МИНИСТЕРСТВО ПРОСВЕЩЕНИЯРОССИЙСКОЙ 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

Обеспечение цифровой безопасности личности студента в едином информационном пространстве образовательной организации

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

Проверка на объем заимствований:
77,53 % авторского текста

Работа рекомендована к защите
«30» 01 2024 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Иванова Светлана Алексеевна

Научный руководитель:
Диденко Галина Александровна, к.п.н.,
доцент

Челябинск
2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Повсеместное развитие, разработка и интеграция информационных технологий является основным вектором развития современного научно-технического прогресса. Рассматриваемые технологии находят свое активное использование практически во всех как бытовых, так и профессиональных сферах жизнедеятельности человека. В частности, одной из наиболее важных с точки зрения необходимости использования информационных технологий сферой является образование. Несмотря на ряд объективных преимуществ, которые несет использование новых технологий в образовании, наблюдается целое множество как потенциальных, так и реальных проблем, связанных с безопасностью студентов. Во многом это связано с обработкой и хранением большого количества конфиденциальной и иной информации ограниченного доступа, владение которой может привести к серьезным негативным последствиям и нарушить цифровую безопасность личности студента. В связи с этим актуализируется задача, связанная с более подробной проработкой и исследованием данного вопроса, а также формированием требований к задаче по обеспечению безопасного информационного пространства [1].

Целью исследования является повышение безопасности личности студента в едином информационном пространстве ГБПОУ «Катав-Ивановский индустриальный техникум».

Объектом исследования является единое информационное пространство ГБПОУ «Катав-Ивановский индустриальный техникум».

Предметом исследования является обеспечение цифровой безопасности студента в информационном пространстве образовательной организации ГБПОУ «Катав-Ивановский индустриальный техникум».

Гипотеза диссертационного исследования состоит в том, что можно повысить уровень цифровой безопасности студента в информационном

пространстве образовательной организации путем разработки новой модели обеспечения безопасного информационного пространства.

Задачи исследования:

1. Анализ актуальности вопроса, связанного с основными угрозами и рисками при обеспечении цифровой безопасности студентов в образовательной организации;

2. Исследование основных методов по обеспечению цифровой безопасности в информационном пространстве образовательных организаций;

3. Анализ системы обеспечения цифровой безопасности личности студента в ГБПОУ «Катав-Ивановский индустриальный техникум»;

4. Формирование требований и разработка модели, направленных на решение задачи по обеспечению безопасного информационного пространства для студентов ГБПОУ «Катав-Ивановский индустриальный техникум»;

5. Реализация и анализ эффективности модели обеспечения цифровой безопасности студента.

Теоретико-методологическая база исследования. Для написания работы использовались теоретические методы научного исследования, такие как анализ и синтез. В качестве методов исследования обеспечения цифровой безопасности студентов были использованы общенаучные методы системного анализа и структурного моделирования, а также проводилась аналитическая оценка нормативных документов, опубликованных результатов соответствующих исследований и экспертные оценки. Информационная база для исследования сформирована на официальных материалах и открытых публикациях авторов по соответствующей тематике, рассматривавших в своих работах вопрос информационной безопасности студентов. Кроме того, информация была собрана автором из реально-существующих документов ГБПОУ «Катав-Ивановский индустриальный техникум».

Положения, выносимые на защиту:

1. Новые алгоритмы анализа уровня обеспечения информационной безопасности личности студента в информационном пространстве образовательной организации. Данные алгоритмы позволяют более детально и объективно оценить уровень текущего обеспечения безопасности студента для формирования наиболее важных и актуальных к решению задач;

2. Новая модель обеспечения цифровой безопасности студента в информационном пространстве ГБПОУ «Катав-Ивановский индустриальный техникум». На основе данной модели имеется возможность получения наиболее эффективной системы, препятствующей несанкционированному доступу к информации студентов, а также повышающей качество и эффективность образовательного процесса.

Научная новизна магистерской диссертации заключается в разработке новой модели обеспечения безопасного информационного пространства, включающей в себя три основных блока: обеспечение безопасности в информационном пространстве образовательной организации; освоение компетенций ИБ студентами; пакет нормативно-правовых документов.

Практическая значимость исследования. Результаты представленной магистерской диссертации могут быть использованы для комплексного обеспечения цифровой безопасности студента в информационном пространстве образовательной организации ГБПОУ «Катав-Ивановский индустриальный техникум». Представленные методики имеют универсальный характер. Так, при соответствующих корректировках разработанной модели возможно получение инструмента, способного выполнять те же задачи по обеспечению цифровой безопасности для другой образовательной организации.

Методы исследования. Для решения поставленных задач и проверки гипотезы используются следующие методы исследования: теоретические

(понятийно-терминологический и сравнительно-сопоставительный анализ научно-педагогической и методической литературы по вопросам обеспечения безопасности личности студента, анализ законодательства в сфере образования; методы систематизации и классификации теоретического материала; обобщение и аксиоматизация теоретических подходов к организации системы по анализу текущего уровня защищенности студентов; моделирование системы обеспечения цифровой безопасности личности студента); эмпирические (педагогический эксперимент, наблюдение, анкетирование).

База исследования. ГБПОУ «Катав-Ивановский индустриальный техникум».

Этапы исследования. На первом этапе исследования были рассмотрены основные положения относительно текущего уровня развития представленного вопроса, а также ключевая информация, касающаяся текущих тенденций в области образования и рисков цифровой безопасности личности студентов в информационном пространстве образовательной организации.

На втором этапе исследования проводится анализ относительно общих сведений об образовательной организации ГБПОУ «Катав-Ивановский индустриальный техникум». Анализируется организационно-правовое обеспечение деятельности и политика безопасности рассматриваемой образовательной организации.

На третьем этапе исследования выполняется формирование новой методики и разработка модели по обеспечению цифровой безопасности личности студентов в информационном пространстве образовательной организации. Также в рамках данного этапа выполняется работа по анализу эффективности модели обеспечения цифровой безопасности студента.

Апробация результатов исследования. Основные результаты научного исследования были представлены в следующих публикациях:

1. Актуальность обеспечения информационной безопасности студентов в информационном пространстве образовательной организации.

2. Анализ основных угроз в информационном пространстве образовательных организаций применительно к студентам.

3. Методы обеспечения цифровой безопасности студентов в информационном пространстве образовательных организаций.

Внедрение результатов исследования. Результаты исследования будут внедрены в образовательную организацию ГБПОУ «Катав-Ивановский индустриальный техникум» для повышения безопасности личности студента и повышения качества образовательного процесса.

Структура и объем работы. Работа состоит из введения, трех основных глав, заключения и списка использованных источников. Основная часть работы изложена на 67 страницах машинописного текста, в число которых входит 17 рисунков и 4 таблицы. Список использованных источников содержит 36 наименований.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЙ АНАЛИЗ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ БЕЗОПАСНОСТИ СТУДЕНТА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Анализ актуальности по проблеме цифровой безопасности студента в информационном пространстве образовательных организаций

Информационные технологии (далее – ИТ) являются неотъемлемой частью развития современного научно-технического прогресса. Интеграция данных инновационных технологий наблюдается во многих профессиональных сферах жизнедеятельности человека. Основным преимуществом использования ИТ является возможность повышения качества и эффективности выполнения целого ряда задач. Именно использование информационных технологий позволяет на качественном уровне изменить принцип решения и выполнения различных задач, значительно сокращая излишние издержки и повышая экономическую эффективность в функционировании предприятий и организаций [2].

Одной из наиболее актуальных сфер с точки зрения интеграции информационных технологий является образование. Образовательная сфера включает в себя большой объем задач и требований, решение и обеспечение которых в современных реалиях уже невозможно без использования ИТ. Так, ученики и студенты должны иметь быстрый доступ к учебным материалам, оперативную связь с учителем и преподавателем, возможность отслеживания результатов обучения и множество иных аспектов. Главной особенностью современной сферы образования является необходимость быстрого доступа и анализа определенной информации [3]. Именно здесь на первый план выходит использование новых информационных технологий,

которые позволяют автоматизировать рутинные процессы, а также повить скорость и эффективность обработки различного рода информации.

Образование и воспитание нового поколения является одной из основных задач Российской Федерации. При этом даже в такой консервативной области как образование основным вектором развития является разработка и использование передовых информационных технологий. Становится очевидным, что ИТ – это главная составляющая в обеспечении эффективного и качественного процесса обучения. Многие учебные заведения непрерывно пересматривают программы обучения, интегрируя в них предметы и курсы, тесно связанные с использованием или освоением использования информационных технологий.

Так, ИТ уже зачастую называют основой современного образования. Их использование наблюдается практически во всех аспектах деятельности современных образовательных организаций. Примерами использования информационных технологий в образовании являются электронные библиотеки, дистанционное обучение, мультимедийные средства, экспериментальные комнату и тренажеры, а также множество иных направлений. Электронные библиотеки, в частности, позволяют повысить доступность студентов к научным материалам всего мира. Дистанционное обучение позволяет обеспечить образовательный процесс для тех студентов, которые не имеют возможности присутствовать на очных занятиях, а мультимедийные средства повышают качество преподавания и мотивацию студентов к обучению.

Совокупность данных факторов свидетельствует о высоком значении и актуальности использования ИТ в современной образовательной сфере. Именно за счет интеграции новых технологий современные студенты получают возможность доступа к всемирным ресурсам знаний и практического опыта, получения новых форматов обучения и множество иного [4]. Помимо этого, использование инновационных информационных технологий позволяет развить глобальные информационные системы по

оказанию услуг в сфере образования, получить возможность использования облачных технологий в дистанционном обучении, а также повысить доступность при накоплении и передачи знаний.

Несмотря на огромное множество объективных преимуществ при использовании информационных технологий в образовании, на сегодняшний день также выделяется ряд угроз и недостатков, наблюдаемых при активной интеграции ИТ в образовательном процессе. Одной из наиболее важных и остро-стоящих проблем повсеместного использования информационных технологий является угроза информационной безопасности (далее – ИБ). Это напрямую связано с тем, что использование информационных технологий предполагает переход бумажного документооборота и иной информации с физического носителя на электронный [5]. Вместе с этим повышаются риски потери доступа или утечки информации ввиду активизации хакерской деятельности и иных неправомерных действий.

Важно подчеркнуть, что использование информационных технологий в образовании предполагает необходимость переноса конфиденциальной информации и информации ограниченного доступа в электронную форму. Вместе с этим для использования множества электронных ресурсов создаются учетные записи для студентов, с помощью которых может быть получен доступ к их использованию. Это, в свою очередь, основывается на использовании специальных информационных систем (далее – ИС), которые представляют собой сеть взаимосвязанных элементов, контролирующих движение информации и обеспечивающих к ней доступ. Так, современные образовательные организации, активно использующие ИТ, обрастают множеством ИС, без использования которых не представляется возможным обеспечение эффективного взаимодействия электронных ресурсов с преподавателями и студентами.

Данные факты свидетельствуют о том, что для использования новых информационных технологий необходима интеграция дополнительных

информационных систем, на основе которых обеспечивается жизнеспособность и возможность использования новых ИТ. Как уже видно, современные образовательные организации представляют собой паутину из новых технологий, что, в свою очередь, повышает актуальность проблемы ИБ.

Использование информационных технологий в стенах современных образовательных организаций наблюдается повсеместно. Интеграция новых технологий наблюдается и при мониторинге образовательного процесса, и при обеспечении его учебными материалами, и при информировании студентов о различных новостях, а также множество иных немаловажных задач, обеспечивающих студенческую жизнь [6]. Важно отметить, что на сегодняшний день можно с уверенностью заявить о том, что именно ИТ являются основой в обеспечении образовательного процесса. Без данных технологий уже невозможно представить возможность функционирования образовательных организаций, тесно сплетенных с использованием инновационных технологий.

Как уже было сказано ранее, интеграция ИТ несет множество проблем, связанных с информационной безопасностью. Здесь важно отметить, что использование в любых информационных технологий в любой сфере по определению несет множество рисков информационной безопасности. Это напрямую связано с потенциальной уязвимостью любых информационных технологий к различного рода атакам и иным рискам ИБ. На сегодняшний день отсутствуют меры защиты, обеспечивающие полную безопасность при использовании рассматриваемых технологий. В связи с этим, актуализируется задача, связанная с максимизацией степени защищенности современных информационных технологий и информационных систем, особенно для образовательных организаций.

Важнейшей задачей при использовании ИТ в образовании является обеспечение цифровой безопасности студента. Современные студенты потенциально подвержены множествам рискам, связанным с

несанкционированным доступом к их личной информации, манипуляторным воздействием, нарушением психоэмоционального и физического здоровья, а также иных последствий. Вследствие этого необходимо более подробное исследование процессов, связанных с обеспечением цифровой безопасности студента в информационном пространстве образовательных организаций.

Более подробное исследование таких вопросов необходимо в первую очередь для понимания основных рисков и уязвимостей, которые непосредственно влияют на личность и состояние студента. Дальнейшим этапом работы с такой информацией может стать разработка новых подходов и методик, интеграция которых в образовательную систему позволит избежать и снизить риски, связанные с информационной безопасностью. Это подтверждает достаточно высокую актуальность и необходимость исследования вопросов, связанных с цифровой безопасностью студента в информационном пространстве образовательных организаций.

Дополнительно важно отметить, что современные учебные заведения включают в себя не только широкую сеть различных информационных технологий, но и представляют собой огромный банк данных. Такие данные включают в себя множество конфиденциальной информации о личности студентов, бухгалтерии, корпоративной информации и множество иных источников, имеющих ограниченный доступ. При этом утечка одного из них, напрямую не связанного со студентом, может иметь значительные последствия в области его цифровой безопасности [7]. Так, к примеру, при нарушении работы бухгалтерии или фальсификации данных студент может остаться без стипендии или иных мерах материальной поддержки. В то время, как средства, перечисленные по измененным счетам, поступают в руки нарушителя или хакера.

Это является только лишь одним из тысячи примеров возможных последствий, определяющих и доказывающих актуальность вопросов

обеспечения информационной безопасности в стенах учебных заведений. Вместе с этим важно отметить, что обеспечение цифровой безопасности личности студента является сложной (составляющей) задачей, требующего комплексного подхода. Это связано ввиду невозможности обеспечения безопасности только лишь по одному из направлений ввиду их взаимосвязанности и непосредственным влиянием друг на друга, пример чего был приведен ранее по тексту.

