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

Проверка на объем заимствований:
81,3 % авторского текста

Работа рекомендована/ не рекомендована
к защите
«10» 01 2024 г.
Зав. Кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ–309–210–2–1
Сидоров Владимир Сергеевич

Научный руководитель:
Зав. Кафедрой АТИТ и МОТД
доцент,к.т.н.
Руднев В.В.

Челябинск
2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете, киберпреступности и хакерах. Но для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование и развитие, то есть о пропаганде различной направленности. Кроме того, все еще слабо осознана та часть проблемы, которая связана с общением в социальных сетях, которые сегодня все чаще подменяют собой живое общение. В виртуальном пространстве действуют совершенно иные правила, где психически неокрепшая личность не может эффективно противостоять угрозам, запугиванию.

И сегодня именно этот фактор начинает выходить на первые роли в обеспечении информационной безопасности в ее широком понимании: не только технической, но и когнитивной сферы во всей ее полноте.

Зарубежный и отечественный опыт позволяет определить следующие угрозы информационной безопасности, которые стоят перед образовательными учреждениями:

- Несанкционированный доступ к данным. Эта группа угроз включает в себя подмену данных в электронных журналах, архивах, хищение информации экзаменационных билетов, личных данных учащихся и их родственников и т.п. В большинстве рекомендаций по организации схем обеспечения информационной безопасности специалисты ограничиваются только этой, технической сферой.
- Фильтрация нежелательной информации. Эта группа угроз напрямую связана с противодействием экстремистской идеологии, но не ограничивается только ей. При рассмотрении угроз доступа к нежелательной информации следует также учитывать вопросы провокационных материалов, пропаганды наркотиков и алкоголя и т.п.

- Проблемы регулирования использования социальных сетей. Именно в этой зоне осуществляется активное давление на учащихся, запугивание, а также сравнительно новый феномен киберхулиганства.
- Кибертерроризм. Несмотря на то, что эта группа угроз находится в ведении соответствующих силовых ведомств, частично она может решаться и на уровне учебных заведений. Создание безопасной информационно–технологической среды серьезно осложняет возможные кибератаки на объекты образования, которые могут привести к нарушению функционирования управляющих автоматических систем и последующему повреждению инфраструктуры. Следует, впрочем, отметить, что эта группа угроз остается пока во многом гипотетической, так как учебные заведения в силу низкой их насыщенности автоматизированными управляющими системами не рассматриваются в качестве приоритетных целей для кибератак.

Сегодня ни один сектор не застрахован от угрозы кибератаки. К сожалению, это относится к школам и университетам.

Объем данных, которыми располагают эти учреждения, более глубокое проникновение технологий в ежедневную деятельность учебных заведений и растущее число подключенных устройств делают этот сектор уязвимым для кибератак.

В учебных заведениях хранится значительное количество чувствительных и конфиденциальных данных, начиная от исследований и заканчивая экзаменационными заданиями, финансовыми данными и личной информацией студентов. Взлом или нарушение работы ИТ–систем учреждений образования может серьезно повлиять на репутацию, эффективность и непрерывность работы заведений.

Угрозы информационной безопасности в образовательных учреждениях:

• DDoS–атаки на веб–ресурсы

• Компрометация данных обучающихся при использовании веб–сервисов

• Эксплуатация уязвимостей устройств

• Компрометация конфиденциальных данных

• Распространение вредоносного ПО

• Нарушение непрерывной работы внутренних систем и сервисов

Задачи информационной безопасности в образовательных учреждениях:

• Обеспечение безопасности корпоративных ресурсов (информационная инфраструктура, веб–ресурсы);

• Защита конечных устройств;

• Защита чувствительной информации и персональных данных;

• Соответствие требованиям регуляторов;

• Предотвращение утечек информации;

• Выявление внутренних злоупотреблений и нелояльных сотрудников. Противодействие различным угрозам информационной безопасности должна вестись на нескольких уровнях, а носить комплексный характер.

