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

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

Информационно-аналитическая система прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе

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

Проверка на объем заимствований:
73,29 % авторского текста

Работа рекомендована к защите
«27» 12 2025 г.
Зав. кафедрой АТИТ и МОТД
_____ Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Колбина Виктория Алексеевна

Научный руководитель:
к.п.н., доцент
Гафарова Елена Аркадьевна

Челябинск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. В современном мире информация является одним из ключевых ресурсов, который влияет на успешное развитие общества. Объемы производимых и потребляемых данных стремительно увеличиваются с каждым днем. Для получения и структуризации огромного количества информации используются электронные носители, которые стали неотъемлемой частью нашей жизни.

С быстро развивающимся миром технологий и массовой компьютеризацией всех сфер деятельности человека большинство данных хранится в электронном виде, что делает их легкодоступными. Увеличивается количество цифровых образовательных ресурсов, используемых в образовательном процессе. Образовательные организации все чаще используют тематические интернет-ресурсы в образовательном процессе, изменяя подход к обучению, в связи с необходимостью подготовки студентов к меняющимся условиям XXI века.

Использование тематических интернет-ресурсов значительно расширяет диапазон доступа к необходимой и полезной в процессе обучения информации. Использование интернет-ресурсов позволяет получить информацию в разных форматах: видео, аудио, инфографика, что делает процесс обучения более интересным и полезным в усваивании учебной информации. Благодаря тематическим интернет-ресурсам студенты имеют возможность ознакомиться с последними исследованиями, статьями и аналитическими материалами из разных областей, которые являются актуальными.

Компетентные специалисты должны уметь критически мыслить и уметь анализировать поступающую информацию. Разнообразие тематических интернет-ресурсов, используемых в образовательном процессе, дает этот навык студентам, когда в процессе поиска необходимой информации они

учатся не только ее искать, но и оценивать, определять авторитетность источников информации и сопоставлять различные точки зрения. Кроме того, многие интернет-ресурсы предлагают платформы для обратной связи, чтобы и ученики, и преподаватели могли быстро и в удобном формате получать обратную связь в процессе обучения.

Но также при большом количестве плюсов использования тематических интернет-ресурсов в образовательном процессе не стоит забывать о важности организации информационной безопасности образовательного учреждения в этот момент. Важно фильтровать информацию, используемую в процессе обучения, и выбирать надежные интернет-источники для работы, избегая возможные угрозы и уязвимости для информационной безопасности образовательной организации. Повышение качества образования и использование современных технологий, также требуют повышение качества организации информационной безопасности образовательного процесса.

Таким образом, наличествует **противоречие**, когда, с одной стороны, имеется потребность в использовании тематических интернет-ресурсов, а с другой стороны, отсутствуют, либо малочисленны подходы по порядку формирования информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации. Названное противоречие определяет **проблему исследования.**

На основании выявленной проблемы исследования была сформулирована **тема исследования**: «Информационно-аналитическая система прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе».

Цель исследования: на основе анализа теоретической и методической литературы и тематических интернет-ресурсов, используемых в процессе обучения, разработать методические рекомендации по использованию

информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации.

Объект исследования: информационная безопасность образовательной организации при использовании в процессе обучения тематических интернет-ресурсов.

Предмет исследования: рекомендации по разработке информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности в образовательной организации.

Гипотеза исследования основана на предположении о том, что информационная безопасность образовательной организации будет эффективнее в случае реализации предложенных методических рекомендаций по разработке информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности в образовательной организации.

В соответствии с объектом, предметом и целью исследования были поставлены следующие **задачи**:

1. изучить сущность информационной безопасности образовательной организации, рассмотреть классификацию угроз и уязвимостей информационной безопасности, характерных для тематических интернет-ресурсов;
2. определить цели и задачи информационно-аналитических систем прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе;
3. разработать методические рекомендации по созданию информационно-аналитической системы угроз и уязвимостей информационной безопасности образовательной организации на основе

анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе;

4. привести экономическое обоснование эффективности разработанных методических рекомендаций по созданию информационно-аналитической системы угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе (на базе ГПБОУ «ЮУрГТК» г. Челябинска).

Теоретико-методологической базой исследования являются отечественные и зарубежные исследования, связанные с проблематикой информационной безопасности, которые широко раскрывают следующие вопросы:

– общие научные и методологические вопросы информационной безопасности поднимаются в трудах А.П. Коваленко, Е.Б. Белов; Р.В. Мещерякова, А.А. Шелупанова [10]; В.П. Шерстюк и др.);

– аспекты нормативно-правового обеспечения информационной безопасности (С.Л. Зефиров, В.М. Алексеев [4]; Ю.М. Батурин; Т.А. Кондратьева, В.С. Горбатов; О.А. Городов, Р.И. Дремлюга, Ю.А. Журавлев, Г.О. Крылов, Т.А. Полякова [49] и др.);

– проблемы подготовки кадров и формирования компетентности в области информационной безопасности (А.П. Коваленко, Е.Б. Белов [25]; Е.Н. Бояров [12] и др.);

– практические аспекты информационной безопасности и защиты информации (В.А. Галатенко [17], В.Н. Максименко [45], А.П. Даньков, Б.И. Скородумов [44], А.А. Круглов, А.В. Крысин, В.П. Мельников [48], Ю.С. Уфимцев [49], В.Л. Цирлов [50] и др.).

Методы исследования: анализ теоретической и методической литературы, нормативных документов и материалов, регулирующих процесс

обеспечения защиты информационной безопасности образовательной организации при использовании тематических интернет-ресурсов в процессе обучения; изучение материалов научных и периодических изданий по проблеме исследования; обобщение, систематизация и анализ собранных данных; разработка методических рекомендаций на основании проделанной работы.

База исследования: Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж» г. Челябинска.

Структура диссертации: работа состоит из введения, двух глав, выводов по главам, заключения, списка использованных источников, включающего в себя 60 наименований.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ ПРОГНОЗИРОВАНИЯ УГРОЗ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ НА ОСНОВЕ АНАЛИЗА ДАННЫХ ТЕМАТИЧЕСКИХ ИНТЕРНЕТ-РЕСУРСОВ, ПРИМЕНЯЕМЫХ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

1.1. Понятие информационной безопасности образовательной организации

ГОСТ «Защита информации. Обеспечение информационной безопасности в организации» (ГОСТ Р 53114–2008): информационная безопасность - состояние защищенности потребностей организации в условиях опасности в информационной сфере [19].

ГОСТ «Защита информации. Основные термины и определения» (ГОСТ Р 50922–2006): информационная безопасность (ИБ) - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Доступность – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно [18].

В образовательной организации термин «информационная безопасность» используется для обозначения двух различных понятий.

В связи с цифровизацией и информатизацией системы образования и широким использованием дистанционных технологий в первом случае понятие информационной безопасности рассматривается как практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача обеспечения информационной безопасности в данном контексте — сбалансированная защита конфиденциальности, целостности и доступности данных, с учетом целесообразности применения и без какого-либо ущерба производительности организации [46]. В данном определении информационной безопасности речь идет о защите информации и о мерах, которые принимает образовательная организация по защите различных видов информации.

Во втором случае понятие «информационная безопасность» используется при обсуждении вопросов безопасности обучающихся. Информационная безопасность рассматривается как «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» [48]. С позиции личностно-ориентированного подхода информационная безопасность определяется как состояние защищенности личности, обеспечивающее ее целостность как активного социального субъекта и возможности развития в условиях информационного взаимодействия с окружающей средой.

Таким образом, основываясь на приведенных выше понятиях, с учетом специфики исследуемой области, можно выделить, что информационная безопасность образовательного учреждения – это система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы, а также защита обучающихся от запрещенной законом пропаганды.

Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим трем группам:

- персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;
- разработки и методические материалы, применяемые в образовательном процессе, являющиеся интеллектуальной собственностью и защищенные законом;
- структурированная учебная информация, обеспечивающая образовательный процесс (библиотеки, базы данных, обучающие программы).

Все эти вышеупомянутые сведения не только могут стать объектом хищения. Намеренное несанкционированное проникновение в них может нарушить сохранность оцифрованных книг, уничтожить хранилища знаний, внести изменения в код программ, используемых для обучения.

Одним из ключевых принципов, лежащих в основе разработки концепций защиты информации и конкретных средств обеспечения информационной безопасности, является комплексность.

Для достижения целей защиты информации необходимо проведение на объектах защиты работ по следующим направлениям, с которыми можно ознакомиться на рисунке 1.

Рисунок 1. Цели защиты информации

Основной целью защиты информации является выявление и устранение либо нейтрализация источников негативных воздействий на информацию, а также их причин и условий. Упомянутые источники создают угрозы безопасности информации.

К основным методам защиты информации относятся:

– предупреждение известных угроз путем принятия упреждающих мер по обеспечению информационной безопасности для нейтрализации возможностей их возникновения;

– обнаружение угроз в результате определения реальных угроз и конкретных несанкционированных действий злоумышленников в отношении защищаемой информации;

– выявление новых угроз в ходе постоянного анализа и контроля за возникновением реальных или возможных угроз, а также своевременное принятие упреждающих мер;

– ликвидация угроз посредством локализации условий, при которых возможно совершение несанкционированных действий;

– ликвидация последствий угроз либо несанкционированных действий и восстановление штатного режима обработки информации [41].

Обнаружение угроз является действием по определению конкретных угроз и их источников, причиняющих определенный вид ущерба. К указанным действиям можно отнести обнаружение фактов разглашения конфиденциальной информации или несанкционированного доступа к системам обработки и хранения информации.

Пресечение и локализация угроз направлены на устранение актуальных угроз и конкретных действий злоумышленников.

Ликвидация последствий заключается в восстановлении состояния, предшествовавшего наступлению угрозы.

Перечисленные способы применяются для защиты информационных ресурсов от несанкционированных действий злоумышленников в целях обеспечения:

– недопущения несанкционированного доступа к конфиденциальной информации;

– предотвращения утечки и разглашения конфиденциальной информации;

– соблюдения конфиденциальности информации;

– сохранения целостности и доступности информации;

– обеспечения авторских прав.

Система обеспечения информационной безопасности образовательной организации базируется на построении и функционировании службы безопасности, формирующей и осуществляющей свою деятельность под руководством главного специалиста по безопасности и имеет разветвленную структуру [25].

Обязанностями лиц, ответственных за защиту информации, является:

- обеспечение сохранности защищаемых данных;

- поддержание информации в состоянии постоянной доступности для авторизованных лиц;

- обеспечение конфиденциальности подлежащих защите сведений, предотвращение доступа к ним со стороны третьих лиц.

Также специалисты по информационной безопасности обязаны не допустить несанкционированные изменения данных и их утрату.

Структура, численность и состав службы обеспечения информационной безопасности определяются реальными потребностями учебного заведения, а также объемом и ценностью основных ресурсов, в том числе и информационных, которые требуют защиты. Данная структура по обеспечению информационной безопасности организации должна быть определена и фиксирована, а также должна предусматривать динамическое развитие, которое будет учитывать информационные, организационные и технические трансформации современных технологий управления в сфере информационной безопасности.

Служба безопасности учебного заведения объединяет самостоятельные структурные подразделения, решает задачи по непосредственному обеспечению защиты жизненно важных интересов образовательной организации в условиях коммерческого и производственного риска, конкурентной борьбы.

