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

Вероятностная модель причинения вреда информационной системе образовательной организации при несанкционированных доступах

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

Проверка на объем заимствований:
70,82 % авторского текста
Работа рекомендована к защите
«13» 05 2023 г.
зав. кафедрой АТ, ИТ и МОТД
_____ В.В. Руднев

Выполнила:
Студентка группы ОФ-209-210-2-1
Тимершина Валентина Фанисовна
Научный руководитель:
к.п.н., доцент кафедры АТ, ИТ и МОТД
_____ Гафарова Елена Аркадьевна

Челябинск
2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Образовательный процесс касается наименее защищенных от пропаганды членов общества – детей и подростков. Поэтому система информационной безопасности образовательного учреждения должна не только обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений, но и гарантировать невозможность доступа в стены колледжа любой пропаганды, как незаконного характера, так и безобидной, но предполагающей воздействие на сознание обучающихся в заведениях среднего профессионального образования.

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность подростков, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус. Выделяются четыре группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

—компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам,

—программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак,

—данные, хранимые как на жестких дисках, так и на отдельных носителях,

—сам персонал, отвечающий за работоспособность IT-систем,

—дети, подверженные внешнему агрессивному информационному влиянию и способные создать в школе криминальную ситуацию. В последнее время перечень таких ситуаций существенно расширился, что

говорит о возможной целенаправленной психологической атаке на сознание детей и подростков.

Угрозы, направленные на повреждение любого из компонентов системы, могут носить как случайный, так и осознанный преднамеренный характер. Среди угроз, не зависящих от намерения персонала, обучающихся или третьих лиц, можно назвать:

—любые аварийные ситуации, например, отключение электроэнергии или затопление,

—ошибки персонала,

—сбои в работе программного обеспечения,

—выход техники из строя,

—проблемы в работе систем связи.

Все эти угрозы информационной безопасности носят временный характер, предсказуемы и легко устраняются действиями сотрудников и специальных служб.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев не могут быть предвидены. Их виновниками могут оказаться обучающиеся, служащие, конкуренты, третьи лица с намерением на совершение кибер-преступления. Для подрыва информационной безопасности такое лицо должно иметь высокую квалификацию в отношении принципов работы компьютерных систем и программ. Наибольшей опасности подвергаются компьютерные сети, компоненты которых расположены отдельно друг от друга в пространстве. Нарушение связи между компонентами системы может привести к полному подрыву ее работоспособности. Важной проблемой может стать нарушение авторских прав, намеренное хищение чужих разработок. Компьютерные сети редко подвергаются внешним атакам с целью воздействия на сознание подростков, но и это не исключено. И самой серьезной опасностью станет

использование оборудования колледжа для вовлечения подростков в криминал и терроризм.

Необходимость в управлении инцидентами информационной безопасности является важной частью системы обеспечения информационной безопасности объекта, и в частности, эффективное обнаружение происходящих инцидентов ИБ в информационной системе образовательных организаций, а также прогнозирование возможных инцидентов ИБ определяют **актуальность** темы исследования.

Проблемой исследования является определение вероятности осуществления вреда при несанкционированных доступах в информационной системе образовательной организации.

Была сформулирована **тема исследования**: «Вероятностная модель причинения вреда информационной системе образовательной организации при несанкционированных доступах».

Цель исследования: теоретико-методическое обоснование и апробация вероятностной модели причинения вреда информационной системы образовательной организации при несанкционированных доступах.

Объект исследования: информационная система образовательной организации.

Предмет исследования: вероятностная модель причинения вреда информационной системе при несанкционированных доступах.

Гипотеза диссертационного исследования состоит в том, что вероятностная модель причинения вреда позволит оценивать текущее состояние защищенности информационной системы и точнее планировать меры её защиты.

Для достижения данной цели были поставлены следующие **задачи**:

1) Изучить аспекты безопасности информационной системы образовательной организации.

2) Провести анализ актуального состояния защищенности информационной безопасности системы образовательной организации.

3) Разработать общую модель причинения вреда информационной системе образовательной организации при несанкционированных доступах.

4) Провести апробацию модели причинения вреда информационной системы образовательной организации при несанкционированных доступах, конкретизировать ее вероятностный аспект.

5) Разработать рекомендации на основе вероятностной модели причинения вреда информационной системы образовательной организации.

Научная новизна проведённых исследований и полученных в работе результатов заключается в следующем: разработана вероятностная модель причинения вреда информационной системе образовательной организации при несанкционированных доступах.

Теоретическая значимость проведенного исследования состоит в том, что результаты исследовательской части и выводы могут быть использованы для теоретических обобщений и дальнейшего более глубокого изучения темы.

Практическая значимость заключается в разработке рекомендаций на основе вероятностной модели причинения вреда информационной системы образовательной организации

Ход исследования и его результаты докладывались и обсуждались на международных конференциях:

✓ МОЛОДЕЖНАЯ ПОЛИТИКА И СОЦИАЛЬНАЯ МИССИЯ ОБРАЗОВАНИЯ В ЭПОХУ ГЛОБАЛИЗАЦИИ И ЦИФРОВИЗАЦИИ: международная научно-практической конференции и молодежного форума (06-08 апреля 2022 г., г. Челябинск) // Тимершина В.Ф. «Компьютерные преступления и злоупотребления», в сб. статей. – Челябинск: Издательство Челябинск: изд-во «ЗАО Библиотека А. Миллера», 2022. – с. 525

✓ НАУЧНАЯ ПЛАТФОРМА: ДИСКУССИЯ И ПОЛЕМИКА: международная научно-практическая конференция (28 ноября 2022 г.) //

Тимершина В.Ф. «Применение информационных систем в современном образовании». В сб. статей. – Кемерово: ЗапСибНЦ, 2022 – с. 46 -48

✓ НАУЧНЫЙ ФОРУМ: ТЕНДЕНЦИИ РАЗВИТИЯ НАУКИ И ОБЩЕСТВА: международная научно-практической конференции (15 декабря 2022 г.) // Тимершина В.Ф. «Формирование культуры кибербезопасности студентов колледжа». [Текст]/В.Ф. Тимершина // сборник материалов – Кемерово: ЗапСибНЦ, 2022 – с. 77

✓ НАСТОЯЩЕЕ И БУДУЩЕЕ СОВРЕМЕННЫХ НАУЧНЫХ НАПРАВЛЕНИЙ: Международная научно-практическая конференция (13 июня 2022 г.) // Тимершина В.Ф. «Мотивационные аспекты личности злоумышленников в процессе причинения вреда информационной системе», в сборнике материалов Международной научно-практической конференции (13 июня 2022 г.), – Кемерово: ЗапСибНЦ, 2022 – с. 95.

Теоретической и методологической основой исследования являются разработки зарубежных и отечественных специалистов, осуществляющих работу по разработке и модернизации политики информационной безопасности в различных секторах бизнеса, а также материалы научных конференция, данные информационно-аналитических отчетов.

Методы исследования: изучение и анализ теоретико-методических источников по проблеме информационной безопасности, анализ угроз и аудит информационной системы образовательной организации на предмет актуального уровня защищенности, моделирование, математические расчеты.

Базой проведения исследования стал ГБПОУ СПО «Южно-Уральский государственный технический колледж», Политехнический комплекс.

Личное участие соискателя состоит в теоретико-методическом обосновании и апробации вероятностной модели причинения вреда

информационной системы на базе ГБПОУ СПО «ЮУрГТК» при несанкционированных доступах.

Структура магистерской диссертации состоит из введения, основной части (двух глав), заключения и списка использованных источников.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАЗРАБОТКИ МОДЕЛИ ПРИЧИНЕНИЯ ВРЕДА ИНФОРМАЦИОННОЙ СИСТЕМЕ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Аспекты безопасности информационной системы образовательной организации

На первый взгляд, информационная безопасность кажется довольно простой и несложной концепцией – это вопрос технической защиты информационных систем и данных от нежелательных злоумышленников, вредоносного программного обеспечения и нежелательного использования, а также поддержание пригодности информации для целей минимизации институционального риска [38]. Однако информационная безопасность – это больше, чем просто IT-безопасность. Это – поддержание брандмауэров, антивирусного программного обеспечения и безопасных паролей.

Безопасность информации представляет собой бесчисленные риски для бизнеса в современном мире: риск нарушения закона об информации, риск значительного ущерба репутации в результате утечки данных, риск неспособности вести бизнес, катастрофический отказ информационных систем и риск стать объектом постоянных политических действий, направленных на нарушение коммерческих операций.

Большинство определений информационной безопасности включают в себя ряд различных вопросов, касающихся информации и управления данными: конфиденциальность, целостность и доступность. Конфиденциальность связана с ограничением доступа к информации для неуполномоченных лиц или организаций, что существенно предотвращает попадание информации в руки злоумышленников. С другой стороны, целостность относится к поддержанию точности и полноты сбора информации в течение его жизненного цикла, включая управление и аудит изменений данных или набора данных.

Доступность информации – это состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно [42].

Чаще всего информационную безопасность связывают с цифровой информацией, которая в настоящее время зависит от современной коммерческой практики и носит цифровой характер. Однако, в отличие от IT-безопасности, информационная безопасность не обязательно должна быть связана с цифровой информацией.

Технологические компоненты информационной безопасности относительно хорошо изучены. Межсетевые экраны отслеживают, блокируют и фильтруют трафик в сетях. Надежное шифрование защищает данные, передачу данных и коммуникации от подслушивания и случайных утечек. Надежное шифрование защищает данные, передачу данных и коммуникации от подслушивания и случайных утечек. Управление доступом, управление версиями и журналы аудита помогают поддерживать целостность информационных систем и прерывать свободный поток информации для обеспечения ее контроля.

Необходимо отметить, что включение информационной безопасности в процессы управления информацией – это вопрос понимания природы возникающих угроз. При этом существует некоторая тенденция преувеличивать внешние угрозы для информации и данных – опасность со стороны хакеров, политических хактивистов и различных форм вредоносного ПО, и недооценивать внутренние угрозы – определенную категорию недобросовестных сотрудников.

Угрозы информационной безопасности можно разделить на несколько видов:

1) Преднамеренные последствия преднамеренных действий, например, взлома, атак типа «отказ в обслуживании», вредоносного программного обеспечения, шпионского по, промышленного шпионажа и преднамеренной кражи данных или утечек.

2) Непреднамеренные последствия преднамеренных действий, например, случайное или неосторожное удаление информации, случайное или неосторожное раскрытие информации, непреднамеренное нарушение конфиденциальности, непреднамеренная утечка данных.

3) Непреднамеренные последствия непреднамеренных действий, например, случайная потеря данных, случайное уничтожение данных.

Во многих отношениях первые из них легче всего предсказать, и от них легче всего защититься. Преднамеренные последствия преднамеренных действий описывают виды вредоносных действий и программного обеспечения, которые привлекают наибольшее внимание: взлом, вредоносное ПО и кража данных. Эти риски относительно легко сформулировать: известные в мире информационной безопасности, события, которые мы можем предвидеть и к которым мы можем подготовиться.

Гораздо сложнее предсказать непреднамеренные последствия запланированных или непреднамеренных действий: важные электронные письма, которые удаляются, а не архивируются, информация, переданная списку рассылки, а не отдельному человеку и др.

Одним из способов решения данной ситуации является предписание о соблюдении политики безопасности, запрещающее сотрудникам устанавливать собственное программное обеспечение, а также привлечение их к ответственности, если они это сделают. Следующим шагом возможно обучение сотрудников понимать риски, связанные с вредоносными и шпионскими программами. Не существует политики, которая могла бы предотвратить потерю кем-либо универсального запоминающего устройства с последовательной шиной или случайное нажатие на кнопку «отправить всем» при отправке электронного сообщения – политика и обучающие последствия этих непреднамеренных и непредсказуемых событий должны быть сосредоточены на минимизации потенциального воздействия этих рисков.

Информационная безопасность — это вопрос понимания и управления рисками, а не устранение угроз. Когда каждое функциональное вычислительное устройство также является сетевым вычислительным устройством, не существует такой вещи, как абсолютно безопасная информационная система. Не менее важно поддерживать не только конфиденциальность информации, но и пригодность информации процессов, в которые она включена, а это неизбежно связано с риском. Чем больше систем безопасности, тем больше риски для организаций, поэтому целенаправленно необходимо сохранять баланс между безопасностью и свободным потоком информации.

Практически все без исключения настоящие слабые места информационной безопасности в любой системе или процессе — это не технологические уязвимости, а человеческий фактор. Процесс использования человеческого фактора в информационной безопасности получил название социальной инженерия. По своей сути это процесс обмана кого-либо лица, имеющего право на доступ для раскрытия паролей, данных доступа или конфиденциальной информации. Как замечает специалист по кибербезопасности Кевин Митник, часто легче обмануть кого-то, чтобы он разрешил вам доступ к системе, чем взламывать ее: «Для социального хакера это самый простой способ достичь своей цели. Почему злоумышленник должен часами пытаться взломать, если он может сделать это с помощью простого телефонного звонка» [39].

Одним из возможных способов решения является недопустимость использовании простых или предсказуемых паролей, использование одних и тех же паролей в нескольких системах, записывание паролей, обмен подробностями своего журнала с коллегами, оставление систем авторизованными, перенос домашних файлов на карты памяти и использование одного адрес электронной почты для личных и профессиональных целей и т.д.

Таким образом, можно сделать вывод о том, что понятие информационной безопасности не следует рассматривать в первую очередь как технологическую проблему. Технология изменила масштаб и интенсивность коммуникационных и информационных практик, но основные принципы человеческой социализации остались прежними. Информационная безопасность – по сути, проблема людей, их беспорядочная, непредсказуемая и органичная природа. Способ решения проблемы информационной безопасности – это понять, как информация входит в рабочие процессы внутри организации и в чем заключаются уязвимости.

Компьютерные преступления — незаконные действия, в которых компьютеры являются основным инструментом. Они ежегодно обходятся мировой экономике во многие миллиарды долларов. К целям так называемого взлома информационных систем относятся вандализм, кража потребительской информации, государственный и коммерческий шпионаж, саботаж и кибервойна. Некоторые из наиболее распространенных средств компьютерных преступлений включают фишинг и внедрение вредоносных программ, таких как компьютерные вирусы и черви, троянские кони и логические бомбы.

Фишинг включает в себя получение логина и другой информации законного пользователя путем уловок с помощью сообщений, мошенническим образом утверждающих, что они исходят от законного лица, такого как банк или государственное учреждение. За успешным фишинговым рейдом с целью получения информации о пользователе может последовать кража личных данных, выдача себя за пользователя с целью получения доступа к ресурсам пользователя [8].

Компьютерные вирусы являются особенно распространенной формой атаки. Это программные инструкции, способные не только совершать вредоносные действия, но и вставлять свои копии в другие программы и таким образом распространяться на другие компьютерные системы.

Подобно вирусам, черви представляют собой полные компьютерные программы, которые размножаются и распространяются по телекоммуникационным сетям. Из-за своей способности быстро и широко распространяться вирусы и черви могут нанести огромный ущерб. Ущерб может быть в форме вмешательства в работу системы, кражи больших объемов данных (например, номеров кредитных карт), известной как утечка данных, или отказа в обслуживании путем перегрузки систем потоком ложных запросов.

При атаке с помощью троянского коня злоумышленник скрывает несанкционированные инструкции в авторизованной программе. Логическая бомба состоит из скрытых инструкций, часто вводимых с помощью техники троянского коня, которые остаются бездействующими до тех пор, пока не произойдет определенное событие, когда инструкции активируются. В одном хорошо известном случае в 1985 году программист страховой компании в Форт-Уэрте, штат Техас, заложил логическую бомбу в систему управления персоналом своей компании. Когда его уволили и его имя было удалено из базы данных сотрудников компании, вся база данных была стерта [31].

