными средствами информационных и телекоммуникационных технологий и использование их в качестве нового педагогического инструмента, позволяют существенным образом повысить эффективность образовательного процесса.

Наряду с этим образовательная организация становится более уязвимой к информационным атакам. Нередки случаи срыва занятий из-за отключения электропитания, «вирусной атаки» на файловую систему компьютеров или сети, сбоев в работе компьютеров и программ. В последние годы в образовательных организациях участились попытки несанкционированного получения информации, в том числе персональных данных педагогов и обучающихся [4].

С темпом роста количества информационных угроз в сети Интернет, изменения нормативно-правовой базы и методов обеспечения ИБ становится актуальным вопрос обеспечения информационной безопасности в образовательной организации. Главным условием в работе образовательной организации является обеспечение бесперебойной работы и сведение к минимуму ущерба от событий, таящих угрозу информационной безопасности.

Информация и обеспечивающие ее системы, и сети являются ценными ресурсами образовательной организации, которым угрожают такие угрозы как:

— вредоносное программное обеспечение;

— вандализм;

— ошибки пользователей;

— кража оборудования;

— потеря данных;

— поломка оборудования;

— перепады напряжения;

— аппаратные и программные сбои.

Противодействовать такой тенденции можно, создав в образовательной организации систему обеспечения информационной безопасности (СОИБ), которая должна отражать основные компоненты информационной безопасности: конфиденциальность, целостность, доступность (рисунок 1).

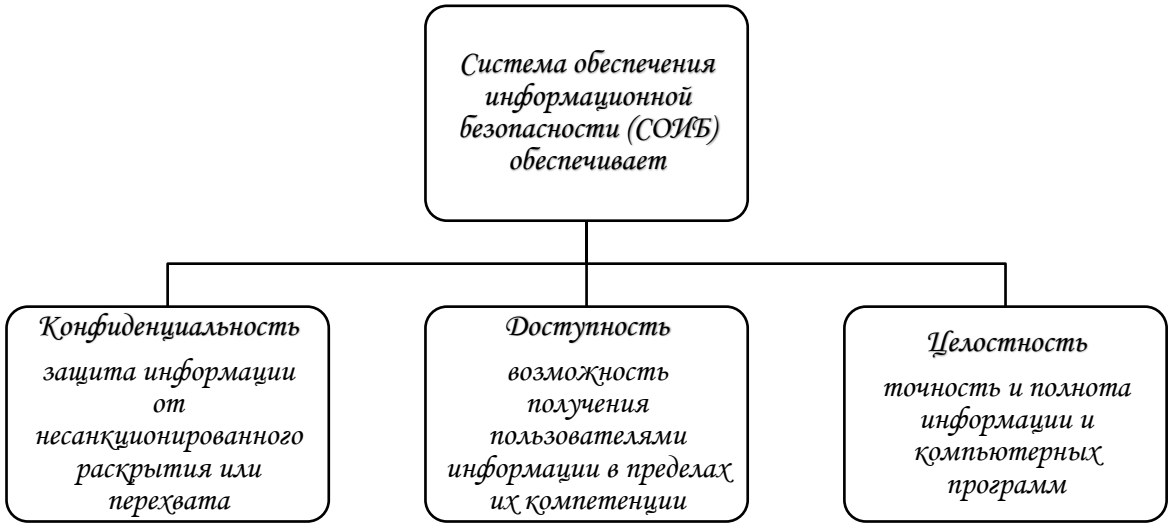

Рисунок 1 – Компоненты системы обеспечения информационной безопасности

При построении СОИБ следует учитывать следующие аспекты:

– безопасность информации может быть обеспечена при комплексном использовании всего арсенала имеющихся средств защиты организации;

– никакая система защиты информации не может обеспечить требуемого уровня безопасности информации без соответствующей подготовки пользователей и соблюдения ими установленных правил в организации;

– система безопасности должна постоянно совершенствоваться.

Построение СОИБ организации может происходить по следующему алгоритму (рисунок 2).

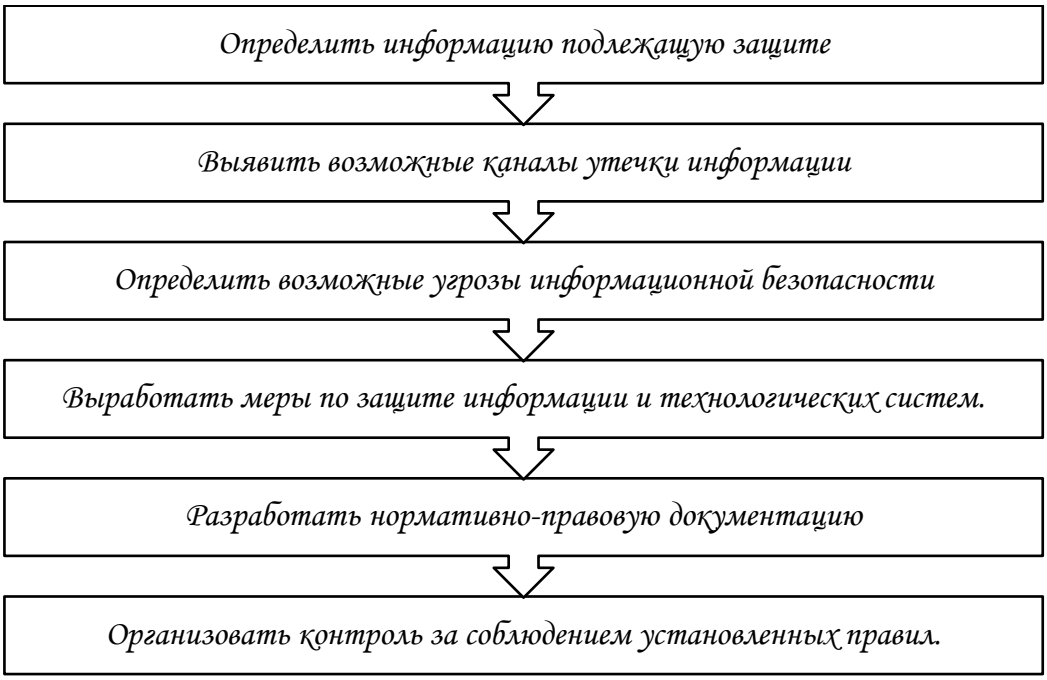

Рисунок 2 – Алгоритм построения СОИБ

При таком подходе система будет направлена на предупреждение, своевременное выявление, обнаружение, локализацию и ликвидацию информационных угроз.

Важную роль в повышении информационной безопасности играет независимый аудит. Он позволяет выявить уязвимые места в системе,

возможные каналы утечки информации, а также объективно оценить режим информационной безопасности. Грамотно проведенный аудит позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание системы безопасности образовательной организации.

Таким образом, можно сказать, что построение системы обеспечения информационной безопасности образовательной организации становится одним из основных видов его деятельности. Без использования новых подходов, поиска современных форм и способов обеспечения ИБ образовательной организации решить эти задачи защиты информации будет невозможно.

1.2 Характеристика угроз информационной безопасности в образовательных организациях

Спецификой СОИБ в образовательных организациях является состав характерных информационных угроз. Сегодня в образовательной организации необходимо не только обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений, но и гарантировать невозможность доступа в стены образовательной организации любой пропаганды, предполагающей воздействие на сознание обучающихся [6].

Наличие интернета в организации уже является угрозой информационной безопасности, и указывает на необходимость построения полноценной системы защиты информации от существующих виртуальных угроз и создании единой политики обеспечения информационной безопасности в образовательном организации [16].

В соответствии с ГОСТ Р 50922-2006 «Угроза безопасности информации» представляет собой совокупность условий и факторов,

создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Угрозам ИБ в образовательной организации могут подвергаться следующие группы объектов:

— оборудование;

— программное обеспечение;

— информация в любом её виде;

— подростки;

— сотрудники организации.

Так как в образовательных организациях чаще всего встречаются угрозы преднамеренного характера, то можно их классифицировать по методам воздействия на информацию (рисунок 3).

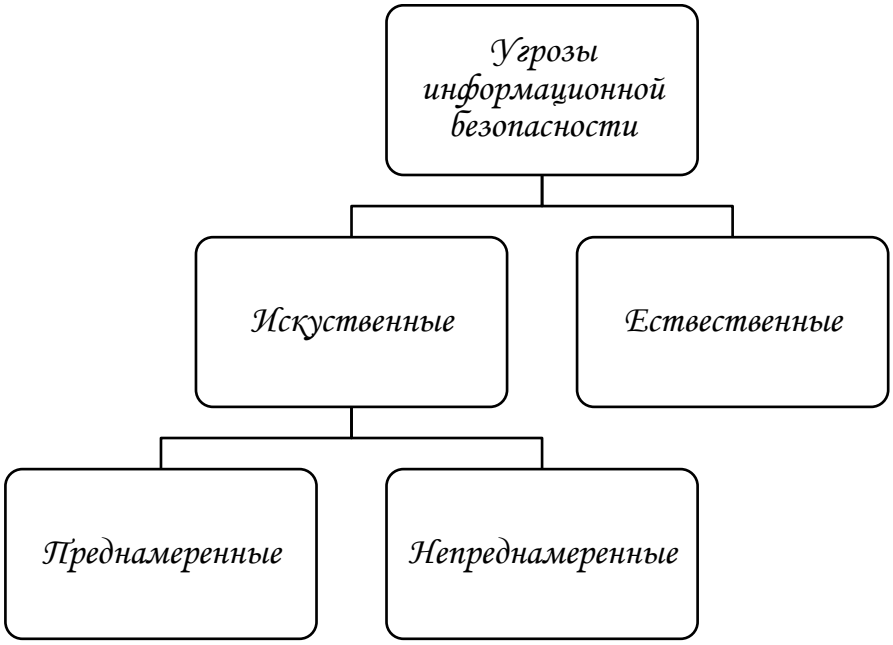

Рисунок 3 – Виды угроз ИБ по методам воздействия на информацию

По методам воздействия на информацию угрозы подразделяются на естественные, которые вызваны воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от действий человека и искусственные, вызванные воздействием на информационную сферу человеком. В свою очередь

искусственные угрозы состоят из преднамеренных, то есть умышленное нарушение информационной безопасности и непреднамеренных, связанных с незнанием или пренебрежением правил информационной безопасности.