В связи с этим для возможности решения изначально поставленной задачи данной магистерской диссертации необходимо учитывать и вторичные факторы, косвенно ил напрямую связанные с цифровой безопасностью личности студента. Так, к примеру, формирование требований при обеспечении безопасности должно включать в себя не только прямые указания и правила применительно к деятельности студентов, но также и требования к материально-технической базе организации и иным взаимосвязанным аспектам. Данные задачи требуют более подробного исследования и могут разниться в зависимости от определенной образовательной организации, для которой планируется разработка новой методики обеспечения цифровой безопасности личности студента.

Подытоживая следует отметить, что на сегодняшний день наблюдается высокий уровень актуальности проблемы, связанной с необходимостью обеспечения цифровой безопасности личности студента. Во многом это связано ввиду непрерывной цифровизации современных образовательных организаций и переводом бумажного документооборота в электронный формат. В связи с этим повышаются риски утечки информации, взлома или фальсификации данных со стороны злоумышленников, что в конечном итоге негативно влияет на студентов учебных заведений. Именно поэтому необходимо выполнение более подробного анализа по теме диссертации с целью разработки новой и

учитывающей все параметры модели обеспечения цифровой безопасности личности студентов.

Первостепенным этапом при разработке новых подходов должен стать анализа основных угроз и проблем обеспечения цифровой безопасности в современных образовательных организациях. Решение данной задачи позволит получить исчерпывающее представление о текущей ситуации относительно рассматриваемого вопроса. Вместе с этим именно на их основе будут проработаны основные задачи, включенные в конечную модель обеспечения цифровой безопасности. Данным вопросам посвящен следующий параграф в работе.

1.2 Угрозы и проблемы обеспечения цифровой безопасности в образовательных организациях

Одним из главных направлений при разработке новой модели обеспечения цифровой безопасности личности студентов является анализ угроз и проблем обеспечения цифровой безопасности в образовательных организациях. Как уже было указано ранее, основными угрозами являются утечка информации, фальсификация, нарушение целостности системы информационной безопасности и ряд других проблем. Каждая из них возникает при определенных обстоятельствах, вызванных несовершенством общей системы ИБ, халатным отношением со стороны руководства, неосведомленностью сотрудников и студентов относительно основ информационных технологий и информационной безопасности и иных аспектов.

Перед началом анализа угроз и проблем обеспечения ИБ, необходимо дать полное определение информационной безопасности в образовательных организациях. Информационная безопасность в образовательных организациях включает в себя меры и практики, применяемые для защиты конфиденциальности, целостности и доступности информации, используемой в учебном процессе [8]. Она направлена на обеспечение

безопасности информационных систем, сетей, данных и операций, связанных с учебным процессом и управлением образовательной организацией. Информационная безопасность включает в себя следующие аспекты:

- защита конфиденциальности данных. Образовательные организации должны обеспечивать защиту личных данных студентов, преподавателей, сотрудников от несанкционированного доступа и использования;

- предотвращение и обнаружение вторжений. Образовательные организации должны применять меры безопасности, чтобы предотвратить несанкционированный доступ к их информационным системам и сетям, а также обнаруживать и реагировать на любые попытки вторжения;

- обеспечение целостности данных. Информация, хранящаяся в информационных системах образовательных организаций, должна быть защищена от неправильной (несанкционированной) модификации или удаления;

- защита от вредоносных программ. Организации должны использовать антивирусные программы, брандмауэры и другие средства защиты для предотвращения и обнаружения вредоносных программ, таких как вирусы, троянские программы и шпионское ПО;

- обеспечение доступности информации. Информационные системы учебных заведений должны быть доступными для использования студентами и преподавателями, безопасность не должна препятствовать нормальному функционированию образовательного процесса;

- обучение и осведомленность. Регулярное обучение сотрудников и студентов об основных принципах информационной безопасности является важной частью управления безопасностью в образовательной организации;

- защита от кибератак. Образовательные организации должны иметь политику и планы кибербезопасности для минимизации рисков кибератак и быстрого восстановления после инцидентов.

Информационная безопасность является одним из важнейших аспектов деятельности образовательных организаций. Вместе с постоянным развитием технологий и повседневным использованием информационных систем в учебном процессе, возрастает и уровень угроз, с которыми сталкиваются такие организации.

Во-первых, следует отметить утечку данных. Образовательные организации часто хранят большие объемы конфиденциальной информации, такой как личные данные учащихся и работников, результаты экзаменов и прочая важная документация. В случае утечки или утраты этих данных, организация получить ряд негативных последствий. Именно поэтому образовательным организациям необходимо внимательно отслеживать доступ к информации и предпринимать меры для ее защиты.

Фишинг и вредоносные программы. Образовательные организации сталкиваются с регулярной угрозой со стороны киберпреступников, использующих методы социальной инженерии для получения доступа к системе или получения чувствительных данных. Поэтому необходимо обучать работников организации, в том числе учителей и администраторов, основам безопасности информации, а также использовать современные антивирусные и антифишинговые программы для защиты от вредоносных программ и фишинговых атак.

Остро стоит вопрос, связанный с DDoS-атаками. Образовательные организации могут быть подвержены DDoS-атакам, когда злоумышленники пытаются перегрузить сеть или серверы организации, что приводит к недоступности ресурсов и создает неудобства для учащихся и преподавателей. Предотвратить такие атаки можно путем установки систем фильтрации входящего трафика с использованием специализированных программных и аппаратных решений для обеспечения надежности сетевой инфраструктуры.

Угрозы внутренних пользователей. Несмотря на то, что основными источниками угроз информационной безопасности образовательных организаций являются внешние атаки, внутренние пользователи (учащиеся, преподаватели, администраторы) также могут быть уязвимыми точками. Небрежное обращение с паролями, использование нелицензионного программного обеспечения или незаконный доступ к сетевым ресурсам могут создать дыры в безопасности [9]. Для уменьшения внутренних угроз необходимо проводить регулярные обучающие мероприятия для пользователей и устанавливать политику безопасности, регламентирующую использование информационных технологий в организации.

Отдельно необходимо отметить риск, связанный с несанкционированным доступом. Несанкционированный доступ - это незаконное или несанкционированное получение доступа к компьютерным системам, программам, данным или устройствам. Различают следующие виды несанкционированного доступа:

- человеческий, предусматривает хищение сведений методом их отправки по электронной почте или копирования на портативные носители, внесение вручную изменений в базы данных при наличии физического доступа к серверу;

- аппаратный, применение специального оборудования для хищения данных или внесения изменений в систему. В том числе может применяться оборудование для перехвата электромагнитных сигналов;

- программный, применение специального программного обеспечения для перехвата данных, копирования паролей, дешифровки и перенаправления трафика, внесения изменений в функционирование другого софта и иное.

Объективная оценка всех возможных угроз информационной безопасности образовательных организаций является достаточно сложной задачей, поскольку сфера кибербезопасности непрерывно развивается и

виды атак постоянно изменяются. Другим направлением для анализа являются проблемы информационной безопасности.

Первостепенно следует отметить, что угроза и проблема информационной безопасности - это два тесно связанных понятия, но они имеют некоторые различия. Угроза информационной безопасности - это потенциальная возможность возникновения события или действия, которое может нанести ущерб системе или нарушить ее работоспособность. Угроза может происходить как из внешней среды, так и изнутри самой организации. Примеры угроз включают вредоносные программы, хакерские атаки, утечку данных, физическую порчу оборудования и другое.

Проблема информационной безопасности - это состояние, когда информационная система оказывается уязвимой перед угрозами и недостаточно защищена от них. Это связано с отсутствием или недостаточной реализацией соответствующих мер безопасности, таких как политики доступа, шифрование данных, мониторинг угроз и прочие технические и организационные меры. Проблемы информационной безопасности могут возникнуть из-за ошибок в проектировании системы, неправильной конфигурации, недостаточного обучения персонала и других факторов.

Итак, угроза - это потенциальная опасность, которая может повлиять на безопасность информационной системы. В то время как проблема информационной безопасности - это отсутствие соответствующих мер и защитных действий, что делает общую систему ИБ более уязвимой перед угрозами. Так, можно выделить несколько основных проблем информационной безопасности применительно к образовательным организациям:

1. Недостаточная осведомленность сотрудников и студентов о вопросах информационной безопасности. Многие люди не знают о потенциальных угрозах и не понимают, как защитить свои данные;

2. Отсутствие строгих политик и процедур по обеспечению информационной безопасности. Многие образовательные организации не имеют четких правил и инструкций о том, как хранить и обрабатывать конфиденциальную информацию;

3. Недостаточная защита сетей и систем от внешних атак. Образовательные организации обычно имеют большие сети с множеством устройств, что делает их уязвимыми для кибератак и взломов;

4. Недостаточное обновление программного обеспечения и операционных систем. Многие образовательные организации не всегда успевают обновлять свое программное обеспечение, что может привести к уязвимостям и взломам;

5. Незаконное использование информационных технологий. В образовательных организациях могут возникать проблемы с несанкционированным доступом к информации и незаконным использованием компьютеров и сетей;

6. Отсутствие регулярного обучения сотрудников и студентов профилактике информационной безопасности. Образовательные организации должны обучать своих сотрудников и студентов эффективным методам предотвращения и реагирования на угрозы безопасности;

7. Недостаточная защита персональных данных. Образовательные организации могут не обладать достаточными средствами для защиты конфиденциальных данных о студентах и сотрудниках, что может привести к утечке информации;

8. Незаконное использование и распространение авторского материала. В образовательных организациях могут возникать проблемы с незаконным использованием и распространением авторского материала, что ведет к нарушению законов о защите интеллектуальной собственности;

9. Угрозы со стороны внутренних сотрудников. Некоторые сотрудники образовательных организаций могут быть недобросовестными и злоупотреблять своими правами доступа к информации;

10. Недостаточное финансирование информационной безопасности. Образовательные организации, особенно те, которые имеют ограниченный бюджет, могут не иметь достаточных средств для обеспечения эффективной информационной безопасности.

Таким образом, активно интегрируемые в образовательных организациях новые информационные технологии приводят к возникновению множества рисков, угроз и проблем ИБ. При этом данные аспекты напрямую влияют на цифровую безопасность студентов, обучающихся по программам каждой конкретной образовательной организации [10]. В связи с этим обеспечение ИБ становится неотъемлемой составляющей образовательного процесса, что необходимо для защиты конфиденциальных данных учеников и персонала, а также обеспечения доступности систем и сохранения непрерывности обучения.

В рамках параграфа представлены результаты анализа, отражающие наиболее актуальные и основные угрозы и проблемы информационной безопасности современных образовательных организаций. Важно отметить, что разработка конечной модели обеспечения цифровой безопасности личности студента должна учитывать возможность снижения вероятности наступления данных угроз и проблем информационной безопасности.

1.3 Методы по обеспечению цифровой безопасности в информационном пространстве образовательных организаций

Для борьбы с угрозами и проблемами ИБ в информационном пространстве образовательных организаций используются специальные методы. Методы по обеспечению цифровой безопасности включают в себя различные стратегии, технологии и процедуры, которые используются для защиты информации в цифровой среде. Данные методы могут включать в себя разнообразные подходы, примерами которых является интеграция проверки легитимности пользователей, установка и разграничение прав

доступа, использование алгоритмов шифрования, систем мониторинга безопасности сети, установка антивирусных программ и многое другое.

Основной задачей при использовании таких методов является снижение влияния и риска возникновения угроз информационной безопасности. Важно отметить, что рассматриваемые методы могут быть программными, аппаратными и комбинированными. Конечный результат при использовании таких технологий направлен на поддержание высокого уровня информационной безопасности образовательной организации и цифровой безопасности студентов [11]. Защита от угроз является основным компонентом снижения рисков ИБ. На рис. 1 представлен полный комплекс управления рисками информационной безопасности.

Рисунок 1 – Комплекс действий при управлении рисками ИБ

Для решения представленных на рис. 1 задач, связанных с обеспечением ИБ информационной среды образовательной организации используются специальные методы, средства и способы защиты. Основные способы защиты информации указаны на рис. 2.

Рисунок 2 – Способы (методы) защиты информации

Представленные на рис. 2 способы защиты информации являются основой для создания реальных инструментов, направленных на противодействие преступным действиям, связанным с нарушением информационной безопасности образовательных организаций. Важно отметить, что в зависимости от каждого риска и проблемы ИБ могут применяться различные способы защиты информации. При этом разработка методов может основываться на использовании комбинации сразу нескольких способов защиты информации, к примеру, регламентации и принуждении. Особое внимание заслуживает анализ конкретных средств защиты информации.

Как уже было указано ранее, инструменты защиты информации разделяются на программные и аппаратные. Каждый из них представляет собой инструмент, направленный на решение задачи защиты информации и укрепление самой системы ИБ. Основные средства защиты информации,

использование которых необходимо в современных образовательных организациях, указаны на рис. 3.

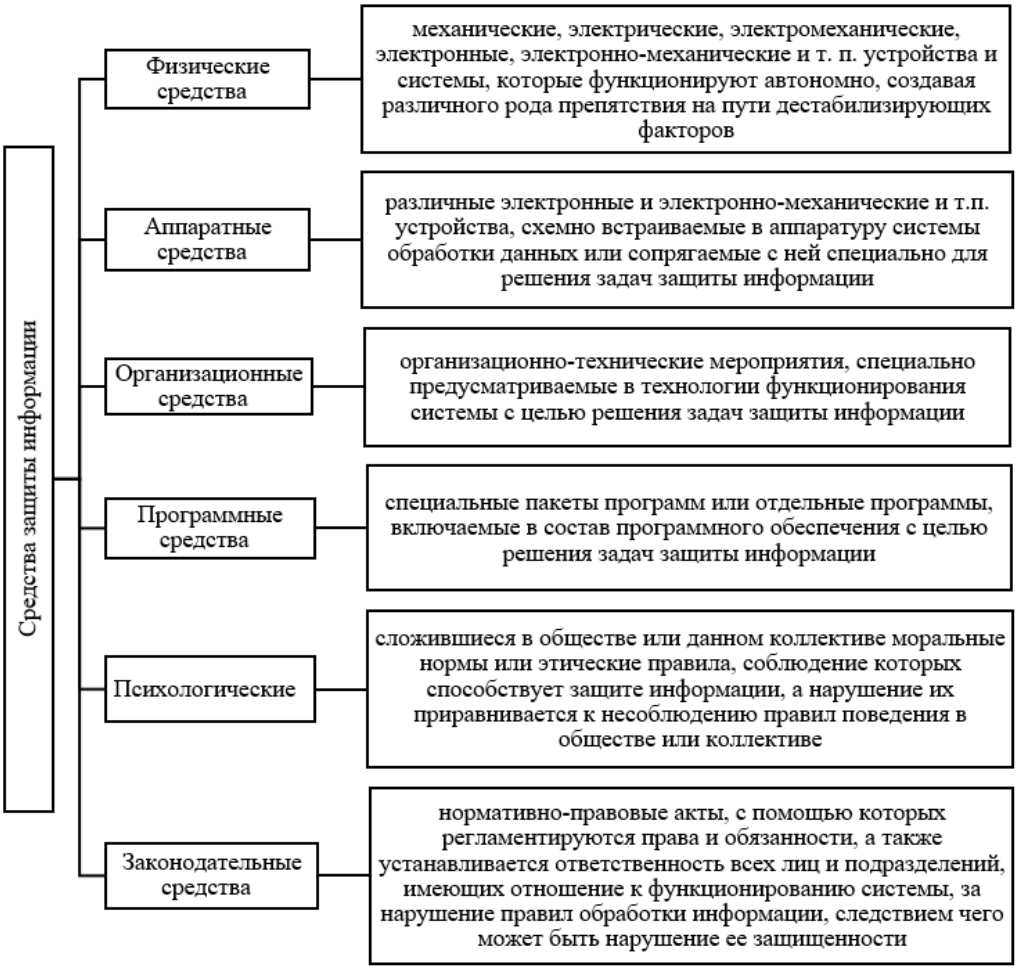


Рисунок 3 – Средства защиты информации

Необходимо отметить, что обеспечение цифровой безопасности личности студента является возможной для решения задачей только в результате использования представленных методов и средств защиты. Современные образовательные организации должны иметь полный набор инструментов для разностороннего повышения безопасности системы ИБ.