Как только система, подключенная к Интернету, подвергается вторжению, она может быть использована для захвата и организации их в так называемые ботнеты, которые могут запускать массовые атаки на другие системы с целью кражи информации или саботажа их работы. Растет обеспокоенность тем, что в Интернете управляемые компьютером устройства, такие как холодильники или телевизоры, могут быть развернуты в ботнетах. Разнообразие устройств затрудняет их защиту от вредоносных программ.

Чтобы обеспечить безопасную и эффективную работу информационных систем, организация устанавливает набор процедур и технологических мер, называемых средствами контроля. Информационные

системы защищены с помощью комбинации общих и прикладных средств контроля.

Общие средства контроля применяются к деятельности информационной системы во всей организации. Наиболее важными общими мерами контроля являются меры, которые контролируют доступ к компьютерным системам и информации, хранящейся в них или передаваемой по телекоммуникационным сетям. Общие средства контроля включают административные меры, которые ограничивают доступ сотрудников только к тем процессам, которые имеют непосредственное отношение к их обязанностям. В результате эти элементы управления ограничивают ущерб, который может нанести любой отдельный сотрудник или сотрудник, выдающий себя за другого. Отказоустойчивые компьютерные системы, устанавливаемые в критических средах, таких как информационные системы больниц или рынки ценных бумаг, предназначены для контроля и изоляции проблем, чтобы система могла продолжать функционировать. Резервные системы, часто расположенные в удаленных местах, могут активироваться в случае выхода из строя основной информационной системы [9].

Элементы управления приложениями относятся к конкретному приложению и включают такие меры, как проверка входных данных, регистрация доступа к системе, регулярное архивирование копий различных баз данных и обеспечение того, чтобы информация распространялась только среди авторизованных пользователей.

Контролировать доступ к информационным системам стало значительно сложнее с распространением глобальных сетей (WAN) и, в частности, Интернета. Пользователи, а также злоумышленники могут получить доступ к системам с любого компьютера, оставленного без присмотра в организации, или практически из любого места через Интернет. В качестве меры безопасности каждый законный пользователь имеет уникальное имя и регулярно изменяемый пароль. Еще одной мерой

безопасности является требование физической аутентификации в той или иной форме, такой как объект (физический токен или смарт-карта) или личная характеристика (отпечаток пальца, рисунок сетчатки глаза, геометрия руки или подпись). Многие системы сочетают эти типы мер, например, банкоматы, которые полагаются на комбинацию личного идентификационного номера (PIN) и удостоверения личности. Меры безопасности, размещенные между внутренними сетями организации и Интернетом, известны как брандмауэры. Эти комбинации аппаратного и программного обеспечения постоянно фильтруют входящий и часто исходящий трафик данных.

Другим способом, позволяющим запретить доступ к информации, является шифрование данных, которое приобрело особое значение в электронной торговле. Шифрование с открытым ключом широко используется в такой коммерции. Для обеспечения конфиденциальности только предполагаемый адресат имеет закрытый ключ, необходимый для расшифровки сообщений, зашифрованных с помощью открытого ключа адресата. Кроме того, аутентификация обеих сторон в электронной транзакции возможна благодаря цифровым сертификатам, выданным обеим сторонам доверенной третьей стороной, и использованию цифровых подписей — дополнительного кода, прикрепляемого к сообщению для подтверждения его происхождения. К сообщению также можно прикрепить тип кода защиты от несанкционированного доступа для обнаружения повреждения. Аналогичные средства доступны для обеспечения того, чтобы стороны электронной транзакции не могли впоследствии отказаться от своего участия. Для некоторых сообщений требуются дополнительные атрибуты. Например, платеж электронными деньгами — это тип сообщения с шифрованием, используемым для обеспечения анонимности покупателя, который действует как наличные деньги [11].

Для постоянного мониторинга информационных систем используются системы обнаружения вторжений. Они обнаруживают

аномальные события и регистрируют информацию, необходимую для составления отчетов и установления источника и характера возможного вторжения. Более активные системы также пытаются предотвратить вторжение при обнаружении в режиме реального времени.

Информационные системы — это дисциплина, которую обычно изучают в бизнес-школах. Основной целью дисциплины является разработка и изучение теорий, методов и систем использования информационных технологий для работы и управления организациями, а также для поддержки их предложений на рынке. Дисциплина использует социотехнический подход, помещая изучение информационных технологий в контекст управления, организаций и общества. Академическое изучение информационных систем зародилось в 1960-х годах. Научным обществом, способствующим развитию дисциплины, является Ассоциация информационных систем (АИС).

Компьютеризированные информационные системы, особенно с появлением Интернета и мобильных компьютеров, оказали глубокое влияние на организации, экономику и общество, а также на людей, чья жизнь и деятельность осуществляются в этих социальных агрегатах. Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить конфиденциальные данные.

1.2 Анализ актуального состояния информационной безопасности системы образовательной организации как основание для построения модели причинения вреда

В ГБПОУ СПО "Южно-Уральский государственный технический колледж" создан и успешно работает информатизационный центр (ИЦ) — структурное подразделение, отвечающее за состояние единой информационной среды колледжа. Главной целью деятельности ИЦ является формирование единого информационного пространства и повышение эффективности работы подразделений колледжа, путем апробации ИТ. Информационная среда колледжа — это все рабочие станции в сети, все сервисы доступны с любого компьютера в соответствии с политикой безопасности, 650 компьютеров, 30 компьютерных аудиторий, корпоративная сеть на основе оптоволокна, 7 современных физических серверов, 28 виртуальных серверов, два канала доступа к сети Интернет, собственный web-хостинг, лицензионное программное обеспечение, организация ИТ-службы по международному стандарту ITIL, собственное вычислительное облако.

Технология виртуальной обучающей среды, система управления курсами Moodle активно внедряется в учебный процесс колледжа. ИЦ разработан сайт dom.sustec.ru, который подключен к сайту колледжа. Преподаватели ПЦК активно используют возможности обучающей среды Moodle в учебном процессе. Таким образом, студенты осваивают работу с системами дистанционного обучения, что тоже пригодится в дальнейшей жизни молодого человека и специалиста.

Использование активных методов обучения, новых ИТ, прикладного программного обеспечения, систем дистанционного обучения, облачных технологий и др. позволяет преподавателям и обучающимся активизировать процесс обучения, сделать его информационно насыщенным. Таким

образом, в учебном процессе и во внеучебной деятельности формируется информационная культура участников учебного процесса.

Ежегодно более трех тысяч южноуральцев и жителей соседних областей выбирают Южно-Уральский государственный технический колледж для получения среднего профессионального образования. За 70 лет учебное заведение стало крупнейшим образовательным учреждением среднего профессионального образования Южно-Уральского региона.

Колледж гордится своей историей, заслуженными выпускниками, чтит сложившиеся традиции и уверенно смотрит в будущее!

ГПБОУ СПО «ЮУрГТК» — это устойчивые результаты деятельности преподавателей и студентов, сформированная разноуровневая образовательная среда, крепкие связи с предприятиями-работодателями, многочисленные награды за победу в престижных конкурсах.

Основное ядро колледжа — педагогические кадры. Непрерывно повышая свой квалификационный уровень, преподаватели ЮУрГТК используют в работе знания современных педагогических и информационных, а также передовых производственных технологий. Это привлекает в учебное заведение целые семейные династии, воспитано уже не одно поколение специалистов, ставших рабочей элитой области, региона, страны.

Южно-Уральский государственный технический колледж всегда идет в ногу со временем. В колледже создана и успешно функционирует сертифицированная система менеджмента качества, реализуются инновационные программы, совершенствуются учебные планы, открываются новые специальности. Непреложными остаются только славные традиции Южно-Уральского государственного технического колледжа, позволяющие всем будущим выпускникам быть востребованными на рынке труда, адаптироваться в непростых современных условиях жизни.

Для проведения анализа уязвимостей существующей системы информационной безопасности ГБПОУ Южно-Уральского государственного технического колледжа наиболее оптимальным методом является разработка модели угроз.

Необходимость разработки модели угроз регламентирована рядом нормативных документов, таких как:

– часть 2 статьи 19 закона №152-ФЗ «О персональных данных»:

«2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

– состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом Федеральной службы по техническому и экспортному контролю России (ФСТЭК России) от 18 февраля 2013г. № 21):

«4. Меры по обеспечению безопасности персональных данных реализуются, в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных».

– требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены ФСТЭК России от 11 февраля 2013г. № 17):

«Формирование требований к защите информации… в том числе включает: …определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в

информационной системе, и разработку на их основе модели угроз безопасности информации».

– требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31):

«Формирование требований к защите информации в автоматизированной системе управления… в том числе включает: … определение угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления, и разработку на их основе модели угроз безопасности информации».

– требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены приказом ФСТЭК России от 25 декабря 2017г. № 239):

«11. Разработка организационных и технических мер по обеспечению безопасности значимого объекта осуществляется субъектом критической информационной инфраструктуры… и должна включать:

а) анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии)».

Итак, отсюда следует вывод: для любых информационных систем, так или иначе подлежащих защите в соответствии с законодательством необходимо разработать модель угроз.

Необходимость создания данного документа для информационной системы ГБПОУ Южно-Уральского государственного технического колледжа очевидна. Наполнение модели угроз описывается в приказе ФСТЭК России от 11 февраля 2013г. № 17:

«Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации».

Таким образом, модель угроз информационной безопасности автоматизированной системы должна содержать:

—описание информационной системы,

—структурно-функциональные характеристики,

—описание угроз безопасности,

—модель нарушителя,

—возможные уязвимости,

—способы реализации угроз,

—последствия от нарушения свойств безопасности информации.

На основании Базовой модели угроз персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России от 15 февраля 2008 г., был разработан перечень угроз персональных данных для ГБПОУ Южно-Уральского государственного технического колледжа, она представлена в таблице 3. В модели угроз отражены все возможные угрозы информационной системе образовательной организации, дана вероятностная оценка реализации угрозы и представлены возможные меры по исключению риска наступления данного события.

Таблица 1 – Угрозы безопасности персональных данных при их обработке в информационной системе ГБПОУ «Южно-Уральского государственного технического колледжа»

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1 Угрозы от утечки по техническим каналам						
1.1 Угрозы утечки акустической информации	Маловероятна	Низкая	Низкая	Неактуальная		Инструктаж пользователей в части проведения переговоров по рабочим вопросам исключительно на территории организации и с людьми, допущенными к обсуждаемой информации
1.2 Угрозы утечки видовой информации	Маловероятна	Низкая	Низкая	Неактуальная	Жалюзи на окнах; Расположение мониторов, исключающее возможность просмотра информации третьими лицами	Инструктаж пользователей в части необходимости блокировки рабочих компьютеров в случае возможности просмотра информации людьми, не допущенными к данным сведениям
1.3 Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН)	Маловероятна	Низкая	Низкая	Неактуальная		

Продолжение таблицы 1

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2 Угрозы несанкционированного доступа к информации						
2.1 Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных (ИСПДн) носителей информации путем физического доступа к элементам ИСПДн						
2.1.1 Кража персональных электронных вычислительных машин (ПЭВМ)	Маловероятна	Низкая	Низкая	Неактуальна		Контролируемая зона для организации технической защиты конфиденциальной информации; Специализированная охрана образовательной организации
2.1.2 Кража носителей информации	Маловероятна	Низкая	Низкая	Неактуальна	Хранение носителей, исключающее несанкционированный доступ	Учет носителей; Инструктаж пользователей в части запрета выноса носителей информации с территории организации и хранения носителей в защищенных местах, исключающих возможность несанкционированного доступа

Продолжение таблицы 1

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.1.3 Кража, модификация, уничтожение информации	Маловероятна	Низкая	Низкая	Неактуальна		Контролируемая зона для организации технической защиты конфиденциальной информации с ограничением доступа посторонних лиц; Ответственность за сохранность конфиденциальной информации и ее носителей в должностных инструкциях сотрудников
2.1.4 Вывод из строя узлов ПЭВМ, каналов связи	Низкая вероятность	Средняя	Низкая	Неактуальна		Контролируемая зона для организации технической защиты конфиденциальной информации с ограничением доступа посторонних лиц; Ответственность за сохранность конфиденциальной информации и ее носителей в должностных инструкциях

Продолжение таблицы 1

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.1.5 Несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ	Маловероятна	Низкая	Низкая	Неактуальна		Ремонт допущенными сотрудниками учреждения; Технологический процесс обработки информации содержит информацию о действиях в случае выхода из строя ПЭВМ
2.1.6 Несанкционированное отключение средств защиты	Низкая вероятность	Средняя	Низкая	Неактуальна	Настройка средств защиты	Инструктаж пользователей в части запрета каких-либо действий в отношении средств защиты; Технологический процесс обработки содержит информацию о действиях в случае выхода из строя или некорректной работе средств защиты информации

Продолжение таблицы 1

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных средств						
2.2.1 Действия вредоносных программ (вирусов)	Низкая вероятность	Средняя	Низкая	Неактуальна	Антивирусное программное обеспечение (ПО)	Инструктаж пользователей в части действий в случае возникновения внештатных ситуаций; Технологический процесс обработки информации регламентирует действия в случае возникновения внештатных ситуаций
2.2.2 Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятна	Низкая	Низкая	Неактуальна	Настройка средств защиты	Приобретение лицензионного ПО у официальных поставщиков

Продолжение таблицы 1

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.2.3 Установка ПО не связанного с исполнением служебных обязанностей	Низкая вероятность	Средняя	Низкая	Неактуальна	Настройка средств защиты	Инструктаж пользователей в запрете использования на рабочих ПЭВМ ПО, не задействованного для выполнения работ; Технологический процесс обработки информации регламентирует действия администраторов безопасности в случае обнаружения ПО
2.3 Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн из-за сбоев в ПО, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера						
2.3.1 Утрата атрибутов доступа	Маловероятна	Низкая	Низкая	Неактуальна		Инструктаж пользователей в части организации хранения в строго определенных местах парольных карточек; Журнал учета паролей

Продолжение таблицы 1

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.3.2 Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкая вероятность	Средняя	Низкая	Актуальна	Настройка средств защиты; Резервное копирование информации	Инструктаж пользователей в части строгого исполнения порядка работ, предусмотренного для исполнения служебных обязанностей
2.3.3 Непреднамеренное отключение средств защиты	Маловероятна	Низкая	Низкая	Неактуальна	Доступ к установлению режимов работы средств защиты предоставляется только администратору; Настройка средств защиты	Инструктаж пользователей в части запрета каких-либо действий в отношении средств защиты
2.3.4 Выход из строя программно-аппаратных средств	Низкая вероятность	Средняя	Низкая	Неактуальна	Резервное копирование информации	
2.3.5 Сбой системы электроснабжения	Маловероятна	Низкая	Низкая	Неактуальна	Использование источников бесперебойного питания для серверов	
2.3.6 Стихийное бедствие	Маловероятна	Низкая	Низкая	Неактуальна	Пожарная сигнализация	Инструкция по действиям в случае возникновения нештатной ситуации

Продолжение таблицы 1

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.4 Угрозы преднамеренных действий внутренних нарушителей						
2.4.1 Доступ к информации, модификация, уничтожение лицами, недопущенными к её обработке	Маловероятна	Низкая	Низкая	Неактуальна		Инструктаж пользователей в части необходимости блокировки рабочих компьютеров в случае возможности просмотра информации людьми, не допущенными к данным сведениям; Парольная система доступа; Разграничение прав пользователей
2.4.2 Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке	Маловероятна	Низкая	Низкая	Неактуальна		Обязательства о неразглашении; Инструктаж пользователей в части проведения переговоров по рабочим вопросам исключительно на территории организации и с людьми, допущенными к обсуждаемой информации

Продолжение таблицы 1

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
2.5 Угрозы несанкционированного доступа по каналам связи						
2.5.1 Угрозы выявления паролей по сети	Маловероятна	Низкая	Низкая	Неактуальна	Антивирусное ПО	
2.5.2 Угрозы навязывания ложного маршрута сети	Маловероятна	Низкая	Низкая	Неактуальна	Использование межсетевого экрана	
2.5.3 Угрозы внедрения ложного объекта в ИСПДн	Маловероятна	Низкая	Низкая	Неактуальна	Использование межсетевого экрана	
2.5.4 Угрозы удаленного запуска приложений	Маловероятна	Низкая	Низкая	Неактуальна	Использование межсетевого экрана	
2.5.5 Угрозы внедрения по сети вредоносных программ	Низкая вероятность	Средняя	Низкая	Неактуальна	Антивирусное ПО; Использование межсетевого экрана	Инструктаж пользователей в части порядка действии в случае возникновения внештатных ситуаций

Таким образом, нами проведен первичный аудит состояния защищенности информационной системы образовательной организации ГПБОУ СПО «ЮУрГТК» на основании нормативных документов [1], рекомендованных ФСТЭК: были определены основные угрозы информационной безопасности, сделан предварительный анализ возможности реализации угроз, проанализированы существующие в ГПБОУ СПО «ЮУрГТК» меры технического и организационного противодействия угрозам и на этом основании определены направления для построения вероятностной модели причинения вреда информационной системе образовательной организации при несанкционированных доступах.