Угрозами непреднамеренного характера оказывают временное воздействие и в большинстве случаев результаты их реализации предсказуемы, что позволяет достаточно эффективно и быстро устранить их подготовленным персоналом.

Преднамеренные угрозы являются более опасными так как результаты их реализации невозможно предвидеть. Чаще всего они могут исходить от любого субъекта учебного процесса (студент, сотрудник, обслуживающий персонал), но иногда от сторонних субъектов (конкуренты, хакеры). Рассмотрим угрозы, которым чаще всего подвержены образовательные организации (рисунок 4).

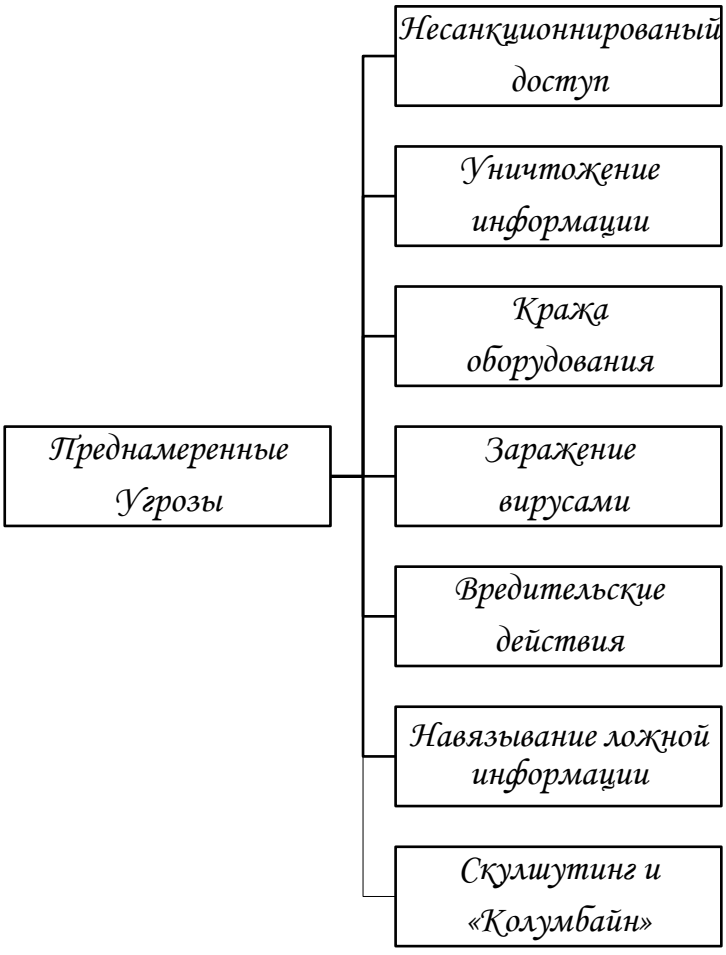

Рисунок 4 –Угрозы ИБ в образовательной организации

Несанкционированный доступ к информации может быть осуществлен случайным образом, в результате чего нарушаются аспекты информационной безопасности. Сюда следует отнести получение доступа к электронному журналу, удаление персональных данных, изменение отчетной документации. Неправильное уничтожение документации так же приводит к несанкционированному доступу.

Уничтожение информации в данном случае можно рассматривать умышленные действия, направленные на удаление персональных данных, архивов, удаление информации. Поджог или несоблюдение техники безопасности сотрудниками.

Кража. Если говорить о краже, то воруют главным образом небольшие по габаритам аппаратные средства, такие как: мониторы, клавиатура, модемы, кабели, информационные носители, в частности флешкарты, а также различное другое имущество. По мнению многих специалистов именно кража является основной проблемой информационной безопасности. Кража носителя информации будет являться следствием утечки информации из организации.

Заражение вирусным программным обеспечением может быть организованно с целью вывода из строя системы организации, или с целью мошеннических действий. Осуществляется это через уязвимости в системе безопасности операционных систем и в программном обеспечении. Наличие уязвимостей позволяет изготовленному злоумышленником сетевому червю или троянской программе проникнуть в компьютер-жертву и самостоятельно запустить себя на исполнение. Ещё одним из способов заражения будет внедрение вредоносного кода через веб-страницы. Пользователь заходит на заражённую страницу срабатывает скрипт-программа, которая через уязвимость закачивает заражённый файл на компьютер и запускает его там на выполнение.

Вредительские действия. Проявляются в самых различных формах подразделяясь на: явные, когда можно увидеть результат, например

фантики внутри системного блока, пролитая вода, вследствие несоблюдения техники безопасности, а также скрытые, жевательная резинка внутри системного блока и других аппаратных систем. По большей части исходят от обучающихся, так как в силу возраста подросткам иногда сложно себя контролировать поэтому в такие периоды они могут сломать или повредить оборудование и т.д.

Навязывание ложной информации и отрицательное влияние на психику обучающихся. Свободный доступ в сеть Интернет открывает для подростков огромное количество информации, где помимо обучающих и развивающих ресурсов, также присутствуют и ресурсы с нежелательной информацией, а также чрезмерное использование обучающимися социальных сетей не по назначению могут привести к разрушению нормального образовательного процесса обучения.

Скулшутинг и «Колумбайн». Это вооруженное нападение обучающегося или стороннего человека внутри образовательной организации. Данная угроза, направленная против безопасности личности, стремительно набирает обороты в силу нестабильности подростковой психики, под чрезмерным влиянием огромного количества информации и неспособности критически мыслить, а также и недостаточной СОИБ в образовательных организациях, где чаще всего отсутствует должная физическая защита объекта. В данном случае это характерная угроза, нарушает Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», главу 3 пункта 26 согласно которой одним из национальных приоритетов страны является «сбережение народа России и развитие человеческого потенциала»

Вышеперечисленные угрозы встречаются чаще всего в образовательных организациях и являются потенциально опасными, принося существенный материальных и нематериальный ущерб для организации в целом.

Выводы по Главе 1

Информатизация образования является неотъемлемой составляющей формирования информационного общества, но и приводит к тому, что образовательная организация становится уязвимой к информационным атакам.

С темпом роста количества информационных угроз, изменения нормативно-правовой базы и методов обеспечения информационной безопасности становится актуальным вопрос обеспечения ИБ в образовательной организации, при этом главным условием должно стать обеспечение бесперебойной работы и сведение к минимуму ущерба от событий, таящих угрозу информационной безопасности.

Информация и обеспечивающие ее системы, и сети являются ценными ресурсами образовательной организации, которым угрожают такие угрозы как: заражение компьютерными вирусами, вандализм, ошибки пользователей, хищение оборудования и так далее. Противодействовать такой тенденции можно, создав в образовательной организации систему обеспечения информационной безопасности (СОИБ), которая в свою очередь должна отражать основные аспекты информационной безопасности: конфиденциальность, целостность, доступность.

Спецификой СОИБ в образовательных организациях является состав характерных угроз. В образовательной организации необходимо не только обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений, но и гарантировать невозможность доступа в стены образовательной организации любой пропаганды, предполагающей воздействие на сознание обучающихся.

В соответствии с ГОСТ Р 50922-2006 «Угроза безопасности информации» представляет собой совокупность условий и факторов,

создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Образовательная организация чаще всего подвержена угрозам преднамеренного характера, которые могут быть реализованы как внутри, так и вне организации. Преднамеренные угрозы являются более опасными так как результаты их реализации невозможно предвидеть. Чаще всего они могут исходить от любого субъекта учебного процесса (студент, сотрудник, обслуживающий персонал), но иногда от сторонних субъектов (конкуренты, хакеры).

К ним относятся такие угрозы как: уничтожение информации, кража и преднамеренная порча оборудования, заражение вирусным программным обеспечением, вредительские действия, навязывание ложной информации и отрицательное влияние на психику обучающихся, скулшутинг и «Колумбайн».

Вышеперечисленные угрозы встречаются чаще всего и являются потенциально опасными для любой образовательной организации, принося существенный ущерб для информационной системы и организации в целом.

ГЛАВА 2. АНАЛИЗ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ГБПОУ «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ КОЛЛЕДЖ»

2.1 Общие сведения об ГБПОУ «Южно-Уральский государственный колледж»

ГБПОУ «Южно-Уральский государственный колледж» является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа.

Главной целью и направлением деятельности образовательной организации является повышение качества знаний и уровня профессиональных компетенций выпускников колледжа за счет разработки, создания и внедрения инновационных образовательных технологий, основанных на системе электронного обучения E-Learning, электронных учебно-методических комплексах, а также компетентностном подходе. Данные технологии и формы обучения позволили повысить качество профессиональной подготовки, прежде всего практического обучения, и сделали выпускников колледжа востребованными на рынке труда. На протяжении многих лет «Южно-Уральский государственный колледж» занимается разработкой и внедрением в учебном процессе интенсивных информационных образовательных технологий, основанных на широком использовании компьютерной и коммуникационной техники, электронных обучающих программ, проектной культуры. Это позволяет активно решать проблемы доступности, эффективности и качества профессиональной подготовки современных специалистов для отраслей предприятий России.

Педагоги колледжа имеют опыт практической работы и глубокую теоретическую подготовку, необходимую для успешной реализации

профессиональных образовательных программ. Среди них — кандидаты наук, заслуженные работники образования Российской Федерации, преподаватели высшей категории.

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

— Информационных технологий и экономики (ул. Курчатова, д.7).

— Промышленной автоматики (ул. Доватора, д.38).

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

В образовательной организации обоснованно распределены функции структурных подразделений учреждения, а также должностные обязанности его работников на основе сочетания принципов единоначалия и коллегиальности.

ГБПОУ «ЮУГК» возглавляет директор, обеспечивающий системную работу организации, определяющий стратегию, цели, задачи и программу его развития, обеспечивающий соблюдение законности в деятельности колледжа, а также осуществляющий иные функции и полномочия, соответствующие уставным целям.

По основным направлениям деятельности управление осуществляется заместителями директора, координирующими работу структурных подразделений ГБПОУ «ЮУГК».