Существенным звеном системы управления безопасностью учебного заведения является постоянно действующая техническая комиссия - коллегиальный орган при руководстве, выполняющий консультативные функции, чьи предложения носят рекомендательный характер. Все члены комиссии назначаются руководителем образовательной организации из числа ведущих специалистов, имеющих опыт работы в данной сфере и заинтересованных в обеспечении безопасности.

Управление информационной безопасностью деятельности учебного заведения осуществляется на основе его организационно-функциональной структуры. При этом все необходимые структурные функции обеспечения функционирования самого учебного заведения и его отдельных структурных подразделений, в том числе и обеспечения информационной безопасности, реализуется в соответствии со структурой управления учебным заведением [38].

1.2. Классификация угроз и уязвимостей информационной безопасности, характерных для тематических интернет-ресурсов

Современный образовательный процесс включает в себя применение тематических интернет-ресурсов, которые содержат часть методического или практического материала по выбранной тематике, необходимого преподавателю для реализации учебных и воспитательных аспектов учебного процесса занятия [24]. Примерами тематических интернет-ресурсов выступают обучающие платформы, виртуальные классы, системы управления обучением (LMS) и ресурсы для совместной работы.

В данном контексте информационная безопасность является неотъемлемой частью процесса образования, так как использование таких технологий сопряжено с различными угрозами и уязвимостями. Ключевыми элементами обеспечения защиты информации являются определение, анализ и классификация угроз и уязвимостей безопасности.

Согласно ГОСТ Р 50922–2006, пункт 2.6.1: угроза (безопасности информации) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Уязвимость (информационной системы); брешь - свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Условием реализации угрозы безопасности, обрабатываемой в системе информации, может быть недостаток

или слабое место в информационной системе. Если уязвимость соответствует угрозе, то существует риск [18].

Уязвимости информационной безопасности образовательной организации при использовании тематических интернет-ресурсов классифицируют так:

1. Уязвимости программного обеспечения:

— недостаточная защита хранилищ данных, когда базы данных не шифруются или не имеют достаточных мер защиты;

— использование устаревших платформ: отсутствие обновлений и патчей для программного обеспечения.

2. Уязвимости конфигурации:

— неправильные настройки безопасности: использование стандартных паролей и недостаточная защита учетных записей;

— отсутствие разделения прав доступа: все пользователи имеют равные права, что увеличивает риск несанкционированного доступа.

3. Уязвимости человеческого фактора:

— некомпетентность в вопросах информационной безопасности у преподавателей и студентов;

— игнорирование протоколов безопасности.

Уязвимости информационных систем, как правило, являются следствием ошибок. Ошибки, формирующие уязвимости, разделяются на ошибки администрирования и ошибки реализации.

К ошибкам реализации относят:

– ошибки синхронизации. Вид ошибок, обусловленный существованием временных окон между операциями обработки данных;

– ошибки проверки условий. Примером может быть неспособность программы обработать исключение, вследствие некорректного определения условия обработки данных;

– ошибки проверки входных данных. Как правило, такие ошибки приводят к уязвимостям переполнения буфера.

К ошибкам администрирования относятся:

– ошибки конфигурирования;

– ошибки окружения. Например, ошибки, связанные с некорректной обработкой переменных окружения, и ошибки командного интерпретатора.

Выявление перечисленных ошибок представляет собой непрерывный процесс, осуществляющийся на всех этапах жизни системы: разработки, тестирования и эксплуатации системы.

В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности, насчитывающий сотни пунктов. Для защищаемой системы составляют не полный перечень угроз, а перечень классов угроз, определяемых по ряду базовых признаков. Связано это с тем, что из-за большого количества факторов, влияющих на информацию описать полное множество угроз невозможно.

В качестве основных видов угроз безопасности информационных систем и информации выделяют следующую классификацию:

1. Природа возникновения:

— естественные угрозы (связанные с природными процессами, неподконтрольными информационным системам защиты и вызванные стихийными бедствиями);

— искусственные (провоцируется деятельностью человека).

2. Степень преднамеренности проявления:

— случайные (утечка информации из-за невнимательности пользователя или некорректная настройка конфиденциальности аккаунта)

— преднамеренные (попытки доступа к закрытым данным со стороны студентов или сотрудников).

3. Источник угроз:

— природная среда;

— человек;

— санкционированные программно-аппаратные средства (перегружение серверов с целью недоступности ресурсов);

— несанкционированные программно-аппаратные средства (наличие багов в коде).

4. Положение источника угроз:

— в пределах образовательной организации;

— вне контролируемой зоны образовательной организации.

5. Зависимость от активности системы:

— проявляются только в процессе обработки данных;

— проявляются в любое время.

6. Степень воздействия на систему:

— пассивные (информация ворується способом копирования, иногда скрытно. Изменения в информационную систему не вносятся);

— активные (вносят коррективы в структуру и содержание системы, например вирусы).

7. Этап доступа к ресурсам:

— на этапе доступа;

— после авторизации пользователя.

8. Способ доступа к ресурсам:

— стандартный (например, незаконное получение паролей и других параметров с дальнейшей маскировкой под зарегистрированного в системе пользователя);

— нестандартный (несанкционированное использование возможностей операционной системы).

9. Место расположения информации:

— внешние носители;

— оперативная память;

— линии связи;

— устройства ввода-вывода.

Вне зависимости от конкретных видов угроз было признано целесообразным связать угрозы с основными свойствами защищаемой информации.

Большинство существующих моделей информационной безопасности основываются на обеспечении целостности, доступности и конфиденциальности информации. Соответственно для информационных систем было предложено рассматривать три основных вида угроз:

1. Угроза нарушения целостности реализуется при несанкционированном изменении информации, хранящейся в информационной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно нарушают часть информации. Также целостность будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (примером является санкционированное изменение периодически запланированной коррекции некоторой базы данных).

2. Угроза нарушения доступа (отказа служб) реализуется в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Блокирование может быть постоянным — запрашиваемый ресурс никогда не будет получен, или может вызывать только задержку запрашиваемого ресурса.

3. Угроза нарушения конфиденциальности реализуется в случае, если информация становится известной лицу, не располагающему полномочиями

доступа к ней. Угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в информационной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой нарушения конфиденциальности используется термин «утечка».

Вышеуказанные виды угроз информационной безопасности можно рассматривать как первичные или непосредственные, т. к. при рассмотрении понятия угрозы как некоторой потенциальной опасности, реализация которой наносит ущерб информационной системе, реализация данных угроз приведет к непосредственному воздействию на защищаемую информацию.

Описанные выше угрозы были сформулированы ещё в 1960-х гг. применительно к открытым UNIX-подобным системам, для которых не предусматривались меры по защите информации. Поэтому непосредственное воздействие на информацию для атакующей стороны возможно в том случае, если система, в которой циркулирует информация, для нее «прозрачна», т. е. не существует никаких систем защиты или других препятствий.

На современном же этапе развития информационных технологий подсистемы или функции защиты являются неотъемлемой частью комплексов по обработке информации. Информация не представляется «в чистом виде», на пути к ней имеется хотя бы какая-нибудь система защиты, и поэтому, для несанкционированной атаки необходимо преодолеть эту систему.

Поскольку преодоление системы защиты информационной безопасности также представляет собой угрозу, рассмотрим ее четвертый вид — угрозу раскрытия параметров системы, включающей в себя систему защиты. На практике любое проводимое мероприятие предваряется этапом разведки, в ходе которой определяются основные параметры системы, ее характеристики и т. п. Результатом разведки является уточнение поставленной задачи, а также выбор оптимального технического средства.

Угрозу раскрытия параметров системы можно рассматривать как опосредованную. Последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность реализации первичным, или непосредственным, угрозам безопасности. Введение данного вида угроз позволяет описывать отличия защищенных информационных систем от открытых. Для последних угроза разведки параметров системы считается реализованной [22].

1.3 Определение, цели и задачи информационно-аналитических систем прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе

Эффективность работы организации и сложность анализа ее деятельности напрямую зависит от того, как организована обработка информации и поддержка защиты информационных процессов. Проведение качественной оценки стало основой для применения необходимых методов и средств защиты информации и позволяет решать данную проблему наиболее эффективно. Традиционно определение требований как по защите информации, так и по оценке угроз безопасности информации осуществляется на основе правового и нормативно-методического обеспечения.

Например, Законом №152-ФЗ «О персональных данных» для операторов, использующих в своей деятельности информационные системы персональных данных, установлена обязанность принимать необходимые меры по обеспечению их безопасности. В свою очередь обеспечение безопасности персональных данных (ПДн) достигается, в частности, определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИС ПДн) [54].

Прежде чем перейти к целям и задачам информационно-аналитических систем безопасности дадим определение данному понятию.

Информационно-аналитическая система прогнозирования угроз и уязвимостей информационной безопасности образовательной организации – это комплексный инструмент, включающий в себя методы, технологии и алгоритмы для сбора, обработки и анализа информации о потенциальных угрозах и уязвимостях в области информационной безопасности и предназначенный для обеспечения защиты информации и минимизации рисков, связанных с утечками данных, несанкционированным доступом и прочими угрозами.

Основными компонентами данного определения являются «информационная безопасность» и «уязвимости», которые мы рассмотрели в предыдущих параграфах, а также:

1. Информационно-аналитическая система (ИАС) — это структура, которая позволяет осуществлять автоматизацию процессов сбора и анализа данных. В контексте образовательной организации информационно-аналитическая система обеспечивает защиту информации, хранящейся в ее системах, а также сопроводительную инфраструктуру.
2. Прогнозирование угроз — это процесс оценки вероятности возникновения новых угроз для информационной безопасности на основе анализа данных, статистики, предыдущих инцидентов и актуальных тенденций в области технологий и киберугроз [23].

Основной целью информационно-аналитических систем безопасности в образовательных учреждениях служит создание комплексной системы защиты информации, которая обеспечивает сохранность данных и защиту интересов всех участников образовательного процесса. Самые важные аспекты данной цели включают:

— защиту персональных данных: обеспечение конфиденциальности и сохранности личной информации сотрудников образовательной организации и обучающихся от несанкционированного доступа и утечек;

— инфраструктурную безопасность: защита сетевой и аппаратной инфраструктуры от внешних и внутренних угроз, включая вирусные атаки и кибератаки;

— содействие в управлении рисками: выявление, оценка и минимизация рисков, связанных с информационной безопасностью, что позволяет образовательной организации более эффективно управлять ресурсами и реагировать на угрозы.

— создание безопасной образовательной среды: формирование условий, в которых все участники образовательного процесса могут безопасно и эффективно взаимодействовать с цифровыми ресурсами.

Для достижения вышеуказанных целей информационно-аналитические системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации решают ряд задач:

— мониторинг и анализ угроз: регулярное отслеживание ситуации в области информационной безопасности. Выявление новых возможных угроз и уязвимостей информационной безопасности, а также анализ инцидентов, имеющих место в организации;

— разработка и внедрение политики безопасности: создание четкой политики информационной безопасности образовательной организации, включая правила доступа, управления данными и использования сетевых ресурсов;

— обучающие мероприятия, повышающие информированность: проведение регулярных обучений для сотрудников и обучающихся по вопросам информационной безопасности, формирование культуры осознанного и безопасного использования цифровых технологий;

— использование технологий защиты: внедрение и поддержка современных решений и технологий для защиты информации, таких как системы обнаружения и предотвращения вторжений, антивирусные программы и средства шифрования данных;

— аудит и оценка мер безопасности: периодическая проверка эффективности существующих в образовательной организации мероприятий по информационной безопасности, а также оценка их воздействия на образовательный процесс. При необходимости совершенствование подходов к применению действующих методик.