1.3 Модель причинения вреда информационной системе образовательной организации (на базе ГПБОУ СПО «ЮУрГТК»)

В научной литературе нет точного понятия «модель причинения вреда информационной системе», однако, исследователи применяют моделирования для процессов оптимизации информационных потоков, защиты информации, построения периметров безопасности и т.д.

Так в работе Варламова О.О. представлен подход к решению создания модели компьютерных угроз информационной безопасности. Была выделена системная *«модель компьютерной угрозы, на основе выделения следующих 9 типов угроз: семантических, алгоритмических, вирусных, разграничительных, сетевых, потоковых, аппаратных, форматных и пользовательских технических компьютерных угроз»* [14, с. 217].

В работе Берзинь М.М. приводятся методы классификации моделей угроз, которые используются для оценки рисков при успешном проведении атаки на информационную систему [15].

В работе Табакова Ф.Б. предложена и описана математическая модель оптимизации системы информационной безопасности организации, основанная на теории графов и теории вероятности [16].

Необходимо отметить исследование [33], проведенное на основании социологического опроса должностных лиц общеобразовательных школ, в котором предложено совершенствовать и развивать законодательную основу риск-ориентированной модели организации контрольно-надзорной деятельности в сфере образования, причем, как федерального, так и регионального уровня. Значимым для нашего исследования является применение метода экспертных оценок самих субъектов образовательной деятельности.

В работе Прокофьевой Е.Н. была предложена модель управления комплексной безопасностью образовательной организации. Приведенная автором модель, позволяет произвести идентификацию процессов комплексной безопасности образовательной организации любого уровня. Также представлен алгоритм деятельности образовательной организации по обеспечению безопасности: определение перечня основных процессов обеспечения безопасности; проведение комплексного анализа; осуществление прогнозной деятельности; разработка научно-педагогических, производственных, организационных и хозяйственных способов достижения поставленной цели; оценка необходимого и располагаемого ресурсного обеспечения процессов обеспечения комплексной безопасности; осуществление мониторинга процессов управления и обеспечения комплексной безопасности [32].

Следуя за Прокофьевой Е.Н. полагаю возможным сформулировать определение «модели причинения вреда информационной системе» в виде:

Это схематическое представление всех компонентов информационной системы, характеризующее существенные свойства и состояние защиты информационной безопасности: защищаемые информационные активы, дескрипторы угроз и необходимые меры защиты информации.

В понятие информационной безопасности образовательной организации входит 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. Вторым аспектом понятия станет защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

В составе массивов охраняемой законом информации, находящейся в распоряжении образовательного учреждения, можно выделить три группы:

1) персональные сведения, касающиеся учащихся и преподавателей, оцифрованные архивы;

2) ноу-хау образовательного процесса, носящие характер интеллектуальной собственности и защищенные законом;

3) структурированная учебная информация, обеспечивающая образовательный процесс (библиотеки, базы данных, обучающие программы).

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

Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и неприкосновенности и обеспечение их:

1) доступности в любое время для любого авторизированного пользователя;

2) защиты от любой утраты или внесения несанкционированных изменений;

3) конфиденциальности, недоступности для третьих лиц.

Угрозы информационной безопасности

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность

подростков, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус. Выделяются четыре группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

1) компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;

2) программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;

3) данные, хранимые как на жестких дисках, так и на отдельных носителях;

4) сам персонал, отвечающий за работоспособность IT-систем;

5) дети, подверженные внешнему агрессивному информационному влиянию и способные создать в школе криминальную ситуацию. В последнее время перечень таких ситуаций существенно расширился, что говорит о возможной целенаправленной психологической атаке на сознание детей и подростков.

Угрозы, направленные на повреждение любого из компонентов системы, могут носить как случайный, так и осознанный преднамеренный характер. Среди угроз, не зависящих от намерения персонала, учащихся или третьих лиц, можно назвать:

—любые аварийные ситуации, например, отключение электроэнергии или затопление,

—ошибки персонала,

—сбои в работе программного обеспечения,

—выход техники из строя,

—проблемы в работе систем связи.

Все эти угрозы информационной безопасности носят временный характер, предсказуемы и легко устраняются действиями сотрудников и специальных служб.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев не могут быть предвидены. Их виновниками могут оказаться учащиеся, служащие, конкуренты, третьи лица с намерением на совершение кибер-преступления. Для подрыва информационной безопасности такое лицо должно иметь высокую квалификацию в отношении принципов работы компьютерных систем и программ. Наибольшей опасности подвергаются компьютерные сети, компоненты которых расположены отдельно друг от друга в пространстве. Нарушение связи между компонентами системы может привести к полному подрыву ее работоспособности. Важной проблемой может стать нарушение авторских прав, намеренное хищение чужих разработок. Компьютерные сети редко подвергаются внешним атакам с целью воздействия на сознание детей, но и это не исключено. И самой серьезной опасностью станет использование школьного оборудования для вовлечения ребенка в криминал и терроризм.

С точки зрения проникновения в периметр информационной безопасности и для совершения хищения информации или создания нарушения в работе систем необходим несанкционированный доступ.

Способы несанкционированного доступа

Можно выделить несколько видов несанкционированного доступа:

1) Человеческий. Информация может быть похищена путем копирования на временные носители, переправлена по электронной почте. Кроме того, при наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

2) Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и

перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.

3) Аппаратный. Он связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

Меры защиты

Борьба с различными видами атак на информационную безопасность должна вестись на пяти уровнях, причем работа должна носить комплексный характер. Существует ряд методических разработок, которые позволят построить защиту образовательного учреждения на необходимом уровне.

Нормативно-правовой способ защиты информационной безопасности

Необходимы действия по ограничению агрессивного воздействия на сознание студентов, которые должны стать основными. На втором месте должно оказаться обеспечение безопасности баз данных.

Защита информации опирается на действующие в этой сфере законы, определяющие отдельные ее массивы как подлежащие защите. Они выделяют те сведения, которые должны быть недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные, коммерческая, служебная или профессиональная тайна). Порядок защиты персональных данных определяется в том числе федеральным законом «Об информации», Трудовым кодексом. Они и Гражданский кодекс помогают разработать методику для обеспечения защиты сведений, относящихся к коммерческой тайне. Кроме законов необходимо выделить действующие в этой сфере ГОСТы, определяющие порядок защиты данных, и применяемые в этих целях методики и аппаратные средства.

Морально-этические средства обеспечения информационной безопасности

В образовательной сфере большую роль играет система морально-этических ценностей. На ней должна основываться система мер, защищающих подростка от травмирующей, этически некорректной, незаконной информации. В целях защиты от пропаганды необходимо применять нормы закона «О защите прав ребенка», определяющие его права на защиту от сведений, которые могут причинить моральную травму. Необходимо создавать перечни документов, программ и иных источников, которые могут травмировать психику, в целях недопущения их проникновения на территорию учебного заведения. Это станет одной из основ информационной безопасности.

Административно-организационные меры

Этот комплекс мер целиком построен на создании внутренних правил и регламентов, определяющих порядок работы с информацией и ее носителями. Это внутренние методики, посвященные информационной безопасности, должностные инструкции, перечни сведений, не подлежащих передаче. Дополнительно должен быть разработан регламент, определяющий порядок взаимодействия с компетентными органами по запросам о предоставлении им тех или иных данных и документов.

Кроме того, эти методики должны определять порядок доступа детей к сети Интернет в компьютерных классах, возможность защиты некоторых ресурсов неоднозначного характера от доступа ребенка, запрет на пользование собственными носителями информации. Должно быть предусмотрено использование системы родительского контроля над ресурсами сети Интернет.

Физические меры

За данную систему мер и ее внедрение должно отвечать руководство образовательного учреждения и сотрудники IT-подразделений. Перекладывать организацию мер физической защиты компьютерной сети и носителей на сотрудников наемных охранных подразделений недопустимо. Среди физических мер должна быть предусмотрена пропускная система

защиты в помещения, содержащие носители информации, организация контроля доступа посетителей, установления различных степеней допуска. Кроме того, к мерам физической защиты может быть отнесено обязательное копирование значимой информации на диски компьютеров, не имеющих доступа к сети Интернет. Обязательно не только установление паролей, но и их регулярная замена.

Технические меры

Комплексную систему защиты всего периметра компьютерной сети должны обеспечивать специализированные программные продукты, например, DLP-системы и SIEM-системы, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними. Для тех учебных заведений, бюджет которых не позволяет внедрение профессиональных систем, необходимо использование разрешенных и рекомендуемых программных мер защиты, в частности антивирусов.

Электронная почта, к которой имеют доступ сотрудники и учащиеся, должна быть контролируема. Оптимально также ввести полный запрет на копирование любой информации с жестких дисков компьютеров образовательного учреждения.

Кроме того, должно быть предусмотрено программное обеспечение, ограничивающее доступ ребенка на определенные сайты (контент-фильтры).

Все меры должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности. Желательно привлечение к этой проблеме родителей учеников, в ряде случаев они помогут провести аудит мер безопасности и порекомендовать современные решения. Кроме того, на родителей должны быть возложены обязанности и по ограничению информации, которую ребенок может получить дома. Необходимо просматривать страницы, посещаемые ребенком. На основании анализа его

поиска можно вносить изменения в перечень сайтов, доступ к которым ограничен с компьютеров, установленных в учебном заведении.

Модель (фр. modèle, от лат. modulus — «мера, аналог, образец») — это система, исследование которой служит средством для получения информации о другой системе; представление некоторого реального процесса, устройства или концепции [10].

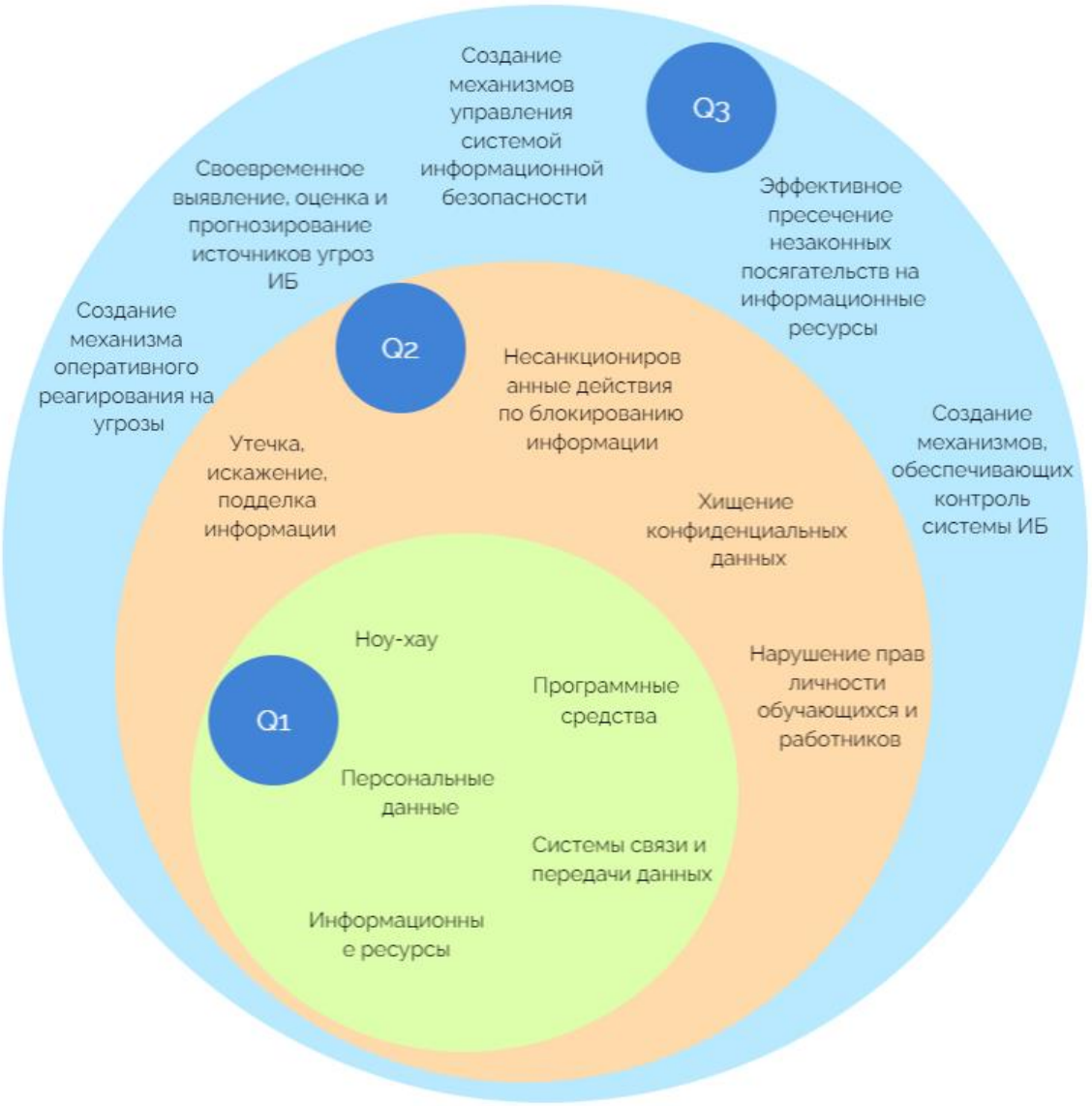

Рисунок 1 – Модель причинения вреда информационной системе образовательной организации

На рисунке 1 представлена модель причинения вреда информационной системе образовательной организации,

где Q1 — информационные активы, к которым относятся персональные данные, системы связи и передачи данных, информационные ресурсы, программные средства и ноу-хау;

Q2 — реальные угрозы, которые направлены на потенциальную возможность тем или иным способом нарушить информационную безопасность;

Q3 — действия, направленные на защиту информационных активов, а также на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Для выявления наиболее вероятных угроз и причинения максимального вреда информационной системе была составлена таблица 2, которая является адаптацией к теме исследования по алгоритму, предложенному в ГОСТ Р ИСО/МЭК ТО 13335-3-2007 [2].