В колледже действуют предметно-цикловые комиссии, деятельность, осуществляющих образовательную деятельность по родственным учебным дисциплинам/модулям, в том числе по совместительству. ГБПОУ «ЮУГК» уделяет большое внимание компьютеризации образовательного процесса.

В колледже оборудованы специализированные лаборатории и студии, для всех направлений обучения.

Для оптимизации учебной деятельности организация владеет всеми необходимыми современными программными пакетами: Microsoft Visio, Cisco Packet Tracer, Microsoft Visual Studio, Dev C++, SASM, Microsoft SQL Server 2017, SQL Management Studio, Android Studio, CorelDraw X4, Atom, Notepad++, Corel Photo Paint, Blender, Unity, Adobe Flash Professional CS6, Open Server, Oracle Virtual Box, IntelliJ IDEA, JDK, Free Pascal, Inkscape, GIMP, 1С Предприятие.

Используются 33 электронных курса по учебным дисциплинам, междисциплинарным курсам и профессиональным модулям.

При подготовке специалистов по всем реализуемым основным образовательным программам используются электронные системы обучения (электронные учебники, электронные таблицы, презентации отдельных тем и предметов, лабораторные и практические работы, обучающие программы на дисках, тестовый контроль).

Система управления ГБПОУ «ЮУГК», обеспечивающая реализацию образовательных программ, являющихся основной целью деятельности учреждения, отвечает требованиям действующего законодательства Российской Федерации и Челябинской области. Организационная структура управления ГБПОУ «Южно-Уральский государственный колледж» (рисунок 5).

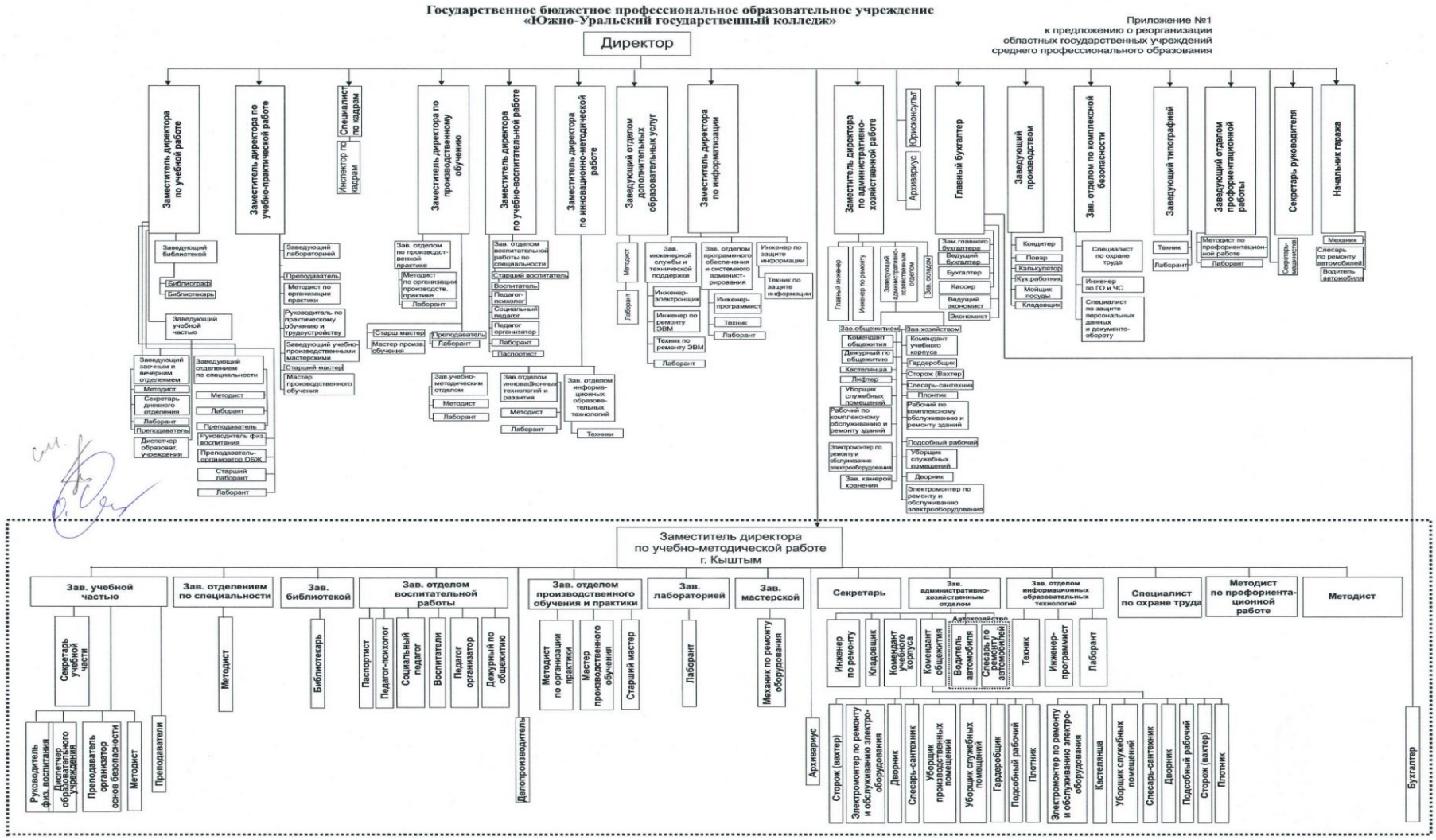

Рисунок 5 – Организационная структура управления ГБПОУ «Южно-Уральский государственный колледж»

2.2 Анализ системы обеспечения информационной безопасности ГБПОУ «ЮУГК»

Одной из основополагающих составных частей успешной деятельности образовательной организации является развитие системы обеспечения информационной безопасности и защиты информации [20]. Необходимость проведения мероприятий в этой области объясняется большим объёмом информации, находящимся в различных представлениях на территории колледжа.

Главной целью СОИБ является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы ГБПОУ «ЮУГК».

Для обеспечения учебного процесса цикловые комиссии и отделы ГБПОУ «ЮУГК» оснащены персональными компьютерами и необходимой техникой. Для решения производственных и учебных задач в колледже организована локальная сеть на одновременную работу 678 компьютеров. Все персональные компьютеры оснащены лицензионным программным обеспечением, подключены к локальной сети и имеют доступ в сеть Интернет, через защищенное соединение. Узлы оптических линий оборудованы управляемыми коммутаторами. В каждом комплексе имеется своя локальная сеть (100/1000 Мбит/с), охватывающая учебные корпуса и общежития. Создана единая локальная сеть колледжа (оптоволокно). В комплексах все компьютеры подключены к сети Интернет со скоростью доступа до 100 Мбит/с. На программном уровне защиты используются различные для студентов и сотрудников домены.

В колледже организованна система электронного обучения – Moodle, она доступна для сотрудников и студентов колледжа, каждый имеет свой

индивидуальный пароль и логин, доступ к системе возможен с любых устройств. Портал построен на основе системы управления образованием (LMS). LMS позволяет управлять и распространять учебный материал и обеспечивать совместный доступ.

Открыт доступ к электронным образовательным ресурсам для студентов колледжа по сети Интернет, что позволяет использовать данные ресурсы в полном объеме.

Информационная система колледжа содержит огромное количество информационных ресурсов, зафиксированных на материальных носителях (информационное обеспечение хозяйственной деятельности, информация научно-технического характера, персональные данные сотрудников и обучающихся, базы данных организации, информация бытового характера о доступе к материальным товарам и услугам, обучающие ресурсы и т.д.), которые, в свою очередь, являются основным объектом защиты.

Информацией ограниченного доступа является:

— 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 колледжа ведется круглосуточное наблюдение через пост охраны. Мониторинг объекта осуществляется через систему

видеонаблюдения, которая установлена по периметру, а также в переходах образовательного комплекса и на главном, и со стороны запасных выходов. Вход на территорию осуществляется по персональным пропускам и студенческим билетам. Посетители имеют право прибывать на территории только в сопровождении сотрудника организации. В колледже осуществлена пожарно - охранная сигнализация и установлены соответствующие датчики. Аппаратные средства хранения информации (сервера) располагаются в отдельном помещении.

Политика безопасности, реализована на избирательном способе управления доступом. Применение избирательной политики, соответствует требованиям по информационной безопасности, разграничению доступа, подотчетности. Реализацией этой политики безопасности занимается системный администратор. Такое управление характеризуется заданным администратором множеством разрешенных отношений доступа.

В качестве программного средства защиты от вредоносного программного обеспечения используется антивирусное решение «Kaspersky Endpoint Security для Windows», которая отвечает требованиям надежности, качества и системы защиты, предъявляемым для защиты корпоративных сетей.

Технически информационная безопасность и защита информации осуществляется при помощи системы паролей для доступа к ресурсам информационной системы разного уровня. Прежде всего, это пароль входа пользователя в операционную систему его рабочего места. Ввод этого пароля открывает пользователю доступ к ресурсам данного компьютера и к документам, хранящимся на нем. Политика безопасности настроена таким образом, чтобы пользователь не обладал полным правом на своем рабочем месте и не мог, например, установить вредоносное программное обеспечение или программы по копированию информации. Ограничение прав дает гарантию защищенности данных.

Для обучающихся не предусмотрены различные пароли для входа в операционную систему, есть единый пароль и логин для всех колледжа, для сотрудников и педагогов предусмотрена замена пароля 1 раз в месяц.

Когда пользователь вводит свой пароль для входа в операционную систему, он получает доступ не только к ресурсам данного компьютера, но и к ресурсам локальной компьютерной сети. Это возможно в том случае, если пользователь входит на компьютер как доменный или сетевой пользователь. В этом случае отнестись к разграничению прав пользователей в сети нужно еще более внимательно. Права сетевого пользователя настроены таким образом, чтобы дать ему возможность беспрепятственно работать со своими документами, но при этом ограничить доступ к документам, прав на работу с которыми у него нет, либо это только права на просмотр. В этом случае решается одновременно задача защиты данных от несанкционированного доступа и от случайной их порчи. Прерогативой распределения прав пользователей обладает системный администратор. Он разграничивает права пользователей по доступу к документам и приложениям как в сети, так и на локальных компьютерах.