Анализируя представленные методы и средства защиты информации применительно к задаче обеспечения цифровой безопасности студентов, можно выделить следующий набор мер, которые необходимо использовать в рамках данной предметной области:

- обучение студентов основам безопасности. Организации могут предоставлять студентам обучающие программы, в которых рассматриваются основные принципы цифровой безопасности, такие как защита паролей, распознавание фишинговых атак, безопасное использование социальных сетей и т.д. Это поможет студентам осознавать возможные угрозы и принимать соответствующие меры предосторожности;

- фильтрация и мониторинг интернет-трафика. Организации могут установить системы фильтрации и мониторинга трафика, чтобы блокировать доступ к нежелательным или вредоносным веб-сайтам. Это поможет предотвратить доступ студентов к вредоносным материалам или сайтам, а также обнаруживать подозрительную активность в сети;

- защита персональных данных студентов. Организации должны обеспечить адекватную защиту персональных данных студентов, таких как имена, адреса, номера телефонов и другая конфиденциальная информация. Это включает использование современных методов шифрования данных, доступа только для авторизованных лиц и установление жестких политик безопасности;

- безопасное использование облачных сервисов. Многие образовательные организации используют облачные сервисы для хранения и обмена файлами. Важно внимательно выбирать надежные облачные провайдеры и следить за безопасностью хранимых данных. Также рекомендуется обучать студентов основам безопасного использования облачных сервисов, включая установку сильных паролей и ограничение доступа;

- резервное копирование данных. Организации могут регулярно создавать резервные копии ценных данных студентов, чтобы минимизировать риск потери информации в случае системных сбоев или вредоносной атаки. Резервные копии следует хранить на надежных и защищенных устройствах или в удаленных хранилищах данных;

- тестирование на проникновение. Организации могут проводить тестирование на проникновение, чтобы выявить уязвимые места в системе и принять меры по их устранению. Это поможет оценить эффективность текущих мер безопасности и улучшить их, если необходимо.

Особое внимание следует уделить такому методу обеспечения цифровой безопасности студентов, как аудит информационной безопасности. При этом аудит может быть использован как для проверки материально-технической базы и самой системы ИБ образовательного учреждения, так и уровня осведомленности и готовности к угрозам со стороны самих студентов. На рис. 4 представлены основные задачи, которые преследуются в результате проведения аудита информационной безопасности.

Рисунок 4 – Задачи проведения аудита ИБ

Аудит информационной безопасности включает в себя проверку и оценку системы безопасности информации, включая: оценку степени угрозы для информационной системы; проверку соответствия политикам и правилам безопасности информации; анализ доступа к информации и правильности настроек безопасности; проверку защиты от несанкционированного доступа; оценку устойчивости и надежности информационной системы при возникновении различных ситуаций; проверку соответствия законодательству и стандартам в области информационной безопасности. При проведении второго вида аудита ИБ исследуется уровень подготовки к внештатным ситуациям и правилам работы с ИТ у самих студентов.

В результате аудита информационной безопасности может быть выявлены недостатки и уязвимости системы безопасности, а также рекомендации по улучшению защиты информации [12]. Так, результатом аудита информационной безопасности является отчет, где описывается: состояние системы информационной безопасности и ее риски; наличие и эффективность мер защиты от угроз; уровень управления безопасностью информации в организации; рекомендации по усовершенствованию системы информационной безопасности.

Такой анализ помогает образовательным организациям определить слабые точки в защите информации и разработать планы по их устранению, а также повышению уровня информационной безопасности и уменьшению рисков. Также результате проведения данного вида аудита образовательная организация получает детализированный отчет, в котором отражается информация о каждом выявленном недочете, уязвимостях и слабых местах в информационной инфраструктуре. Именно этот отчет является основой в формировании рекомендаций по доработке и улучшению уровня ИБ организации.

Итак, развитие сегмента ИТ происходит непрерывно и очень быстро, что ведет к постоянному обновлению используемого аппаратного и программного обеспечения в образовательных организациях. Это влечет за собой и совершенствование методов, направленных на нарушение системы информационной безопасности современных образовательных организаций со стороны злоумышленников. В результате этого стоит отметить, что, учитывая быстрое развитие технологий, важно постоянно обновлять и адаптировать меры безопасности, чтобы получить возможность защиты студентов от новых угроз. Также важно отметить, что точный перечень действий и вид модели для обеспечения безопасности личности студента будет отличаться в зависимости от определенной организации. В рамках следующей главы будут рассмотрены данные задачи применительно к конкретной образовательной организации.

Выводы по Главе 1

В рамках первой главы магистерской диссертации проведен теоретико-методологический анализ проблемы обеспечения цифровой безопасности студента в информационном пространстве образовательной организации. Определено, что современные образовательные организации активно интегрируют в своей деятельности инновационные информационные технологии, позволяющие рационализировать образовательный процесс, а также повысить его качество и эффективность.

Однако несмотря на ряд объективных преимуществ, при использовании новых информационных технологий современные образовательные организации сталкиваются с рядом сложностей. Актуальной проблемой в рассматриваемой предметной области является обеспечение информационной безопасности и цифровой безопасности личности студентов, в частности. Влияние со стороны злоумышленников может повлечь серьезные негативные последствия, нарушающие целостность информационной среды образовательной организации и приводящие к потере эффективности образовательного процесса.

Также важно отметить, что неправомерные действия со стороны хакеров могут привести к нарушению физического и психоэмоционального состояния студентов, что значительно сказывается на качестве освоения образовательных программ. В связи с этим, необходимо уделять все больше внимания в сторону развития вопросов, связанных с обеспечением ИБ в современных образовательных организациях.

Первая глава диссертации была посвящена анализу по таким аспектам как анализ актуальности по проблеме цифровой безопасности студента в информационном пространстве образовательных организаций, угрозы и проблемы обеспечения цифровой безопасности в образовательных организациях, а также методы по обеспечению цифровой безопасности в информационном пространстве образовательных организаций. В результате

выполнения данной главы диссертации актуализирована задача обеспечения цифровой безопасности личности студентов, а также рассмотрены основные риски и угрозы ИБ, а также методы по борьбе с ними.

Определено, что основными угрозами и проблемами обеспечения ИБ в образовательной организации являются утечка данных, фишинг и вредоносные программы, угрозы внутренних пользователей, несанкционированный доступ и иные. Основными проблемами ИБ являются недостаточная осведомленность сотрудников и студентов о вопросах информационной безопасности, отсутствие строгих политик и процедур по обеспечению информационной безопасности, недостаточная защита сетей и систем от внешних атак, недостаточное обновление программного обеспечения и операционных систем, незаконное использование информационных технологий, отсутствие регулярного обучения сотрудников и студентов профилактике информационной безопасности и иные.

Для возможности снижения влияния и полного исключения данных угроз и проблем в модели обеспечения безопасности необходимо предусмотреть использование таких инструментов, как обучение студентов основам безопасности, фильтрация и мониторинг интернет-трафика, защита персональных данных студентов, тестирование на проникновение и иных вариантов решения задач по обеспечению ИБ применительно к современным образовательным организациям. Отдельно важно подчеркнуть необходимость использования аудита информационной безопасности, которое может дать детализированное представление об уровне готовности образовательной организации и студентов к угрозам ИБ.

Результаты первой главы будут использованы для разработки методики, алгоритмов, требований и самой модели обеспечения цифровой безопасности личности студентов. Следующим этапом исследования

является проработка данных вопросов применительно к реальной образовательной организации.

ГЛАВА 2. АНАЛИЗ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ СТУДЕНТА В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1. Общие сведения об образовательной организации

Рассмотренные проблемы и угрозы информационной безопасности на сегодняшний день применимы практически ко всем учебным заведениям. Это связано с тем, что основное внимание при цифровизации данных организаций уделяется только в сторону повышения качества и эффективности образовательного процесса. В то время, как аспекты информационной безопасности учитываются на недостаточном уровне или же вовсе не берутся в счет [13]. Вследствие этого возникает ряд проблем, ставящих под сомнение реальную эффективность и пользу при интеграции таких технологий. Ведь именно эффективная система ИБ способна снизить основные риски, связанные с интеграцией ИТ и построить в безопасное информационное пространство для эффективного взаимодействия отдельных подсистем.

Объектом для исследования и интеграции разрабатываемой модели обеспечения цифровой безопасности личности студента в рамках диссертации является Государственное бюджетное профессиональное образовательное учреждение «Катав-Ивановский индустриальный техникум». Данное учебное заведение было основано 12 июля 1954 года (Распоряжением Совета Министров СССР от 9.07.1954г. № 7390-р и приказанием Министра промышленности строительных материалов СССР от 12.07.1954 года №1035) и за все время существования выпустило тысячи специалистов по различным областям. Так, основными специальностями, по которым ведется подготовка в данном техникуме являются:

- 09.02.07 Информационные системы и программирование;
- 15.02.08 Технология машиностроения;

- 44.02.01 Дошкольное образование;

- 15.02.12 Монтаж, техническое обслуживание и ремонт промышленного оборудования (по отраслям);

- 08.02.09 Монтаж, наладка и эксплуатация электрооборудования промышленных и гражданских зданий;

- 23.01.17 Мастер по ремонту и обслуживанию автомобилей.

Учебное заведение имеет несколько корпусов для обеспечения образовательной деятельности. В табл. 1 указаны основные адресы осуществления данной деятельности.

Таблица 1 – Адреса осуществления данной деятельности

№ п/п	Адрес места осуществления образовательной деятельности
1	456110, Челябинская область, г. Катав-Ивановск, ул. Гагарина д. 6
2	456110, Челябинская область, г. Катав-Ивановск, ул. Гагарина д. 8
3	456110, Челябинская область, г. Катав-Ивановск, ул. Гагарина д. 10
4	456110, Челябинская область, г. Катав-Ивановск, ул. Остров д. 7

ГБПОУ Катав-Ивановский индустриальный техникум ведет активную студенческую жизнь, организовывая множество различных мероприятий и предоставляя студентам возможности дистанционного взаимодействия с основными ресурсами для обучения. Так, ГБПОУ «Катав-Ивановский индустриальный техникум» имеет разнообразное информационное пространство, которое обеспечивает учащихся и преподавателей всем необходимым для обучения, исследований и развития.

К информационному пространству рассматриваемой организации относятся классные комнаты, оборудованные компьютерами, проекторами и другими техническими устройствами, которые позволяют преподавателям проводить занятия с использованием современных образовательных технологий. В классных комнатах также установлены интерактивные доски, которые помогают визуализировать материал и сделать процесс обучения более интерактивными и привлекательными для студентов.

Для самостоятельной работы студентов доступны компьютерные классы и читальные залы, где студенты могут выполнять учебные задания, исследовать новые темы, писать рефераты и выполнять другие задания, требующие доступа к информационным ресурсам. Также в ГБПОУ «Катав-Ивановский индустриальный техникум» функционирует библиотека, которая содержит большой набор учебников, справочников, художественной литературы и других печатных материалов, необходимых для обучения, исследования и творческого развития студентов. Библиотека также предоставляет доступ к электронным базам данных, журналам и другим источникам информации в формате электронных книг и журналов для возможности бесплатного доступа к закрытым материалам.

Также исследуемая образовательная организация имеет собственный сайт (https://k-iit74.ru) с возможностью входа в личный кабинет студента и преподавателя для более эффективного взаимодействия каждого из них с электронными ресурсами техникума. На сайте выкладываются основные новости, связанные со студенческой жизнью, присутствует форма обратной связи для гостей сайта, возможность связи в социальных сетях, уведомления для участников обучения, а также виден удобный интерфейс для взаимодействия с основными модулями портала. На рис. 5 представлен интерфейс сайта ГБПОУ «Катав-Ивановский индустриальный техникум».