Таблица 2 – Ранжирование угроз по мерам риска

Дескриптор угроз	Оценка воздействия	Вероятность возникновения угрозы	Мера риска	Ранг угрозы	Вероятность причинения вреда информационной системе
Искажение и подделка информации	5	4	20	1	Высокая
Угрозы утечки акустической информации	1	1	1	7	Низкая
Нарушения прав личности обучающихся, работников	4	2	8	3	Средняя
Хищение конфиденциальных данных	5	3	15	2	Высокая
Несанкционированные действия по блокированию информации	3	1	3	5	Средняя
Угрозы утечки видовой информации	1	1	1	7	Низкая

Продолжение таблицы 2

Дескриптор угроз	Оценка воздействия	Вероятность возникновения угрозы	Мера риска	Ранг угрозы	Вероятность причинения вреда информационной системе
Кража персональных электронных вычислительных машин (ПЭВМ)	1	2	2	6	Низкая
Кража носителей информации	2	1	2	6	Низкая
Вывод из строя узлов ПЭВМ, каналов связи	1	2	2	6	Низкая
Несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ	1	1	1	7	Низкая
Несанкционированное отключение средств защиты	2	2	4	4	Средняя
Действия вредоносных программ (вирусов)	1	2	2	6	Низкая
Недекларированные возможности системного ПО и ПО для обработки персональных данных	1	1	1	7	Низкая
Установка ПО не связанного с исполнением служебных обязанностей	1	2	2	6	Низкая
Утрата атрибутов доступа	1	1	1	7	Низкая
Непреднамеренная модификация (уничтожение) информации сотрудниками	1	2	2	6	Низкая
Непреднамеренное отключение средств защиты	1	1	1	7	Низкая
Выход из строя программно-аппаратных средств	1	2	2	6	Низкая

Продолжение таблицы 2

Дескриптор угроз	Оценка воздействия	Вероятность возникновения угрозы	Мера риска	Ранг угрозы	Вероятность причинения вреда информационной системе
Стихийное бедствие	1	1	1	7	Низкая
Доступ к информации, модификация, уничтожение лицами, недопущенными к её обработке	1	2	2	6	Низкая
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке	1	1	1	7	Низкая
Угрозы выявления паролей по сети	1	1	1	7	Низкая
Угрозы навязывания ложного маршрута сети	1	1	1	7	Низкая
Угрозы внедрения ложного объекта в ИСПДн	1	1	1	7	Низкая
Угрозы удаленного запуска приложений	1	1	1	7	Низкая
Угрозы внедрения по сети вредоносных программ	1	2	2	6	Низкая

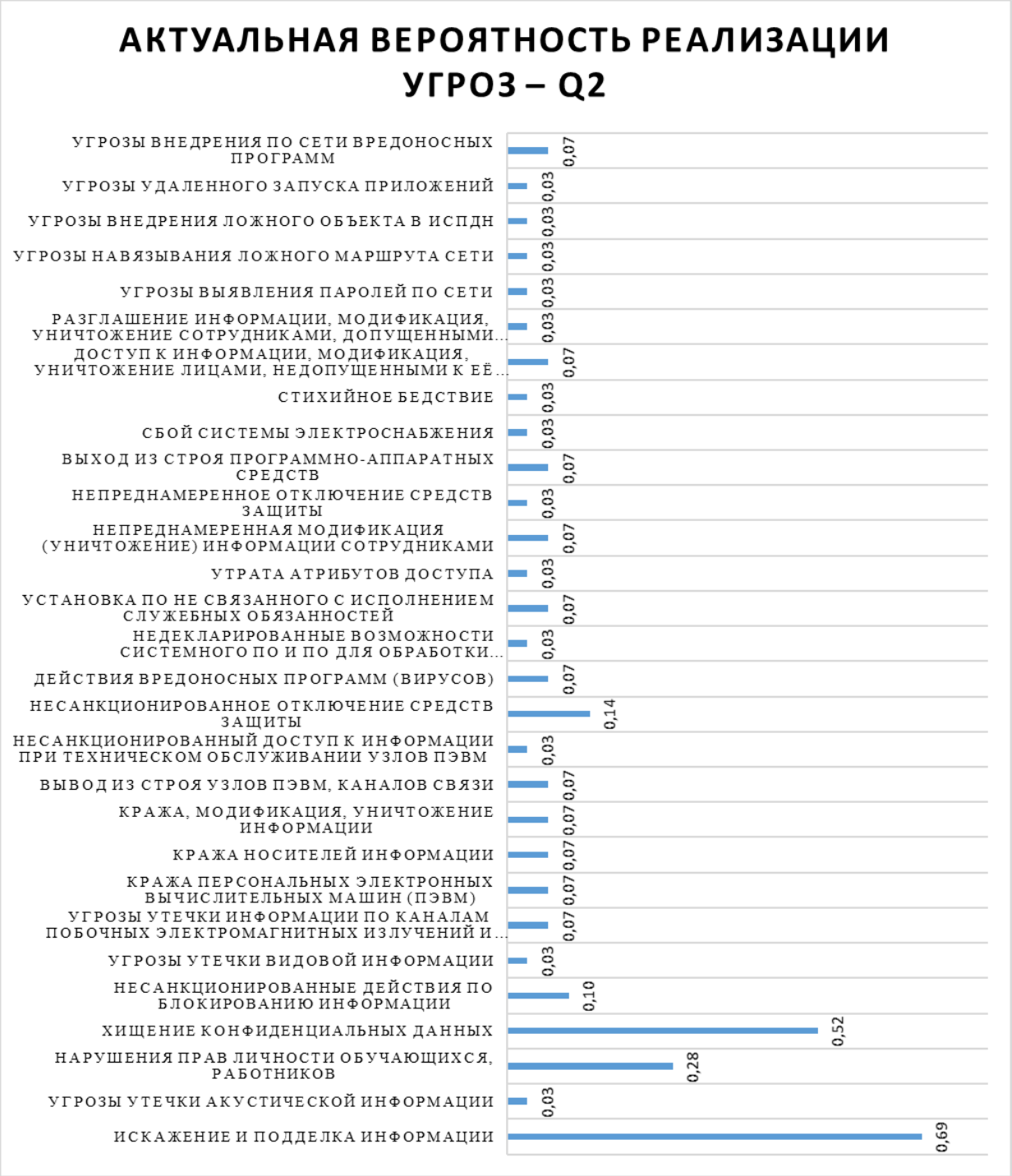

Рисунок 2 – Актуальная вероятность реализации угроз – Q2

На рисунке 2 наглядно указана вероятность возникновения угроз. Совместно с рисунком 1 образует вероятностную модель причинения вреда информационной системе образовательной организации при несанкционированных доступах – рис. 3.

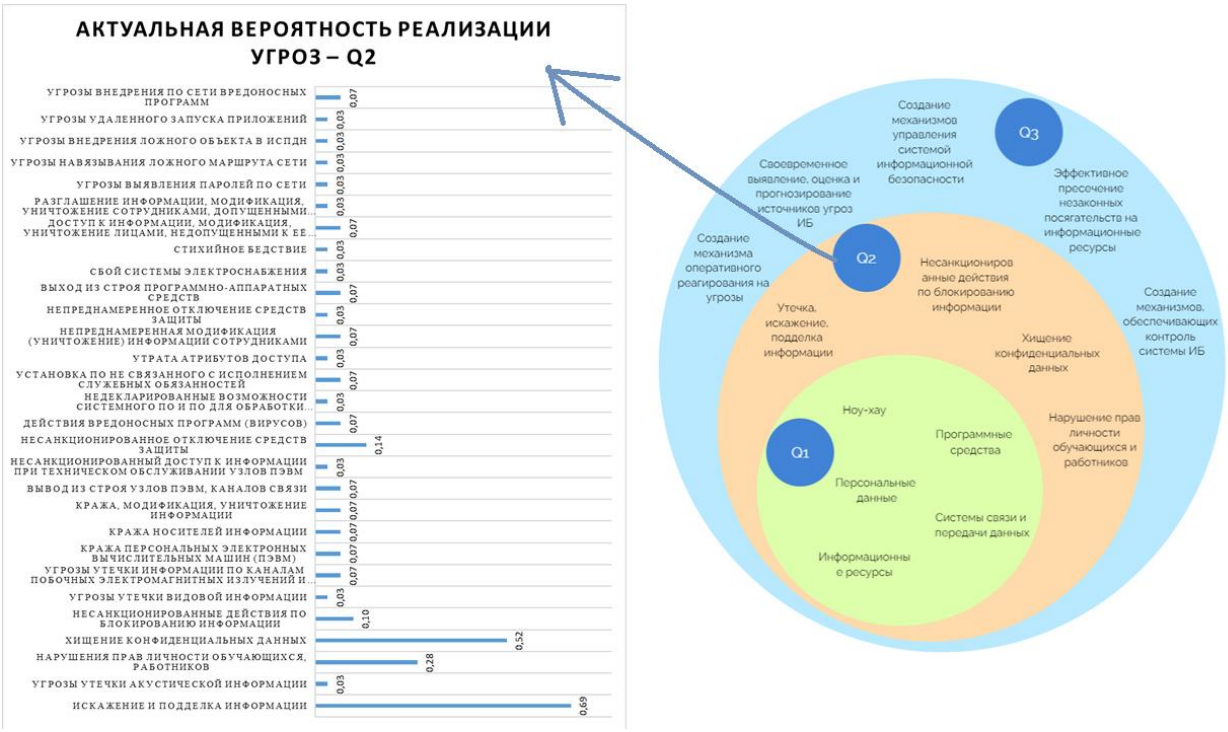

Рисунок 3 – Вероятностная модель причинения вреда информационной системе образовательной организации

Таким образом можно сделать вывод, что угроза утечки и искажения информации и хищение конфиденциальных данных наиболее вероятны, чем, например, несанкционированные действия по блокированию информации, в связи с чем, несанкционированный доступ в систему будет определяющим для общей безопасности системы в целом.

Выводы по главе I

В главе I были рассмотрены теоретические аспекты разработки модели причинения вреда информационной системе образовательной организации.

Компьютеризированные информационные системы, особенно с появлением Интернета и мобильных компьютеров, оказали глубокое влияние на организации, экономику и общество, а также на людей, чья жизнь и деятельность осуществляются в этих социальных агрегатах. Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают

огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить конфиденциальные данные.

В первом параграфе главы рассмотрены аспекты безопасности информационной системы образовательной организации.

Во втором параграфе главы был проведен анализ актуального состояния информационной безопасности системы образовательной организации как основание для построения модели причинения вреда.

В Южно-Уральском государственном техническом колледже создана и успешно функционирует сертифицированная система менеджмента качества, реализуются инновационные программы, совершенствуются учебные планы, открываются новые специальности – все это позволяет выпускникам быть востребованными на рынке труда, адаптироваться в непростых современных условиях жизни.

Для проведения анализа уязвимостей существующей системы информационной безопасности ГБПОУ Южно-Уральского государственного технического колледжа наиболее оптимальным методом является разработка модели угроз.

В третьем параграфе первой главы была представлена в общем виде модель причинения вреда информационной системе образовательной организации ГПБОУ СПО «ЮУрГТК».

Также были проанализированы меры защиты информационных систем, такие как: нормативно-правовой способ, морально-этические средства, административно-организационные меры, физические меры, технические меры.

Отмечаемая в течение последних десятилетий в России тенденция к росту числа компьютерных преступлений говорят о необходимости повышения уровня информационной безопасности, поиска наиболее рациональных методов защиты информации и разработка модели

причинения вреда может стать эффективным методом для защиты информационной системы образовательной организации.

ГЛАВА 2. ОПЫТНО-ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО АПРОБАЦИИ МОДЕЛИ ПРИЧИНЕНИЯ ВРЕДА ИНФОРМАЦИОННОЙ СИСТЕМЕ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Цель, задачи и организация опытно-экспериментальной работы по апробации модели причинения вреда информационной системы образовательной организации

В наше время информация имеет огромную роль в современной жизни. Получение третьими лицами конфиденциальной информации или личного сообщения может принести непоправимый ущерб не только обладателю информации, но и окружающим людям. С каждым годом роль информации возрастает, поэтому она имеет огромную ценность. Вследствие чего главной задачей является ее защита.

Во время оценки проблемы информационной безопасности отмечаются такие проблемы: неисправности, ошибки ПО, стихийные бедствия, а также преднамеренные или непреднамеренные действия человека. Данные проблемы предположительно могут привести к изменению или уничтожению информации. Также главной проблемой является несанкционированный доступ [6].

Несанкционированный доступ (НСД) — это доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС). Под штатными средствами здесь понимается совокупность технического, программного и микропрограммного обеспечения СВТ или АС [5].

Одним из принципов защиты от НСД является контроль эффективности средств защиты информации (СЗИ) — проверка соответствия эффективности мероприятий по защите информации

установленным требованиям или нормам по безопасности информации. Такое управление может быть периодическим или инициироваться по мере необходимости пользователем.

Контроль функционирования системы защиты информации от НСД проводится с использованием программных или программно-технических средств, соответствующий требованиям по безопасности с учетом классификации АС и степени секретности обрабатываемой информации. Если нужно защитить конфиденциальную информацию, то контролю подвергнуты три из четырех подсистем системы защиты информации от НСД согласно требований, изложенных в «Руководящем документе. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [4]:

—подсистема управления доступом,

—подсистема регистрации и учета,

—подсистема обеспечения целостности.

Методика защиты конфиденциальной информации в АС от НСД состоит из трех основных этапов [23]:

1) Планирование.

2) Тестирование.

3) Анализ результатов.

На этапе планирования анализируются все исходные данные и документация по АС, а также анализ защищаемых информационных ресурсов, структуры АС, цели и задачи системы защиты конфиденциальной информации в АС от НСД. Перед началом тестирования следует определить, что в документации на объект испытаний декларируется соответствие АС требованиям руководящих документов.

Заказчику необходимо предоставить комиссии, производящей контроль защищенности, описание технологического процесса обработки информации в АС, которое имеет следующую информацию [3]:

—перечень объектов доступа,

—перечень субъектов доступа,

—перечень штатных средств доступа к информации,

—перечень используемых средств защиты информации,

—описание реализованных правил разграничения доступа (матрицу доступа),

—схему или описание информационных потоков.

Этап тестирования включает в себя комплекс организационно-технических мероприятий по оценке показателей защищенности конфиденциальной информации в АС от НСД. Производится проверка каждой из подсистем системы защиты:

1) Проверка подсистемы управления доступом.

В данной подсистеме контролируются организационные мероприятия, устанавливающие требования к парольной политике, проводится анализ установленных параметров функционирования средств идентификации и аутентификации, осуществляется контроль корректности функционирования механизмов идентификации и аутентификации, а также контролируется процедура смены паролей пользователями. Порядок проверки выполнения каждого требования представлен в виде таблицы (таблица 3).

Таблица 3 – Порядок проверки подсистемы управления доступом

Проверяемое требование	Порядок действий при проверке
Проверка механизма идентификации и аутентификации субъектов доступа при входе в систему	1. На исследуемом АРМ выполнить запросы на идентификацию и проведение аутентификации с использованием различных сочетаний учетных данных: зарегистрированный (незарегистрированный) идентификатор, верный (неверный) пароль. 2. Проверить реакцию системы защиты на вход в ОС с неправильно введенным идентификатором (логином). 3. Проверить реакцию системы защиты на вход в ОС с неправильно введенным паролем. 4. Проверить реакцию системы защиты на вход в ОС с правильно введенным логином и паролем.

Продолжение таблицы 3

Проверяемое требование	Порядок действий при проверке
Проверка соблюдения требований к паролю (длина пароля должна быть не менее 6 символов, пароль должен включать буквы и цифры)	1. Проверить наличие эксплуатационной документации на АС, в которой регламентирован порядок проведения парольной защиты АС. Проверить наличие следующих положений: – требования к паролям (длина, сложность); – обязанности администратора безопасности по реализации парольной политики АС (генерация паролей, распределение паролей); – обязанности пользователей по реализации парольной политики АС (генерация паролей, смена паролей). 2. Определить значения, установленные средствами СЗИ от НСД, для следующих параметров: минимальная длина пароля, сложность пароля (алфавит паролей), максимальный срок действия пароля, максимальное число неудачных попыток входа пользователей в ОС, после которого осуществляется блокировка работы пользователя, реакция СЗИ на превышение максимального числа неудачных попыток входа пользователя. 3. Под учетными записями пользователей произвести попытки установить пароль, не соответствующий нормативным требованиям. Для этого осуществить: – попытку установить пароль, длина которого менее 6 символов; – попытки установить пароль, состоящий исключительно из цифр, либо только из букв.
Проверка механизма идентификации внешних устройств по именам	1. Проверить возможность загрузки ОС с внешних носителей (с flash-накопителя или CD-диска) в обход системы защиты информации в АС. Попытки загрузки с внешних устройств должны быть проигнорированы системой защиты информации.
Проверка механизма идентификации программ, каталогов, файлов, записей, полей записей по именам при обращении к ним средствами ОС и средствами установленных на СЗИ от НСД	1. Провести идентификацию программ путем их запуска (через «Проводник») и проверить их соответствие заданным параметрам. 2. Провести идентификацию каталогов (папок), в которых расположены защищаемые файлы путем обращения к ним с помощью штатных средств ОС (программа «Проводник»). 3. Проверка механизма идентификации записей и полей записей проводится только в том случае, если в АС присутствуют системы управления базами данных (СУБД).