Парольная защита доступа осуществляется в информационной системе «1С: Предприятие 8.3». Данная ИС имеет в своем составе механизм ведения списка пользователей и разграничения их прав доступа к данным. В результате можно гибко настроить доступ пользователей скрыв от несанкционированного доступа и от возможности случайной порчи данных, доступа к которым у пользователя нет. Обязанность распределения прав доступа пользователей лежит на системном администраторе колледжа.

Для того чтобы понять, насколько хорошо организованна система обеспечения информационной безопасности колледжа, была проведена комплексная проверка состояния безопасности информационных систем

ГБПОУ «ЮУГК» и выявлены следующие уязвимости системы и несоответствия.

Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторам и нежелательного их воздействия на защищаемую информацию [15]. Источники угроз используют уязвимости для нарушения безопасности информации. Кроме того, возможны действия источников угроз по активизации тех или иных уязвимостей, не связанных со злым умыслом [13].

Нормативное регулирование системы информационной безопасности ГБПОУ «ЮУГК» представлено документом «Политика безопасности», которая определяет цели и задачи СОИБ и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области ИБ, которыми руководствуются работники образовательной организации при осуществлении своей деятельности.

Основной целью «Политики безопасности» является защита информации при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных.

Ознакомиться с нормативной документацией в области информационной безопасности можно непосредственно в организации. Политика безопасности разработана в соответствии с:

— Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».

— Федеральным законом от 27.07.2006 № 152-ФЗ «О

персональных данных».

— Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

— Федеральным законом от 29.12. 2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

— Приказом Министерства связи и массовых коммуникаций РФ от 16 июня 2014 г. № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

— Указом Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».

— Постановлением Правительства РФ от 01.11.2012. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

— Постановлением Правительства от 15.09.2008 РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

— Приказом ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и иными нормативными правовыми актами в сфере защиты информации.

Выполнение требований «Политики безопасности» является обязательным для всех структурных подразделений, ответственность за соблюдение информационной безопасности несет каждый сотрудник ГБПОУ «ЮУГК».

Проанализировав образовательную организацию, удалость выявить следующие уязвимости:

1. *Отсутствие сертификата SSL*. Сайт колледжа активно используется студентами и родителями, через сайт осуществляется вход в «Систему электронного обучения», где находятся образовательные материалы колледжа, а также «Электронный журнал», в котором отражена успеваемость студентов. На сайте расположено расписание и информация для сторонних организаций (портфолио педагогов, нормативные документы). Но отсутствие сертификата SSL может вызвать проблемы. Адресная строка браузера сейчас выглядит следующим образом (рисунок 6).

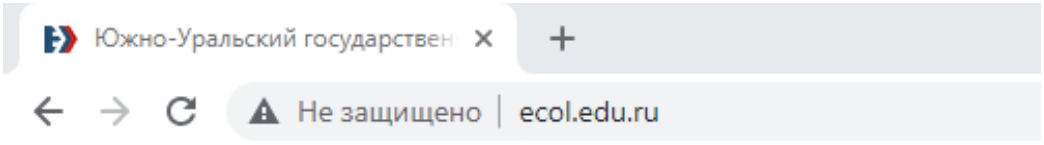

Рисунок 6 – Адресная строка браузера

В данном случае это может быть просто сбой даты на компьютере или же вирусное программное обеспечение, с помощью которого злоумышленник может завладеть персональными данными пользователей или нарушить свойство доступности информации на сайте.

2. *Несанкционированный доступ на территорию*. На входе осуществляется термометрия сотрудников, обучающихся колледжа, при этом студент должен предъявить на входе студенческий билет. Уязвимостью является то, что никто не сверяет этот студенческий билет с оригиналом, и не ведет учет лиц, попадающих на территорию колледжа, потенциальный злоумышленник может пройти под видом родителя студента, либо пройти под видом студента, предъявив любой документ вахтеру.

3. *Неквалифицированный персонал*. Следует выделить отдельным пунктом данную уязвимость, которая может привести к потере важной документации, краже оборудования, разглашению персональных данных и

т.д. Если мы говорим об обслуживающем персонале (уборщица, электрик, дворник, сантехник), то они спокойно перемещаются по территории колледжа и имеют доступ ко всем помещениям организации, уборка кабинетов происходит после занятий, поэтому сложно отследить их действия. Сюда же относится незнание базовых правил информационной безопасности педагогами и сотрудниками колледжа, которые могут привести к сбою в работе информационной системы. Невнимательность обучающихся при авторизации приводит к блокировке всей локальной сети, что ведет за собой нарушение доступности.

4. *Отсутствие видеонаблюдения в учебных лабораториях*. В колледже есть система видеонаблюдения, но она направлена на территорию при колледже. Хотя отсутствие видеонаблюдения в компьютерных классах оправдано, тем его что наличие может нарушать права несовершеннолетних обучающихся, но это приводит к тому, что перечисленные выше уязвимости приводят к более серьезным угрозам. Стоит отметить, что при случаях кражи или доступа на внутрь организации посторонних лиц будет тяжело опознать злоумышленника, так как видеонаблюдение на входе может быть не достаточным для опознания источника угрозы.

9. *Некорректная работа программного обеспечения*, приводящая к потере или порче данных из-за: ошибок в прикладном или сетевом программном обеспечении; заражения систем компьютерными вирусами.

10. *Технические сбои оборудования*. Могут быть вызваны отключением электропитания; отказом дисковых систем и систем архивации данных; нарушением работы серверов, рабочих станций, сетевых карт, модемов, неправильная эксплуатация оборудования.

11. *Отсутствие в общем доступе документов*, регулирующих информационную безопасность в организации.

Выводы по Главе 2

ГБПОУ «Южно-Уральский государственный колледж» является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа.

Главная цель и направление деятельности ГБПОУ «Южно-Уральский государственный колледж» – повышение качества знаний и уровня профессиональных компетенций выпускников колледжа за счет разработки, создания и внедрения инновационных образовательных технологий, основанных на E-Learning, электронных учебно-методических комплексах, компетентностном подходе. Данные технологии и формы обучения позволили реально повысить качество профессиональной подготовки, прежде всего практического обучения, и сделали выпускников колледжа востребованными на рынке труда.

Система управления ГБПОУ «ЮУГК», обеспечивающая реализацию образовательных программ, являющихся основной целью деятельности учреждения, отвечает требованиям действующего законодательства Российской Федерации и Челябинской области.

Одной из основополагающих составных частей успешной деятельности образовательной организации является развитие системы обеспечения информационной безопасности и защиты информации. Необходимость проведения мероприятий в этой области объясняется большим объёмом информации, находящимся в различных представлениях на территории колледжа.

В ходе анализа ГБПОУ «ЮУГК» были выявлены следующие уязвимости:

— отсутствие сертификата SSL/TLS на сайте колледжа из-за чего невозможно выполнить защищённое соединение с шифрованием данных, что существенно уменьшит шансы злоумышленнику провести атаку на целевой хост;

— контрольно-пропускной режим, на входе которого никто не проверяет этот студенческий билет, поэтому в колледж может пройти кто угодно под видом студента, предъявив документ вахтеру;

— участники образовательного процесса, которые могут действовать в своих интересах;

— незнание базовых правил информационной безопасности педагогами и сотрудниками колледжа, которые могут привести к сбою в работе информационной системы;

— отсутствие видеонаблюдения в учебных лабораториях;

— некорректная работа программного обеспечения, приводящая к потере или порче данных;

— технические сбои оборудования;

— отсутствие в общем доступе нормативно-правовой документации, регулирующей информационную безопасность в организации.

ГЛАВА 3. РАЗРАБОТКА ПРОГРАММЫ РЕКОМЕНДАЦИЙ ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ГБПОУ «ЮУГК»

3.1 Мероприятия и средства по совершенствованию системы информационной безопасности колледжа

Проведя исследование объекта, удалось выделить характерные виды угроз, с помощью кого или чего может произойти реализация, а также меры защиты, которые следует организовать это представлено в таблице 1.

Таблица 1 – Угрозы ГБПОУ «ЮУГК»

Угроза	Реализация	Меры защиты
Естественные угрозы (природные явления)		
Грозы	Погодные явления	Резервное копирование данных
Внутренние случайные угрозы (персонал)		
Неумышленный запуск вредоносных программ	Запуск сотрудником вредоносного программного обеспечения	Наличие антивирусного программного обеспечения, обучение персонала, разграничение прав доступа
Модификация, удаление или блокирование информации в результате неумышленных действий	Непреднамеренные действия сотрудников	Резервное копирование важной информации по расписанию, настройка теневого копирования на рабочих станциях, обучение персонала правилам работы при обработке информации
Неумышленное разглашение информации ограниченного доступа в результате разговора с персоналом фирмы	Ведение разговоров сотрудниками организации в присутствии посторонних лиц	Инструктаж сотрудников с записью под подпись об ответственности.
Неумышленная утрата или порча документированной информации	Халатное отношение персонала к своим обязанностям	Наличие ответственности в трудовом договоре; хранение важных документированной информации в сейфах

Продолжение таблицы 1

Угроза	Реализация	Меры защиты
Некорректное уничтожение бумажных носителей информации	Халатное отношение персонала к своим обязанностям; незнание о возможных потерях информации	Инструктаж сотрудников, обучение правилам документооборота
Внутренние преднамеренные угрозы (персонал)		
Хищение или копирование информации на бумажном или электронном носителе	Злоумышленные действия персонала при работе с электронными или бумажными документами	Наличие ответственности в трудовом договоре; хранение важных документированной информации в сейфах, инструктаж об ответственности
Несанкционированный доступ к серверам, ЛВС, рабочим станциям	Злоумышленные действия персонала.	Антивирусное ПО; парольная защита, запрещение неавторизованного доступа
Сговор со злоумышленником и помощь ему	Злоумышленные действия персонала	Наличие ответственности в трудовом договоре
Фото и видеосъемка документов	Злоумышленные действия персонала	Хранение важных документов в сейфах Наличие ответственности в трудовом договоре
Вандализм	Злоумышленные действия персонала и/или обучающихся колледжа	Резервное копирование данных инструктаж об ответственности Наличие ответственности в трудовом договоре
Внешние угрозы (злоумышленник)		
Физическое хищение или разрушение средств вычислительной техники	Проникновение в организацию; нарушение штатного режима функционирования СВТ	Сигнализация; Резервное копирование данных Хранение важных документов в сейфах
Несанкционированный доступ к серверам, ЛВС, рабочим станциям	Атака на сервера организации, коммутационное оборудовании и рабочие станции	Антивирусное программное обеспечение; резервное копирование; внутренние механизмы защиты операционной системы, межсетевого экрана.
Программные закладки	Перехват информации	Использование сертифицированного программного обеспечения; использование средств антивирусной защиты

Приведенные в таблице 1 меры защиты будут статичны, то есть следует их выполнять всегда, а, чтобы контролировать исполнение этих защитных мер необходимо проводить целенаправленные мероприятия по информационной безопасности, приведенные ниже.