Тематические интернет-ресурсы, применяемые в образовательном процессе (форумы, блоги и специализированные сайты по кибербезопасности) также могут быть использованы в образовательном процессе и при этом содержать полезную информацию для анализа угроз и уязвимостей информационной безопасности.

Методы для анализа данных тематических-интернет ресурсов могут включать в себя:

— сбор данных с применением автоматизированных инструментов, предназначенных специально для мониторинга и сбора информации о текущих угрозах на специализированных платформах;

— обработка данных с применением алгоритмов обработки текстовой информации для извлечения ключевых угроз и уязвимостей;

— анализ с использованием методов машинного обучения и аналитических инструментов для выявления закономерностей и прогнозирования потенциальных угроз [1].

Проектирование и внедрение информационно-аналитической системы безопасности в образовательной организации может быть реализовано в несколько этапов:

1. Разработка стратегии. Данный пункт включает в себя определение основных целей образовательной организации по защите информационной безопасности при использовании тематических интернет-ресурсов в процессе образования, постановка задач для реализации поставленной цели и выбор необходимых ресурсов для реализации системы по прогнозированию угроз и уязвимостей информационной безопасности образовательной организации.

2. Сбор и обработка данных.

— Одним из наиболее распространенных методов является веб-скрейпинг - техника автоматизированного извлечения данных с веб-сайтов с помощью специализированных программ и скриптов. Существуют такие инструменты, как BeautifulSoup и Scrapy для Python, которые предоставляют возможности для парсинга HTML и извлечения нужной информации. Важно отметить, что нужно соблюдать юридические и этические нормы при использовании веб-скрейпинга, так как многие сайты имеют определенные ограничения на автоматический доступ.

— Активно развиваются технологии API (Application Programming Interface), которые позволяют получать данные с внешних платформ и сервисов более структурированным и легким способом. Многие компании предлагают открытые API, через которые можно получать необходимые данные в формате JSON (JavaScript Object Notation – стандартный текстовый формат для хранения и передачи структурированных данных) или XML (eXtensible Markup Language – регулярный формат, используемый для создания, хранения и обмена структурированными данными), что значительно упрощает их обработку и анализ.

— Машинное обучении и технологии анализа данных. С помощью алгоритмов машинного обучения можно обрабатывать большие объемы данных, выделять из них полезную информацию и делать прогнозы на основе анализа трендов и паттернов.

— Необходимо учитывать и новые подходы, например, когнитивные технологии и облака данных, позволяющие интегрировать различные

источники информации, проводить сложный анализ и обеспечивать доступ к данным почти в реальном времени.

— Инструменты визуализации данных, такие как Tableau или Power BI, также играют важную роль, т. к. позволяют не только собирать информацию, но и представлять её в удобной для восприятия форме, что способствует лучшему пониманию и анализу.

3. Анализ и обработка собранной информации. Применение методов аналитики для прогнозирования и оценки рисков возникновения угроз и уязвимостей информационной безопасности образовательной организации.

4. Внедрение информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности в процессы работы образовательной организации и разработка или организация материалов для обучения по правилам пользования системой. Обновление политики информационной безопасности образовательной организации, а также проведение обучающих мероприятий по основам кибербезопасности при использовании тематических интернет-ресурсов в процессе обучения как для педагогов, так и для студентов.

Выводы по главе 1

В первой главе магистерской диссертации мы рассмотрели теоретические аспекты информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе.

В первом параграфе дали определение термину «информационная безопасность» и ее трем главным составляющим, которые входят в это понятие: конфиденциальность, целостность и доступность. Рассмотрели понятие информационной безопасности в образовательной организации в двух аспектах: защита общей информационной среды организации и защита безопасности обучающихся. Выделили основные информационные сведения, которые могут стать объектами хищения в образовательной организации. Также ознакомились со структурой организации службы информационной безопасности в образовательной организации.

Во втором параграфе ознакомились с примерами тематических-интернет ресурсов, применяемых в образовательном процессе, и определили значение терминов: угроза (безопасности информации) и уязвимость (информационной системы). Рассмотрели две группы ошибок, формирующих уязвимости: ошибки реализации и ошибки администрирования. Из обширного перечня угроз информационной безопасности выделили основные виды угроз и их вариативность. Также подробно рассмотрели три вида угроз информационной безопасности, связанных с основными свойствами защищаемой информации.

В третьем параграфе подробно рассмотрели понятие информационно-аналитической системы безопасности в образовательной организации и ее основные компоненты. Определили основную цель этих систем и выделили ее важные аспекты: защита персональных данных, инфраструктурная безопасность, содействие в управлении рисками, создание безопасной

образовательной среды. Также выделили ряд задач для решения поставленной цели информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации: мониторинг и анализ угроз, разработка и внедрение политики безопасности, проведение обучающих мероприятий по формированию культуры безопасного использования цифровых технологий, использование технологий защиты, аудит и оценка мер безопасности. Рассмотрели методы, применяемые для анализа данных тематических интернет-ресурсов, используемых в образовательном процессе, и ознакомились с этапами проектирования и внедрения информационно-аналитической системы в образовательных организациях.

ГЛАВА 2. РАЗРАБОТКА МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО ЭФФЕКТИВНОМУ ВНЕДРЕНИЮ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ ПРОГНОЗИРОВАНИЯ УГРОЗ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ НА ОСНОВЕ АНАЛИЗА ДАННЫХ ТЕМАТИЧЕСКИХ ИНТЕРНЕТ-РЕСУРСОВ, ПРИМЕНЯЕМЫХ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ ГБПОУ «ЮУрГТК» Г. ЧЕЛЯБИНСКА

2.1. Анализ единого информационного пространства образовательной организации и анализ тематических интернет-ресурсов, применяемых в процессе обучения

Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж» (ГБПОУ «ЮУрГТК») реализует основные профессиональные образовательные программы среднего профессионального образования — программы специалистов среднего звена. Некоторые из них: 09.02.06 Сетевое и системное администрирование, 09.02.07 Информационные системы и программирование (Квалификация – программист и квалификация – разработчик веб- и мультимедийных приложений), 11.02.11 Сети связи и коммуникации, 11.02.15 Инфокоммуникационные сети и системы связи.

Организационная структура управления ГБПОУ «Южно-Уральский государственный технический колледж» представлена на рисунке 2.

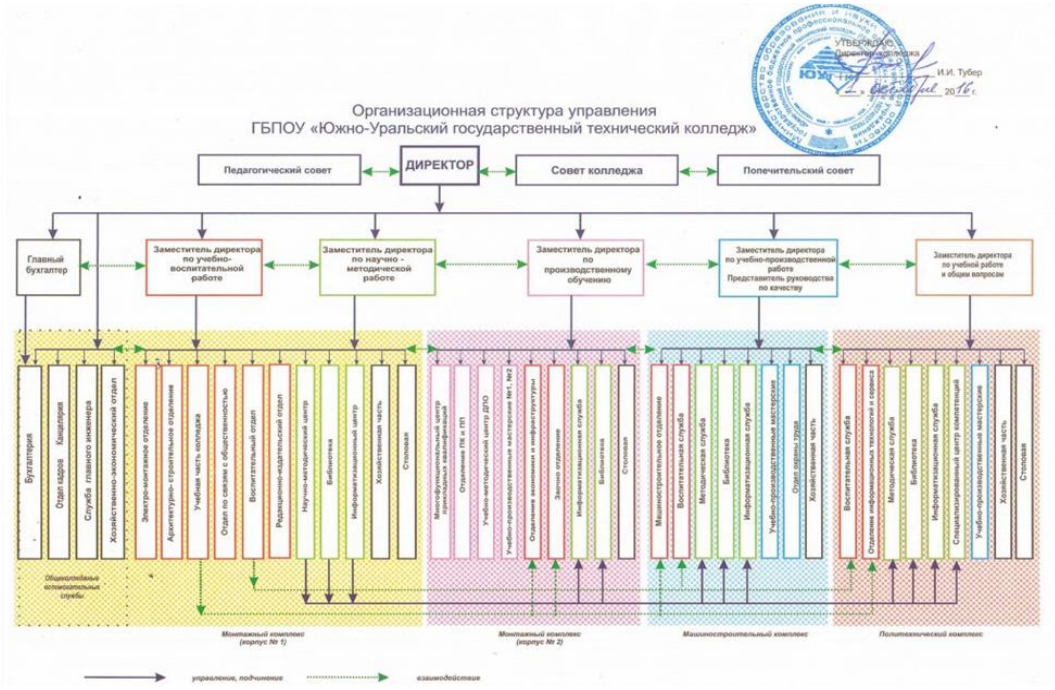

Рисунок 2 – Организационная структура управления ГБПОУ «ЮУрГТК»

Учебно-материальная база колледжа по объему и содержанию отвечает лицензионным требованиям и условиям осуществления образовательной деятельности по образовательным программам, заявленным в лицензии. Образовательный процесс организован в зданиях и помещениях общей площадью 59596 кв.м. Материальная база ГБПОУ «ЮУрГТК» включает в себя:

— четыре учебных корпуса;
— 2 стадиона;
— 1 лыжную базу;
— 2 спортивные площадки;
— 5 спортивных залов;
— 9 учебно-производственных мастерских;
— 3 учебных полигона, библиотеки;
— 36 кабинетов по общеобразовательным дисциплинам и дисциплинам циклов ОГСЭ и ЕН;

— 80 кабинетов профессионального цикла;

— 55 учебных лабораторий;

— 30 компьютерных классов;

— 25 аудиторий, оснащенных интерактивными досками или мультимедийными установками.

Учебные лаборатории оснащены учебно-лабораторными стендами и другим лабораторным оборудованием, обеспечивающим выполнение лабораторных работ и практических занятий, предусмотренных основными профессиональными образовательными программами. Специальные технические средства обучения коллективного и индивидуального пользования для инвалидов и лиц с ОВЗ имеются. Применяется электронное обучение с применением дистанционного образования система moodle, dom.sustec.ru, e.lanbook.ru.

Колледжем разработан значительный объем электронных образовательных ресурсов – электронных учебных курсов, собранных и систематизированных в системе дистанционного обучения ЮУрГТК, доступ к которым не ограничен. Вход в систему дистанционного обучения осуществляется по логину и паролю, полученному при зачислении на обучение.

Для студентов, обучающихся на базе основного общего образования, организовано использование верифицированного образовательного контента на платформе мобильного электронного образования (МЭО).

В колледже организован доступ студентов к информационным системам и информационно-коммуникационным сетям, обеспечивающий освоение образовательных программ. В библиотеках всех комплексов оборудованы электронные зоны для самоподготовки с открытым доступом к информационным системам и информационно-коммуникационным сетям, а также организованы WiFi-зоны открытого доступа к сети Интернет.