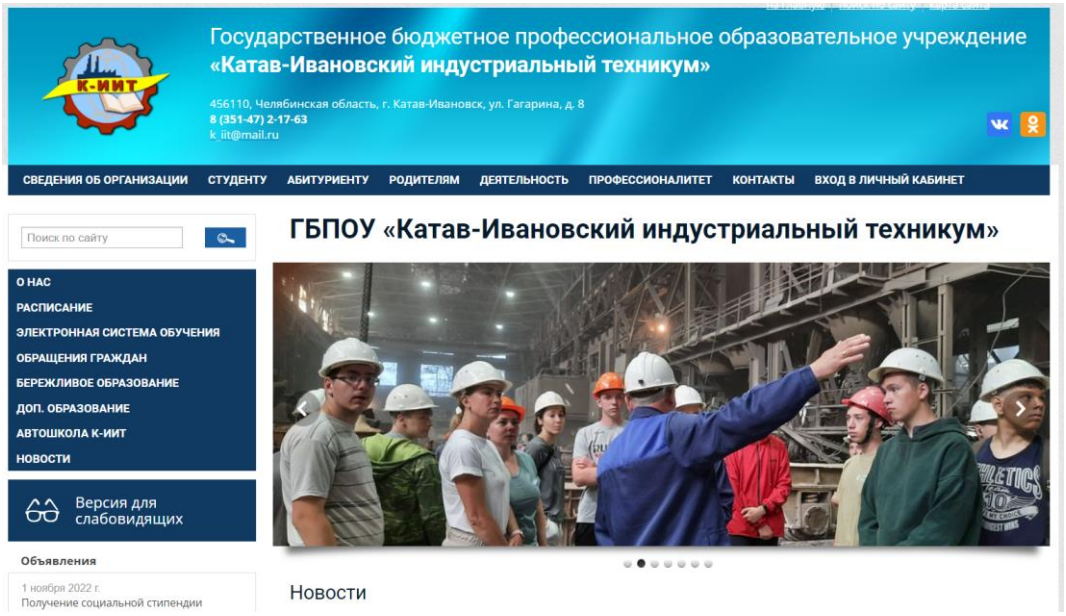


Рисунок 5 – Интерфейс сайта учебного заведения

Кроме того, студенты и преподаватели имеют доступ к интернету через беспроводные сети Wi-Fi, что позволяет им быстро получать информацию, общаться с другими участниками образовательного процесса и использовать онлайн-ресурсы для изучения новых тем и проведения исследований. Так, информационное пространство ГБПОУ «Катав-Ивановского индустриального техникума» является неотъемлемой частью образовательного процесса, обеспечивающей студентам возможность получить доступ к современным знаниям и ресурсам, необходимым для их профессионального роста и развития.

Рассматриваемое учебное заведение ведет подготовку будущих специалистов в форматах очного и заочного обучения. Это подтверждает актуальность и необходимость более глубокого исследования вопросов, связанных с информационной безопасностью личности студентов. Во-первых, студенты очного отделения непрерывно функционируют и взаимодействуют с информационным пространством учебного заведения, в результате чего может наблюдаться множество рисков ИБ, последствия которых будут негативно сказываться не только на технической составляющей самого техникума, но и на студентах. Эта же проблема актуальна и для студентов заочного отделения, которые хоть и меньше

функционируют с информационным пространством учебного заведения, но все также подвержены негативным последствиям при нарушении ИБ.

Важно отметить, что руководство ГБПОУ «Катав-Ивановский индустриальный техникум» понимает указанные риски и активно ведет работу, связанную с минимизацией рисков ИБ. Основным недостатком данной политики является то, что основных усилий недостаточно, а преимущественная их часть направлена только на методические аспекты решения проблемы. На сайте техникума также присутствует специальная памятка для родителей, студентов и преподавателей, ознакомившись с которой можно улучшить навыки работы с информационными технологиями для снижения угроз и проблем информационной безопасности.

2.2. Организационно правовое обеспечение деятельности образовательной организации

Для регулирования вопросов, связанных с обеспечением информационной безопасности на базе ГБПОУ «Катав-Ивановский индустриальный техникум» приняты и используются ряд документов и иных ресурсов. Так, на сайте образовательной организации присутствует специальный раздел «Информационная безопасность», в котором находятся не только нормативные акты и документы, но также памятки по противодействию мошенническим практикам, безопасные сайты и правила работы с информационным пространством [14]. Основными документами для регулирования работы с электронными ресурсами и информацией являются:

- Положение о хранении и использовании персональных данных обучающихся от 19.10.2016;

- Положение о хранении и использовании персональных данных работников техникума от 30.12.2015;

- Положение об информационной безопасности от 30.12.2015.

Также для обеспечения безопасности информационного пространства ГБПОУ «Катав-Ивановский индустриальный техникум» используются определенные нормативные документы. Так, актуальные сведения об федеральных и региональных законах, письмах органов власти и другие нормативно-правовые документы, регламентирующие обеспечение информационной безопасности несовершеннолетних в рамках образовательной организации следующие:

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

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

- Федеральный закон РФ от 29.12.2010 г. № 436 - ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

- Указ Президента РФ от 04.03.2013 г. № 183 «О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием Интернет-ресурса «Российская общественная инициатива».

В состав законодательства по обеспечению информационной безопасности включаются федеральные законы, подзаконные нормативные правовые акты федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты субъектов Российской Федерации. К числу наиболее значимых нормативных правовые актов в области обеспечения информационной безопасности ГБПОУ «Катав-Ивановский индустриальный техникум» относятся следующие законы и подзаконные акты:

- Конституция Российской Федерации (содержит нормы, которые определяют правовые основы информационной безопасности);

- Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» (закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции,

устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности);

- Федеральный закон от 27.07.2006, г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (фиксирует базовые нормы для всей системы информационного законодательства);

- Федеральный закон от 21 июня 1993 № 5485-1 «О государственной тайне», Федеральные законы от 29 июля 2004 № 98-ФЗ «О коммерческой тайне» и от 27.07.2006 г. № 152-ФЗ «О персональных данных» (устанавливают правовые режимы информации ограниченного доступа, в том числе, сведений, составляющих государственную и коммерческую тайну);

- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (нормы названного закона определяют правовой режим технологического обеспечения защиты информации в системе базовых законов информационного законодательства);

- Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Помимо этого, организационно правовое обеспечение ГБПОУ «Катав-Ивановский индустриальный техникум» в отношении обеспечения информационной безопасности включает в себя ряд памяток и требований применительно к работникам и студентам. Так, для работников действуют методические рекомендации «Формирование информационной культуры у обучающихся как основа безопасного поведения в интернет-пространстве (О правилах безопасности при посещении сети Интернет)». Для студентов принята «Памятка для обучающихся об информационной безопасности детей». Для родителей «Памятка родителям об информационной безопасности детей».

Организационно-правовое обеспечение деятельности ГБПОУ «Катав-Ивановский индустриальный техникум» регулирует вопросы информационной безопасности путём установления нормативных правовых актов, которые определяют правила и требования по защите информации, используемой в образовательном процессе. Организационно-правовое обеспечение включает в себя различные нормативно-правовые акты, регламентирующие процессы информационной безопасности. Эти акты определяют правила и требования, которым должна соответствовать образовательная организация для обеспечения безопасности информации.

В первую очередь, к организационно-правовому обеспечению ИБ образовательной организации относятся законы и нормативные акты, регулирующие сохранность информации [15]. Например, законы о государственной тайне могут содержать положения, которые непосредственно относятся к охране информации в образовательных учреждениях. Также важным элементом организационно-правового обеспечения является наличие учредительных документов образовательной организации, где прописаны ее права, обязанности и ответственность в отношении информационной безопасности. Устав, положение и другие документы могут содержать указания по обработке, хранению и передаче информации обучающихся.

Документы, регламентирующие процедуры информационной безопасности, также включают в себя внутренние нормативные документы образовательной организации. Например, это может быть положение о защите информации или инструкции по безопасности, которые определяют порядок работы с информацией, требования к защите от несанкционированного доступа и использования [16]. Важным элементом организационно-правового обеспечения информационной безопасности является также наличие специализированной должности или отдела, ответственных за обеспечение безопасности информации в рассматриваемой образовательной организации. Учреждение имеет

ответственное лицо, которое контролирует и координирует процессы обеспечения информационной безопасности, включая разработку и внедрение соответствующих мер и политик.

Организационно-правовое обеспечение включает в себя также контроль и надзор за выполнением установленных требований по информационной безопасности, назначение ответственных лиц и организацию механизмов реагирования на инциденты информационной безопасности. Таким образом, организационно-правовое обеспечение деятельности образовательной организации регулирует вопросы ИБ путем разработки и применения нормативных актов, учредительных документов, внутренних положений и инструкций, а также создания структурных подразделений или должностей, ответственных за безопасность информации.

В рамках исследования организационно-правового обеспечения ГБПОУ «Катав-Ивановский индустриальный техникум» определено, что данное учебное заведение активно принимает и использует в своей деятельности свежие нормативные акты, документы и иные регулирующие ресурсы. Это позволяет сделать вывод о готовности техникума к угрозам ИБ в методическом отношении.

2.3. Политика безопасности образовательной организации

Политика информационной безопасности образовательной ГБПОУ «Катав-Ивановский индустриальный техникум» включает комплекс мер и правил, направленных на обеспечение защиты информационных ресурсов и данных, обрабатываемых и хранимых в системах и сетях образовательного учреждения. Она охватывает все аспекты информационной безопасности, включая защиту от несанкционированного доступа, вредоносного программного обеспечения, утечки данных, манипуляций информацией и других угроз.

Политика информационной безопасности также должна определять цели и задачи в области защиты информации, а также принципы и правила, которые образовательное учреждение будет соблюдать при работе с информацией [17]. Она должна устанавливать также ответственность за информационную безопасность, роли и обязанности сотрудников образовательной организации, связанные с защитой информации.

Политика ИБ также должна включать планы и процедуры по противодействию инцидентам информационной безопасности. Она должна определять процедуры по обнаружению и реагированию на угрозы, процедуры резервного копирования и восстановления данных, а также процедуры обработки инцидентов и уведомления о них. Более того, политика информационной безопасности должна включать механизмы контроля и мониторинга для обеспечения соблюдения всех установленных правил и мер безопасности.

Все сотрудники образовательной организации должны быть ознакомлены с данной политикой и соблюдать ее требования. Образовательное учреждение должно проводить регулярное обучение и тренинги по вопросам информационной безопасности для своих сотрудников, чтобы повысить их осведомленность и готовность к действиям в случае инцидента информационной безопасности.

В ходе исследования определено, что в ГБПОУ «Катав-Ивановский индустриальный техникум» действует достаточно эффективная политика информационной безопасности, четко определяющая цели и задачи при обеспечении безопасной работы с информационным пространством. Также, как уже было указано ранее, на сайте определены методические рекомендации для студентов, родителей и преподавателей, ознакомление с которыми позволит существенно снизить вероятность возникновения угроз и проблем ИБ, что в конечном итоге повысит цифровую безопасности личности студента в образовательной деятельности.

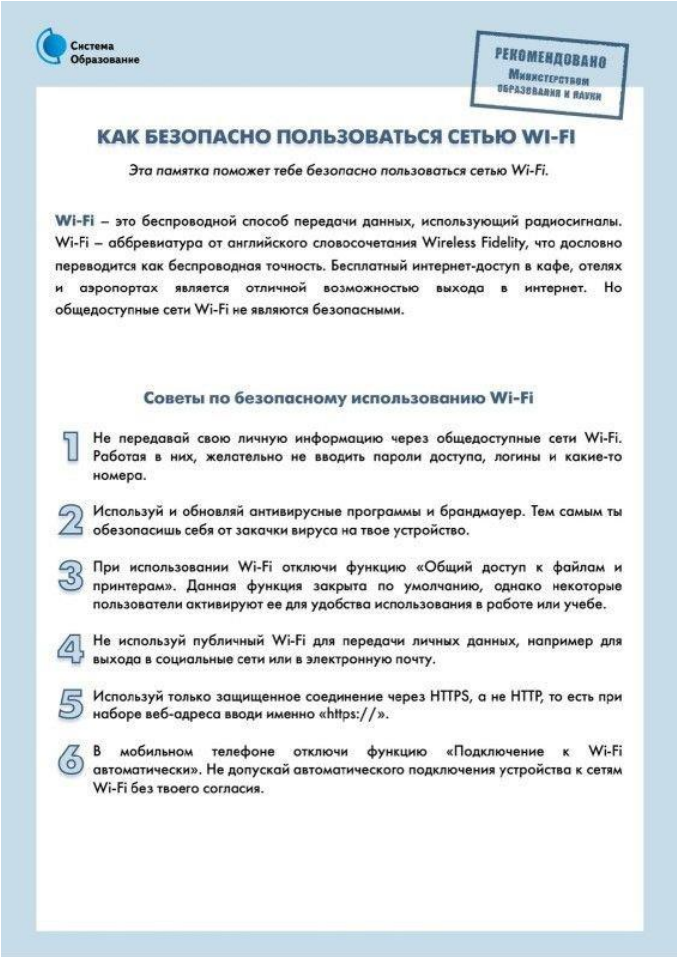
Так, к примеру, для педагогов действуют методические рекомендации «Формирование информационной культуры у обучающихся как основа безопасного поведения в интернет-пространстве (О правилах безопасности при посещении сети Интернет)». Данные рекомендации разработаны с целью обеспечения реализации образовательными организациями системы мероприятий, направленных на обучение учащихся правилам безопасного поведения в интернет-пространстве, профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность.

Памятка для обучающихся «Памятка для обучающихся об информационной безопасности детей» определяет четкий перечень того, что можно и нельзя делать в информационном пространстве образовательной организации. Вместе с этим, данная памятка включает описание методов защиты от вредоносных программ, советы по безопасности работе в общедоступных сетях Wi-Fi, основные советы по безопасности в социальных сетях, основные советы по безопасной работе с электронными деньгами, основные советы по безопасной работе с электронной почтой и множество иных рекомендаций для обеспечения безопасности при работе в информационном пространстве.

Для родителей принята «Памятка для родителей об информационной безопасности детей». В основе данной памятки включены основные правила и советы для обеспечения безопасности работы детей с информационными технологиями силами родителей [18]. Включены советы по безопасной работе и конкретные действия для родителей, выполнение которых позволит снизить вероятность наступления угроз информационной безопасности и повысит в конечном итоге цифровую безопасность личности студентов.

Материалы из памяток для студентов и их родителей дополнительно оформлены в слайдовой форме для дальнейшей печати и развешивания на

информационных плакатах в стенах учебного заведения. На рис. 6-7 представлены примеры информационных памяток для обучающихся.



Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СЕТЬЮ WI-FI

Эта памятка поможет тебе безопасно пользоваться сетью Wi-Fi.

Wi-Fi – это беспроводной способ передачи данных, использующий радиосигналы. Wi-Fi – аббревиатура от английского словосочетания Wireless Fidelity, что дословно переводится как беспроводная точность. Бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но общедоступные сети Wi-Fi не являются безопасными.

Советы по безопасному использованию Wi-Fi

1. Не передавай свою личную информацию через общедоступные сети Wi-Fi. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера.
2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство.
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.
4. Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети или в электронную почту.
5. Используй только защищенное соединение через HTTPS, а не HTTP, то есть при наборе веб-адреса вводи именно «https://».
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Рисунок 6 – Памятка «Как безопасно пользоваться сетью Wi-Fi»

Данная памятка акцентирует внимание на основных советах при работе с общедоступными сетями Wi-Fi. Их использование позволяет снизить риски и угрозы, возможные при работе с такими сетями.

Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК ЗАЩИТИТЬСЯ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Эта памятка поможет тебе безопасно находиться в сети

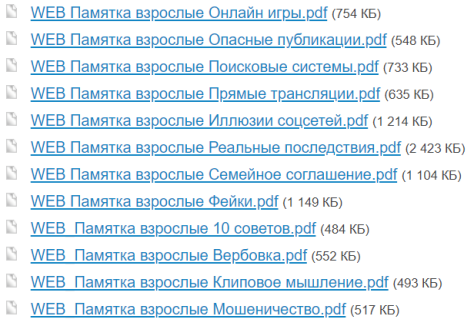
Компьютерный вирус – это программа, отличительной особенностью которой является способность к размножению. Вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ.
2. Постоянно устанавливай патчи (цифровые заплатки для программ) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его.
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере.
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз.
5. Ограничь физический доступ к компьютеру для посторонних лиц.
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников.
7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Рисунок 7 – Памятка «Как защититься от компьютерных вирусов»

Памятка на рис. 7 включает в себя определение компьютерного вируса и конкретные методы, использование которых позволяет снизить вероятность заражения рабочих ноутбуков и компьютеров студентов вредоносным программным обеспечением. Помимо этих памяток на сайте техникума также представлены общие памятки для всех тех, кто использует в своей досуговой и образовательной деятельности ИТ (рис. 8).



- WEB Памятка взрослые Онлайн игры.pdf (754 КБ)
- WEB Памятка взрослые Опасные публикации.pdf (548 КБ)
- WEB Памятка взрослые Поисковые системы.pdf (733 КБ)
- WEB Памятка взрослые Прямые трансляции.pdf (635 КБ)
- WEB Памятка взрослые Иллюзии соцсетей.pdf (1 214 КБ)
- WEB Памятка взрослые Реальные последствия.pdf (2 423 КБ)
- WEB Памятка взрослые Семейное соглашение.pdf (1 104 КБ)
- WEB Памятка взрослые Фейки.pdf (1 149 КБ)
- WEB_Памятка взрослые 10 советов.pdf (484 КБ)
- WEB_Памятка взрослые Вербовка.pdf (552 КБ)
- WEB_Памятка взрослые Клиповое мышление.pdf (493 КБ)
- WEB_Памятка взрослые Мошеничество.pdf (517 КБ)

Рисунок 8 – Общие памятки для пользователей ИТ

В результате анализа политики безопасности ГБПОУ «Катав-Ивановский индустриальный техникум» можно сделать вывод о том, что руководство учебного заведения заинтересовано в обеспечении цифровой безопасности личности студентов и других участников образовательного процесса и предпринимает все необходимые для этого действия. Действующие нормативно-правовые акты, документы, рекомендации и памятки способствуют повышению цифровой грамотности и развитию компетенций информационной безопасности.

Основным недостатком, выявленным в результате анализа, стало отсутствие проведения контроля для отслеживания уровня подготовки студентов к безопасной работе с информационными технологиями. Помимо этого, на базе техникума отсутствует материально-техническая база, позволяющая в режиме реального времени отслеживать атаки и иные угрозы информационной безопасности. В связи с этим следует отметить, что при разработке модели обеспечения цифровой безопасности личности студента необходимо проводить работу параллельно в двух направлениях – обеспечение цифровой безопасности в техническом аспекте и обеспечение безопасности в методологическом аспекте, в частности, путем интеграции средств контроля и мониторинга компетенций информационной безопасности для студентов и работников.

Предполагается, что разработка и интеграция разрабатываемых политик и требований приведет к значительному повешению цифровой безопасности личности студента, а также позволит практически полностью исключить вероятность возникновения различных угроз и проблем ИБ [19]. При этом полное исключение всех угроз, как было указано ранее в работе, невозможно ввиду непрерывного развития самих ИТ, так и технологий нарушения целостности ИБ со стороны злоумышленников. Несмотря на это возможно сведение вероятности негативных последствий к минимуму, что позволит обеспечить высокий уровень цифровой безопасности студентов ГБПОУ «Катав-Ивановский индустриальный техникум».

Выводы по Главе 2

В рамках второй главы магистерской диссертации проведен полный анализ системы обеспечения цифровой безопасности личности студента в образовательной организации ГБПОУ «Катав-Ивановский индустриальный техникум». Автором проанализированы общие сведения об образовательной организации, организационно правовое обеспечение деятельности образовательной организации, а также действующая политика безопасности образовательной организации.

Выяснено, что исследуемое учебное заведение активно интегрирует и использует в своей деятельности множество инновационных информационных технологий, которые позволяют существенно повысить качество и эффективность освоения студентами образовательных программ. Так, в информационном пространстве рассматриваемой организации включены комнаты, оборудованные компьютерами, проекторами и другими техническими устройствами. Также в аудиториях установлены интерактивные доски, которые помогают визуализировать материал и сделать процесс обучения более интерактивными и привлекательными для студентов.

ГБПОУ «Катав-Ивановский индустриальный техникум» имеет собственный сайт с личным кабинетом для каждого студента и работника. Информационное пространство включает в себя множество информационных систем, электронную библиотеку и иные инструменты. Совокупность данных факторов свидетельствует о наличии рисков, связанных с нарушением системы информационной безопасности и наличием угрозы утечки, фальсификации и изменении информации со стороны злоумышленников.

Для предотвращения противоправных действий и снижения вероятности негативных последствий руководством техникума активно разрабатываются и внедряются нормативно правовые акты, документы и

памятки, ознакомление с которыми способствует повышению осведомленности студентов о рисках работы с ИТ и развитию компетенций в области ИБ.

На рис. 6-8 в качестве примера приведены реально существующие памятки для студентов, ознакомление с которыми позволяет снизить степень потенциальных проблем при работе с информационными технологиями. Ресурсом для их создания стали памятки для студентов и родителей, принятые руководством ГБПОУ «Катав-Ивановский индустриальный техникум». Лаконичный дизайн позволяет привлечь интерес студентом и родителей, а также ознакомить с правилами работы в информационном пространстве и повысить компетенции, связанные с ИБ.

Несмотря на это, анализ показал объективные недостатки в системе обеспечения цифровой безопасности личности студента. Так, ключевым недостатком стало отсутствие проведения контроля для отслеживания уровня подготовки студентов к безопасной работе с информационными технологиями. Также выяснено, что на базе техникума отсутствует полная материально-техническая база, позволяющая в режиме реального времени отслеживать атаки и иные угрозы информационной безопасности.

В результате проведенного анализа определено, что при разработке модели обеспечения цифровой безопасности личности студента необходимо проводить работу сразу в двух направлениях – обеспечение цифровой безопасности в техническом аспекте и обеспечение безопасности в методологическом аспекте. Во втором направлении предполагается повышение уровня безопасности в результате интеграции средств контроля и мониторинга компетенций ИБ для студентов и работников.

Следующим этапом исследования станет формирование требований к задаче по обеспечению безопасного информационного пространства и разработка модели. Предполагается, что разработка и использование новой модели позволит существенно повысить уровень цифровой безопасности личности студента и до минимума снизить потенциальные проблемы,

наблюдаемые при использовании студентами новых информационных технологий в образовательной деятельности.

ГЛАВА 3. ОПЫТНО-ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО ОБЕСПЕЧЕНИЮ ЦИФРОВОЙ БЕЗОПАСНОСТИ СТУДЕНТА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

3.1 Формирование требований к задаче по обеспечению безопасного информационного пространства

Как уже было определено ранее, обеспечение безопасного информационного пространства является главной частью в решении задачи по обеспечению цифровой безопасности личности студента. ГБПОУ «Катав-Ивановский индустриальный техникум» активно интегрирует в своей деятельности передовые информационные технологии, что актуализирует задачу по разработке эффективной модели безопасного использования информационного пространства образовательной организации.

Анализ, проведенный в предыдущих главах настоящей магистерской диссертации, определил, что формирование требований и разработка модели должны происходить по двум основным направлениям. Первым из них является материально-техническая часть учебного заведения [20]. В рамках данного направления необходимо определить основные требования аппаратно-программной части используемых технологий, исполнение которых будет способствовать повышению уровня информационной безопасности при использовании ИТ в техникуме.

Вторым направлением формирования требований к задаче по обеспечению безопасного информационного пространства является разработка модели аудита студентов с целью освоения последними навыков безопасной работы с информационными технологиями и получения возможности отслеживания результатов [21]. Так можно выделить первое и самое главное требование при разработке модели – комплексность. Только

при таком подходе можно получить эффективный инструмент обеспечения ИБ студента.

На рис. 9-10 представлены основные требования к задаче по обеспечению безопасного информационного пространства по каждому из данных направлений.

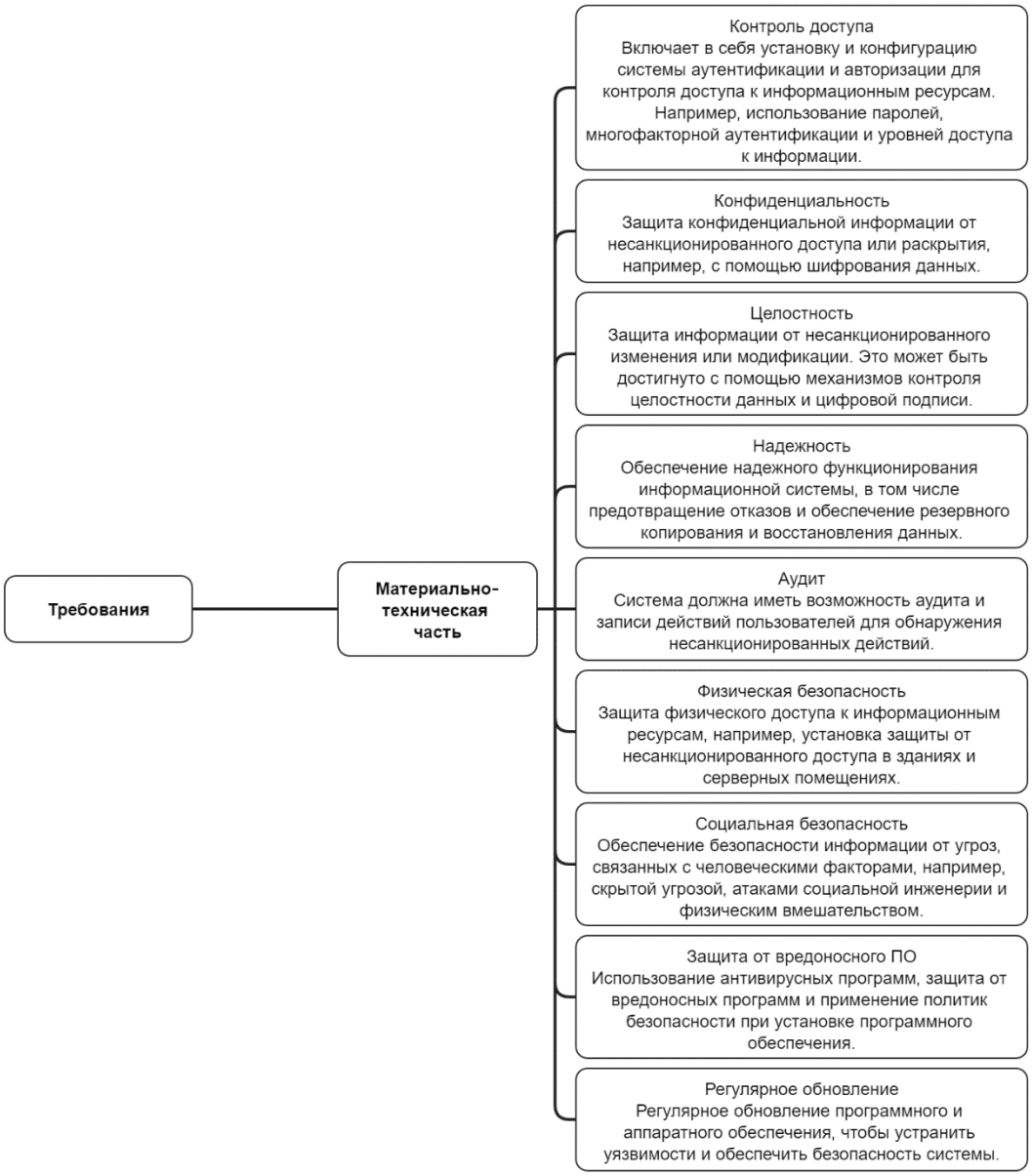


Рисунок 9 – Требования по материально-технической части

Обеспечение указанных на рис. 9 требований, позволит повысить безопасность информационного пространства образовательного учреждения в техническом отношении.

Основным требованием к студентам является освоение компетенций информационной безопасности. Для этого необходимо обеспечить выполнение пунктов, указанных на рис. 10.