Мероприятия по формированию и расширению компетентности в области информационной безопасности участников образовательных отношений:

1. *Сотрудники организации.*

Серьезным недостатком в образовательной организации является отсутствие взаимопонимания между специалистами отдела информационной безопасности, и пользователями информационной системы, отсюда следует отсутствие мотивации соблюдения информационной безопасности. Пользователи, в данном случае сотрудники должны понимать, как та или иная угроза безопасности может повлиять на организацию. Говоря о том, что действительно мотивирует сотрудников соблюдать правила информационной безопасности необходимо обратить внимание на общие подходы и методы к поддержанию мотивации у участников образовательного процесса:

1.1. Разместить на рабочих местах и информационных стендах плакаты, а на руки выдать краткие памятки и флаеры, пропагандирующие соблюдение правил информационной безопасности. Подразумевается, что, посмотрев на плакаты или печатные пособия, будут соблюдать основные правила информационной безопасности. Главное, чтобы они были доступны, кратки и понятны каждому.

1.2. Система штрафов и наказания, является достаточно действенным способом повышения мотивации, однако имеет ряд минусов, главным из которых – это то, что он не находит отклика у участников образовательного процесса. Все понимают, что необходимо соблюдать правила, но не потому, что это важно для них, а потому что их могут наказать.

1.3. Обучение, через курсы повышения квалификации. При проведении обучения, можно улучшить мотивацию сотрудников при условии, что занятия, им интересны. Необходимо заинтересовать сотрудников, показывать фильмы, презентации, приглашать специалистов в области информационной безопасности, делать практические отработки.

1.4. Дни, недели или месяцы, которые будут посвящены вопросам информационной безопасности. С помощью мероприятий, таких как семинары, круглые столы, вебинары, можно показать сотрудникам, почему важно соблюдать правила безопасности.

1.5. Нематериальная мотивация. Сюда можно отнести вознаграждения благодарственными письмами, грамотами, свобода высказывать свое мнение.

2. *Обучающиеся колледжа.* В качестве мероприятий для обучающихся предусмотрены классные часы, викторины, участие в Областных и Всероссийских конкурсах. Подготовка творческого задания, в рамках изучения дисциплины «Информационная безопасность», для формирования устойчивого понимания соблюдения основ безопасности (см. приложения 1-5).

3. *Родители.*

С родителями можно взаимодействовать следующим образом:

3.1. Проводить тестирование на знание правил информационной безопасности.

3.2. В рамках родительских собраний раздавать памятки об информационной безопасности детей

Организация пропускного режима.

Чтобы обеспечить безопасность в организации от проникновения посторонних лиц, в вестибюле колледжа устанавливается электронная проходная PERCo KT02.3 – турникет со встроенной системой контроля доступа Система «Электронная проходная PERCo-KT02.3» — готовое экономичное решение для организации контроля доступа на объект.

Электронная проходная КТ02.3 может применяться в составе систем повышения эффективности для организации контроля дисциплины труда и учета рабочего времени (рисунок 7).

Рисунок 7 – Электронная проходная PERCo КТ 02.3

Сотрудникам и обучающимся выдают электронные карты доступа (рисунок 8), данные которых заносят в память системы, после этого можно начинать работу.

Рисунок 8 – Электронная карта- доступа

Чтобы пройти через турникет, необходимо поднести свою карточку-пропуск к специальному табло на турникете. Наглядная индикация

позволяет безошибочно определить, куда поднести карточку, разрешен ли проход или запрещен (рисунок 9).

Рисунок 9 – Индикация турникета

Информация с карточки считывается автоматически, и, если карта зарегистрирована в системе, то турникет откроется для прохода.

Дополнительные возможности системы позволяют предотвратить проход через турникет по чужому пропуску. При поднесении карты к табло на компьютере охранника отображается фотография пользователя, которому была выдана эта карта (рисунок 10).

Рисунок 10 – Идентификация пользователя по электронной карте-доступа

Если карта утеряна, охранник может пропустить при помощи пульта дистанционного управления турникетом.

Все события фиксируются в энергонезависимой памяти системы, впоследствии их можно просмотреть.

Электронная проходная может быть дополнена ограждениями, которые предназначены для формирования зон прохода, выполнены в едином дизайне с турникетами различных моделей и легко интегрируются с ними. Конструкция прямых и поворотных патрубков позволяет создавать всевозможные конфигурации ограждения с поворотом секций на требуемый угол. Для освобождения прохода в экстренной ситуации устанавливается поворотная секция ограждения, снабженная шарнирным поворотным устройством. В менее критических ситуациях, используется ключ разблокировки турникета (рисунок 11, а) – планки при этом будут вращаться свободно. Дополнительно можно установить в турникете специальные складывающиеся планки «Антипаника» (рисунок 11, б), что еще увеличивает зону свободного выхода.

Рисунок 11 – Дополнительные функции электронной проходной: а – механическая разблокировка ключом; б – складывающиеся планки «Антипаника»

Электромеханические замки оптимально подходят для эксплуатации в учебных заведениях. При пропадании питания замки переходят в

открытое состояние, что позволяет применять их при наличии повышенных требований к гарантированному открытию двери.

В стандартном комплекте Электронной проходной поставляется бесплатное программное обеспечение для организации прохода сотрудников по бесконтактным картам.

Сайт колледжа

В качестве защитных мер для сайта колледжа можно перенести его на сервер CloudFlare — это сеть серверов по всему миру, к которой можно подключить свой сайт, чтобы увеличить скорость их загрузки и защитить от DDoS-атак. Cloudflare обеспечивает безопасность и надежность общедоступных ресурсов, а также защищает внутренние ресурсы: приложения за межсетевым экраном и устройства сотрудников.

Установка кондиционера в компьютерных классах.

Чтобы избежать технического сбоя аппаратуры необходимо поддерживать температурный режим помещения в пределах 20-24 °С, если в помещении с работающими ПК будет приближаться к 40, то жёсткий диск может быстро выйти из строя. Так же согласно СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» в оборудованных индивидуальными рабочими местами с персональным компьютером параметры температурного режима должны быть в пределах 18-24°С. [23].

Повышение температуры неблагоприятно сказывается на самочувствие обучающихся, что может привести таким угрозам как «ошибка пользователя» и т.д. Поэтому необходимо создавать благоприятные условия в учебной аудитории для этого можно установить систему кондиционирования. С ее помощью можно поддерживать такие параметры (температуры, влажности, чистоты, скорости движения воздуха). В данном случае установка кондиционера позволит значительно

в дальнейшем сэкономить средства, за счет правильной эксплуатации компьютерного оборудования.

В качестве оптимального варианта подойдет настенная сплит-система – это бытовые системы кондиционирования большой мощности, так как подходят для небольших аудиторий и классов (рисунок 12).

Рисунок 12 – Настенная сплит-система

Видеонаблюдение.

В рамках борьбы с терроризмом и ввиду того, что колледж – это публичное образовательное учреждение, законы Российской Федерации обязывают иметь камеры видеонаблюдения (на 1-ом этаже и по периметру территории). При этом согласие работников и посетителей не требуется, а расходы по установке камер несет руководство региона. Срок хранения записей – не менее 30 суток. А вот покупка и монтаж камер в других помещения не регламентируется законом. При этом необходимо согласие в письменном виде от родителей несовершеннолетних лиц, которые попадают в поле зрения камеры [21].

В РФ существует целый ряд нормативно-правовых актов, включающих нормы, регулирующие этот вопрос. К ним относятся:

— Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.

— Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ.

— Письмо Федерального агентства по образованию Министерства образования и науки Российской Федерации от 29 июля 2009 г. № 17-110 «Об обеспечении защиты персональных данных».

Во всех этих актах описывается как процедура ознакомления с видеозаписями, так и порядок осуществления видеонаблюдения в течение определенного периода времени.

Все нюансы обустройства системы видеонаблюдения в колледже, должны быть оговорены в положении, который принимается и будет действовать в ГБПОУ «ЮУГК». Но пока колледж не готов этим вкладывать средства в это мероприятие.

3.2 Оценка эффективности мероприятий по совершенствованию информационной безопасности в организации профессионального обучения

Оценка эффективности мероприятий информационной безопасности является сложной задачей, так как основана на субъективной точке зрения и нет универсальных методов для объективной оценки [32]. При этом затраты на обеспечение информационной безопасности следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной безопасности организации.

Перед подсчетом оценки эффективности предложенных мероприятий, необходимо произвести расчет затрат на комплекс мероприятий и оценить возможный ущерб от инцидентов нарушения информационной безопасности. Из анализа организации следует, что информация и обеспечивающие ее системы являются основными компонентами для бесперебойной работы в ГБПОУ «ЮУГК». Тут стоит

уточнить, что огромное количество информации не оцифровано и храниться в архивах в бумажном виде.

Чтобы оценить стоимость ущерба, было принято решение воспользоваться услугами аутсорсинговой компании, занимающейся восстановлением информации.

Итоговая стоимость информационных активов представлена в таблице 2.

Таблица 2 – Перечень информации, циркулирующей в ГБПОУ «ЮУГК».