Для работы читателей с электронными изданиями, электронным каталогом, справочно-поисковыми системами и интернетом в библиотеке МНК оборудована автоматизированная зона на 14 единиц компьютерной техники. В колледже организовано активное использование студентами электронных библиотечных систем “Академия” и “Знаниум”. С обучающимися проводятся инструктажи по работе в ЭБС, организовано распространение логинов и паролей. Сотрудники библиотеки проводят обучающие занятия для студентов 1-х курсов и преподавателей (в рамках школы молодых педагогов), где рассказывают и показывают приёмы работы с ЭБС. Выпускаются закладки с правилами работы с ЭБС.

Обучающиеся имеют неограниченный доступ к следующим ресурсам:

- Министерство просвещения РФ;
- Федеральный портал “Российское образование”;
- Единая коллекция цифровых образовательных ресурсов.

Организацией и предоставлением доступа к электронным сетевым сервисам для повышения эффективности работы подразделений ГБПОУ «ЮУрГТК» занимается Информатизационный Центр колледжа.

В своей деятельности Информатизационный Центр руководствуется следующими документами:

- Конституцией РФ;
- Законом Российской Федерации от 29 декабря 2012 г. №273–1 «Об образовании в Российской Федерации»;
- Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- Уставом колледжа;
- Документацией внутриколледжной системы менеджмента качества;
- Документацией внутриколледжной системы менеджмента охраны труда и техники безопасности;

— Законодательными и нормативными актами по охране труда, пожарной безопасности и обеспечения защиты персональных данных;

— Положением об информатизационном центре колледжа.

Информатизационный центр осуществляет свою деятельность как структурное подразделение колледжа. Структура информатизационного центра состоит из лабораторий, специализирующихся по направлениям:

— Лаборатория технического обеспечения;

— Лаборатория информационных технологий.

Руководство лабораторией осуществляет заведующий лабораторией, который подчиняется непосредственно руководителю информатизационного центра.

Руководство информатизационного центра осуществляет руководитель информатизационного центра, который подчиняется непосредственно заместителю директора по учебно-методической работе;

Руководитель информатизационного центра и заведующие лабораториями назначаются на должность и освобождаются от нее приказом директора колледжа.

Структуру и штатную численность информатизационного центра утверждает директор колледжа.

Сотрудники информатизационного центра являются штатными сотрудниками колледжа.

Для достижения поставленной цели информатизационный центр решает следующие задачи:

— разработка и осуществление единой технической политики и практического использования современных достижений информационных технологий в бизнес-процессах колледжа;

— выполнение работ по созданию и развитию единой информационной сети колледжа;

— выполнение работ, ориентированных на создание новых информационных технологий в целях информационного обеспечения учебного процесса и управления в колледже;

— организация разработки нового программного обеспечения и рекомендаций по использованию готовых программных продуктов, ориентированных на применение компьютерных технологий в учебном и управленческом процессах;

— участие в планировании повышения квалификации сотрудников колледжа по проблемам использования новых информационных технологий в учебном процессе и управлении;

— координация организации и проведение научно-методических конференций, школ-семинаров, курсов в области информационных технологий;

— проектирование, создание и развитие автоматизированной системы управления колледжем;

— анализ потребностей служб и подразделений колледжа в средствах вычислительной и оргтехники, организация работы по их оснащению средствами информатизации;

— предоставление платных дополнительных услуг для сотрудников и студентов согласно утвержденному положению.

Основные функции лаборатории технического обеспечения:

1. Текущее обслуживание и организация ремонта (замены) средств вычислительной и офисной техники.

2. Организация и проведение комплекса работ по грамотной технической эксплуатации средств вычислительной и офисной техники.

3. Оказание помощи преподавателям и студентам по вопросам, связанным с эксплуатацией вычислительной техники и программного обеспечения.

Основные функции лаборатории и информационных технологий:

1. Создание, обслуживание и развитие защищенного центрального серверного центра колледжа.

2. Проектирование и развитие компьютерной сети с использованием современных достижений в данной области.

3. Установка, настройка и сопровождение сетевых программных продуктов.

4. Создание надежных условий для доступа всех пользователей к компьютерной сети колледжа.

5. Предоставление сетевых сервисов и целях обеспечения учебных и управленческих работ.

6. Организация централизованной антивирусной защиты информационных ресурсов.

7. Предоставление сетевых ресурсов для автоматизации управленческой деятельности подразделений.

8. Проектирование, разработка, размещение и поддержка внешних и внутренних Web-серверов.

9. Подбор, адаптация, разработка нового и внедрение программного обеспечения с целью создания и развития автоматизированной системы управления колледжем.

10. Адаптация и внедрение программного обеспечения для организации процесса дистанционного образования и независимой проверки знаний.

11. Организация работ по обеспечению защиты информационных систем персональных данных.

Информатизированный центр осуществляет свою деятельность совместно со структурными подразделениями колледжа в соответствии с нормативными документами колледжа, приказами и распоряжениями директора и заместителя директора по учебно-методической работе.

Информатизированный центр имеет право:

— требовать от сотрудников колледжа соблюдения правил работы с компьютерным и офисным оборудованием, выполнения инструкций по работе с программным обеспечением, обязательной прохождение обучения на внутренних курсах информатизационного центра при получении неудовлетворительной оценки за проверочное тестирование знаний сотрудников колледжа в области информационных технологий;

— выполнять работы только по размещенным на внутреннем портале электронным заявкам, за исключением случаев, когда заявки не могут быть размещены в результате недоступности сетевых сервисов;

— запрашивать и получать от руководства информацию, необходимую для выполнения работ, реализующих функции информатизационного центра;

— формировать заявки на приобретение необходимой нормативной, технической и справочной документации;

— участвовать в разработке текущих и перспективных планов работы колледжа;

— представлять перспективные планы развития единого информационного пространства колледжа, докладывать о текущем состоянии их реализации;

— вносить предложения руководству колледжа по формированию внутренней структуры и штатного расписания информатизационного центра.

Информатизационный центр обязан:

— осуществлять стратегическое планирование деятельности колледжа в области информационных технологий;

— обеспечивать бесперебойную работу компьютерной техники, сетевых сервисов и офисного оборудования;

— своевременно предоставлять отчетную документацию;

— принимать участие в мероприятиях, предусмотренных планами работ;

— осуществлять деятельность в соответствии с руководством по качеству и другой документации СМК и СУОТ колледжа.

Также на официальном сайте колледжа в разделе «Студенту» размещён «Белый список» образовательных тематических интернет-ресурсов для каждой реализующейся образовательной программы СПО.

Для студентов по специальности 09.02.01 Информационные системы и программирование (Квалификация – Программист) список рекомендуемых для использования в образовательном процессе безопасных тематических интернет-ресурсов выглядит таким образом:

1. https://metanit.com/ Сайт о программировании

   METANIT.COM. Данный сайт посвящен различным языкам и технологиям программирования, компьютерам, мобильным платформам и ИТ-технологиям. Содержит различные руководства и учебные материалы, статьи по теме. Благодаря обновлению и дополнению информации в соответствии с развитием технологий информация остается актуальной [3].

2. https://learn.microsoft.com/ru-ru/ Microsoft Learn

   Это портал для самостоятельного прохождения коротких учебных курсов по большим данным, искусственному интеллекту, облачным технологиям, DevOps и т. п. Здесь можно оценить собственные знания, изучить тему по представленным материалам и выполнить проверочные задания [37].

3. https://intuit.ru/ Национальный открытый университет

   Национальный Открытый Университет «ИНТУИТ» (от ИНТернет-Университет Информационных Технологий) — организация, предоставляющая с помощью собственного сайта услуги дистанционного обучения по нескольким образовательным

программам, многие из которых касаются информационных технологий [35].

4. https://stepik.org/ Образовательная платформа «stepik»

   Stepik — российская образовательная платформа и конструктор бесплатных и платных открытых онлайн-курсов и уроков. Позволяет любому зарегистрированному пользователю создавать интерактивные обучающие уроки и онлайн-курсы, используя видео, тексты и разнообразные задачи с автоматической проверкой и моментальной обратной связью. В процессе обучения студенты могут вести обсуждения между собой и задавать вопросы преподавателю на форуме [33].

5. https://practicum.yandex.ru/catalog/programming/free/ Яндекс-практика, бесплатные курсы

   Образовательная платформа от Яндекс. Программа онлайн-курсов постоянно обновляется, что позволяет получить актуальные знания. Обучение языкам программирования для начинающих бесплатно включает теоретическую часть и объёмный практический блок. Есть возможность сразу закрепить полученные знания, применив их в задачах, максимально приближенных к реальности. А отработанные кейсы лягут в основу портфолио обучающихся и помогут в поиске работы [11].

С помощью технологии Safe Browsing Яндекс [60] статус данных веб-ресурсов был проверен на безопасность, в результате чего было подтверждено, что данные интернет-ресурсы действительно являются безопасными для использования в процессе обучения, не включены в реестр небезопасных сайтов и не содержат в себе вредоносных составляющих. На рисунке 3 представлен результат проверки сайта Остальные интернет-ресурсы были проверены аналогичным образом.

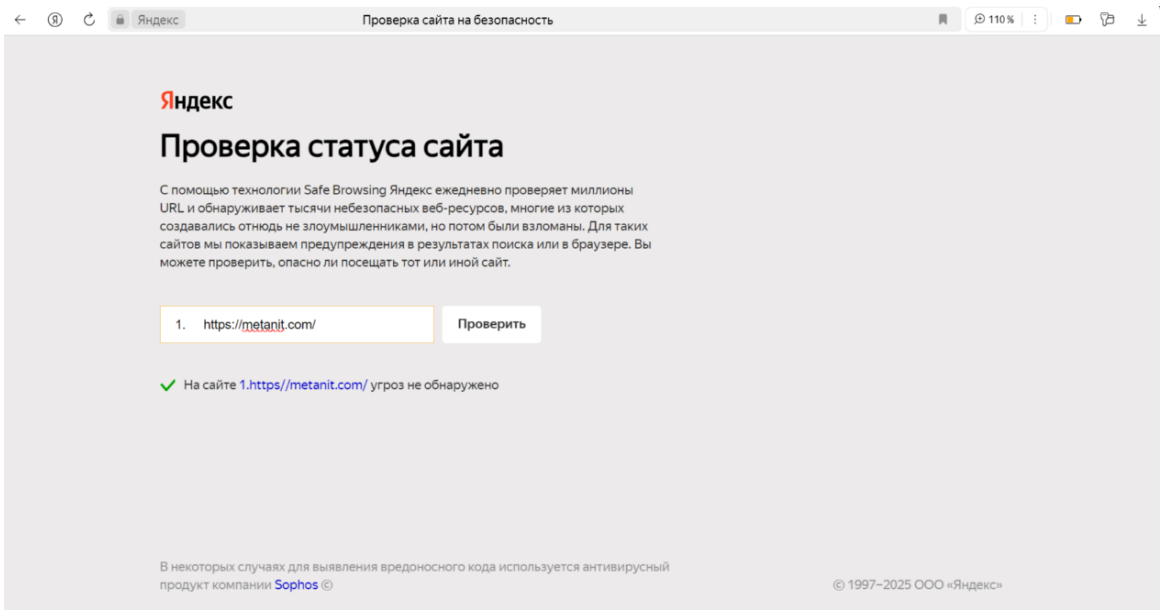

Рисунок 3. Проверка сайта METANIT.COM. на наличие угроз

Анализ вышеуказанных тематических интернет-ресурсов, используемых в образовательном процессе «ЮУрГТК» был также проведен на основании изучения процесса авторизации пользователей, пользовательского соглашения и политики конфиденциальности сайтов, еще отмечалось наличие рекламных баннеров в процессе работы с интернет-площадками.