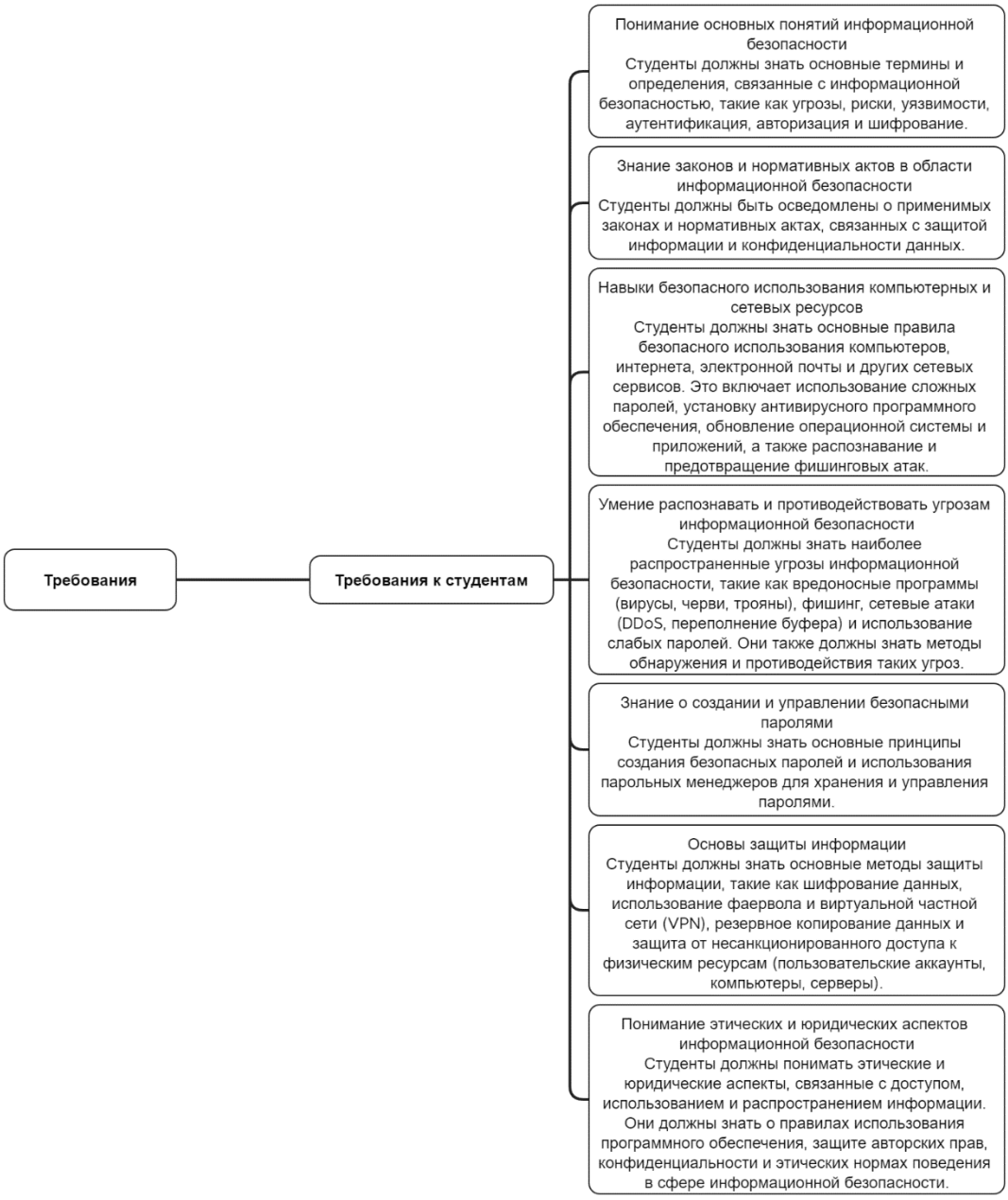


Рисунок 10 – Требования к студентам

На рис. 10 представлены базовые требования к компетенциям по информационной безопасности, которые позволят снизить риски, связанные с использованием информационных технологий.

При этом для обеспечения выполнения требований, предъявляемых студентам, необходимо использовать подход, основанный на методическом аудите информационной безопасности. В данном случае необходимо проводить две формы аудита, первый из которых направлен на освоение студентами компетенций, а второй на контроль знаний и оценку уровня освоения компетенций [22]. Важно подчеркнуть, что освоение компетенций также может быть реализовано путем интеграции в образовательные программы дополнительного модуля или дисциплины, в рамках которой будет производиться обучение студентов по основным угрозам и мерам их противодействие при работе с информационным пространством образовательной организации.

На рис. 11 представлен основной перечень требований, предъявляемых к данному аудиту. В данный перечень включены основные аспекты, касающиеся как самого обучения, так и контроля знаний с последующей корректировкой. Важно отметить, что проведение такого аудита должно быть систематическим (каждый семестр/курс). Это позволит удерживать уровень компетенций ИБ студентами на протяжении всего обучения.

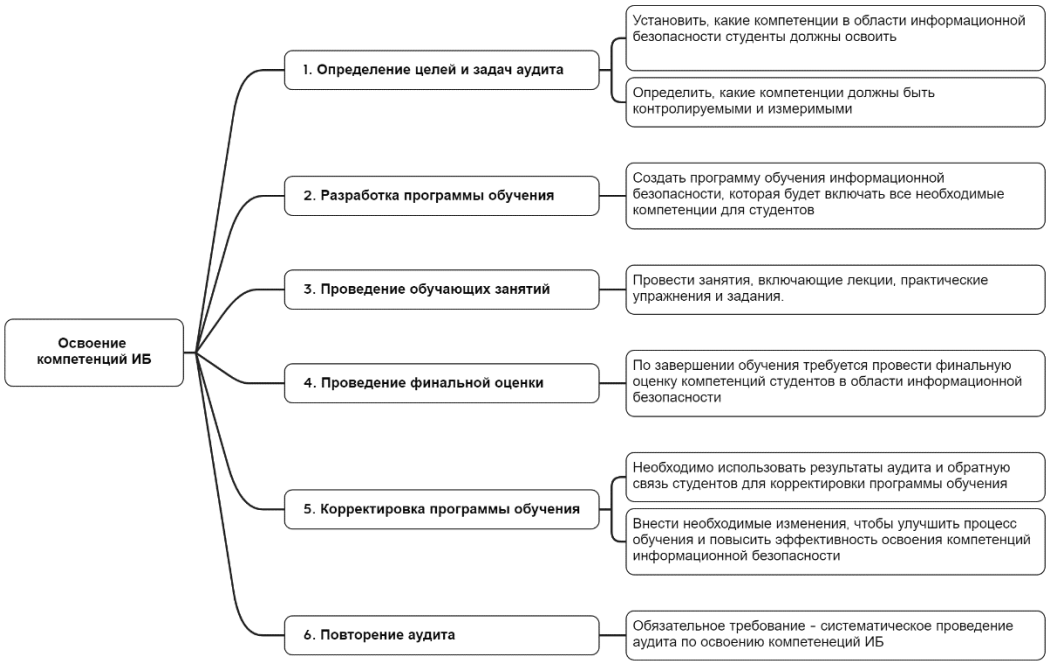


Рисунок 11 – Требования к составу аудита освоения компетенций ИБ

3.2 Разработка модели по обеспечению безопасного информационного пространства

В составе модели по обеспечению безопасного информационного пространство должно быть 3 основных блока. Первый из них определяет выполнение требований к материально-технической части учебного заведения, обеспечивая безопасность при работе с информационным пространством техникума [23]. Второй блок модели должен включать в себя исполнение требований, предъявляемых к студентам в части освоения компетенций информационной безопасности. Третий блок должен иметь регулирующую функцию, состав которого будет направлен на контроль взаимодействия всех блоков с целью получения наибольшего эффекта и результата при обеспечении цифровой безопасности личности студента.

Важной частью обеспечения безопасного информационного пространства должен стать аудит технической составляющей взаимодействующих компонентов [24]. В данном случае под компонентами понимаются используемые в техникуме информационные системы, аппаратные инструменты, программы и иные решения. Также необходимо

отметить, что главным требованием должно стать проведение именно комплексного аудита информационной безопасности.

Основными преимуществами проведения комплексного аудита ИБ является получение наиболее полной, объективной и в то же время независимой оценки состояния информационной инфраструктуры. Фактически говоря, комплексный аудит информационной безопасности является симбиозом всех видов аудита информационной безопасности. Именно по результатам его проведения заказчик может получить оценку уровня и состояния существующей системы информационной безопасности, а также защищенность внутренних и внешних информационных ресурсов [25]. Вместе с этим, рассматриваемый метод проведения аудита также основывается на стандартах информационной безопасности.

На рис. 12 представлен состав мероприятий при проведении комплексного аудита информационной безопасности в ГБПОУ «Катав-Ивановский индустриальный техникум».

Рисунок 12 – Направления при проведении комплексного аудита ИБ

В общем виде комплексный аудит имеет в своем составе и такие виды аудита, как: экспертный аудит; тестирование на проникновение; аудит Web-безопасности; аудит информационных систем [26]. Также важно отметить, что состав работ в рамках его проведения заранее обсуждается и

утверждается с заказчиком. Провести данный вид аудита можно как внешними, так и внутренними силами специалистов в организации. Однако во втором случае не всегда наблюдается объективная оценка уровня защиты информационных систем. Именно поэтому для получения всесторонне объективной оценки прибегают к использованию внешних экспертов.

На рис. 13 представлен алгоритм, интеграция которого необходима для оценки текущего уровня защищенности информационного пространства образовательной организации. В результате проведения данного вида аудита организация получает детализированный отчет, в котором отражается информация о каждом выявленном недочете, уязвимостях и слабых местах в информационной инфраструктуре [27]. Именно этот отчет является основой в формировании рекомендаций по доработке и улучшению уровня ИБ организации.

Рисунок 13 – Алгоритм проведения комплексного аудита ИБ

При этом видом выбранного аудита должен стать именно риск-ориентированный аудит ИБ. Данный подход подразумевает наличие систематических процедур, инструментов и методов, которые помогают анализировать и оценивать риски в ИБ на стадии планирования, реализации

и эксплуатации. Риск-ориентированный подход позволяет выявлять уязвимости и определять наиболее значимые угрозы, которые могут нарушить безопасность информационной системы, а также определять эффективность контрольных мер, которые применяются для управления рисками безопасности информации. Основным принципом данного подхода является максимальная ориентация на защиту самых ценных активов организации и сокращение рисков до приемлемого уровня [28]. Таким образом, риск-ориентированный подход к аудиту ИБ помогает улучшить уровень безопасности информационных систем организации и значительно снизить вероятность негативных последствий нарушения безопасности.

Риск-ориентированный подход к проведению аудита ИБ позволяет решить целый ряд задач, представленных на рис. 14.

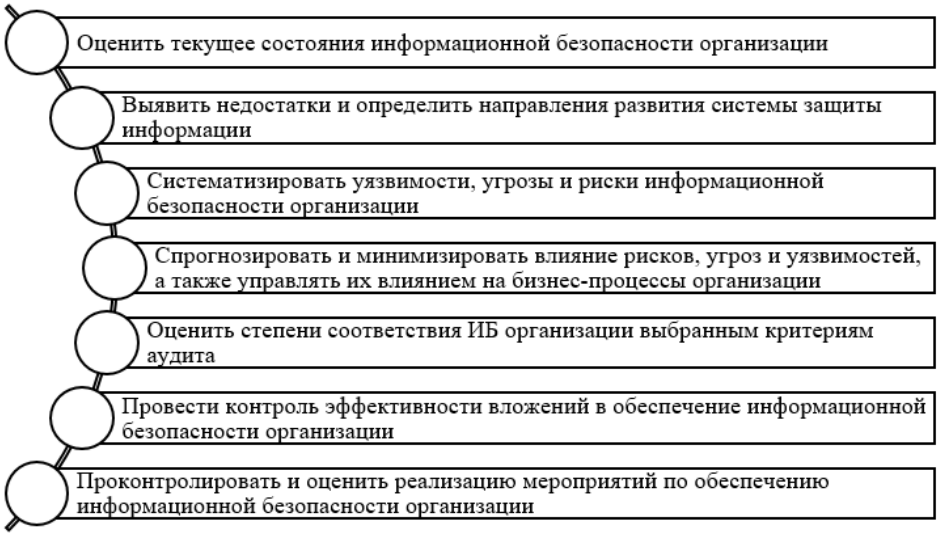


Рисунок 14 – Задачи риск-ориентированного подхода аудита ИБ

Проведение аудита ИБ на основе риск-ориентированного подхода включает в себя пять основных действий, в составе каждого из которых можно выделить конкретное действие, значение и результат. Представленная ниже модель отражает каждый из этапов проведения данного аудита.

Этап 1. Проведение анализа бизнес-процессов:

1.1 Действие: Данный анализ помогает идентифицировать и документировать важные бизнес-процессы и лежащие в их основе зависимости, а также оценивать и ранжировать их на основе критичности. Технические и нетехнические факторы включены в качестве зависимостей (например, активы, персонал, данные, оборудование и приложения).

1.2 Значение: Анализ показывает, как эти ключевые операции и функции повлияют на непрерывность бизнеса, если они будут затруднены или устранены.

1.3 Результат: Проведение анализа влияния на бизнес - это первый шаг в создании планов обеспечения непрерывности бизнеса и аварийного восстановления. Анализ идентифицирует критически важные бизнес-процессы в ГБПОУ «Катав-Ивановский индустриальный техникум» и поддерживающие их элементы, помогая понять среду и, что наиболее важно, прежде чем будут приняты шаги для ее защиты.

Этап 2. Проведение оценки рисков:

2.1 Действие: Оценка риска - это количественный и качественный процесс, который выявляет угрозы, уязвимости и нормативные требования, применимые к соответствующим бизнес-процессам и базовым зависимостям [29]. Затем он рассчитает возможные последствия, и если эти угрозы будут реализованы, то выдаст выходное значение риска.

2.2 Значение: Выходное значение риска дает руководству возможность понять и помочь определить приоритеты различных рисков, с которыми сталкивается организация. Этот результат является одним из самых больших преимуществ этого подхода, позволяющего создавать персонализированные показатели на основе вашей организации. По сравнению с использованием готовых обобщенных «рисков» для организации программы кибербезопасности, которые могут не иметь

значения и не защищать организацию от конкретных проблем, с которыми оно сталкивается.

2.3 Результат: Знание выходного значения риска дает возможность ранжировать определенные уязвимости в реестре рисков (инструмент управления рисками, который объединяет результаты оценки рисков в одном месте). Реестр рисков обеспечивает действенную отправную точку для сосредоточения стратегических ресурсов на снижении рисков, представляющих наибольшую угрозу для непрерывности бизнеса и соблюдения нормативных требований.

Этап 3. Определение и внедрение необходимых средств контроля:

3.1 Действие: на этом этапе эксперт берет во внимание наиболее опасные риски, определяет, адаптирует, внедряет и назначает ответственность за элементы управления, которые смогут их уменьшить. Средство контроля - это основанное на действиях заявление, в котором содержатся инструкции о том, как уменьшить или свести к минимуму риски безопасности. Примеры систем контроля кибербезопасности: NIST 800-53, CIS, HITRUST CSF, ISO 27001/27002, COBIT, PCI DSS. Это предварительно упакованные средства управления безопасностью в отрасли рисков, которые можно настроить для каждой конкретной организации.

3.2 Значение: Персонализированные риски позволят специалистам ГБПОУ «Катав-Ивановский индустриальный техникум» лучше настраивать средства контроля для устранения выявленных уязвимостей и угроз. Это также позволяет организации использовать компенсирующие меры, поскольку весь процесс принятия решений документируется. Документация демонстрирует, что организация понимает угрозу, которую средство контроля должно покрывать, и адекватно применяет другие компенсирующие средства контроля на основе анализа затрат и рисков.