Информационные активы ГБПОУ «ЮУГК»	**Сумма ущерба в рублях**
Персональные данные: сведения о студентах, преподавателях и т.д.	1 000 000
Служебная тайна: информация, содержащая сведения о финансах, производстве, управлении и других видах деятельности субъекта, разглашение которой может нанести экономический ущерб.	900 000
Профессиональная тайна - сведения, содержащие организацию учебной деятельности и процессов.	250 000
Информация о нормах, приказах, распоряжениях, связанных с охраной труда на предприятии	50 000
Всего:	2 200 000

Отдельным пунктом стоит выделить косвенный ущерб, в частности потеря имиджа образовательной организации, который может быть получен в результате террористических движений таких как «Колумбайн» или «скулшутинг».

Этот вид угроз характерен для образовательных организаций, и сегодня является одной из опасных угроз, направленных против безопасности личности. Оценить ущерб в денежном эквиваленте после реализации данной угрозы не представляется возможным, так как человеческие жизни бесценны.

Для предотвращения этих угроз были предложены мероприятия по совершенствованию системы. Затраты на их реализацию указаны в таблице 3.

Таблица 3 – Затраты на мероприятия по совершенствованию СОИБ в ГБПОУ «ЮУГК»

Методы и средства защиты	**Вид угрозы**	**Стоимость внедрения в рублях**	**Стоимость поддержки в год, в рублях**
Система контроля управления доступом	Несанкционированное проникновение в организацию и нарушение штатного режима функционирования организации	558 420	0
Установка кондиционера в компьютерных классах.	Технический сбой компьютерного оборудования	175 000	14 000
Сервер CloudFlare	Отсутствие сертификата SSL/TLS на сайте колледжа из-за чего невозможно выполнить защищённое соединение с шифрованием данных, что существенно уменьшит шансы злоумышленнику провести атаку на целевой хост	156 000	0
Мероприятия по формированию и расширению компетентности в области информационной безопасности.	Непреднамеренные действия сотрудников (ошибка пользователя, Ведение разговоров сотрудниками организации в присутствии посторонних лиц	125 000	0
ИТОГО:		1 014 420	14 000

Из вышеприведенной таблицы следует, что реализация мероприятий по совершенствованию системы обеспечения информационной безопасности ГБПОУ «ЮУГК» требует значительных денежных вложений, которые позволяют устранить выявленные уязвимости и предотвратить возможные угрозы.

Соотношение оценки затрат на внедрение мероприятий к возможному ущербу составляет 21% и является достаточным, чтобы поддерживать СОИБ ГБПОУ «ЮУГК» на необходимом уровне. Следует отметить, что нет идеальной системы, которая будет обеспечивать защиту на 100 %, в данном случае предложенные мероприятия позволяют приблизиться к отметке в 90%, при условии, что все в организации будут к этому стремиться.

Выводы по Главе 3

В третьей главе была проведена оценка эффективности предложенных мероприятий по совершенствованию системы информационной безопасности. Оценка эффективности является сложной задачей, так как основана на субъективной точке зрения и нет универсальных методов для объективной оценки. При этом затраты на обеспечение информационной безопасности следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной безопасности организации.

Перед подсчетом оценки эффективности предложенных мероприятий, был произведен расчет затрат на комплекс мероприятий и произведена оценка возможного ущерба с помощью сторонней организации, занимающихся восстановлением информации. Итоговая стоимость информационных активов составила 2 200 000 рублей, и отдельным пунктом выделили косвенный ущерб организации, в частности потеря имиджа организации, который может быть получен в результате террористических движений таких как «Колумбайн» или «скулшутинг». Оценить ущерб в денежном эквиваленте после реализации данной угрозы не представляется возможным, так как человеческие жизни бесценны.

Для совершенствования СОИБ были предложены следующие мероприятия:

— Мероприятия по формированию и расширению компетентности в области информационной безопасности участников образовательных отношений.

— Установка кондиционера в компьютерных классах.

— Организация пропускного режим.

Реализация данных мероприятий требует значительных денежных вложений, которые в свою очередь позволяют устранить выявленные

уязвимости и предотвратить возможные угрозы. Затраты на эти услуги составляют 1 028 420 рублей.

Соотношение оценки затрат на внедрение мероприятий к возможному ущербу составляет 21% и является достаточным, чтобы поддерживать СОИБ ГБПОУ «ЮУГК» на необходимом уровне. Следует отметить, что нет идеальной системы, которая будет обеспечивать защиту на 100 %, в данном случае предложенные мероприятия позволяют приблизиться к отметке в 90%, при условии, что все в организации будут к этому стремиться.

ЗАКЛЮЧЕНИЕ

В первой главе были проанализированы сущность системы обеспечения информационной безопасности образовательной организации и выявлены характерные виды информационных угроз, такие как вандализм; ошибки пользователей; кража оборудования; потеря данных; поломка оборудования; перепады напряжения; аппаратные и программные сбои.

Вторая глава отражает результаты анализа системы обеспечения информационной безопасности ГБПОУ «Южно-Уральского государственного колледжа», которые позволили выявить следующее:

— отсутствие сертификата SSL/TLS на сайте колледжа из-за чего невозможно выполнить защищённое соединение с шифрованием данных;

— возможность несанкционированного доступ на территорию организации;

— участники образовательного процесса, которые могут действовать в своих интересах;

— незнание базовых правил информационной безопасности педагогами и сотрудниками колледжа, которые могут привести к сбою в работе информационной системы;

— некорректная работа программного обеспечения, приводящая к потере или порче данных;

— технические сбои оборудования;

— отсутствие в общем доступе нормативно-правовой документации, регулирующей информационную безопасность в организации.

В третьей главе были сформулированы предложения по совершенствованию системы информационной безопасности колледжа и произведен расчёт эффективности предложенных мероприятий и средств.

В качестве рекомендаций по применению результатов диссертации предлагается:

— установить систему контроля управления доступом;

— установить систему кондиционирования для корректной работы компьютерного оборудования;

— перенести сайт на сервер CloudFlare;

— проводить мероприятия по формированию и расширению компетентности в области информационной безопасности среди всех участников образовательного процесса.

Реализация данных мероприятий потребует денежных вложений в размере 1 028 420 рублей, при этом соотношение оценки затрат на внедрение мероприятий к возможному ущербу будет являться достаточным, чтобы поддерживать СОИБ ГБПОУ «ЮУГК» на необходимом уровне.

Основные положения и результаты работы докладывались и обсуждались на научно-практических конференциях и были отражены в статьях:

1. Чераева, О. А. Обеспечение информационной безопасности образовательной организации/ О. А. Чераева // Проблемы современных интеграционных процессов. Пути реализации инновационных решений: сборник статей по итогам Всероссийской научно-практической конференции, Стерлитамак, 06 ноября 2020 года. – Стерлитамак: Общество с ограниченной ответственностью «Агентство международных исследований», 2020. – С. 35-37.

2. Чераева, О. А. Мотивирование сотрудников образовательных организаций на соблюдение информационной безопасности/ О. А. Чераева, Е. В. Рыскулова, О. А. Якупов // Модели и методы повышения эффективности инновационных исследований: Сборник статей по итогам Международной научно-практической конференции, Воронеж, 04 июня

2021 года. – Стерлитамак: Общество с ограниченной ответственностью «Агентство международных исследований», 2021. – С. 70-74.

3. Чераева, О. А. Обеспечение кибербезопасности в условиях дистанционного обучения на примере ГБПОУ «Южно - Уральский государственный колледж»]/ О. А. Чераева, А. Р. Халиуллин, Д. Р. Ахметшин // Инновационные проекты и программы в психологии, педагогике и образовании: сборник статей по итогам Международной научно-практической конференции, Екатеринбург, 29 сентября 2021 года. – Стерлитамак: Общество с ограниченной ответственностью «Агентство международных исследований», 2021. – С. 103-107.

Перспективы дальнейшей разработки темы диссертационного исследования имеют важное научно-практическое значение для образовательной организации с целью повышения эффективности имеющейся системы обеспечения информационной безопасности.

Библиографический список

1. Ажмухамедов И.М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования [Электронный ресурс]: URL: https://arxiv.org/ftp/arxiv/papers/1204/1204.3245.pdf (дата обращения 13.03.2022).

2. Александрова, А.В. Информационная безопасность и конституционные права личности [Текст]/ А. В. Александрова, Е. И. Образумов // Наука. Общество. Государство. — 2021. — № 1. — С. 63-70.

3. Баранова, Е.К. «Информационная безопасность и защита информации»: учеб. пособие [Текст]/ Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с.

4. Баранова, Е.К. Основы информационной безопасности: учебник [Текст] / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019. — 202 с.

5. Белим, С.В. Проблемы построения политики безопасности при объединении информационных систем [Текст]/ С. В. Белим, С. Ю. Белим // Математические структуры и моделирование. — 2018. — № 3. - С. 126-131

6. 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.

7. Белякова, Е.Г. Информационная культура и информационная безопасность школьников [Текст]/ Е. Г. Белякова, Э. В. Загвязинская, А. И. Березенцева // Образование и наука. — 2017. — № 8. — С. 147-162.

8. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учеб. пособие [Текст]/ В.В. Бондарев. — Москва: Издательство МГТУ им. Н. Э. Баумана, 2016. — 250 с.

9. Гафнер, В. В. Информационная безопасность: учебное пособие [Текст]/ В.В. Гафнер. - Рн/Д: Феникс, 2017. - 324 с.

10. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие [Текст]/ Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.

11. Государственная дума Федерального собрания Российской Федерации седьмого созыва Комитет по образованию и науке решение от 20 февраля 2018 года N 40-5 Развитие информатизации системы образования. Совершенствование законодательства в области электронного обучения и дистанционных образовательных технологий [Электронный ресурс]: URL: https://docs.cntd.ru/document/556985932 (дата обращения: 30.05.2022)

12. Грачева, Е.А. Информационная безопасность [Текст]/ Е. А. Грачева // The Newman in Foreign Policy. — 2020. — № 54 (98) Vol. 3. — С. 57-59.

13. Гришина Н.В. Основы информационной безопасности предприятия [Текст]: учебное пособие/ Н.В. Гришина. - Инфра-М., 2019. – 216 с.

14. Гришина, Н.В. Информационная безопасность предприятия [Текст]: учебное пособие/ Н.В. Гришина. - М.: Форум, 2018. - 118 с.