Для работы с интернет-ресурсами 2–5 пользователям необходимо пройти процесс регистрации (авторизоваться), что включает в себя идентификацию и аутентификацию.

Идентификация — это определение пользователя в системе по его признаку [7]. Обычно речь идёт о логине, которым является электронная почта, мобильный телефон или комбинация чисел и цифр, придуманная системой или пользователем. Пример идентификатора участника интернет-ресурса «Microsoft Learn» представлен на рисунке 4.

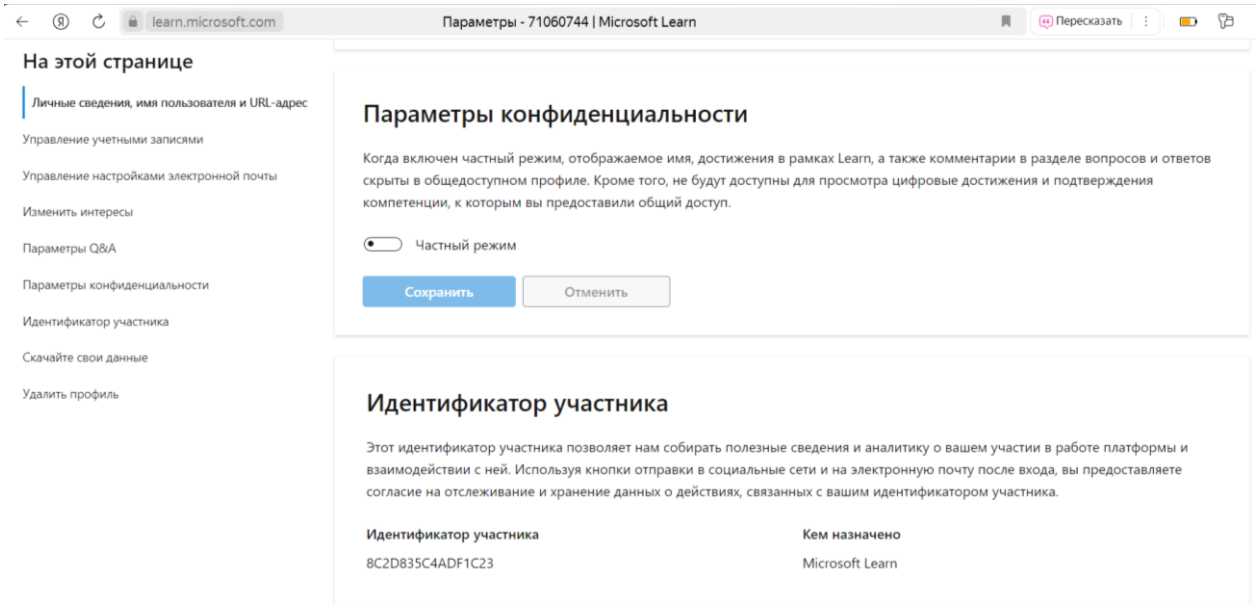

Рисунок 4. Идентификатор участника интернет-ресурса «Microsoft Learn»

Аутентификация — это подтверждение личности пользователя путём введения пароля [7]. Если система поймёт, что пароль совпадает с логином, происходит аутентификация пользователя и вход в систему, рисунок 5.

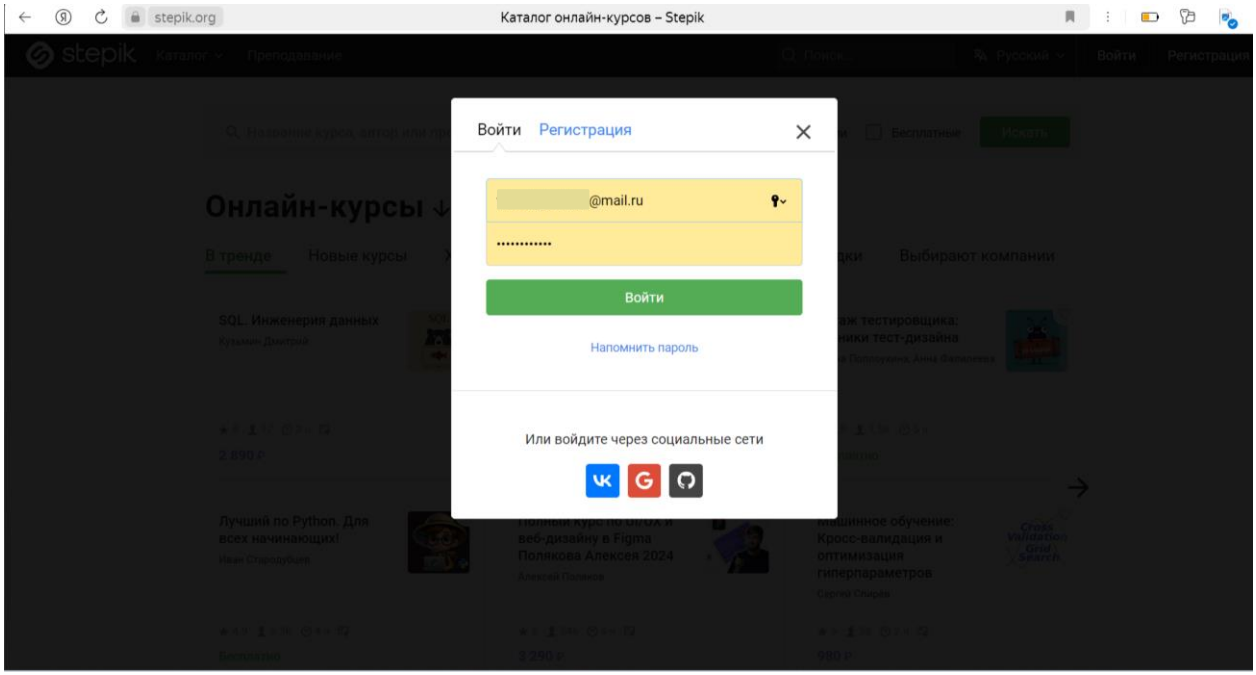

Рисунок 5. Процесс аутентификации пользователя образовательной платформы «Stepik»

Также при регистрации пользователю предлагается ознакомиться и согласиться для продолжения работы с интернет-ресурсом с

«Пользовательским соглашением» и «Политикой конфиденциальности», которые необходимы для обеспечения правовой защиты как для пользователя сайта, так и для его владельцев.

Политика конфиденциальности устанавливает обязательства Компании по неразглашению и обеспечению режима защиты конфиденциальности персональных данных, которые Пользователь предоставляет по запросу Компании при регистрации на Сайте. В основном это минимальный набор персональных данных: фамилия, имя, адрес электронной почты, номер телефона, дата рождения.

Компания, являясь оператором персональных данных, осуществляет обработку персональных данных Пользователей с учетом необходимости обеспечения защиты прав и свобод Пользователей, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

— обработка персональных данных осуществляется Компанией на законной и справедливой основе;

— обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

— не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

— обработке подлежат только персональные данные, которые отвечают целям их обработки;

— содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки;

— хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, в том числе в соответствии с настоящей Политикой конфиденциальности и пользовательским соглашением Сайта, если иной срок хранения персональных данных не установлен действующим законодательством Российской Федерации;

— обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки, в случае утраты необходимости в достижении этих целей, а также в случае истечения срока, установленного в п. 2.9 настоящей Политики конфиденциальности, если иное не предусмотрено действующим законодательством Российской Федерации.

Но также стоит учитывать тот факт, что Компания не несет ответственности за разглашение персональных данных Пользователя другими Пользователями Сайта, а также пользователями сети Интернет, получившими доступ к таким данным.

Также отметим тот факт, что представленные тематические интернет-ресурсы имеют ссылки на социальные сети и содержат рекламные баннеры.

Учитывая данные анализа тематических интернет-ресурсов, используемых в процессе обучения в образовательной организации и опираясь на теоретические данных из 1 главы работы, не стоит забывать про ещё один немаловажный фактор, влияющий на состояние информационной безопасности организации, даже если используемые в процессе образования интернет-ресурсы прошли проверку на безопасность и отсутствие угроз и уязвимостей. По степени преднамеренности появления ошибки могут быть случайными, в то время как по природе их возникновения они могут быть спровоцированы человеком. Исходя из этих данных был также проведен сценарный анализ угроз и уязвимостей информационной безопасности образовательной организации при использовании интернет-ресурсов в процессе обучения.

Сценарный анализ угроз и уязвимостей информационной безопасности образовательной организации представляет собой структурированный подход к оценке потенциальных рисков и слабых мест в системах защиты информации. Данный метод включает в себя создание и анализ различных возможных сценариев угроз и уязвимостей информационной безопасности, которые могут возникнуть при использовании тематических интернет-ресурсов в процессе обучения. Сценарный анализ предназначен для того,

чтобы можно было заранее выявить наиболее вероятные и потенциально разрушительные угрозы, оценить их влияние на информационные ресурсы и разработать меры по снижению рисков.

Ниже представлены несколько потенциальных ситуаций, которые могут возникнуть в результате различных угроз и уязвимостей при использовании тематических интернет-ресурсов, даже если они относятся к проверенным информационным источникам.

— Сценарий 1: Фишинг-атака.

Ситуация: студенты получили электронные письма, которые выглядят так, будто они отправлены от имени администрации используемого в процессе обучения интернет-ресурса. В письмах содержится просьба обновить информацию о личных данных через предложенную ссылку. Некоторые студенты, увидев этот запрос, перешли по ссылке и ввели свои учетные данные на поддельной странице.

- Угроза: фишинг через электронную почту, при котором злоумышленник пытается получить учетные данные пользователей.
- Уязвимость: легкий доступ к учетным записям при отсутствии двухфакторной аутентификации и недостаточная защита электронных почтовых ящиков.
- Потенциальные последствия:
    - утечка конфиденциальной информации студентов;
    - доступ к системам управления курсами и оценками.

— Сценарий 2: Рекламные баннеры на образовательных платформах.

Ситуация: на странице используемого интернет-ресурса появились рекламные баннеры, которые ведут на внешние сайты с ненадежным контентом. Пользователи, кликнув на эти баннеры, были перенаправлены на страницы, которые могут содержать вредоносные программы или неправомерное программное обеспечение.

- Угроза: загрузка вредоносного кода.

- Уязвимость: несоответствующий контроль доступа к веб-ресурсам, использование небезопасных протоколов передачи данных.
- Потенциальные последствия:
    - заражение устройств вредоносными программами;
    - утечка личной информации преподавателей или студентов;
    - потеря данных образовательной организации.

— Сценарий 3: Утечка данных через социальные сети.

Ситуация: преподаватели и студенты активно используют социальные сети для общения, обсуждая учебные материалы и задания или используют для получения информации тематические группы, ссылки на которые предлагают используемые в процессе обучения интернет-платформы. Злоумышленники, используя фальшивые аккаунты под именем студентов, сделали информационную рассылку об обновлениях «Пользовательского соглашения» используемого в процессе обучения интернет-ресурса со ссылкой на подтверждение аккаунта и просьбой ввести личные данные.

- Угроза: утечка данных или компрометация учетных записей.
- Уязвимость: недостаточная защита аккаунтов в социальных сетях.
- Потенциальные последствия:
    - увеличение вероятности кибербуллинга;
    - нанесение вреда репутации студентов или образовательной организации;
    - утечка личных данных.