3.3 Результат: Определение и внедрение правильных или необходимых средств контроля обеспечивает структуру и возможность

обновлять или создавать политики и процедуры, которые укрепляют и передают видение и приоритеты организации в отношении ее кибербезопасности [30]. Точно так же этот подход может обеспечить более активное участие и соблюдение требований, поскольку он создает возможность для диалога с отдельными заинтересованными сторонами, которые «владеют» процессом, включая поддержку со стороны критически важного руководства среднего звена. По сути, этот подход, основанный на оценке рисков, дает руководству убедительную причину для адаптации и принятия решений при бездействии и возможных последствий.

Этап 4. Тестирование, проверка и отчет:

4.1 Действие: После того, как средства безопасности будут реализованы, их необходимо протестировать и подтвердить. Примеры различных типов тестирования включают тесты на проникновение, дополнительные оценки рисков, тесты управления уязвимостями, упражнения на обеспечение непрерывности бизнеса, внутренние аудиты и оценки контроля соответствия [31]. Именно это этап является одним из наиболее важных при решении задачи обеспечения цифровой безопасности личности студента, снижая влияния внешнего воздействия.

4.2 Значение: Тестирование и проверка не только вам уверенность в том, что элементы управления работают и обеспечивают необходимую безопасность, но и при периодической переоценке предоставляют возможности для включения недавно реализованных элементов управления безопасностью. Теперь руководство может получить новую оценку стоимости риска, называемую остаточным риском, которая документируется и добавляется в реестр рисков для будущего анализа и определения приоритетов. Основываясь на инвестициях в новый контроль, рейтинг риска может снизиться, что указывает на совершенствование системы ИБ.

4.3 Результат: Действия по тестированию и проверке должны быть задокументированы и зарегистрированы. Наличие эффективного механизма

отчетности продемонстрирует ваш прогресс на пути к исполнительному руководству и соответствие требованиям регулирующих органов. Кроме того, эффективная отчетность закладывает основу для создания процессов устранения рисков.

Фаза 5. Непрерывный мониторинг и управление:

5.1 Действие: На этом последнем этапе цель - оформить этапы 1–4 в воспроизводимый бизнес-процесс. Оценки рисков должны проводиться не реже одного раза в год, а действия по устранению последствий должны осуществляться, контролироваться и включаться в реестр рисков. Кроме того, должны быть созданы механизмы отчетности для внутренних сотрудников, чтобы выявлять и делиться потенциальными рисками для образовательной организации [32]. Часто у менеджеров и других сотрудников есть важные сведения о слабых сторонах или нарушениях нормативно-правовых требований, которые могут быть скрыты от группы управления рисками. Если организация придерживается всего цикла, то точно обнаружит пробелы в процессах либо из-за плохо реализованных средств контроля, либо из-за упущений в процессе выявления рисков.

5.2 Значение: Соблюдение цикла может гарантировать, что любые новые уязвимости или угрозы будут выявлены и устранены последовательно и своевременно, что снизит вероятность того, что основные проблемы останутся незамеченными. На этом этапе сотрудники могут отмечать проблемы, уведомлять организацию, а также оценивать ущерб в случае эксплуатации.

5.3 Результат: Непрерывное управление на протяжении всего жизненного цикла подхода, основанного на оценке рисков, будет способствовать подотчетности за внедрение и оценку средств контроля. Это создает пути эскалации для сложных или несоответствующих заинтересованных сторон и обеспечивает последовательность в адаптации контроля [33]. Наконец, цикл предоставляет возможность обновлять или

создавать необходимые политики или процедурную документацию и последовательно сообщать об изменениях в организацию.

Подход к программе кибербезопасности, основанный на оценке рисков, а не на соответствии или контрольных списков, принесет много преимуществ, включая персонализированную оценку риска, расставленные по приоритетам пробелы, адаптированные средства контроля и более надежный цикл для устранения новых рисков и уязвимостей. Аудит ИБ на основе риск-ориентированного подхода способен предоставить руководству ГБПОУ «Катав-Ивановский индустриальный техникум» возможность получения независимого взгляда на существующую систему ИБ и выявить шаги, необходимые для совершенствования системы информационной безопасности [34]. Данный аудит дает оценку защищенности образовательной организации, выявляет риски и создает план конкретных действий, направленных на минимизацию их влияния.

Второй блок модели обеспечения безопасной работы в информационном пространстве техникума должен включать порядок действий при проведении аудита, направленного на освоение компетенций информационной безопасности и их контроля студентами образовательной организации [35]. Основными составляющими данного аудита должны стать постановка целей и задач аудита, сбор исходных результатов перед началом освоения компетенций, результаты после освоения и систематический повтор.

На рис. 15 представлен алгоритм проведения аудита по освоению компетенций ИБ студентами совместно с модулями контроля знаний, анализа и систематического повтора обучения.

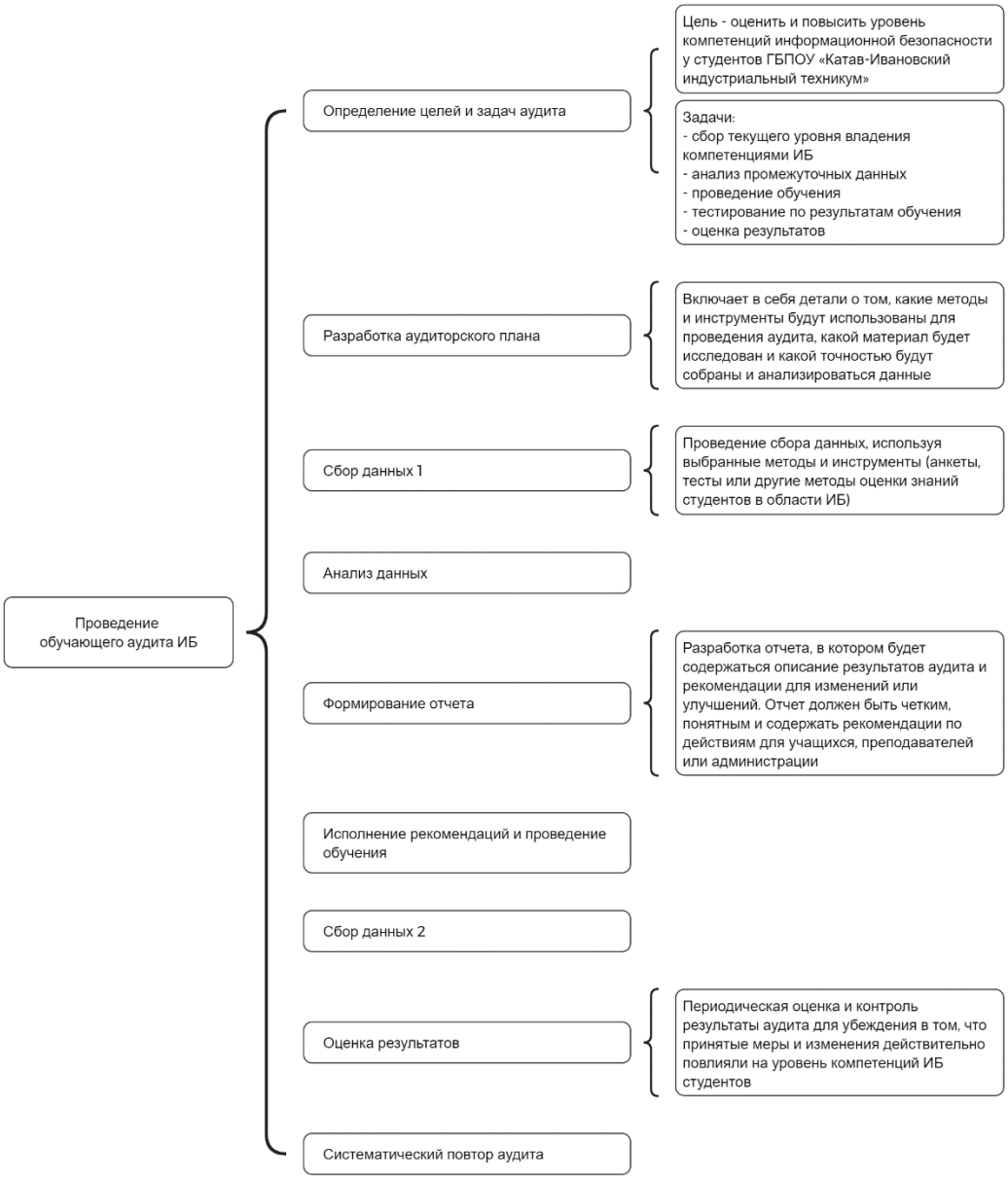


Рисунок 15 – Порядок проведения обучающего аудита ИБ

Третий блок модели обеспечения цифровой безопасности студента должен включать в себя регулирующую документацию, нормативно-правовые акты и иные ресурсы, обеспечивающие контроль взаимодействия всех блоков, обучения студентов и порядок работы с ИТ организации [36].

На рис. 16 представлен итоговый вид модели по обеспечению безопасного информационного пространства, направленной на повышение цифровой безопасности студента ГБПОУ «Катав-Ивановский индустриальный техникум».

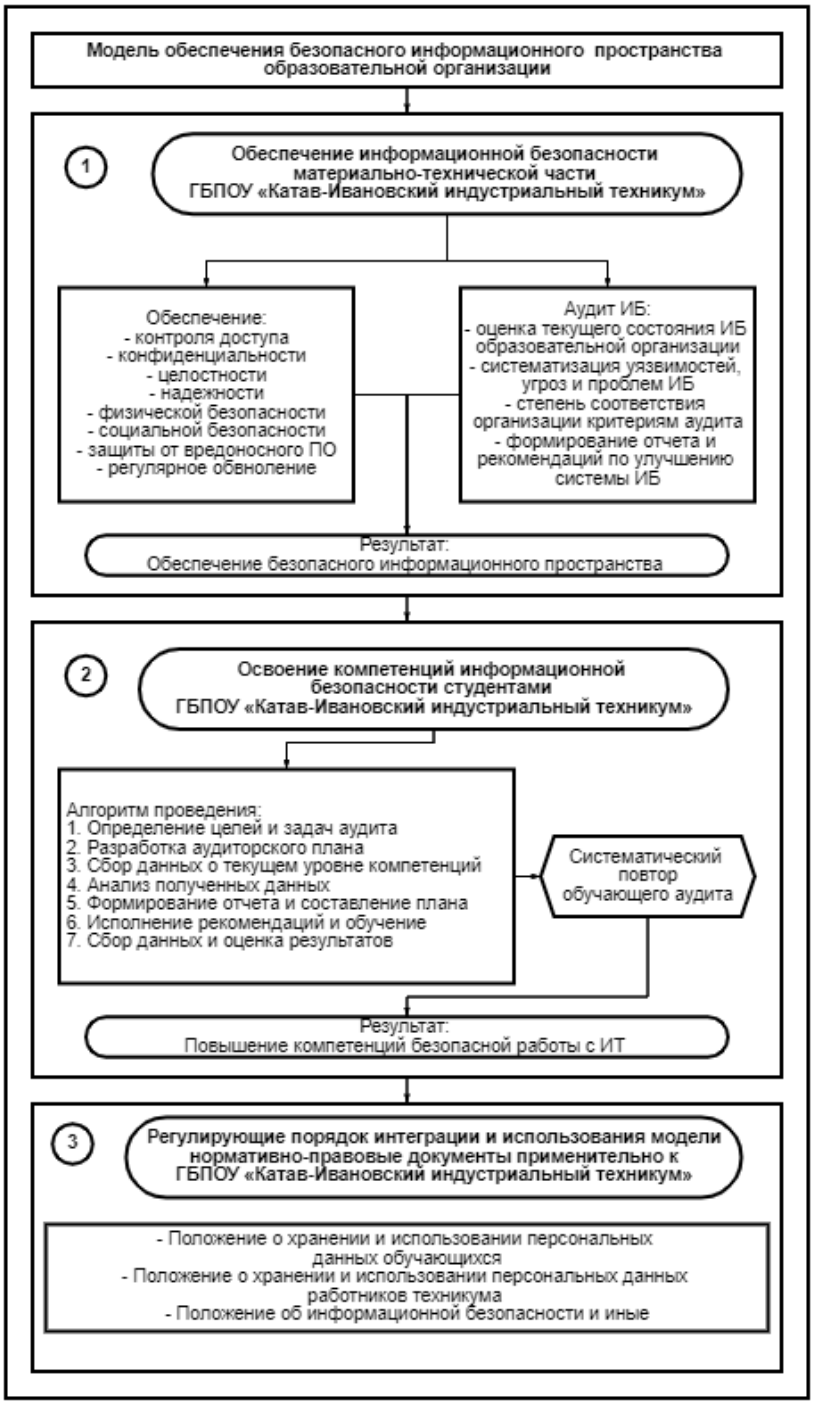


Рисунок 16 – Модель обеспечения безопасного информационного пространства образовательной организации

3.3 Реализация и анализ эффективности модели обеспечения цифровой безопасности студента

Для проведения анализа эффективности разработанной модели был использован метод анкетирования. Оценка результатов производилась в 2 этапа, первый из которых проводился для сбора информации об уровне безопасности работы в информационном пространстве ГБПОУ «Катав-Ивановский индустриальный техникум» до интеграции модели и после. Для оценки студентам группы ИС-31 в количестве 30 человек для заполнения был дан следующий бланк, представленный на табл. 2.

Таблица 2 – Бланк для оценки уровня ИБ студентов

	Оценка влияния (0-5)	Затрудняюсь ответить (×)
1. Сталкиваетесь ли вы с фишинговыми атаками при работе в информационном пространстве техникума?		
2. Как часто на вашем рабочем столе компьютера (ноутбука) всплывает навязчивая реклама?		
3. Бывают ли ситуации смены пароля от аккаунтов без вашего уведомления?		
4. Часто ли ваша антивирусная система предупреждает вас о возможных угрозах и вредоносном ПО?		
5. Происходит ли влияние на ваше психоэмоциональное состояние при работе в информационном пространстве техникума?		
6. Происходят ли ситуации, когда ваша личная информация попадает на сторонние сайты?		
7. Замечаете ли вы списание денежных средств с электронных счетов без вашего уведомления?		

Для ответа на вопрос было предложено использование 5-балльной системы оценки, где: 1 – отсутствие влияния угроз (проблем) ИБ; 2 – низкий

уровень влияния угроз (проблем) ИБ; 3 – средний уровень влияния угроз (проблем) ИБ; 4 – ощутимый уровень влияния угроз (проблем) ИБ; 5 – высокий уровень влияния угроз (проблем) ИБ. Затрудняюсь ответить – поле для выставления пометки при невозможности дать ответ на поставленный вопрос. В результате проведения анкетирования в сентябре 2023 года были получены результаты, представленные в табл. 3.