15. Гультяева, Т. А. Основы информационной безопасности [Текст]: учебное пособие/ Т. А. Гультяева. — Новосибирск: НГТУ, 2018. — 79 с.

16. Жарникова, Ю. С. Угрозы информационной безопасности образовательного учреждения / Ю. С. Жарникова. — Текст: непосредственный // Молодой ученый. — 2017. — № 11.2 (145.2). — С. 60-63. — URL: https://moluch.ru/archive/145/40613/ (дата обращения: 30.05.2022)

17. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите [Текст]/ С.В. Запечников, Н. Г. Милославская. — М.: ГЛТ, 2017. — 536 с.

18. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях [Текст]/ С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

19. Ильченко, Л.М. Расчет рисков информационной безопасности телекоммуникационного предприятия [Текст]/ Л.М. Ильченко, Е.К. Брагина, И.Э. Егоров, С.И. Зайцев // Открытое образование, 2018. – С. 61-70.

20. Информационная безопасность образовательных учреждений [Электронный ресурс]: URL:https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/ (дата обращения 13.03.2022)

21. Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации [Текст]: учебное пособие/ В. Я. Ищейнов, М. В. Мецатунян. — 2-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 216 с.

22. Как равнодушие сотрудников может повысить уязвимость вашей компании [Электронный ресурс]: URL: https://www.wrike.com/ru/blog/chelovecheskij-faktor-v-voprosah-informatsionnoj-bezopasnosti-kak-ravnodushie-sotrudnikov-mozhet-povysit-uyazvimost-vashej-kompanii/ (дата обращения 13.03.2022)

23. Киреева, Н. В. Аудит информационной безопасности [Текст]: методические указания/ Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара: ПГУТИ, 2019. — 21 с.

24. Коджешау, М.А. Технологии и алгоритмы информационной безопасности [Текст]/ М.А. Коджешау // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. — 2017. — № 2. — С. 129-135.

25. Конкин, Ю. В. Основы информационной безопасности [Текст]: учебное пособие/ Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань: РГРТУ, 2021. — 96 с.

26. Конституция Российской Федерации [Электронный ресурс]: (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) URL: http://www.consultant.ru/ (дата обращения 23.11.2020)

27. Лучинкина, А.И. Информационно-психологическая безопасность образовательной среды [Текст]/ А.И. Лучинкина // Научное мнение. — 2018. — № 1. — С. 73-78.

28. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]/ А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.

29. Маслова, М.А. Анализ и определение рисков информационной безопасности [Текст]/ М. А. Маслова // Научный результат. Информационные технологии. — 2019. — № 1. — С. 31-37. — ISSN 2518-1092.

30. Метод оценки экономической эффективности подразделения по защите информации [Электронный ресурс]: URL: https://lib.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii (дата обращения 23.11.2020)

31. Минин, А.Я. Информационная безопасность в образовании: обучающихся и обучающих [Текст]/ А.Я. Минин // Наука и школа. — 2017. — № 1. — С. 29-36.

32. Моргунов, А. В. Информационная безопасность [Текст]: учебно-методическое пособие/ А. В. Моргунов. — Новосибирск: НГТУ, 2019. — 83 с.

33. Мызникова, Т. А. Основы информационной безопасности [Текст]: учебное пособие/ Т. А. Мызникова. — Омск: ОмГУПС, 2017. — 82 с.

34. Нормативное обеспечение эксплуатации средств защиты информации [Текст]: учебное пособие/ А. В. Красов, И. И. Лившиц, Д. В.

Юркин [и др.]. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 67 с.

35. Обеспечение информационной безопасности организации [Электронный ресурс]: URL: https://iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/ (дата обращения 13.03.2022). – Текст: электронный

36. Поздняк, И. С. Управление информационной безопасностью [Текст]: методические указания/ И. С. Поздняк, И. С. Макаров. — Самара: ПГУТИ, 2019. — 43 с.

37. Поздняк, И. С. Экспертные системы оценки информационной безопасности [Текст]: методические указания/ И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара: ПГУТИ, 2019. — 23 с.

38. Поликарпов, А. В. Социально-философские аспекты проблемы информационной безопасности России: дис. ... канд. философ. наук. - М., 2000.- Режим доступа: https://www.dissercat.com/content/sotsialno-filosofskie-aspekty-problemy-informatsionnoi-bezopasnosti-rossii

39. Полякова А.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для академического бакалавриата и магистратуры: для студентов высших учебных заведений, обучающихся по юридическим направлениям и специальностям [Текст]/ под ред. Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2017. — 324,

40. Постановление Правительства Российской Федерации № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» URL: http://base.garant.ru/70252506/ (дата обращения 23.11.2020)

41. Привалов, А.Н. Методологические подходы к организации безопасной информационно-образовательной среды вуза [Текст]/ А. Н. Привалов, Ю. И. Богатырева, В. А. Романов // Образование и наука. — 2017. — № 4. — С. 169-183.

42. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты». URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/471-informatsionnoe-pismo-fstek-rossii-2 (дата обращения 23.11.2020)

43. Прокудин, Дмитрий Евгеньевич. Информационные технологии в образовании и их роль в формировании техногенной культуры: диссертация ... доктора философских наук: 24.00.01 / Прокудин Дмитрий Евгеньевич; [Место защиты: Санкт-Петербургский государственный университет]. - Санкт-Петербург, 2012. - 336 с.

44. Пугин, В. В. Защита информации в компьютерных информационных системах [Текст]: учебное пособие/ В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара: ПГУТИ, 2018. — 119 с.

45. Резниченко, М.Г. Профессиональная успешность специалистов в сфере информационной безопасности [Текст]/ М. Г. Резниченко, Е. А. Помельникова // Вестник Самарского университета. История, педагогика, филология. — 2019. — № 3. — С. 82-88.

46. Риски информационной безопасности [Электронный ресурс]: URL: https://arinteg.ru/articles/riski-informatsionnoy-bezopasnosti-26222.html (дата обращения 13.03.2022)

47. Риск-модели информационной безопасности [Текст]: учебное пособие/ А. А. Корниенко, С. В. Корниенко, А. П. Глухов, М. Л. Глухарев. — Санкт-Петербург: ПГУПС, 2021. — 79 с.

48. Санжаров, А.С. Методы оценки исследований информационной безопасности и компьютерных угроз [Текст]/ А.С. Санжаров, Ж.Т. Баранова // Известия Кыргызского государственного технического университета им. И.Раззакова. — 2018. — № 46. — С. 296-301.

49. Скулябина, О. В. Системный анализ в информационной безопасности [Текст]: учебное пособие/ О. В. Скулябина, С. Ю. Страхов. — Санкт-Петербург: БГТУ «Военмех» им. Д.Ф. Устинова, 2021. — 50 с.

50. Соколова, А.А. Информационно-образовательная среда и безопасность современной личности [Текст]/ А. А. Соколова, С. Н. Соколова, О. В. Пчелина // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. — 2020. — № 2. — С. 89-93.

51. Соколова, С.Н. Информационное общество: образовательное пространство и национальная безопасность [Текст]/ С.Н. Соколова, Т.В. Каленчук // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. — 2018. — № 1. — С. 36-42.

52. Угрозы информации https://siblec.ru/telekommunikatsii/osnovy-informatsionnoj-bezopasnosti-v-telekommunikatsiyakh/10-ugrozy-informatsii

53. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [Текст]. – Москва: Легион, 2022. – 144 с.

54. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Текст]. – Москва: Омега-Л, 2022. – 96 с.

55. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» [Текст]. – Москва: Гросс-Медиа, 2022. – 16 с.

56. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» [Текст]. – Москва: Норматика, 2022. – 144 с.

57. Чераева, О. А. Мотивирование сотрудников образовательных организаций на соблюдение информационной безопасности [Текст]/ О. А. Чераева, Е. В. Рыскулова, О. А. Якупов // Модели и методы повышения эффективности инновационных исследований: Сборник статей по итогам Международной научно-практической конференции, Воронеж, 04 июня

2021 года. – Стерлитамак: Общество с ограниченной ответственностью «Агентство международных исследований», 2021. – С. 70-74.

58. Чераева, О. А. Обеспечение информационной безопасности образовательной организации [Текст]/ О. А. Чераева // Проблемы современных интеграционных процессов. Пути реализации инновационных решений: сборник статей по итогам Всероссийской научно-практической конференции, Стерлитамак, 06 ноября 2020 года. – Стерлитамак: Общество с ограниченной ответственностью «Агентство международных исследований», 2020. – С. 35-37.

59. Чераева, О. А. Обеспечение кибербезопасности в условиях дистанционного обучения на примере ГБПОУ «Южно - Уральский государственный колледж» [Текст]/ О. А. Чераева, А. Р. Халиуллин, Д. Р. Ахметшин // Инновационные проекты и программы в психологии, педагогике и образовании: сборник статей по итогам Международной научно-практической конференции, Екатеринбург, 29 сентября 2021 года. – Стерлитамак: Общество с ограниченной ответственностью «Агентство международных исследований», 2021. – С. 103-107.

60. Чераева, О. А. Применение активных и интерактивных методов обучения при изучении дисциплины «Информационная безопасность» [Текст]/ О. А. Чераева // Реализация образовательных программ (отдельных их частей) в форме практической подготовки обучающихся. Особенности преподавания общеобразовательных дисциплин с учетом профессиональной направленности среднего профессионального образования: материалы педагогических чтений. Челябинск, 20 января 2022 года. – Челябинск: Издательский центр ГБПОУ «ЮУГК», Выпуск 9. – С. 141-146.