2.2. Разработка рекомендаций по эффективному внедрению информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе

Учитывая факт быстро развивающихся цифровых технологий и значительное увеличение объема учебного материала, размещаемого на тематических интернет-ресурсах, образовательные организации все чаще

сталкиваются с угрозами информационной безопасности. В задачи образовательной организации входит не только навык борьбы с этими угрозами и уязвимостями информационной безопасности, но и прогнозирование таких ситуаций, в которых может быть нарушена безопасность информационных систем организации. Поэтому актуальным решением будет использование информационно-аналитической системы по прогнозированию угроз и уязвимостей информационной безопасности образовательной организации.

По ходу исследования темы выпускной квалификационной работы на основе анализа данных тематических интернет-ресурсов, используемых в процессе обучения образовательной организацией, были сформулированы методические рекомендации, которые помогут эффективно интегрировать информационно-аналитическую систему прогнозирования угроз и уязвимостей информационной безопасности в деятельность образовательной организации.

1. Оценка потребностей организации и определение задач.

1.1. Идентификация ресурсов и данных:

— определить все ресурсы, используемые в образовательном процессе (онлайн-библиотеки, образовательные платформы, научные базы данных, тематические интернет-ресурсы и т. д.);

— оценить уровень защищенности и безопасность каждого интернет-ресурса (наличие сертификатов, используемые протоколы и т. д.);

— отметить данные, которые являются конфиденциальными и которые в первую очередь требуют особой защиты (персональные данные сотрудников и студентов образовательной организации; учебные материалы, разработанные педагогами и студентами, которые являются интеллектуальной собственностью).

1.2. Определение основных угроз и уязвимостей информационной безопасности:

— исследовать потенциальные угрозы и уязвимости, характерные для образовательных интернет-ресурсов (внутренние и внешние) для определения наиболее уязвимых мест;

— оценить уровень возможного ущерба, который может быть причинен образовательной организации от возникновения каждой угрозы и уязвимости информационной безопасности.

2. Выбор и внедрение информационно-аналитических систем в структуру информационной безопасности организации.

2.1. Анализ доступных информационно-аналитических систем прогнозирования угроз и уязвимостей:

— сравнить функциональные возможности различных информационно-аналитических систем, представленных на рынке. Особое внимание уделить системам, которые предназначены именно для образовательного сектора и которые соответствуют поставленным задачам;

— рассмотреть возможности интеграции информационно-аналитической системы с уже используемыми системами управления информацией и обучением в образовательной организации;

— изучить уровень поддержки обновлений и технической документации.

2.2. Запрос предложений от поставщиков:

— провести тендер или запрос предложений в организации, специализирующиеся на предоставлении услуг по анализу информационной безопасности посредством анализа интернет-платформ и выявить наиболее подходящие решения для вашей организации.

2.3. Тестирование и пилотирование системы:

— организовать тестирование выбранной информационно-аналитической системы в ограниченном масштабе для выявления возможных проблем с интеграцией и использованием;

— запросить отзывы от конечных пользователей системы: сотрудников образовательной организации и студентов;

— скорректировать работу информационно-аналитической системы при возникновении некорректных процессов работы.

3. Обучение пользователей.

3.1. Разработка учебных программ:

— создайте программы для обучения пользователей, которые будут включать в себя основные аспекты работы с информационно-аналитическими системами;

— включите в программу разделы о принципах информационной безопасности и о самостоятельных способах выявления угроз и уязвимостей во время работы с тематическими интернет-ресурсами;

— разработайте памятку с рекомендациями для сотрудников и студентов при использовании тематических интернет-ресурсов.

3.2. Проведение обучающих мероприятий:

— организуйте регулярные семинары для студентов и преподавательского состава с использованием реальных сценариев реализации угроз, тренинги и вебинары с приглашенными экспертами в сфере организации информационной безопасности организаций, практические занятия по анализу данных и реагированию на инциденты.

3.3. Обратная связь.

— создайте механизмы обратной связи для пользователей, чтобы они могли сообщать о возникающих проблемах в работе системы и предлагать решения для улучшения ее работы.

4. Постоянный мониторинг и обновление информационно-аналитической системы.

4.1. Мониторинг угроз и уязвимостей:

— используйте системы для анализа больших объемов данных на предмет выявления закономерностей и аномалий, которые могут указывать на потенциальные угрозы;

— создайте команду для постоянного мониторинга интернет-ресурсов и систем, используемых в образовательном процессе для выявления инцидентов и оперативной реакции по их решению.

4.2. Анализ эффективности информационно-аналитической системы:

— определите ключевые индикаторы эффективности использования информационно-аналитической системы:

- уровень обнаружения угроз: отражает способность системы идентифицировать и фиксировать потенциальные угрозы в режиме реального времени;
- уровень ложных срабатываний: помогает оценить качество работы системы;
- скорость реагирования на инциденты: время, необходимое для обработки зарегистрированной угрозы, от момента ее выявления до принятия соответствующих мер;
- степень интеграции системы с другими инструментами и процессами управления безопасностью;
- уровень удовлетворенности пользователей.

— периодически проводите анализ работы информационно-аналитической системы: насколько она соответствует индикаторам

эффективности, как хорошо выявляет и прогнозирует угрозы и уязвимости используемых в процессе обучения интернет-ресурсов;

— внедряйте изменения и улучшения на основе проведенного анализа, а также новых возникающих угроз и уязвимостей.

4.3. Аудиты и оценка рисков:

— регулярно проводите аудиты информационной безопасности и оценку рисков для проверки работы системы и актуальности ее использования;

— оценивайте реализацию предложенных мероприятий и их воздействие на уровень безопасности образовательной организации.

5. Разработка политики безопасности образовательной организации при использовании тематических интернет-ресурсов, используемых в образовательном процессе.

5.1. Формирование политики информационной безопасности:

— разработайте четкие правила и процедуры для использования тематических интернет-ресурсов и работы с информационно-аналитической системой;

— включите в политику информационной безопасности аспекты конфиденциальности и защиты данных.

5.2. Повышение осведомленности пользователей:

— обеспечьте доступность информации о политике безопасности образовательной организации при работе с тематическими интернет-ресурсами для всех пользователей и инициируйте кампании по повышению осведомленности в вопросах информационной безопасности.

2.3. Экономическая эффективность разработанных методических рекомендаций по внедрению информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых образовательном процессе

Разработанные методические рекомендации по эффективному внедрению информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, используемых в процессе обучения, имеют теоретико-методологический характер. Методические рекомендации являются первым шагом на пути внедрения информационно-аналитической системы в процесс образования, представляют собой подробный план действий и содержат пункты, которые необходимо рассмотреть и проанализировать на стадии принятия решения о внедрении информационно-аналитической системы.

Сравнительный анализ экономической выгодности использования информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности в образовательной организации можно провести, выделив несколько ключевых аспектов:

— стоимость внедрения и эксплуатации системы прогнозирования угроз и уязвимостей информационной безопасности;

— риски, связанные с безопасностью;

— эффект от повышения безопасности образовательной организации;

— влияние на образовательный процесс и репутацию учреждения.

1. Стоимость внедрения и эксплуатации информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации предполагает первоначальные инвестиции в программное обеспечение и аппаратное

обеспечение, консультирование со специалистами, расходы на обучение сотрудников и студентов правилам пользования системой и последующее техническое обслуживание системы.

— Стоимость программного обеспечения может варьироваться в зависимости от выбранного решения задач информационной безопасности, стоящих перед образовательной организацией. На современном рынке представлены как открытые программные продукты, так и коммерческие с возможностью использовать демо версию продукта для знакомства с ним. Стоимость коммерческих продуктов может варьироваться в зависимости от объема функционала и необходимых лицензий для работы: 10000–100000 рублей.
— Аппаратное обеспечение. При условии установки информационно-аналитической системы на собственные серверы, образовательной организации необходимо будет приобрести мощные сервера, стоимость которых может быть от 5000 до 30000 рублей. При использовании облачных решений, затраты на облачные серверы и услуги составят примерно 1000–10000 рублей в год.
— Консультирование у специалистов и поддержка. На первоначальном этапе данный пункт является одним из основных для получения информации о предполагаемых затратах при использовании информационно-аналитической системы и необходимых условий для ее функционирования. Услуги внешних консультантов могут обойтись в диапазоне 3000–20000 рублей. Стоимость зависит от объема работы и продолжительности сотрудничества.
— Обучение сотрудников образовательной организации. Примерные затраты на обучающие курсы, тренинги и необходимые методические материалы для сотрудников могут составить 2000–

15000 рублей, в зависимости от количества обучающихся и типа обучения.

— Последующее техническое обслуживание и обновление системы. Данный аспект финансовых затрат может составлять 10–20% от первоначальных затрат на программное обеспечение и составлять годовые расходы в размере 10000–15000 рублей.

Таким образом, суммарная стоимость всех расходов на начальном этапе внедрения информационно-аналитической системы прогнозирования угроз и уязвимостей в образовательной организации может составить от 30000 до 200000 рублей, в зависимости от выбранных поставщиков услуг и их условий функционирования. Оценка затрат приблизительна и может варьироваться от конкретных условий, нужд и возможностей образовательной организации.

2. Риски, связанные с безопасностью, являются критическим элементом для оценки экономической выгоды. Использование информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности позволяет выявлять не только текущие угрозы, но и прогнозировать возможные инциденты. Такой подход значительно минимизирует возможные убытки образовательной организации, снижает вероятность успешных атак на информационные системы организации, т. к. благодаря информационно-аналитической системе появляется возможность решить еще не возникшую угрозу или уязвимость, которая может привести к значительным финансовым потерям.

3. Эффект от повышения безопасности в образовательной организации также играет важную роль. Надежная система защиты конфиденциальной информации повышает уровень доверия к образовательной организации как со стороны сотрудников, так и со стороны студентов и их родителей. Это приводит к увеличению числа студентов, что в свою очередь положительно сказывается на финансовой устойчивости учреждения.

4. Безопасная информационная среда благоприятно влияет на образовательный процесс, создавая комфортные условия для учебы и работы, способствуя учебному процессу и снижая затраты, связанные с перерывами и перебоями в обучении из-за инцидентов. Что также является условием повышения репутации образовательной организации, а репутация учебного заведения – это один из важных экономических активов.

Возвращаясь к пункту, где мы рассматривали стоимость внедрения информационно-аналитической системы угроз и уязвимостей информационной безопасности образовательной организации, может показаться, что несмотря на последующие плюсы системы, ее стоимость может быть не столь выгодна. Для сравнения мы также рассмотрели возможные финансовые затраты образовательной организации на устранение рисков и потерь при отсутствии информационно-аналитической системы прогнозирования угроз и уязвимостей в области информационной безопасности образовательной организации.

Аспекты, которые могут повлечь за собой немалые финансовые затраты при несвоевременном обнаружении угроз и уязвимостей:

1. Возможные последствия утечек данных или кибератак. При утечке персональных данных сотрудников или студентов, образовательная организация может столкнуться с затратами на юридические услуги, в том числе на защиту своих интересов в суде. Данные расходы могут варьироваться от 5000 до 100000 рублей, что зависит от масштабов утечки и сложности дела. Также дополнительными потерями финансов может обернуться ходатайство о назначении штрафов.