Таблица 3 – Результаты анкетирования до интеграции модели

Вопрос	Суммарное количество баллов
1. Сталкиваетесь ли вы с фишинговыми атаками при работе в информационном пространстве техникума?	122 балла
2. Как часто на вашем рабочем столе компьютера (ноутбука) всплывает навязчивая реклама?	136 баллов
3. Бывают ли ситуации смены пароля от аккаунтов без вашего уведомления?	72 балла
4. Часто ли ваша антивирусная система предупреждает вас о возможных угрозах и вредоносном ПО?	134 балла
5. Происходит ли влияние на ваше психоэмоциональное состояние при работе в информационном пространстве техникума?	112 баллов
6. Происходят ли ситуации, когда ваша личная информация попадает на сторонние сайты?	84 балла
7. Замечаете ли вы списание денежных средств с электронных счетов без вашего уведомления?	61 балл

Следующим этапом проведения исследования стала интеграция разработанной модели на базе ГБПОУ «Катав-Ивановский индустриальный техникум». Так, в течение семестра выполнялись мероприятия, направленные на устранение возможных угроз и проблем информационной безопасности в информационном пространстве техникума, а также развития компетенций информационной безопасности студентов.

В декабре 2023 было проведено повторное анкетирование группы ИС-31 в количестве 30 человек по ранее заданным 7 вопросам. В табл. 4 представлены результаты повторного анкетирования.

Таблица 4 – Результаты анкетирования после интеграции модели

Вопрос	Суммарное количество баллов
1. Сталкиваетесь ли вы с фишинговыми атаками при работе в информационном пространстве техникума?	98 баллов
2. Как часто на вашем рабочем столе компьютера (ноутбука) всплывает навязчивая реклама?	106 баллов
3. Бывают ли ситуации смены пароля от аккаунтов без вашего уведомления?	61 балл
4. Часто ли ваша антивирусная система предупреждает вас о возможных угрозах и вредоносном ПО?	102 балла
5. Происходит ли влияние на ваше психоэмоциональное состояние при работе в информационном пространстве техникума?	76 баллов
6. Происходят ли ситуации, когда ваша личная информация попадает на сторонние сайты?	52 балла
7. Замечаете ли вы списание денежных средств с электронных счетов без вашего уведомления?	21 балл

На рис. 17 представлена схема, визуально отражающая динамику изменений уровня цифровой безопасности личности студентов до и после интеграции разработанной модели.

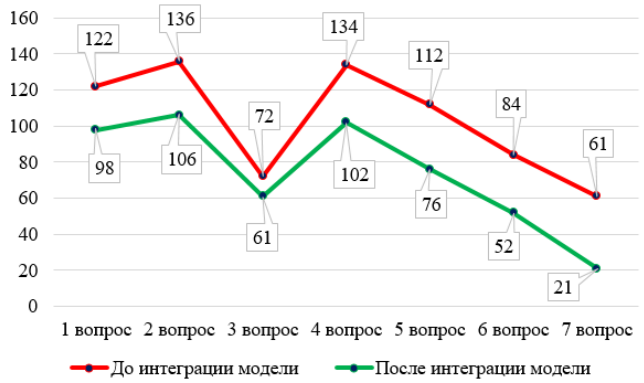


Рисунок 17 – Динамика изменений до и после интеграции модели

Как видно из приведенных таблиц и графика, наблюдается снижение уровня влияния угроз и проблем информационной безопасности на студентов ГБПОУ «Катав-Ивановский индустриальный техникум». Итоговые результаты после первого тестирования разработанной модели составили:

- влияние фишинговых атак: -20%;
- влияние спам-рекламы: -22%
- случаи кражи паролей от личных аккаунтов: -15%;
- срабатывание антивирусной системы: - 24%;
- влияние на психоэмоциональное состояние: -32%;
- утечка конфиденциальной информации: -38%;
- незаконное списание денежных средств: -65%.

Приведенные результаты свидетельствуют о значительном сокращении влияния угроз и проблем ИБ и, как следствие, повышении безопасности работы в информационном пространстве, а также повышении цифровой безопасности личности студентов образовательной организации ГБПОУ «Катав-Ивановский индустриальный техникум».

Выводы по Главе 3

В рамках третьей главы магистерской диссертации проведена опытно-экспериментальная работа по обеспечению цифровой безопасности личности студента в информационном пространстве образовательной организации ГБПОУ «Катав-Ивановский индустриальный техникум». Для достижения конечной цели были сформированы требования к задаче по обеспечению безопасного информационного пространства, разработана модель, а также описаны результаты интеграции разработанной модели в техникуме и приведены итоговые данные по оценке уровня изменений обеспечения цифровой безопасности студента. Полученные данные подтверждают целесообразность использования разработанной модели, а

также указывают на необходимость дальнейшего использования данной системы в деятельности данного образовательного учреждения.

ЗАКЛЮЧЕНИЕ

Основной целью представленного исследования являлось повышение безопасности личности студента в едином информационном пространстве ГБПОУ «Катав-Ивановский индустриальный техникум».

Для достижения изначально-поставленной цели были решены следующие задачи:

- проведен анализ актуальности вопроса информационной безопасности, основных угроз и рисков при обеспечении цифровой безопасности студентов в образовательной организации;

- проведено исследование основных методов по обеспечению цифровой безопасности в информационном пространстве образовательных организаций;

- проведен анализ системы обеспечения цифровой безопасности студента в ГБПОУ «Катав-Ивановский индустриальный техникум»;

- сформированы требования и разработана модель, направленная на решение задачи по обеспечению безопасного информационного пространства для студентов ГБПОУ «Катав-Ивановский индустриальный техникум»;

- реализована и проведена оценка эффективности модели обеспечения цифровой безопасности студента.

Представленная работа содержит три основных главы, каждая из которых решает отдельные задачи, необходимые для формирования требований и разработки будущей модели обеспечения цифровой безопасности студента на примере ГБПОУ «Катав-Ивановский индустриальный техникум». В результате работы проведен полный анализ основных вопросов относительно угроз и проблем ИБ при работе студентов в информационном пространстве данного техникума. Определены

основные угрозы, степень их влияния и текущая ситуация по решению данной проблемы. Выяснено, что руководство техникума активно проводит мероприятия, направленные на решение данной задачи.

Несмотря на это, текущих мероприятий и действий было недостаточно для получения полностью безопасного информационного пространства образовательной организации. В связи с этим, было решено разработать новую модель, полностью учитывающую основные особенности и факторы, влияющие на цифровую безопасность студентов ГБПОУ «Катав-Ивановский индустриальный техникум». Автором на основе проведенного анализа были сформированы ключевые требования к данной модели и разработаны основные модули, участвующие в полной системе обеспечения цифровой безопасности. Итоговая модель включает в себя 3 основных блока, каждый из которых решает 3 ключевые задачи по обеспечению безопасности при работе с информационным пространством техникума, освоение компетенций информационной безопасности студентами учебного заведения, а также организационно правовые ресурсы для регулирования данной системы.

Итогом работы стала разработка модели обеспечения безопасного информационного пространства образовательной организации ГБПОУ «Катав-Ивановский индустриальный техникум». Для анализа эффективности разработанной модели было проведено дополнительное исследование на основе анкетирования. Полученные результаты до и после интеграции модели свидетельствуют о значительном снижении негативного влияния угроз и проблем информационной безопасности на студентов. В связи с этим, необходимо отметить, что изначально поставленная цель магистерской диссертации выполнена в полном объеме. Также важно акцентировать внимание на том, что успешные результаты тестирования разработанной модели говорят о необходимости использования интегрированного инструмента и в дальнейшем. Ожидается, что в течение первого года использования модели снижение влияния угроз и проблем

информационной безопасности будет сведено к минимуму. При этом продолжение использование модели позволят сохранить данный уровень на протяжении всего времени ее использования в стенах образовательной организации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Красноплахтова Л.И., Танкаян А.И. Информационные технологии в педагогике и образовании // Интерактивная наука. 2018. №7 (29). С. 22-24.

2. Медведев П.Н., Малий Д.В., Папочкина Е.С. Современные информационные технологии в сфере образования: возможности и перспективы // МНИЖ. 2021. №6-4 (108). С. 110-113.

3. Ажмухамедов И.М., Кузнецова В.Ю. Информационная безопасность в цифровой образовательной среде: анализ информационных рисков и выработка стратегий защиты школьников от негативных последствий цифровизации образования // Прикаспийский журнал: управление и высокие технологии. 2020. №3 (51). С. 74-83.

4. Казинец В.А., Редько Е.А. Информационная безопасность как часть цифровой культуры выпускников педагогических университетов // Современное педагогическое образование. 2022. №5. С. 22-25.

5. Красовская Л. В., Исабекова Т. И. Использование информационных технологий в образовании // Научный результат. Педагогика и психология образования. 2017. №4 (14). С. 29-36.

6. Евстигнеева И.А., Евстигнеев М.Н., Клочихин В.В. Обеспечение информационной безопасности студентов в процессе использования проектной методики в обучении иностранному языку в университете // Вестник ТГУ. 2022. №4. С. 1009-1019.

7. Адольф В.А., Адольф К.В. Угрозы цифровизации образования и их решение // Научный компонент. 2022. №1 (13). С. 88-95.

8. Степанова Т.Ю. Обеспечение информационной безопасности в образовательной организации // Электронный научно-методический журнал Омского ГАУ. 2020. №4 (23). С. 25-29.

9. Величко А.Н. Информационная безопасность образовательной организации: проблемы управления // Известия вузов. Социология. Экономика. Политика. 2020. №4. С. 32-42.

10. Кожеуров И.В. Информационная безопасность образовательной среды // Наука в жизни человека. 2023. №2. С. 73-89.

11. О. В. Гукаленко, В. Н. Пустовойтов Обеспечение информационной безопасности молодежи в современном образовательном пространстве // Отечественная и зарубежная педагогика. 2019. №2 (64). С. 117-131.

12. Курмакаева О.Н., Милютина А.А. Пути формирования навыков информационной безопасности обучающихся // Вестник ЮУрГГПУ. 2022. №4 (170). С. 91-108.

13. Штейникова Л.С. Актуализация социальных компетенций педагогического работника СПО // Инновационное развитие профессионального образования. 2018. №3 (19). С. 114-122.

14. Ли А.С. Профессиональная образовательная организациякак пространство формирования культуры безопасности // Вестник Нижегородского университета им. Н. И. Лобачевского. Серия: Социальные науки. 2019. №4 (56). С. 194-200.

15. Колодкин А.С., Щеголихина А.К., Щербинина Ю.А., Мельникова Ю.В. Формирование безопасного поведения студентов вуза // Международный журнал гуманитарных и естественных наук. 2023. №2-1 (77). С. 121-123.

16. Хлебникова М.А., Долинина И.Г. Модель формирования компетентности информационной безопасности педагогов в процессе повышения квалификации // Мир науки. Педагогика и психология. 2020. №3. С. 50-56.

17. Майнагашева Е.В. Комплексная политика обеспечения безопасности образовательных учреждений: зарубежный опыт и практики // Известия ВГПУ. 2020. №6 (149). С. 21-27.

18. Полякова Т.А., Минбалеев А.В. Актуальные проблемы формирования системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе и трансформации права // Вестник Академии права и управления. 2019. №3 (56). С. 67-73.

19. Дубень А.К. Приоритетные задачи обеспечения информационной безопасности в условиях современных вызовов и угроз // Вопросы безопасности. 2023. №2. С. 45-56.

20. Бахтиярова В.Ф., Гайфуллина З.А. Формирование готовности студентов высшей школы к созданию безопасной цифровой образовательной среды как педагогическая проблема // Вестник Башкирского государственного педагогического университета им. М. Акмуллы. 2022. №1-3 (62). С. 62-67.

21. Сидельникова Н.В., Беседина Т.В. Информационная безопасность // Образование. Карьера. Общество. 2018. №1 (56). С. 71-72.

22. Челнокова Т.А. Профессиональное развитие студента в условиях цифрового общества // Современное педагогическое образование. 2020. №9. С. 99-103.

23. Молчанова И.И., Макушкин С.А., Серикова Н.А. Проектно-цифровая деятельность как средство формирования цифровой компетентности студентов гуманитарных специальностей // МНКО. 2023. №1 (98). С. 59-62.

24. Зубалова О.А. Проблемы информационной безопасности образовательной среды в современных условиях // МНКО. 2018. №3 (70). С. 36-38.

25. Алижанова Х.А., Тохчуков М.О., Бенев А.К. Опыт применения киберигр в процессе профессиональной подготовки студентов направления «информационная безопасность» // МНКО. 2022. №6 (97). С. 344-347.

26. Бобылев А.В. Развитие учебной самоорганизации студентов в условиях цифровизации высшего образования // КПЖ. 2020. №4 (141). С. 80-85.

27. Козлов Олег Александрович, Гузикова Людмила Александровна Информационная безопасность как условие деятельности образовательных организаций // Вопросы методики преподавания в вузе. 2017. №22. С. 43-50.

28. Бойченко О.В., Иванюта Д.В. Модели информационной безопасности // Экономика строительства и природопользования. 2021. №3 (80). С. 33-39.

29. Астахова Л. В. Развитие цифровой культуры студентов в условиях вузовской библиотеки // Вестник ЧГАКИ. 2019. №4 (60). С. 47-57.

30. Рихтер Т. В., Абрамова И. В. Разработка модели информационной безопасности баз знаний // ФМО. 2020. №1 (23). С. 106-110.

31. Кальницкая И.В., Максимочкина О.В. Акторы цифровой образовательной среды и их влияние на развитие цифровых компетенций студентов // Преподаватель XXI век. 2022. №2-1. С. 64-77.

32. Поляков М.С., Вахания Г.А., Разработка модели информационной безопасности автоматизированной информационной системы // Скиф. 2019. №5-1 (33). С. 353-358.

33. Яриков В.Г. Информационная безопасность обучающихся в образовательной организации // NBI-technologies. 2021. №4. С. 19-24.

34. Какорин И.А. Основные принципы информационной безопасности // Международный журнал гуманитарных и естественных наук. 2023. №2-2 (77). С. 25-27.

35. Мельников П.В., Ешенко Р.А. Проблемы формирования модели угроз информационной безопасности в информационных системах // Вестник науки. 2020. №6 (27). С. 185-189.

36. Сайгушев Н.Я., Веденеева О.А., Гарипов М.А. Актуализация информационной грамотности студентов в процессе профессиональной подготовки // МНКО. 2021. №4 (89). С. 77-80.