Продолжение таблицы 3

Проверяемое требование	Порядок действий при проверке
Проверка правильности предоставления доступа конкретным субъектам к защищаемым объектам (каталогам, файлам) в соответствии с установленными правами (матрицей доступа)	1. Проверить наличие матрицы доступа в числе документации на АС. 2. Дальнейшая проверка производится при помощи специализированных программных средств, таких как «Ревизор 1 XP» и «Ревизор 2 XP» (или их аналогов).

2) Проверка подсистемы регистрации и учета.

Во время исследования подсистемы регулируется регистрация и учет событий средствами установленного СЗИ от НСД на всех этапах технологического процесса обработки и хранения информации (вход и выход субъектов в ОС, запуск и завершение программ, попытки доступа программ к защищаемым файлам, каталогам, узлам сети, терминалам, линиям связи), выдача защищаемых материалов на печать, порядок регистрации и учета носителей защищаемой информации, а также качество очистки освобождаемых областей памяти внешних накопителей и оперативной памяти.

Порядок проверки подсистемы регистрации и учета представлен в таблице 4.

Таблица 4 – Порядок проверки подсистемы регистрации и учета

Проверяемое требование	Порядок действий при проверке
Проверка регистрации входа (выхода) пользователя в (из) ОС, входа (выхода) компьютера из спящего режима	1. Произвести выход из системы, вход в систему от имени пользователя или администратора. 2. Произвести попытку предоставления неправильного идентификатора (или ввода неправильного имени пользователя), пароля. 3. Вести компьютер, на котором осуществляется проверка, в спящий режим и вывести из него. 4. Зайти в журнал «Безопасность» ОС Windows или в соответствующий журнал используемого СЗИ от НСД. 5. Проверить наличие записей о каждом из событий п. 1–3.

Продолжение таблицы 4

Проверяемое требование	Порядок действий при проверке
Проверка регистрации запуска и завершения программ	1. Запустить и завершить программы, используемые для обработки защищаемой информации. 2. Зайти в журнал «Безопасность» ОС Windows или в соответствующий журнал используемого СЗИ от НСД. 3. Проверить наличие записей о каждом из событий п. 1.
Проверка регистрации попыток доступа к защищаемым файлам и каталогам	1. Открыть и закрыть файлы и папки, содержащие защищаемую информацию (согласно матрице доступа). 2. Попробовать создать (удалить) файлы и папки (согласно матрице доступа). 3. Зайти в журнал «Безопасность» ОС Windows или в соответствующий журнал используемого СЗИ от НСД. 4. Проверить наличие записей о каждом из событий п. 1,2.
Проверка регистрации выдачи защищаемых материалов на печать	1. Проверить, что пользователю, осуществляющему печать, разрешен доступ к порту, к которому подключен принтер. 2. Проверить, что факт вывода документа на печать, дата и время выдачи, имя файла, уровень конфиденциальности, количество экземпляров документа, количество листов в экземпляре, имя файла, с которого выполнена печать документа, идентификатор пользователя, запросившего документ, регистрируется установленным СЗИ от НСД или сотрудником, ответственным за вывод документов из АС. 3. Проверить, что бракованные листы уничтожаются в установленном в организации порядке.
Проверка регистрации и учета носителей защищаемой информации	1. Проверить, что учет носителей защищаемой информации проводится в журнале с регистрацией их выдачи (приема). 2. Проверить, что носители защищаемой информации уничтожаются в установленном в организации порядке с записью об этом в журнале учета.

Продолжение таблицы 4

Проверяемое требование	Порядок действий при проверке
Проверка качества очистки освобождаемых областей памяти внешних накопителей и оперативной памяти	1. Проверка очистки (обнуления, обезличивания) освобождаемых областей внешних накопителей и оперативной памяти производится при помощи специализированных программных средств контроля защищённости, таких как «Terrier 3.0» и его аналоги.

3. Проверка подсистемы обеспечения целостности.

При проверке подсистемы происходит проверка обеспечения целостности СЗИ от НСД и неизменности программной среды компьютера, анализ проведения периодического тестирования системы защиты информации от НСД, проверка наличия средств восстановления программной среды компьютера и СЗИ от НСД, а также контроль наличия САВЗ в исследуемой АС.

Порядок проверки подсистемы обеспечения целостности представлен в таблице 3.

Средствами восстановления СЗИ от НСД в АС являются дистрибутивы (инсталляционные файлы) с системным и прикладным ПО. Копии дистрибутивов хранятся отдельно для обеспечения возможной полной замены (переустановки) ПО в случае каких-либо отказов или нарушений в работе технических средств АС. Автоматическое оперативное восстановление функций СЗИ НСД при сбоях проверяется путем моделирования сбойных ситуаций и последующей проверке (тестирования) функций СЗИ НСД.

Помимо проверки наличия средств антивирусной защиты проводится выборочная проверка используемых в системе программных средств на наличие компьютерных вирусов [24].

Таблица 5 – Порядок проверки подсистемы обеспечения целостности

Проверяемое требование	Порядок действий при проверке
Проверка обеспечения целостности программных СЗИ от НСД	1. Проверка обеспечения целостности программных СЗИ от НСД и неизменности программной среды производится при помощи специализированных средств контроля защищенности, таких как «ФИКС 2.0.1», «ФИКС 2.0.2» или их аналогов.
Проверка неизменности программной среды компьютера	
Проверка проведения периодического тестирования системы защиты информации от НСД	1. Проверить наличие организационно-распорядительной документации, определяющей периодичность и порядок тестирования всех функций СЗИ от НСД. 2. Проверить возможность периодического тестирования СЗИ путем анализа применяемых разработчиком средств контроля целостности компонентов системного ПО, реализующих функции СЗИ от НСД и наборов данных, используемых этими средствами.
Порядок проверки наличия средств восстановления	1. Проверить, что средства восстановления программной среды компьютера имеются в наличии 2. Проверить, что средства восстановления СЗИ от НСД имеются в наличии (например, дистрибутивы ПО СЗИ от НСД, которые хранятся отдельно, для того, чтобы обеспечить переустановку в случае каких-либо сбоев в работе программных или технических средств АС).
Проверка наличия средств антивирусной защиты	Проверить, что средства антивирусной защиты имеются в наличии.

На заключительном этапе анализа результатов производится сравнение фактических значений показателей защищенности, и норм (требований), определенных в нормативно-методических документах по защите конфиденциальной информации в АС от НСД.

2.2 Апробация модели причинения вреда на базе ГПБОУ СПО «ЮУрГТК»

Важным условием проектирования систем защиты информации (СЗИ) от несанкционированного доступа (НСД) для автоматизированных систем (АС) считается анализ потенциальных угроз безопасности. Целью является

определение исходных данных и граничных условий для разработки средств защиты, чтобы наиболее точно определить адекватные средства и способы защиты необходим более детальный анализ угроз.

Также необходимо определить систему критериев и показателей защищенности АС от НСД для решения задачи адекватности и эффективности средств защиты. При этом, если состав и характеристики угроз задают, по сути, исходные данные для проектирования системы защиты, то система критериев и показателей защищенности позволяет не только оценивать результат разработки, но и контролировать ее ход [18].

Сегодня развитие научного направления, которое объединено с исследованием и оцениванием защищенности данных от НСД в АС, ограничивается отсутствием единого понятийного аппарата в области защиты информации от НСД, преобладанием в руководящих документах качественных подходов к оценке защищенности от НСД в АС, ориентацией на статические условия функционирования систем защиты. Для аттестации АС и сертификации средств вычислительной техники согласно требованиям действующих в РФ нормативных документов (руководящих документов Федеральной службы по техническому и экспортному контролю РФ ГОСТ Р ИСО/МЭК 15408—2002, ГОСТ Р ИСО/МЭК 17799—2005) необходимы высокая квалификация персонала, обработка больших объемов данных и значительные затраты времени [7].

Адаптируя предложенную в [22] методику для условий нашей экспериментальной работы, планируем работы по следующим этапам.

Этап планирования

Описание технологического процесса обработки информации в АС:

1) Объекты доступа: ноу-хау, программные средства, персональные данные, системы связи и передачи данных, информационные ресурсы.

2) Субъекты доступа: преподаватели, студенты, IT-специалист, администрация, директор.

3) Штатные средства доступа к информации: Moodle, сайт dom.sustec.ru, 650 компьютеров, 30 компьютерных аудиторий, корпоративная сеть на основе оптоволокна, 7 современных физических серверов, 28 виртуальных серверов, два канала доступа к сети Интернет, собственный web-хостинг, лицензионное программное обеспечение, организация ИТ-службы по международному стандарту ITIL, собственное вычислительное облако.

4) Используемые средства защиты информации: антивирусное программное обеспечение, резервное копирование информации, использование источников бесперебойного питания для серверов, пожарная сигнализация, парольная система доступа, разграничение прав пользователей, обязательства о неразглашении, использование межсетевого экрана.

5) Описание реализованных правил разграничения доступа (матрица доступа):

Таблица 6 – Матрица доступа

Объект / Субъект	*Информационные ресурсы*	*Программные средства*	*Системы связи и передачи данных*	*Ноу-хау*
IT-специалист	Полные права	Полные права	Полные права	Полные права
Директор колледжа	Полные права	Полные права	Полные права	Полные права
Преподаватель	Полные права	Полные права	Частичные права	Частичные права
Студент	Полные права	Частичные права (некоторые программы)	Запрет	Запрет

6) Схема или описание информационных потоков.

Рисунок 4 – Схема информационных потоков ЮУрГТК

Этап тестирования

1) Проверка подсистемы управления доступом:

Проверка подсистемы управления доступом представлена в таблице 7.

Таблица 7 – Проверка подсистемы управления доступом

Проверяемое требование	Порядок действий при проверке
Проверка механизма идентификации и аутентификации субъектов доступа при входе в систему	При входе в ОС с неправильно введенным идентификатором (логином) высвечивается сообщение «Неверный логин пользователя», с неправильно введенным паролем высвечивается сообщение «Неверный пароль». Когда пользователь вводит правильные логин и пароль, вход в учетную запись проходит успешно.
Проверка соблюдения требований к паролю (длина пароля должна быть не менее 6 символов, пароль должен включать буквы и цифры)	Требования к паролям установлены следующие: длина не менее 6 символов, использование латинских букв, заглавных букв, цифр. IT-специалист случайным образом, используя генератор паролей, присваивает пароли к учетным записям. Смена пароля пользователями производится по согласованию с IT-специалистом. Срок действия паролей – бессрочный. Количество попыток входа неограниченно. Установку пароля, длина которого менее 6 символов и состоящий исключительно из цифр, либо только из букв, система запрещает.

Продолжение таблицы 7

Проверяемое требование	Порядок действий при проверке
Проверка механизма идентификации внешних устройств по именам	Попытки загрузки с внешних устройств проигнорированы системой защиты информации.
Проверка механизма идентификации программ, каталогов, файлов, записей, полей записей по именам при обращении к ним средствами ОС и средствами установленных на СЗИ от НСД	Программы и каталоги (папки), в которых расположены защищаемые файлы, соответствуют заданным параметрам.
Проверка правильности предоставления доступа конкретным субъектам к защищаемым объектам (каталогам, файлам) в соответствии с установленными правами (матрицей доступа)	Матрица доступа соответствует таблице 4.

2) Порядок проверки подсистемы регистрации и учета

Таблица 8 – Проверка подсистемы регистрации и учета

Проверяемое требование	Порядок действий при проверке
Проверка регистрации входа (выхода) пользователя в (из) ОС, входа (выхода) компьютера из спящего режима	Был произведен выход из системы, вход в систему от имени пользователя. При вводе неправильного идентификатора и пароля высвечиваются сообщения «Неверный логин пользователя» и «Неверный пароль». При выходе из спящего режима система требует пароль. В журнале событий все события записаны.
Проверка регистрации запуска и завершения программ	В журнале событий описаны запуск и завершение программ, которые используются для обработки защищаемой информации.
Проверка регистрации попыток доступа к защищаемым файлам и каталогам	В журнале событий описаны действия по открытию и закрытию файлов и папок, содержащие защищаемую информацию, также создание файлов и папок.
Проверка регистрации выдачи защищаемых материалов на печать	Пользователю, осуществляющему печать, разрешен доступ к порту, к которому подключен принтер. Факт вывода документа на печать, дата и время выдачи, имя файла, уровень конфиденциальности, количество экземпляров документа, количество листов в экземпляре, имя файла, с которого выполнена печать документа, идентификатор пользователя, запросившего документ, регистрируется сотрудником, ответственным за вывод документов из АС. Бракованные листы выбрасываются в мусорные ведра, находящиеся в кабинетах и аудиториях.

Продолжение таблицы 8

Проверяемое требование	Порядок действий при проверке
Проверка регистрации и учета носителей защищаемой информации	Выдача носителей защищаемой информации не регистрируется. Носители защищаемой информации не уничтожаются, записи в журнале учета не ведутся.
Проверка качества очистки освобождаемых областей памяти внешних накопителей и оперативной памяти	Очистка освобождаемых областей внешних накопителей и оперативной памяти производится при помощи специализированных программных средств контроля защищённости с помощью «Terrier 3.0».

3) Проверка подсистемы обеспечения целостности.

Таблица 9 – Проверка подсистемы обеспечения целостности

Проверяемое требование	Порядок действий при проверке
Проверка обеспечения целостности программных СЗИ от НСД	Проверка обеспечения целостности программных СЗИ от НСД и неизменности программной среды не производится.
Проверка неизменности программной среды компьютера	
Проверка проведения периодического тестирования системы защиты информации от НСД	Организационно-распорядительная документация, определяющая периодичность и порядок тестирования всех функций СЗИ от НСД отсутствует. Периодическое тестирование СЗИ путем анализа применяемых разработчиком средств контроля целостности компонентов системного ПО не проводится.
Порядок проверки наличия средств восстановления	Средства восстановления программной среды компьютера имеются в наличии. Средства восстановления СЗИ от НСД имеются в наличии, дистрибутивы ПО хранятся на сервере.
Проверка наличия средств антивирусной защиты	Средства антивирусной защиты имеются в наличии.

Заключительный этап

В параграфе 1.3. была описана модель причинения вреда информационной системе образовательной организации. Данная модель позволила нам наглядно рассмотреть необходимые действия, направленные на защиту информационных активов, такие как создание механизма оперативного реагирования на угрозы, своевременное выявление, оценка и прогнозирование источников угроз ИБ, создание механизмов управления системой ИБ, эффективное пресечение незаконных посягательств на

информационные ресурсы, создание механизмов, обеспечивающих контроль системы ИБ.

На стадии апробации модели были проведены все работы согласно описанного ранее регламенту, описанному в п.2.1.

Анализ результатов проведенной методики представим в виде таблицы 10.