2. Восстановление информационных систем и данных после инцидента. При атаке с использованием вредоносного программного обеспечения восстановление работы информационной системы образовательной организации: восстановление работы сети и данных, их резервное копирование, могут занять значительное количество временных и финансовых затрат. Стоимость подобных мероприятий варьируется от 10000

до 50000 рублей, включая процесс восстановления данных и покупку новых лицензий на программное и аппаратное обеспечение.

3. Потери от ухудшения репутации образовательной организации. В ситуации публичного обсуждения инцидентов, связанных с информационной безопасность образовательной организации, могут привести к потере студентов и в будущем абитуриентов, потере финансирования или спонсорства. Конкретно оценить данный вид потерь сложно, однако в некоторых случаях они могут составить 50000–200000 рублей или даже больше, особенно в случаях, если образовательная организация является статусной и известной, т. к. любые инциденты быстро становятся предметом общественных обсуждений.

4. Потери или приостановка учебного процесса. При атаке или инциденте, связанным с информационной безопасностью образовательной организации, могут быть отменены или перенесены занятия, что также влияет на доходы организации. Если это приведет к вынужденным долгосрочным перерывам в обучении или серьезным изменениям в расписании, организация может потерять до 20000–70000 рублей из-за уменьшения числа студентов или дополнительных затрат на организацию учебного процесса.

Таким образом, суммируя все потенциальные затраты на решение вопросов организации информационной системы организации при отсутствии системы анализа угроз и уязвимостей, общие финансовые потери могут варьироваться в среднем от 20000 до 300000 рублей или даже больше в зависимости от серьезности инцидента и его последствий.

Сравнивая финальные суммы, которые у нас получились при подсчетах затрат на внедрение информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности и затрат на исправление последствий вовремя невыявленных угроз и уязвимостей при отсутствии системы прогнозирования, мы пришли к таким результатам:

— сумма, которую образовательная организация может потратить на исправление последствий в случае возникновения в информационной системе угроз и уязвимостей, составила в среднем от 20000 до 300000 рублей.

— сумма, которая необходима для внедрения и поддержания функционирования информационно-аналитической системы прогнозирования угроз и уязвимостей образовательной организации, приблизительно получилась от 30000 до 200000 рублей.

Сравнивая вышеуказанные суммы, на первый взгляд может показаться, что выгоды для образовательной организации не так уж и много в использовании информационно-аналитических систем, т. к. финансовые затраты имеют незначительное отличие.

Внедрение информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации действительно требует на первоначальном этапе значительного финансового вклада, но главный плюс данного процесса состоит в том, что он является долгосрочным вкладом, что в перспективе приведет к более стабильному финансовому положению образовательной организации. Вместо того, чтобы тратить финансы организации на исправление периодически возникающих ошибок, угрожающим информационной безопасности организации, и их последствий, стоит инвестировать в превентивные меры для защиты активов образовательной организации и воспользоваться возможностью избежать реализации большинства угроз и их неприятных последствий.

Таким образом, внедрение информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности в деятельность образовательной организации является не только необходимостью, но и вкладом в совершенствование качества информационной безопасности организации и ее учебных процессов, что в долгосрочной перспективе приносит значительные экономические выгоды и обеспечивает стабильность организации в условиях цифровой

трансформации, помогает избежать большую часть ситуаций, которые могут принести большой финансовый ущерб организации или испортить репутацию образовательного учреждения.

Выводы по Главе 2

В первом параграфе второй главы магистерской диссертации мы провели анализ единого информационного пространства базы исследования и анализ тематических интернет-ресурсов, применяемых в процессе обучения. В ходе анализа выделили организационную структуру колледжа с его функциональным назначением ролей, а также состав учебно-материальной, учебно-лабораторной и информационно-технической базы. Рассмотрели группу тематических интернет-ресурсов, рекомендуемых для использования в образовательном процессе студентам, обучающимся по специальности 09.02.01 Информационные системы и программирование (Квалификация – Программист). Проверили безопасность этих ресурсов, проанализировали процесс авторизации, пользовательское соглашение и политику конфиденциальности, наличие рекламных баннеров при использовании ресурсов. На основании чего был также проведен сценарный анализ угроз и уязвимостей информационной безопасности образовательной организации при использовании интернет-ресурсов в процессе обучения.

Во втором параграфе были разработаны методические рекомендации по эффективному внедрению информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе.

В третьем параграфе была обоснованна полезность использования разработанных методических рекомендаций по эффективному внедрению информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа данных тематических интернет-ресурсов, применяемых в образовательном процессе. Был проведен сравнительный анализ финансовых вложений при условии внедрения информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности

образовательной организации в процессы организации и при условии отказа использовать информационно-аналитические системы. По результатам сравнительного анализа определили важность использования информационно-аналитических систем прогнозирования угроз и уязвимостей информационной безопасности в образовательных организациях и привели аргументы в пользу вклада финансовых средств в приобретение этих систем.

ЗАКЛЮЧЕНИЕ

Современное образование все чаще ориентируется на использование тематических интернет-ресурсов в образовательном процессе, что связано с развитием технологий и доступностью информации. Однако с ростом возможностей появляются и новые угрозы и уязвимости, что требует значительного внимания к информационной безопасности образовательных организаций. Обеспечение безопасности информации становится одной из важнейших задач в учебном процессе, особенно в условиях стремительного развития технологий и ростом числа киберугроз.

Образовательные учреждения, как правило, содержат в себе большое количество конфиденциальной информации, которая включает в себя личные данные студентов и преподавателей, результаты интеллектуальной деятельности и финансирование. Это делает их привлекательными для киберпреступников. Информационная безопасность в образовательных организациях включает меры по защите данных от несанкционированного доступа, утечек и разрушений. Препятствие кибератакам и ответственность за утечку данных требует внедрения современных технологий и разработки эффективной стратегии безопасности.

Образовательные сайты, посвященные тематическим областям, онлайн-курсы и платформы для обмена знаниями предоставляют возможность получения актуальной информации, участия в дискуссиях, а также доступа к ресурсам, которые могут обогатить учебный процесс. Однако, взаимодействие с такими ресурсами несет в себе риски, включающие возможность заражения вирусами, фишинга и кражи личных данных.

Исходя из этого, важно определить то, какие инструменты и механизмы необходимо применять, чтобы сформировать информационную безопасность образовательной организации при использовании тематических интернет-ресурсов, сохраняя при этом интересы всех его участников.

В процессе исследования темы была изучена сущность информационной безопасности образовательной организации, рассмотрена классификация угроз и уязвимостей информационной безопасности при применении тематических интернет-ресурсов, рассмотрена сущность информационно-аналитической системы безопасности в образовательной организации и ее основные компоненты, разработаны методические рекомендации по эффективному внедрению информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе анализа тематических интернет-ресурсов, применяемых в образовательном процессе, проанализирована экономическая эффективность разработанных методических рекомендаций.

Исследовательская работа осуществлялась на базе ГБПОУ «Южно-Уральский государственный технический колледж» и показала, что даже тематические интернет-ресурсы, используемые в образовательном процессе, которые входят в «Белый список», могут нести в себе угрозы информационной безопасности образовательной организации.

Соответственно можно сделать вывод, что разработанные методические рекомендации, направленные на эффективное внедрение информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности образовательной организации на основе данных тематических интернет-ресурсов, используемых в процессе обучения, являются практичным планом по внедрению информационно аналитической системы для экономии времени на стадии принятия решения.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций среднего профессионального образования с целью повышения эффективности формирования информационной безопасности образовательной организации при использовании тематических интернет-ресурсов в процессе обучения.

Таким образом, цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. [Электронный ресурс]. — URL: https://www.ec-rs.ru/blog/informacionnaja-bezopasnost/analiz-i-otsenka-informatsionnoy-bezopasnosti / (Дата обращения: 15.12.2024).

2. [Электронный ресурс]. – Режим доступа: https://www.center-rpo.ru/images/files/Методические%20материалы.pdf. – Дата обращения: 18.04.2024.

3. METANIT.COM Сайт о программировании URL: https://metanit.com/ (дата обращения: 25.09.2024).

4. Алексеев В.М., Зефиров С.Л., ГолованоВ.Б. Обеспечение доверия к информационной безопасности: Учебное пособие. — Пенза. Изд-во Пензен. гос. ун-та, 2005.

5. Аргунова Т.Г. Комплексное учебно-методическое обеспечение образовательного процесса: [методическое пособие] / Т. Г. Аргунова, И. П. Пастухова; - М. - Б-ка журн. "Среднее профессиональное образование", 2008. – 109 с. – URL: https://rusist.info/book/1665180 (дата обращения: 16.05.2023)

6. Астахова Л.В. Теория информационной безопасности и методология защиты информации: Конспект лекций / Л.В Астахова. – Челябинск, 2006. – 361 с. – [Электронный ресурс]. – URL: https://studwork.ru/shop/242094-vnedrenie-sistemy-informacionno-analiticheskogo-obespecheniya-bezopasnosti-organizacii (дата обращения: 15.12.2024).

7. Аутентификация, идентификация, авторизация. URL: https://www.banki.ru/wikibank/identifikatsiya/ (дата обращения: 25.09.2024).

8. Баранкова И.И. Минимизация рисков информационной безопасности на основе моделирования угроз безопасности / И. И. Баранкова, У. В. Михайлова, М. В. Афанасьева. — [Электронный ресурс] https://cyberleninka.ru/article/n/minimizatsiya-riskov-informatsionnoy-

bezopasnosti-na-osnove-modelirovaniya-ugroz-bezopasnosti/viewer (Дата обращения: 13.05.2024).

9. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — М.: РИОР : ИНФРА-М, 2018. — 336 с. — (Высшее образование) [Электронный ресурс] // URL: https://publications.hse.ru/mirror/pubs/share/direct/218576514 (дата обращения: 05.10.2024).

10. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие — Москва: Горячая линия-Телеком, 2011. — 558 с. — ISBN 5-93517-292-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/111016 (дата обращения: 13.05.2024). — Режим доступа: для авториз. пользователей.

11. Бесплатные курсы по программированию URL: https://practicum.yandex.ru/catalog/programming/free/ (дата обращения: 25.09.2024).

12. Бояров Е.Н. Теоретические основы построение безопасной информационной образовательной среды подготовки педагогов в области безопасности жизнедеятельности. Социосфера. — 2012. № 4. — с. 101–106

13. Бузинов А.С., Жигулин Г.П., Шабаев Р.И. Моделирование и прогнозирование информационных угроз как составная часть Концепции информационной безопасности РФ // Известия Российской академии ракетных и артиллерийских наук. – 2010. – № 4(66) – [Электронный ресурс]. – URL: http://faculty.ifmo.ru/ikvo/MPES/downloads/ modinfygr.doc (дата обращения: 15.06.2023).

14. Василькова, Н.А. Методика профессионального обучения: конспект лекций. Ч. 1. / Н.А. Василькова; ЮУРГГПУ. — Челябинск: Изд-во ЮУРГГПУ, 2017. — URL: http://elib.cspu.ru/xmlui/handle/123456789/2198 (дата обращения: 16.12.2022)

15. Владимирова Т.В. Сетевые коммуникации как источник информационных угроз [Электронный ресурс] // URL: http://ecsocman.hse.ru/data/2011/09/20/1267451215/Vladimirova.pdf (дата обращения 25.11.2024)

16. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. — Екатеринбург: Изд-во Урал. ун-та, 2019.— 204 с.