ПРИЛОЖЕНИЕ 1

#МЕДИА БЕЗОПАСНОСТЬ74
Региональная образовательная платформа

СЕРТИФИКАТ

УЧАСТНИКА

Силкин Михаил Вячеславович
Басов Владислав Дмитриевич
Осокин Дмитрий Алексеевич
Белоусова Ульяна Сергеевна
Квитков Сергей Сергеевич
(Рук.: Чераева Ольга Александровна)

ГБПОУ «Южно-Уральский государственный колледж»

приняли участие
в региональном кейс-чемпионате по киберсоциализации
#медиабезопасность74

Ректор
ГБУ ДПО Челябинский институт развития
развития профессионального образования
Е. П. Сичинский

Директор
АНО «Агентство социальных проектов
и молодежных инициатив»
Д. А. Бабушкин

Росмолодежь
Ресурсный Молодежный Центр
АГЕНТСТВО СОЦИАЛЬНЫХ ПРОЕКТОВ И МОЛОДЕЖНЫХ ИНИЦИАТИВ
ЧЕЛЯБИНСКИЙ ИНСТИТУТ РАЗВИТИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Челябинск, 2020

ПРИЛОЖЕНИЕ 2

ПРИЛОЖЕНИЕ 3

Государственное бюджетное профессиональное образовательное учреждение
«Южно-Уральский государственный колледж»

Областная студенческая научно-практическая конференция «Обеспечение комплексной безопасности общества и личности: проблемы и решения»

ПРОГРАММА

22 апреля 2021 года

г. Челябинск, ул. Курчатова д. 7

09.30–10.00	**Регистрация участников** Фойе
10.00–10.30	**Открытие конференции** Актовый зал
10.30–13.00	**Работа секций**
13.00 -14.30	**Подведение итогов. Торжественное закрытие** Актовый зал

ПРОГРАММА СЕКЦИЙ

1 СЕКЦИЯ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ауд. 310	
Модераторы Петров Павел Петрович – зам. директора по информационным технологиям **Назарова Наталья Александровна – председатель ПЦК «Информационные технологии»** **Техническая поддержка – Махно Анна Сергеевна**	
10.30 -10.40	**Участники:** Комяков Глеб Игоревич, группа ПСО247Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема**: Проблемы взаимодействия IT-технологий и развития личности **Руководитель:** Антоненко Мария Александровна
10.40-10.50	**Участники:** Штенников Владислав Александрович, Сементинова Вероника Евгеньевна, группа ПК351Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема**: Нужна ли нам киберграмотность? **Руководитель:** Чераева Ольга Александровна
10.50-11.00	**Участники:** Потрошилина Дарья Дмитриевна, Захарова Мария Константиновна, группа ПО-101 ФГБОУ ВО "ЧелГУ" **Тема**: Компьютерная зависимость **Руководитель:** Курносова Светлана Александровна
11.00-11.10	**Участники:** Хохлов Никита Егорович, группа ИС217Д ГБПОУ "Южно-Уральский государственный колледж" **Тема**: Место и роль анонимности и псевдоанонимности в современном обществе. **Руководитель:** Маслов Руслан Андреевич
11.10-11.20	**Участники:** Фаттахов Никита Сергеевич, группа МЭ-14-20 ГБПОУ Челябинский энергетический колледж им. С.М. Кирова **Тема**: Взлом страниц в социальных сетях взглядом мошенника и жертвы **Руководитель:** Рахимов Амир Галиуллович
11.20-11.30	**Участники:** Шпенглер Герман Викторович, группа ИС217Д ГБПОУ "Южно-Уральский государственный колледж" **Тема**: BIG DATA: крупные утечки персональных данных за последние несколько лет. **Руководитель:** Маслов Руслан Андреевич
11.30-11.40	**Участники:** Панов Даниил Сергеевич, группа ИС117Д ГБПОУ "Южно-Уральский государственный колледж" **Тема**: Значение и применение электронной цифровой подписи в целях обеспечения национальной безопасности Российской Федерации. **Руководитель:** Маслов Руслан Андреевич
11.40-11.50	**Участники:** Алеев Артур Андреевич, группа ИС217Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема**: Кибертерроризм как угроза национальной безопасности Российской Федерации. способы противодействия кибертерроризму. **Руководитель:** Маслов Руслан Андреевич

Областная студенческая научно-практическая конференция
Обеспечение комплексной безопасности общества и личности: проблемы и решения

ГБПОУ ЮУГК

ДИПЛОМ

III

степени

Штенникова Владислава Александровича

студента

ГБПОУ «Южно-Уральский государственный колледж»

группа ПК351Д

Тема исследования и публикации:

Нужна ли нам киберграмотность?

Научный руководитель:

Чераева Ольга Александровна

Директор колледжа В.Г. Лапин

Челябинск

22 апреля 2021

ПРИЛОЖЕНИЕ 4

Диплом

награждается команда ГБПОУ «Южно-Уральский государственный колледж» в составе:
Пятынин Никита Витальевич,
Золотарёв Дмитрий Александрович,
Ушаков Михаил Дмитриевич,
Яковлев Евгений Константинович,
Демин Артем Викторович
за II место в кейс-чемпионате «Управляй информацией безопасно!»

Заведующий кафедрой АТ,ИТиМОТД ФГБОУ ВО «ЮУрГГПУ»_____ Руднев В.В.

ноябрь-декабрь 2021 год, Челябинск

ПРИЛОЖЕНИЕ 5

Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный колледж»

V Областная студенческая научно-практическая конференция «Обеспечение комплексной безопасности общества и личности: проблемы и решения»

ПРОГРАММА

21 апреля 2022 года

г. Челябинск, ул. Курчатова д. 7

10.00–10.30 **Открытие конференции**
Актовый зал

10.30–13.00 **Работа секций**

13.00 -14.30 **Подведение итогов. Торжественное закрытие**
Актовый зал

ПРОГРАММА СЕКЦИЙ

1 СЕКЦИЯ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ауд. 227	
Модераторы Милюков Иван Васильевич – зам. директора по производственному обучению Петров Павел Петрович – зам. директора по информационной безопасности Техническая поддержка – Махно Анна Сергеевна	
10.30-10.40	**Участники:** Мальчер Анастасия Олеговна ГБПОУ «Южно-Уральский государственный колледж» **Тема**: Использование интернет-ресурсов для формирования основ информационной безопасности обучающихся СПО в рамках учебной дисциплины «Информатика»
10.40 -10.50	**Участники:** Гужавина Антонина Владимировна, Субачева Анна Евгеньевна, группа ПСА146Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема**: Сайты-подделки. Как не стать жертвой мошенников **Руководитель:** Мальчер Анастасия Олеговна
10.50-11.00	**Участники:** Сапожников Евгений Сергеевич, Женин Иван Ваганович, группа ИС119Д. ГБПОУ «Южно-Уральский государственный колледж» **Тема**: DEEPFAKE: Как не стать жертвой обмана **Руководитель:** Чераева Ольга Александровна
11.00-11.10	**Участники:** Попков Платон Михайлович, группа АТП157Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема**: Киберпреступность **Руководитель:** Кочетков Владимир Юрьевич
11.10-11.20	**Участники:** Панов Даниил Сергеевич, группа ИС217Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема**: Проблематика облачного хранения данных **Руководитель:** Назарова Наталья Александровна
11.20-11.30	**Участники:** Загребина Дарья Андреевна, группа ИС-32 Златоустовский индустриальный колледж им. П.П. Аносова **Тема**: Проблемы взаимодействия IT-технологий и развития личности **Руководитель:** Майер Юлия Владимировна
11.30-11.40	**Участники:** Васильев Артем Фанисович, Кисслер Кирилл Юрьевич, Костян Антон Александрович, группа АТП357Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема:** Осторожно - спам! **Руководитель:** Сидоренко Ольга Валентиновна
11.40-11.50	**Участники:** Шапкина Юлия Михайловна**,** группа Д161Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема:** Информационное превосходство как фактор выживания в 21 веке **Руководитель:** Котова Наталья Олеговна
11.50 – 12.00	**Участники:** Муратова Виктория Константиновна, группа Ис-31. Златоустовский индустриальный колледж им. П.П. Аносова **Тема:** Современная угроза виртуального пространство: механизмы манипуляция и методы контрпропаганды **Руководитель:** Рогова Виктория Ринатовна
12.00-12.10	**Участники:** Кичигина Татьяна Сергеевна, Малеева Анна Александровна, группа СР-201. ГБПОУ «Челябинский социально – профессиональный колледж «Сфера» **Тема:** Мошенничество в сфере информационно-коммуникационных технологий **Руководитель:** Чикулина Анна Викторовна
12.10-12.20	**Участники:** Пятынин Никита Витальевич, Кузнецов Владимир Алексеевич, Яковлев Евгений Константинович, группа ИС119Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема:** DDOS-АТАКИ на образовательные организации в условиях дистанционного обучения **Руководитель:** Чераева Ольга Александровна
12.20-12.30	**Участники:** Ахмадиев Богдан Русланович, группа СТ-9-20. ГБПОУ Челябинский энергетический колледж им. С.М. Кирова **Тема:** Информационные фейки **Руководитель:** Рахимов Амир Галиуллович
12.30-12.40	**Участники:** Глазырина Ксения Алексеевна, группа 174К. ГБПОУ «Южно-Уральский государственный колледж» Кыштымский филиал **Тема:** КИБЕРПРЕСТУПНОСТЬ – ПРОБЛЕМА 21 ВЕКА **Руководитель:** Булаева Марина Юрьевна
12.40-12.50	**Участники:** Минин Владимир Валерьевич, Сибриков Владислав Владимирович, Понькин Дмитрий Денисович, группа АТП356Д, АСУ358Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема:** КИБЕРСОЦИАЛИЗАЦИЯ ЧЕЛОВЕКА: ОТ «HOMO SAPIENS'A» ДО «HOMO CYBERUS'A»? **Руководитель:** Сидоренко Ольга Валентиновна
12.50-13.00	**Участники:** Терентьева Анна. группа ИС217Д. ГБПОУ "Южно-Уральский государственный колледж" **Тема:** Информационная безопасность в образовательных организациях среди студентов **Руководитель:** Назарова Наталья Александровна

Областная студенческая научно-практическая конференция

Обеспечение комплексной безопасности общества и личности: проблемы и решения

ГБПОУ ЮУГК

ДИПЛОМ

II

степени

Женина Ивана Вагановича

студента

ГБПОУ «Южно-Уральский государственный колледж»

группа ИС119Д

Тема исследования и публикации:

DEEPFAKE: Как не стать жертвой обмана

Научный руководитель:

Чераева Ольга Александровна

Директор ГБПОУ «ЮУГК» В.Г.Лапин

21 апреля 2022