Таблица 10 – Сравнение фактических значений показателей защищенности, и норм (требований)

Требования	Фактические показатели	Соответствие норме
Проверка механизма идентификации и аутентификации субъектов доступа при входе в систему	При входе в ОС с неправильно введенным идентификатором (логином) высвечивается сообщение «Неверный логин пользователя», с неправильно введенным паролем высвечивается сообщение «Неверный пароль». Когда пользователь вводит правильные логин и пароль, вход в учетную запись проходит успешно.	Показатели соответствуют норме.
Проверка соблюдения требований к паролю	Требования к паролям установлены следующие: длина не менее 6 символов, использование латинских букв, заглавных букв, цифр. IT-специалист случайным образом, используя генератор паролей, присваивает пароли к учетным записям. Смена пароля пользователями производится по согласованию с IT-специалистом. Срок действия паролей – бессрочный. Количество попыток входа неограниченно. Установку пароля, длина которого менее 6 символов и состоящий исключительно из цифр, либо только из букв, система запрещает.	Срок действия паролей должен быть не менее 42 дней.

Продолжение таблицы 10

Требования	Фактические показатели	Соответствие норме
Проверка механизма идентификации внешних устройств по именам	Попытки загрузки с внешних устройств проигнорированы системой защиты информации.	Соответствует норме.
Проверка механизма идентификации программ, каталогов, файлов, записей, полей записей по именам при обращении к ним средствами ОС и средствами установленных на СЗИ от НСД	Программы и каталоги (папки), в которых расположены защищаемые файлы, соответствуют заданным параметрам.	Соответствует норме.
Проверка правильности предоставления доступа конкретным субъектам к защищаемым объектам (каталогам, файлам) в соответствии с установленными правами (матрицей доступа)	Матрица доступа соответствует таблице 4.	Соответствует норме.
Проверка регистрации входа (выхода) пользователя в (из) ОС, входа (выхода) компьютера из спящего режима	Был произведен выход из системы, вход в систему от имени пользователя. При вводе неправильного идентификатора и пароля высвечиваются сообщения «Неверный логин пользователя» и «Неверный пароль». При выходе из спящего режима система требует пароль. В журнале событий все события записаны.	Соответствует норме.
Проверка регистрации запуска и завершения программ	В журнале событий описаны запуск и завершение программ, которые используются для обработки защищаемой информации.	Соответствует норме.
Проверка регистрации попыток доступа к защищаемым файлам и каталогам	В журнале событий описаны действия по открытию и закрытию файлов и папок, содержащие защищаемую информацию, также создание файлов и папок.	Соответствует норме.

Продолжение таблицы 10

Требования	Фактические показатели	Соответствие норме
Проверка регистрации выдачи защищаемых материалов на печать	Пользователю, осуществляющему печать, разрешен доступ к порту, к которому подключен принтер. Факт вывода документа на печать, дата и время выдачи, имя файла, уровень конфиденциальности, количество экземпляров документа, количество листов в экземпляре, имя файла, с которого выполнена печать документа, идентификатор пользователя, запросившего документ, регистрируется сотрудником, ответственным за вывод документов из АС. Бракованные листы выбрасываются в мусорные ведра, находящиеся в кабинетах и аудиториях.	Бракованные листы должны быть уничтожить с помощью шредера в специализированном помещении.
Проверка регистрации и учета носителей защищаемой информации	Выдача носителей защищаемой информации не регистрируется. Носители защищаемой информации не уничтожаются, записи в журнале учета не ведутся.	Учет носителей защищаемой информации должен проводится в журнале с регистрацией их выдачи (приема). Носители защищаемой информации должны быть уничтожены с записью об этом в журнале учета.
Проверка качества очистки освобождаемых областей памяти внешних накопителей и оперативной памяти	Очистка освобождаемых областей внешних накопителей и оперативной памяти производится при помощи специализированных программных средств контроля защищённости с помощью «Terrier 3.0».	Соответствует норме.

Продолжение таблицы 10

Требования	Фактические показатели	Соответствие норме
Проверка обеспечения целостности программных СЗИ от НСД Проверка неизменности программной среды компьютера	Проверка обеспечения целостности программных СЗИ от НСД и неизменности программной среды не производится.	Проверка обеспечения целостности программных СЗИ от НСД и неизменности программной среды производится при помощи специализированных средств контроля защищенности.
Проверка проведения периодического тестирования системы защиты информации от НСД	Организационно-распорядительная документация, определяющая периодичность и порядок тестирования всех функций СЗИ от НСД отсутствует. Периодическое тестирование СЗИ путем анализа применяемых разработчиком средств контроля целостности компонентов системного ПО не проводится.	Должна вестись организационно-распорядительная документация, определяющая периодичность и порядок тестирования всех функций СЗИ от НСД. Проводится периодическое тестирование СЗИ путем анализа применяемых разработчиком средств контроля целостности компонентов системного ПО, реализующих функции СЗИ от НСД и наборов данных, используемых этими средствами.
Порядок проверки наличия средств восстановления	Средства восстановления программной среды компьютера имеются в наличии. Средства восстановления СЗИ от НСД имеются в наличии, дистрибутивы ПО хранятся на сервере.	Соответствует норме.
Проверка наличия средств антивирусной защиты	Средства антивирусной защиты имеются в наличии.	Соответствует норме.

Проанализировав таблицу 10, мы можем убедиться в том, что есть необходимость в периодической смене паролей пользователей, уничтожении бракованных листов в установленном в организации порядке, проверке обеспечения целостности программных СЗИ от НСД и неизменности программной среды, организационно-распорядительной документации, которая определяет периодичность и порядок тестирования

всех функций СЗИ от НСД, периодическом тестировании СЗИ, также важно регистрировать и уничтожать носители защищаемой информации с записью об этом в журнале учета.

Примененная методика позволила в совокупности с вероятностной моделью причинения вреда наиболее обширно рассмотреть необходимые действия по защите и предотвращению утечки информационных активов, оценивать текущее состояние защищенности и точнее планировать меры защиты.

2.3 Рекомендации на основе модели причинения вреда информационной системы образовательной организации ГПБОУ СПО «ЮУрГТК»

Для того, чтобы обеспечить безопасность информационной системе образовательной организации, необходимо разработать положения, регламенты и процессы взаимодействия. Некоторые понятия нормативных актов регламентируется требованиями законодательства, к ним могут относиться, например, положение об обработке персональных данных, которое должен разработать и разместить на своем сайте каждый оператор персональных данных.

Действия, направленные на защиту информационной системы, не ограничиваются разработкой положений. Также, необходимо произвести:

— документирование и оптимизацию бизнес-процессов,

— установку градации сотрудников и их уровней доступа к информации, содержащей коммерческую тайну,

— создание подразделений или назначение лиц, ответственных за обеспечение информационной безопасности, иногда изменение структуры предприятия в соответствии с требованиями безопасности,

— информирование или переобучение персонала,

— организацию мероприятий по тестированию подготовки персонала к работе с системой в критических ситуациях,

— получение лицензий, например, на работу с государственной тайной,

— обеспечение технической защиты помещений и оборудования с дальнейшей сертификацией классов защиты, определение их соответствия нормативно-правовым требованиям,

— создание системы безопасности для цепочки поставщиков, во взаимодействии с которыми передаются конфиденциальные данные, внесение в договоры с контрагентами оговорок о сохранении коммерческой тайны и мер ответственности за ее разглашение,

— установка пропускной системы для сотрудников, выдача им электронных средств идентификации,

— выполнение всех требований законодательства по защите персональных данных,

— разработка системы взаимодействия с государственными органами в случае запроса ими у организации информации, которая может быть отнесена к конфиденциальной.

К техническим средствам и мерам обеспечения информационной безопасности относятся не только программные продукты, например, DLP-системы, но и другие инструменты, находящиеся в распоряжении компании. Меры защиты информации с технической точки зрения должны опираться на модель причинения вреда информационной системе образовательной организации, которая позволяет выстроить оборону против посягательств на конфиденциальные сведения.

К принципам построения такой системы относятся:

1) простота архитектуры, упрощение компонентов, сокращение числа каналов и протоколов межсетевого взаимодействия. В системе должны

присутствовать только те элементы, без которых она окажется нежизнеспособной;

2) внедрение только протестированных программных решений, уже не раз опробованных другими предприятиями, плюсы и минусы которых очевидны;

3) минимальные доработки имеющихся лицензионных программных продуктов силами собственных или привлеченных исполнителей;

4) использование только лицензированного ПО, при возможности оно должно быть внесено в государственный реестр программ для ЭВМ и баз данных;

5) использование для построения системы только аутентичных компонентов, надежных и долговечных, не способных неожиданно выйти из строя и подорвать работоспособность системы. Все они должны быть совместимыми друг с другом;

6) управляемость, легкость администрирования как самой системы, так и применяемых программных продуктов, минимальное использование сторонней технической поддержки;

7) протоколирование и документирование любых действий пользователей, осуществляемых с файлами, содержащими конфиденциальную информацию, случаев несанкционированного доступа;

8) эшелонированность обороны. Каждый потенциальный канал утечки должен иметь несколько рубежей системы защиты, затрудняющих работу потенциального похитителя информации.

При реализации этих принципов обеспечения информационной безопасности рассматриваются вопросы об использовании дополнительных технических средств защиты информации, к которым относятся:

— средства криптографической защиты, обеспечивающие шифрование на рабочих станциях и серверах, передаваемой по каналам связи,

— средства антивирусной защиты,

— SIEM-системы и DLP-системы, обеспечивающие закрытие всех потенциальных каналов утечки информации и перехват исходящего трафика [41].

Разнообразие и количество средств защиты информации весьма велико. В наиболее общем виде их можно разделить на:

—физические средства защиты информации,

—аппаратные средства,

—программные (в том числе криптографические).

Подбор технических мер защиты для использования в конкретной организации опирается на концепцию информационной безопасности, принятую в регионе. Концепция обосновывает, что именно и каким образом необходимо защищать.

При построении системы защиты информации с использованием технических средств необходимо следовать определенным принципам:

1) использование только лицензированного программного обеспечения (далее – ПО);

2) использование только совместимого ПО, все части системы должны быть совместимыми друг с другом;

3) управляемость, легкость администрирования системы, минимальное использование сторонней технической поддержки;

4) протоколирование и документирование любых действий пользователей, осуществляемых с файлами, содержащими конфиденциальную информацию, а также случаев несанкционированного доступа;

5) затраты на организацию защиты информации должны быть соразмерны величине ущерба, который может быть нанесен собственнику информации.

Физические средства защиты информации – это любые механические, электрические и электронные механизмы, которые функционируют

независимо от информационных систем и создают препятствия для доступа к ним. К ним относятся:

—замки, в том числе электронные – один из простейших и эффективных способов физически ограничить доступ к чему-либо;

—экраны, жалюзи создают препятствия для визуального съема информации с систем обработки данных;

—системы контроля и управления доступом (СКУД) – задают правила доступа сотрудников к определенным помещениям;

—системы видеонаблюдения, видеорегистраторы – отслеживают перемещения работников, позволяют зафиксировать факт несанкционированного проникновения в защищаемые помещения;

—датчики, выявляющие движение или превышение степени электромагнитного излучения в зоне расположения защищаемого оборудования – по сути «бюджетная версия» предыдущего пункта.

Аппаратные средства защиты информации – это любые устройства, которые либо затрудняют несанкционированный съем информации, либо помогают обнаружить потенциальные каналы утечки информации. Это самый узкоспециализированный класс средств защиты информации.

Съем информации через технические каналы утечки возможен только при использовании специального, часто очень дорогостоящего оборудования. Как правило, информация, которой располагают образовательные организации, не является объектом попыток ее несанкционированного получения. В обычной деятельности организации из всех видов утечки информации по техническим каналам наиболее актуальными являются: просмотр информации с экранов дисплеев, бумажных и иных носителей информации (возможно, с помощью оптических средств) и прослушивание конфиденциальных переговоров, в том числе телефонных.

В данной ситуации могут использоваться как физические средства защиты информации, рассмотренные выше, так и организационные мероприятия. Также необходимо следовать правилам:

—не рекомендуется располагать защищаемые помещения на первых этажах зданий;

—независимо от этажа, следует закрывать окна жалюзи или экранами, в идеале для конфиденциальных мероприятий или обработки информации ограниченного распространения использовать помещения вообще без окон;

—использовать двойные двери с тамбурами;

—исключить пребывание посторонних в местах, где обрабатывается конфиденциальная информация;

—располагать мониторы таким образом, чтобы исключить просмотр информации с них посторонними;

—всегда блокировать рабочие станции при оставлении рабочего места. Для этого следует установить на компьютер пароль и при оставлении рабочего места производить выход из операционной системы. Необходимо также настроить компьютер на отключение при определенном периоде бездействия.

Программные средства защиты информации – это программное обеспечение, предназначенные для решения задач, связанных с обеспечением информационной безопасности. Это самая многочисленная и распространенная группа средств защиты информации. К ним относят [30]:

1) Средства операционных систем (далее – ОС). Современные ОС предоставляют широкий спектр встроенных решений по защите конфиденциальной информации на рабочих станциях и серверах:

—вход на свой компьютер, в рабочую группу, в домен происходит по паролю, смарт-карте, сертификату собственного удостоверяющего центра,

—минимизация прав при помощи учетных записей (локальных и доменных),

—ограничение прав с помощью локальной и групповой политик безопасности – запрет доступа к реестру, настройкам компьютера и др.,

—защита от угроз по сети при помощи встроенного брандмауэра,

—ограничение прав на доступ к общим ресурсам организации через механизм разрешений.

2) Антивирусные программы. Современные антивирусные средства кроме своих «основных обязанностей» умеют управлять доступом к съемным устройствам (запрет, белый список), сообщать об уязвимостях в установленном ПО, производить удаленную установку и удаление программ, шифровать данные на жестких дисках и съемных устройствах.

3) Программы резервного копирования и восстановления данных. Выделяют штатные программы резервного копирования, то есть встроенные в ОС и дополнительные, например, Acronis.

4) Прикладные программы, в которых существует разграничение прав пользователей – пароли, роли, и т.д.

5) Программные межсетевые экраны. Межсетевой экран – программа, контролирующая и фильтрующая на основе заданных правил входящий и исходящий сетевой трафик, определяет пропускать его или нет. Помимо этого, сетевой экран используется для защиты сети или рабочих станций от несанкционированного проникновения через уязвимости программного обеспечения или протоколов сети. Таким образом, межсетевой экран – это барьер между внутренней сетью организации, содержащей конфиденциальные или персональные данные, и глобальными информационными сетями. Если не хватает возможностей встроенного в Windows межсетевого экрана, используются программы и программно-аппаратные решения.

6) Прокси-серверы. Прокси-сервер – это компьютер, выполняющий роль посредника между пользователем и запрашиваемым адресом в сети интернет. Пользователь сначала подключается к прокси-серверу и запрашивает необходимый ресурс, расположенный на другом сервере.

Например, почту или htmlстраницу. Затем прокси либо подключается к указанному серверу и получает у него ресурс, либо возвращает ресурс из собственного кэша

7) Системы обнаружения и предотвращения вторжений. Считается, что в современных условиях защита, обеспечиваемая файерволом и антивирусом, уже недостаточно эффективна против сетевых атак злоумышленников.

Причина в том, что вредоносное программное обеспечение может «замаскироваться» и отправлять сетевые пакеты, которые с точки зрения межсетевого экрана выглядят полностью легитимными. Антивирус плохо работает с еще неизвестными, неописанными угрозами. Повысить уровень защиты внутренней сети организации призваны системы обнаружения вторжений и системы предотвращения вторжений. Соответственно – IDS (Intrusion Detection Systems) и IPS (Intrusion Prevention Systems). Различия между ними заключаются лишь в том, что одна система может автоматически блокировать атаки, а другая просто предупреждает об этом сотрудника с помощью передачи сообщения на консоль управления, отправки электронного письма, SMS-сообщения на мобильный телефон и т.п.