17. Галатенко, В.А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. — 2-е изд. — Москва: ИНТУИТ, 2016. — 266 с. — ISBN 978-5-94774-821-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/100295 (дата обращения: 25.04.2024). — Режим доступа: для авториз. пользователей.

18. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200058320 (дата обращения 08.06.2024).

19. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200075565 (дата обращения: 15.05.2023).

20. Жиделев, М.А. Современные методы обучения / М.А. Жиделев / — М: Высш. шк., 1985. — 72 с. — URL: https://obuchalka.org/20201216127662/sovremennie-metodi-obucheniya-jidelev-m-a-1985.html (дата обращения 14.12.2022)

21. Зырянова Т.Ю. Информационно-аналитические системы безопасности: учебно-методическое пособие / Т. Ю. Зырянова. – Екатеринбург: УрГУПС, 2016. – 160 с. — [Электронный ресурс]. — URL: file:///C:/Users/Виктория/Downloads/umm_12189%20(1).pdf (дата обращения: 25.05.2024)

22. Информационная безопасность [Электронный ресурс]. URL: https://www.oknemuan.ru/files/infosequrity/Lektsiya_2_Informatsionnaya_bezopasnost_1702668964.pdf (дата обращения: 26.05.2024)

23. Информационно-аналитические системы: определение, цели, задачи. — [Электронный ресурс]. — URL: https://ozlib.com/1037589/tehnika/informatsionno_analiticheskie_sistemy (дата обращения: 25.05.2024).

24. Киричек Т.А., Архипова А.И. Тематический интернет-ресурс для учителя. Обоснование проблемы, структура, программная составляющая // г. Краснодар: Кубанский государственный университет [Электронный ресурс] — URL: https://cyberleninka.ru/article/n/tematicheskiy-internet-resurs-dlya-uchitelya-obosnovanie-problemy-struktura-ogrammnayasostavlyayuschaya/viewer (дата обращения: 26.05.2024)

25. Коваленко А.П., Белов Е.Б. Концепция подготовки кадров в области обеспечения информационной безопасности (проблемы, анализ, подходы) //Научные и методологические проблемы информационной безопасности/под ред. В.П Шерстюка. – М.: МЦНМО. – 2004. – 115 с.

26. Коваленко, Ю. И., Методика защиты информации в организациях: монография / Ю. И. Коваленко, Г. И. Москвитин, М. М. Тараскин. — Москва: Русайнс, 2020. — 162 с. — ISBN 978-5-4365-0887-0. — [Электронный ресурс] — URL: https://book.ru/book/934719 (дата обращения: 15.12.2024).

27. Максименко В.Н., Ясюк Е.В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. 2017. №2 (4). URL: https://cyberleninka.ru/article/n/osnovnye-podhody-k-analizu-i-otsenke-riskov-informatsionnoy-bezopasnosti (дата обращения: 13.12.2023).

28. Мельников В.П. Информационная безопасность: учеб пособие для студ. учреждений сред. проф. образования / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 8-е изд., испр. – М.: Издательский центр «Академия», 2013. – 336 с.

29. Мельников В.П. Информационная безопасность: учеб пособие для студ. учреждений сред. проф. образования / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 8-е изд., испр. – М.: Издательский центр «Академия», 2013. – 336 с.

30. Методика оценки рисков информационной безопасности [Электронный ресурс]. — URL: https://kontur.ru/articles/1691 (Дата обращения: 29.11.2024).

31. Методы и приемы обеспечения информационной безопасности [Электронный ресурс]. URL: http://med-sayansk.ru/wp-content/uploads/2020/05/12.05.20-2B-Lektsiya-15.-Metody-i-priemy-obespecheniya-informatsionnoj-bezopasnosti.pdf (дата обращения: 12.12.2022).

32. Минаев, Г. А. Образование и безопасность: учебное пособие [Текст] / Г. А. Минаев. — Москва: Логос, 2020. — 312 с.

33. Моё обучение - Stepik URL: https://stepik.org/learn (дата обращения: 25.09.2024).

34. Назаров Д. М. Основы обеспечения безопасности персональных данных в организации: учеб. пособие [Текст] / Д. М. Назаров, К. М. Саматов; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. - Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2019. - 118 с.

35. Национальный открытый университет "ИНТУИТ" URL: https://intuit.ru/intuituser/userpage (дата обращения: 25.09.2024).

36. Нестеров С. А. Основы информационной безопасности: учеб. пособие. — 5-е изд., стер. — Санкт-Петербург: Лань, 2019. — 324 с. [Электронный ресурс] // URL: https://e.lanbook.com/book/114688 (дата обращения 07.12.2024)

37. Новости| CS IT URL: https://csitltd.ru/company/news/2020/plany-na-prokachku-podborka-obrazovatelnykh-resursov-ot-microsoft/ (дата обращения: 25.09.2024).

38. Обеспечение информационной безопасности деятельности учебного заведения: монография. / В. В. Шевцов, В. П. Мельников, А. И.

Куприянов, А. О. Шемяков. - М.: ЗАО «Издательское предприятие «Вузовская книга», 2012. - 343 с. [Электронный ресурс] — URL: https://new-disser.ru/_avtoreferats/01006664422.pdf (дата обращения: 13.05.2023)

39. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва: ЮНИТИ-ДАНА, 2023. — 287 с. — ISBN 978-5-238-02857-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/141624.html (дата обращения: 29.11.2024). — Режим доступа: для авторизир. Пользователей

40. Плотникова П. В. Киберпреступность как угроза обществу / П. В. Плотникова, Р.С. Усенко // Проблемы информационной безопасности: Труды VI Всероссийской с международным участием научно-практической конференции, Симферополь-Гурзуф, 13–15 февраля 2020 года. - Симферополь-Гурзуф: ИП Зуева Т.В., 2020. - С. 105–107.

41. Понятие, сущность, цели и значение защиты информации [Электронный ресурс]. URL: https://textarchive.ru/c-2525943.html (дата обращения: 14.12.2024).

42. Российская государственная библиотека [Электронный ресурс]. – Режим доступа: https://search.rsl.ru/ru/record/01001407209. – Дата обращения: 18.04.2024.

43. Саранов, А.М. Теоретические основы становления и развития инновационных образовательных систем / А.М. Саранов. – 2000. – 385 с. — URL: https://www.dissercat.com/content/teoreticheskie-osnovy-stanovleniya-i-razvitiya-innovatsionnykh-obrazovatelnykh-sistem (дата обращения: 11.11.2023)

44. Скородумов Б.И. О понятийно терминологическом аппарате информационной безопасности // Безопасность информационных технологий. - 2008. - С. 43–45.

45. Сластенин, В.А. Учебное пособие для студентов высших педагогических учебных заведений / В. А. Сластенин, И. Ф. Исаев, Е. Н.

Шиянов; Под ред. В.А. Сластенина. - М.: Издательский центр "Академия", 2002. - 576 с. – URL: https://refdb.ru/look/1033857-pall.html (дата обращения: 15.11.2023)

46. Тимофеева Л.Л. Компетентность педагога в обеспечении информационной безопасности детей дошкольного возраста // Образование в Орловской области. 2019. № 1. С. 43—53.

47. Тимофеева Л.Л. Методические рекомендации по обеспечению информационной безопасности в образовательной организации / сост. Л. Л. Тимофеева. – Орёл: Бюджетное учреждение Орловской области дополнительного профессионального образования «Институт развития образования», 2020. – 58. с.– Текст: непосредственный. [Электронный ресурс]. – URL: https://xn--h1albh.xn--p1ai/wp-content/uploads/2021/06/Metodicheskie-rekomendacii-po-obespecheniju-informacionnoj-bezopasnosti-v-obrazovatelnoj-organizacii.pdf (Дата обращения: 15.05.2024).

48. Тимофеева Л.Л. Создание безопасной информационной среды в дошкольной образовательной организации // Детский сад от А до Я. 2020. № 1. С. 26—38.

49. Угрозы информационной безопасности [Электронный ресурс] // URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozyinformatsionnoj-bezopasnosti/ (дата обращения: 25.04.2023).

50. Угрозы информационной безопасности [Электронный ресурс] // URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozyinformatsionnoj-bezopasnosti/ (дата обращения: 15.05.2023).

51. Уфимцев Ю.С. Методика информационной безопасности Московская академия экономики и права. - Москва: Экзамен, 2004. - 542 с. — ISBN 5-94692-517-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://search.rsl.ru/ru/record/01002429306 (дата обращения: 25.05.2024). — Режим доступа: для авториз. пользователей.

52. Учебник для студентов, обучающихся по педагогическим специальностям и направлениям. Под ред. Батышева С.Я., Новикова А.М.

Издание 3-е, переработанное. М.: Из-во ЭГВЕС, 2009 г., - 456 с. — URL: https://www.studmed.ru/batyshev-sya-professionalnaya pedagogika_d5535ef1363.html (дата обращения: 11.11.2023)

53. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере: учебное пособие / А. Е. Фаронов. — 4-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 с. — ISBN 978-5-4497-2418-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/133957.html (дата обращения: 29.11.2024). — Режим доступа: для авторизир. Пользователей

54. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 30.05.2023).

55. Федоров, В.А. Организация научно-исследовательской работы студентов в вузе: учебно-методическое пособие / В. А. Федоров, А. В. Ефанов [и др.]; Рос. гос. проф.-пед. ун-т. — Екатеринбург: Издательство РГППУ, 2009. — 143 с. — URL: ISBN 978-5-8050-0375-3. (дата обращения: 18.04.2024)

56. Фот, Ю. Д. Методы защиты информации: учебное пособие [Текст] / Ю. Д. Фот. — Оренбург: ОГУ, 2019. — 230 с.

57. Цирлов, В.Л. Основы информационной безопасности: краткий курс / Цирлов В.Л. — Ростов-на-Дону: Феникс, 2008. — 254 с.: ил. — (Профессиональное образование). —Библиогр.: с. 167-170 — ISBN 978-5-222-13164-0 — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://www.livelib.ru/book/1000364986-osnovy-informatsionnoj-bezopasnosti-kratkij-kurs-tsirlov-vl (дата обращения: 25.05.2024). — Режим доступа: для авториз. пользователей.

58. Шарафутдинова, А.Р. Защита информации в образовательных учреждениях / А.Р. Шарафутдинова, В.С. Пядышева [Электронный ресурс].

URL: http://www.rusnauka.com/17_APSN_2013/Matemathics/2_140911.doc.htm (дата обращения: 30.05.2023).

59. Шипилова, Т.Н. Методика профессионального обучения в вопросах и ответах: учебное пособие / Т. Н. Шипилова, В. П. Тигров, О. Ю. Добромыслова [и др.]; под редакцией Ю. А. Гречишникова. — Липецк: Липецкий ГПУ, 2017. — 195 с. — ISBN 978-5-88526-792-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/111947 (дата обращения: 18.04.2024). — Режим доступа: для авторизованных пользователей.

60. Яндекс: Проверка сайта на безопасность URL: https://yandex.ru/safety/ (дата обращения: 25.09.2024).

61. Ярочкин, В.И. Информационная безопасность: учебник для вузов [Текст] / В.И. Ярочкин. — Москва: Академический Проект, 2020. — 544 с.