Из приведенных рекомендаций в ГПБОУ СПО «ЮУрГТК» реализована только часть мер, остальные мероприятия необходимо включить в перспективный план модернизации системы обеспечения информационной безопасности.

В качестве одной из рекомендаций был разработан обучающий курс на платформе Stepik.

Stepik — это 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. Основные охватываемые курсами дисциплины — программирование, математика, биоинформатика и биология, экономика; основной язык курсов — русский, есть курсы на английском языке. По состоянию на 2020 год на платформе зарегистрировано 5 миллионов пользователей. Целевые аудитории — школьники (в основном курсы по подготовке к ЕГЭ), студенты, начинающие специалисты.

Курсы на платформе состоят из уроков, сгруппированных в тематические модули, однако уроки могут существовать отдельно и собираются в библиотеку на платформе. Уроки состоят из шагов, которые могут представлять собой текст, видео-лекцию или практическое задание. На платформе можно использовать 20 типов заданий, включая тесты, числовые задачи, задания с математическими формулами и химическими уравнениями, пазлы, задачи на программирование.

Существуют также годовые и короткие онлайн-программы. В зависимости от договорённости с вузом, слушателям по результатам могут выдаваться дипломы о профессиональной переподготовке.

Также платформа может функционировать как площадка для проведения конкурсов и олимпиад, среди проведённых мероприятий — отборочный этап Олимпиады НТИ (2016—2020) (всероссийской инженерной олимпиады школьников, в рамках программы Национальная технологическая инициатива), онлайн-этап акции Тотальный диктант в 2017 году, соревнования по информационной безопасности StepCTF—2015.

Таким образом было решено разработать курс на платформе Stepik.

Модуль по теме «Матрица вероятностей (рисков) и влияния управления проектов» состоит из пяти уроков. В каждом уроке составлен лекционный материал и тестовые вопросы для самопроверки.

Слева находится панель навигации. На рисунке 5 представлен лекционный материал первого урока «Риски проекта».

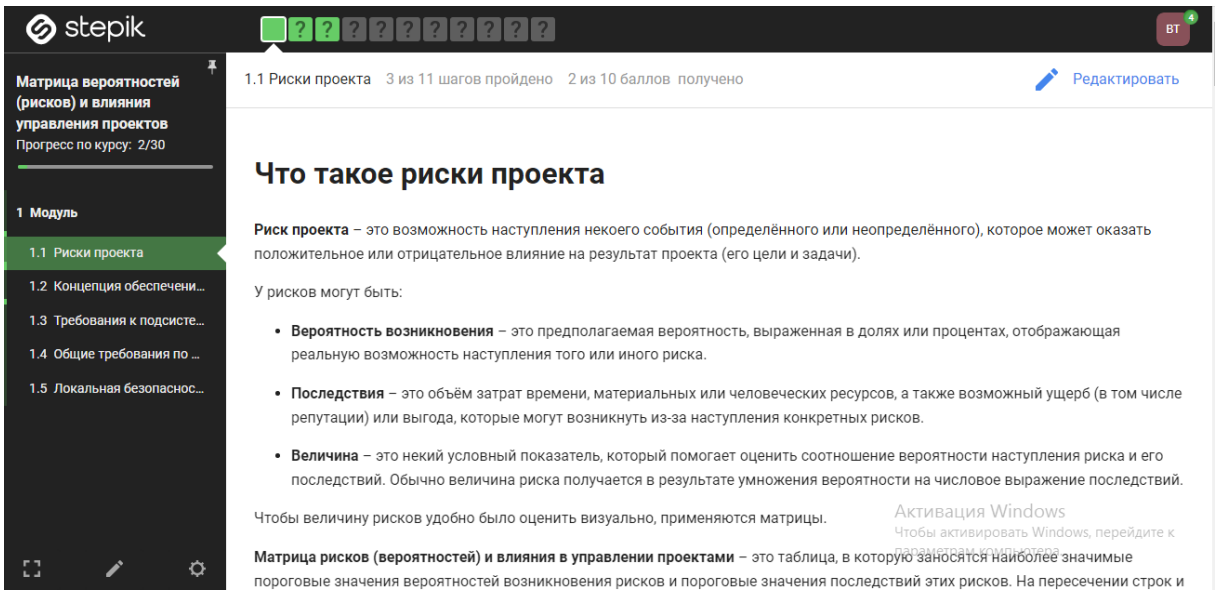

Рисунок 5 – Урок «Риски проекта»

На рисунке 6 представлена страница с тестовым вопросом урока «Риски проекта».

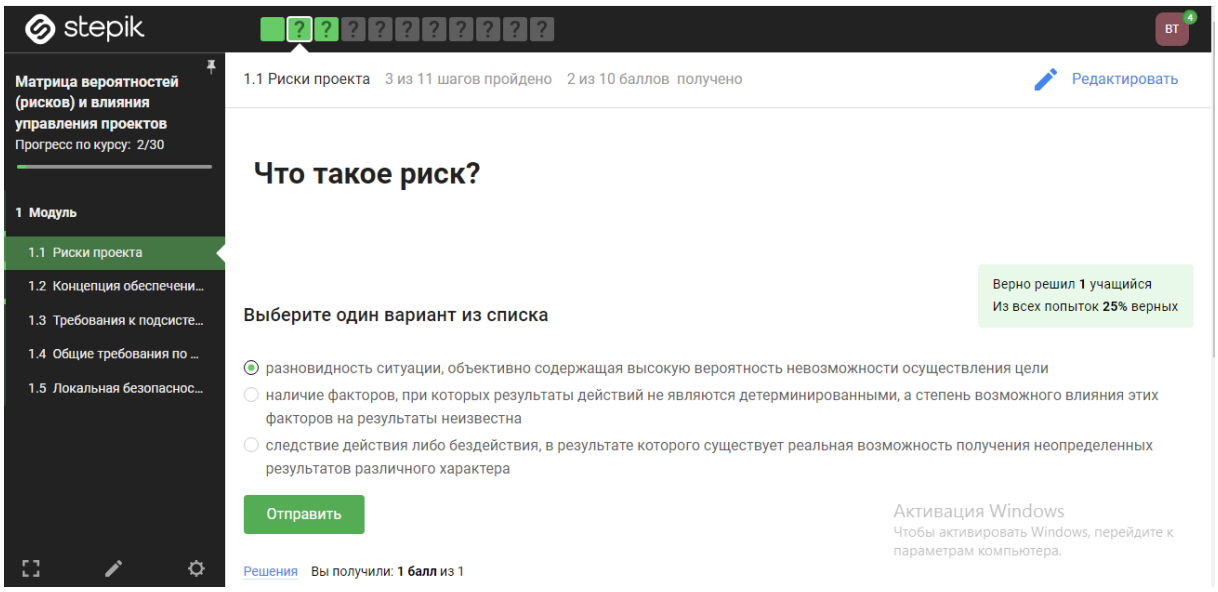

Рисунок 6 – Тестовый вопрос

На рисунке 7 представлено сообщение при верном ответе на вопрос.

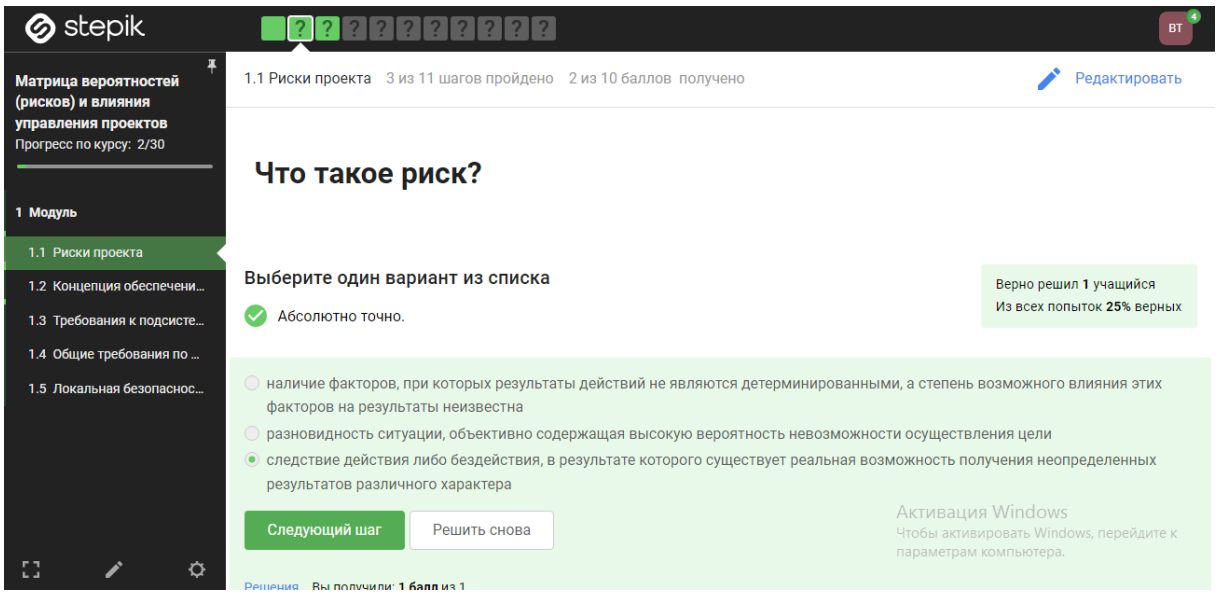

Рисунок 7 – Верный ответ на вопрос

На рисунке 8 представлено сообщение при неверном ответе на вопрос.

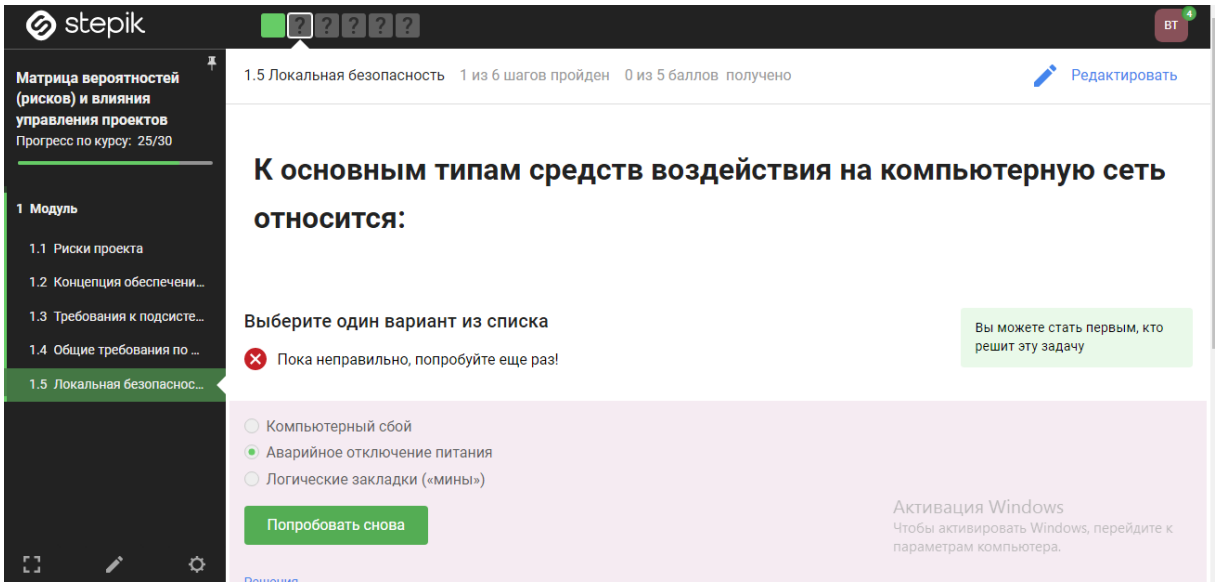

Рисунок 8 – Неверный ответ на вопрос

На рисунке 9 представлен прогресс изучения модуля. Также при наведении на тему урока в навигации высвечивается прогресс изучения отдельного урока.

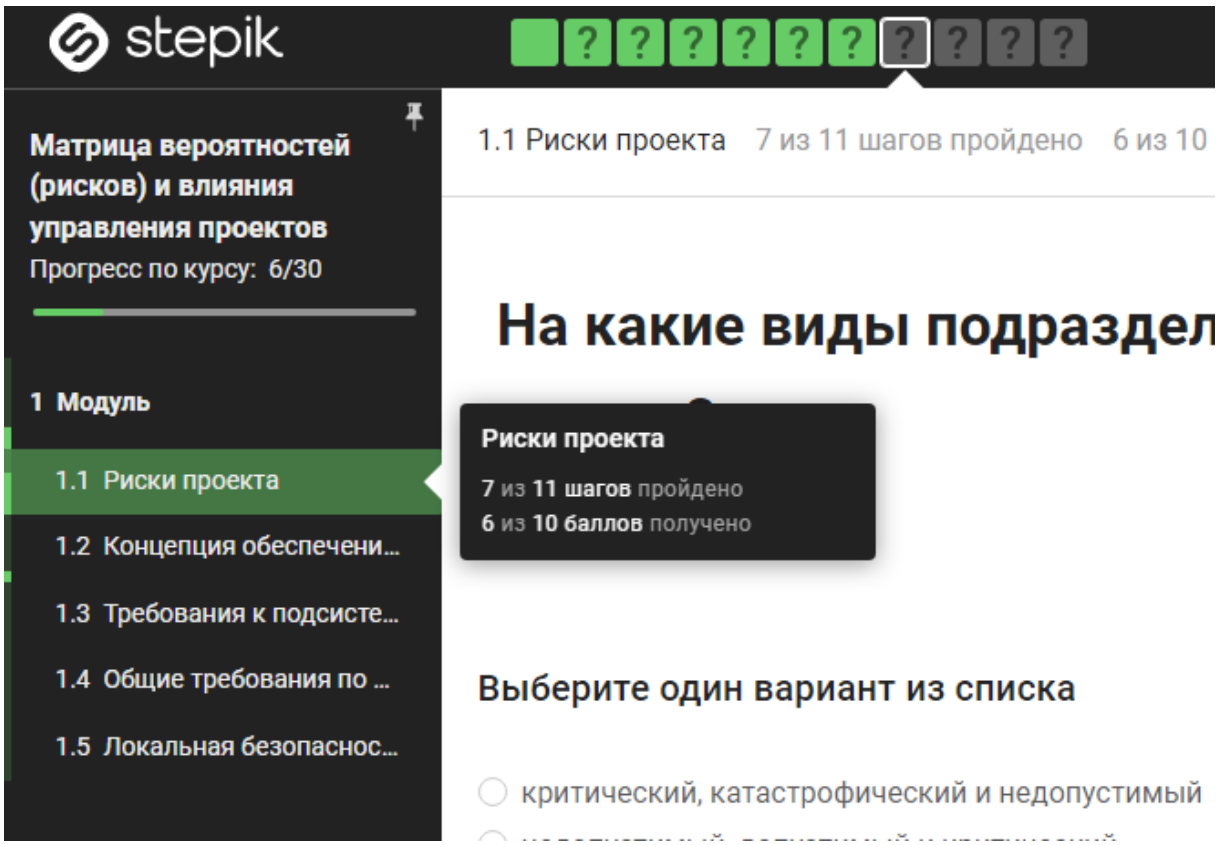

Рисунок 9 – Прогресс изучения модуля

На каждой странице курса можно оставить комментарий и поделиться своим решением определенного задания. Данная возможность представлена на рисунке 10.

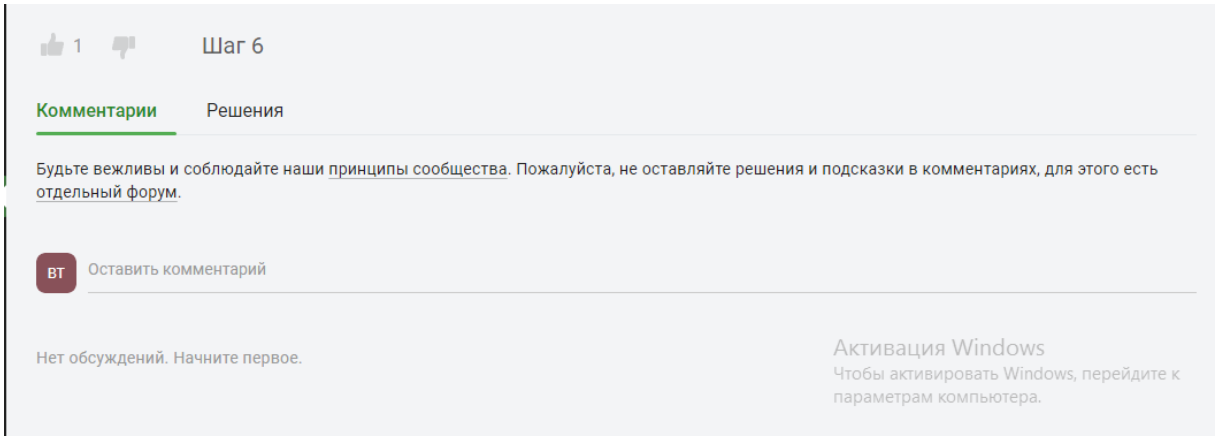

Рисунок 10 – Добавление комментариев

Курс также может быть использован в образовательном процессе студентов специальности 09.02.06 Сетевое и системной администрирование.

Выводы по главе II

В главе II была описана проведенная опытно-экспериментальная работа по апробации модели причинения вреда информационной системе образовательной организации.

В параграфе 2.1. рассмотрены цель, задачи и организация опытно-экспериментальной работы по апробации модели причинения вреда информационной системы образовательной организации.

В наше время информация имеет огромную роль в современной жизни. Получение третьими лицами конфиденциальной информации или личного сообщения может принести непоправимый ущерб не только обладателю информации, но и окружающим людям. С каждым годом роль информации возрастает, поэтому она имеет огромную ценность. Вследствие чего главной задачей является ее защита.

Дано определение понятию несанкционированный доступ — это доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС).

Рассмотрена методика защиты конфиденциальной информации в АС от НСД, которая состоит из трех основных этапов:

1) Планирование.

2) Тестирование.

3) Анализ результатов.

В параграфе 2.2. описан процесс апробации модели причинения вреда информационной системе образовательной организации.

Важным условием проектирования систем защиты информации (СЗИ) от несанкционированного доступа (НСД) для автоматизированных систем (АС) считается анализ потенциальных угроз безопасности. Целью является определение исходных данных и граничных условий для разработки

средств защиты. Чтобы наиболее точно определить адекватные средства и способы защиты необходим более детальный анализ угроз.

С точки зрения проникновения в периметр информационной безопасности и для совершения хищения информации или создания нарушения в работе систем необходим несанкционированный доступ.

Рассмотрены дополнительные технические средства защиты информации. Проанализированы уровни защиты от несанкционированного доступа к информационной системе.

Была адаптирована методика, которая рассматривалась в параграфе 2.1. Описан технологический процесс обработки информации в автоматизированной системе. Составлена матрица доступа к информационным ресурсам, программным средствам, системам связи и передачи данных, а также ноу-хау. Проведена проверка подсистемы управления доступом, подсистемы регистрации и учета, подсистемы обеспечения целостности. Было проведено сравнение значений показателей защищенности, и норм (требований). Была проанализирована опытно-экспериментальная работа по модели причинения вреда информационной системы образовательной организации.

В параграфе 2.3. изложены рекомендации для образовательной организации на основе проведенной апробации модели причинения вреда при несанкционированных доступах. Поскольку модель причинения вреда при несанкционированных доступах была разработана на базе ГПБОУ СПО «ЮУрГТК», рекомендации применимы для данной образовательной организации. Однако, они будут полезны и для иной образовательной организации среднего профессионального образования.

В качестве одной из рекомендаций был предложен обучающий курс (на платформе Stepik) по управлению рисками в информационной безопасности, предназначенный для сотрудников, обеспечивающих функционирование информационной системы образовательной организации. Курс может быть использован в образовательном процессе

студентов специальности 09.02.06 Сетевое и системной администрирование.

ЗАКЛЮЧЕНИЕ

В ходе выполненного исследования были изучены аспекты безопасности информационной системы образовательной организации. обеспечение безопасности информационных систем образовательных организаций является важной задачей, которая становится все более актуальной в наши дни. Современные технологии не только облегчают и ускоряют процессы обучения, но также повышают уровень угроз безопасности информации.

Был проведен анализ актуального состояния защищенности информационной безопасности системы образовательной организации. При разработке вероятностной модели причинения вреда информационной системе образовательной организации используются статистические данные о причинах аварий и сбоев в информационных системах. После анализа этих данных разрабатывается модель, которая может использоваться для определения вероятности различных событий в информационной системе образовательной организации.

Нами была разработана общая модель причинения вреда информационной системе образовательной организации при несанкционированных доступах. Вероятностная модель причинения вреда информационной системе образовательной организации — это необходимый инструмент для управления рисками и обеспечения безопасности информационных систем. Разработка и использование такой модели помогает провести анализ рисков и принять меры по их снижению, что обеспечивает безопасность информационных систем образовательных организаций.

Проведена апробация модели причинения вреда информационной системы образовательной организации при несанкционированных доступах, конкретизирован ее вероятностный аспект. В данной работе была проведена оценка рисков безопасности информационной системы

образовательной организации на основе параметров возможности, вероятности и воздействия.

Были разработаны рекомендации на основе вероятностной модели причинения вреда информационной системы образовательной организации. Для уменьшения рисков были предложены меры по защите от угроз безопасности, такие как разработка и реализация политики безопасности данных, установление парольной защиты, регулярное обновление системы безопасности, разработка экстренного плана действий при возникновении угроз безопасности, обучение персонала и студентов основам информационной безопасности и другие.

Целью исследования было: теоретико-методическое обоснование и апробация вероятностной модели причинения вреда информационной системы образовательной организации при несанкционированных доступах. Данная цель в ходе работы была достигнута таким образом: была разработана вероятностная модель причинения вреда информационной системе образовательной организации при несанкционированных доступах, которая в свою очередь может помочь оценить вероятность возникновения угрозы и определить наиболее эффективные меры для защиты информации.

Можно обозначить перспективы данной темы, так как разработка и использование вероятностной модели причинения вреда информационной системе образовательной организации является чрезвычайно важной задачей для обеспечения безопасности информационных систем образовательных организаций. Модель позволяет учитывать риск и принимать меры по снижению этого риска.

В ходе работы все цели были достигнуты, задачи решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1) "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) утв. ФСТЭК РФ 15.02.2008) // ФСТЭК РФ – 11.02.2013– № 17.

2) ГОСТ Р ИСО/МЭК ТО 13335-3-2007. URL: http://vsegost.com/Catalog/54/5475.shtml

3) Программа и методики проведения аттестационных испытаний объектов информатизации (Аттестация АС) // Документы по информационной безопасности. URL: http://securitypolicy.ru/index.php/Программа_и_методики_проведения_аттестационных_испытаний_объектов_информатизации_(Аттестация_АС).

4) Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утв. Гостехкомиссией РФ 30.03.1992 г.).

5) Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утв. Гостехкомиссией РФ 30.03.1992 г.).

6) Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утв. Гостехкомиссией РФ 30.03.1992 г.).

7) Авраменко В. С., Козленко А. В., Модель для количественной оценки защищенности информации от НСД в АС по комплексному показателю, Тр. СПИИРАН, 2010, выпуск 13, 172–181. URL: https://www.mathnet.ru/links/7c8a3ed8a37535151cae4a4b2f7abad4/trspy382.pdf (дата обращения: 20.04.2023).

8) Аксюхин, А.А. Информационные технологии в образовании и науке / Аксюхин А.А., Вицен А.А., Мекшенева Ж.В. // Современные наукоемкие технологии, 2019. № 11. С. 50–52.

9) Бабин С. А. Лаборатория хакера. — СПб.: БХВ-Петербург, 2016. — 240 с.: ил. — (Глазами хакера).

10) Барабанов А. В., Марков А. С., Цирлов В. Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. — 2011. — № 3. — С. 48–53.

11) Берзинь М. М. Модели угроз информационной безопасности и методы их оценки // Интеллектуальный потенциал XXI века: ступени познания. 2011. №7. URL: https://cyberleninka.ru/article/n/modeli-ugroz-informatsionnoy-bezopasnosti-i-metody-ih-otsenki (дата обращения: 08.02.2023).

12) Бирюков А.А. Информационная безопасность: защита и нападение. – 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.: ил.

13) Блинов В. И. Цифровая дидактика: модный тренд или новая наука? / Профессиональное образование // Столица. 2019. – №3. – С. 27

14) Варламов О. О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ЮФУ. Технические науки. 2006. №7. URL: https://cyberleninka.ru/article/n/o-sistemnom-podhode-k-sozdaniyu-modeli-kompyuternyh-ugroz-i-ee-roli-v-obespechenii-bezopasnosti-informatsii-v-klyuchevyh-sistemah (дата обращения: 08.02.2023).

15) Гафнер В. В. Информационная безопасность: учебное пособие в 2 ч. / В. В. Гафнер; ГОУ ВПО «Урал. гос. пед. ун-т». – Екатеринбург, 2019. – Ч.1. – 155 с

16) Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.: ил.

17) Зайцев А. П., Мещеряков Р. В., Шелупанов А. А., Технические средства и методы защиты информации. Учебник для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков. Под ред. А. П. Зайцева и А. А. Шелупанова. – 7-е изд., испр. – М.: Горячая линия–Телеком, 2012. – 442 с: ил.

18) Карпов В. В. Критерии и показатели защищенности автоматизированных систем от несанкционированного доступа // Программные продукты и системы. 2001. №1. URL: https://cyberleninka.ru/article/n/kriterii-i-pokazateli-zaschischennosti-avtomatizirovannyh-sistem-ot-nesanktsionirovannogo-dostupa (дата обращения: 20.04.2023).

19) Кашина, Е.А. Прогнозирование структуры интегрированного курса информатики: дис. канд. пед. наук / Е.А. Кашина. Екатеринбург, 2017. 187 с.

20) Комплексная защита информации в организации / М. М. Тараскин, А. Г. Захаров, Ю. И. Коваленко, Г. И. Москвитин. — Москва: РУСАЙНС, 2020. — 354 с.

21) Лушников, И.Д. Цифровая школа как ресурсный центр сетевого взаимодействия [Текст]: Справочник заместителя директора школы / Лушников И.Д. 2013. – С.66-88.

22) Михайловская, А. С. Методика контроля защищенности конфиденциальной информации в автоматизированной системе от несанкционированного доступа / А. С. Михайловская. — Текст: непосредственный // Молодой ученый. — 2016. — № 12 (116). — С. 327-331. — URL: https://moluch.ru/archive/116/31904/ (дата обращения: 14.03.2023).

23) Неуймин Я. Г. Модели в науке и технике. История, теория, и практика. Л., 1984.

24) Носкова, Т. Н. Проблемы воспитания средствами информационной образовательной среды [Текст]: Известия Российского

государственного педагогического университета им. А. И. Герцена / Т.Н. Носкова. – 2015. – № 177. – С. 61-69.

25) Нургалиева Г.К. Индикаторы оценки внедрения ИКТ в организациях образования [Текст]: учебное пособие по спецкурсу / Г.К.Нургалиева, 90 А.И.Тажигулова. – Алматы: Национальный центр информатизации, 2010. - 65с.

26) Организация коллективной учебной деятельности с использованием сетевых технологий: учебное пособие. / М.: МГПУ. – 2020. 93 с. (В соавторстве Азевич А.И., Баженова С.А., Заславская О.Ю., Заславский А.А., Львова О.В., Рудакова Д.Т.).

27) Определение подходов к комплексному исследованию информационной образовательной среды в системах общего, профессионального и дополнительного образования [Текст]: // Вестник Российского университета дружбы народов. Серия «Информатизация образования». – Москва: РУДН, 2019. №1. С. 12-21.

28) Парошин, А.А. Нормативно-правовые аспекты защиты информации [Текст] / А.А. Парошин. – Изд-во Дальневосточного федерального университета, 2010. – 116с.

29) Проблемы и пути эффективного использования технологий информатизации в образовании [Текст]: Вестник московского университета. Серия 20. Педагогическое образование – Москва: Изд-во МГУ – 2018. – №2. –С. 34-47.

30) Прокофьева Елена Николаевна Модель управления комплексной безопасностью образовательных организаций // КПЖ. 2016. №3 (116). URL: https://cyberleninka.ru/article/n/model-upravleniya-kompleksnoy-bezopasnostyu-obrazovatelnyh-organizatsiy (дата обращения: 08.02.2023).

31) Табаков А. Б. Разработка моделей оптимизации средств защиты информации для оценки страхования информационных рисков // Научный журнал КубГАУ. 2005. №12. URL: https://cyberleninka.ru/article/n/razrabotka-

modeley-optimizatsii-sredstv-zaschity-informatsii-dlya-otsenki-strahovaniya-informatsionnyh-riskov (дата обращения: 08.02.2023).

32) Тимофеева Л.Л. Методические рекомендации по организации информационной безопасности в образовательном учреждении // КРЫМСКИЙ ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО РАЗВИТИЯ. – 2020. – URL: https://dpo-kipr.ru/wp-content/uploads/2022/11/Metodicheskie_rekomendacii_po_obespecheniju_informacionnoj_bezopasnosti.pdf

33) Титор Светлана Евгеньевна ВНЕДРЕНИЕ РИСК-ОРИЕНТИРОВАННОЙ МОДЕЛИ КОНТРОЛЯ (НАДЗОРА) В СФЕРЕ ОБРАЗОВАНИЯ (РЕГИОНАЛЬНЫЙ АСПЕКТ): ВЗГЛЯД ОБЩЕОБРАЗОВАТЕЛЬНЫХ ШКОЛ (АНАЛИЗ СОЦИОЛОГИЧЕСКОГО ОПРОСА) // Вестник экономической безопасности. 2022. №2. URL: https://cyberleninka.ru/article/n/vnedrenie-risk-orientirovannoy-modeli-kontrolya-nadzora-v-sfere-obrazovaniya-regionalnyy-aspekt-vzglyad-obscheobrazovatelnyh-shkol (дата обращения: 08.02.2023).

34) Фленов М. Е. PHP глазами хакера: 2-е изд., доп. и перераб. – СПб.: БХВ-Петербург, 2010. – 336 с.: ил. + CD-ROM.

35) Хорев П.Б. Программно-аппаратная защита информации. Учебное пособие / П.Б. Хорев. М.: ФОРУМ, 2019. 352 с.

36) Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. /В.Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.

37) Vladimir Zwass. Britannica: information system https://www.britannica.com/topic/information-system/Computer-crime-and-abuse (дата обращения 21.03.2022).

38) ClaireLaybats, LukeTredinnick. Informationsecurity// ResearchGate. Июнь 2016 г. URL: https://www.researchgate.net/publication/303869808_Information_security (дата обращения: 18.12.2021).

39) Википедия: Свободная энциклопедия. Кевин Дэвид Митник // Материал из Википедии – свободной энциклопедии: [сайт]. – 2021. – URL: https://ru.wikipedia.org/wiki/Митник,_Кевин (дата обращения: 20.04.2023).

40) Информационная безопасность образовательных учреждений // «СёрчИнформ»: [сайт]. – 2019. – URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/ (дата обращения: 02.05.2023).

41) Меры по обеспечению информационной безопасности // «СёрчИнформ»: [сайт]. – 2019. – URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/mery-po-obespecheniyu-informatsionnoj-bezopasnosti/ (дата обращения: 13.05.2023).

42) Словари и энциклопедии на Академике. Доступность информации // Академик: [сайт]. – 2019. – URL: https://dic.academic.ru/dic.nsf/ruwiki/636300 (дата обращения: 02.05.2023).