Меры защиты:

- Нормативно–правовые
- Административно–организационные
- Физические
- Технические

Решения кибербезопасности в образовательных учреждения:

- Регулярные ИБ тренинги – для повышения осведомленности персонала в вопросах информационной безопасности;
- Аудит информационной безопасности и инструменты сканирования сети для обнаружения и предотвращения эксплуатации уязвимостей, своевременного патчинга;
- Корректная сегментация сети – для лучшего контроля сетевого трафика и повышения эффективности систем кибербезопасности;
- Межсетевые экраны и системы обнаружения и предотвращения вторжений (IDS/IPS) – для защита периметра сети, блокировка

несанкционированного доступа, ограничения доступа к сторонним веб–ресурсам и обнаружения потенциально вредоносного трафика;

- WAF (Web Application Firewall) – для защиты веб–ресурсов с помощью межсетевых экранов приложений от таких атак, как межсайтовая подделка запроса (CSRF), межсайтовыйскриптинг (XSS), SQL–инъекция и других угроз;
- Защита конечных точек для снижения риска заражения программами и вирусами, шифрования информации, соблюдения соответствия политикам и регламентам ИБ;
- Организация безопасного удаленного доступа к сети через VPN;
- СЗИ от НСД – для защиты стационарных и мобильных устройств от несанкционированного доступа, а также обеспечения соответствия требованиям регуляторов;
- DLP системы – для предотвращения утечки конфиденциальных материалов, а именно анализа и блокировки данных, передаваемых с помощью электронной почты, мессенджеров, интернет–ресурсов и других источников;
- Системы управления доступом (IDM, PIM) – для контроля жизненного цикла учетных записей и разграничения прав доступа к сегментам сети;
- Решения для управления сетевым доступом (NAC) – для инвентаризации устройств, обеспечения видимости и контроля подключений к корпоративной сети;
- Системы классификации данных для повышения безопасности конфиденциальной информации путем классификации, определения пользователей, взаимодействовавших с документами, упрощения доступа, поиска и отслеживания данных, а также устранения дублирований.

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 применение 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 модель причинения вреда информационной системе образовательной организации при несанкционированных доступах.

4) 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.

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

Теоретической и методологической основой исследования являются разработки зарубежных и отечественных авторов в сфере информационной безопасности в различных секторах, а также материалы научных статей.

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.

Базой проведения исследования стал ГБПОУ «Челябинский радиотехнический техникум».

Личное участие соискателя состоит в теоретико–методическом обосновании и применение вероятностной модели причинения вреда информационной системы на базе ГБПОУ «Челябинский радиотехнический техникум» 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

Образовательный процесс касается наименее защищённых 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 школы и института любой пропаганды, как незаконного характера, так и безобидной, но предполагающей воздействие на сознание учащихся в заведениях среднего полного общего и высшего образования.

В понятие информационной безопасности образовательного учреждения 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 [8].

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

- персональные сведения, касающиеся учащихся и преподавателей, оцифрованные архивы;
- ноу–хау образовательного процесса, носящие характер интеллектуальной собственности и защищённые законом;

- 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:

- доступности в любое время для любого авторизированного пользователя;
- защиты от любой утраты или внесения несанкционированных изменений;
- конфиденциальности, недоступности для третьих лиц [7].

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов данных 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 жёстких 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, 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 её 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 ребёнка в криминал и терроризм [17].

Фишинг (от англ. fishing — рыбачить, выуживать) — это вид кибератаки, при которой злоумышленник пытается получить доступ к личной информации пользователя, например к логину и паролю от электронной почты или данным банковской карты.

Фишинг отличается от других видов хакерских атак тем, что мошенники активно манипулируют базовыми человеческими эмоциями, такими как любопытство и страх, а также используют информацию, которые смогли собрать из открытых источников о человеке.

Фишинг по электронной почте

Самый распространенный вид фишинга. Этот тип атаки использует такие приемы, как фальшивые гиперссылки, чтобы заманить получателей электронной почты и заставить их поделиться своей личной информацией. Злоумышленники часто маскируются под крупных поставщиков учетных записей, таких как Microsoft или Google, или даже под коллег по работе.

Вредоносный фишинг

Еще один распространенный метод фишинга. Этот тип атаки предполагает установку вредоносного ПО, замаскированного под надежное вложение (например, резюме или банковскую выписку) в электронном письме. В некоторых случаях открытие вложения с вредоносным ПО может парализовать работу всей ИТ–системы.

Целевой фишинг

Большинство фишинговых атак охватывают широкую сеть людей, однако существуют и целевой фишинг, который адресован конкретным людям и использует информацию, собранную в ходе изучения их работы и социальной жизни. Эти атаки отличаются высокой степенью адаптации, что делает их особенно эффективными при обходе базового уровня системы кибербезопасности.

Уэйлинг–мошенничество

Когда злоумышленники нацеливаются на "крупную рыбу", такую как руководитель предприятия или знаменитость, это называется уйэлингом (whaling — китобойный промысел). В этом случае мошенники часто проводят значительные исследования своих целей, чтобы найти удобный момент для кражи учетных данных или другой конфиденциальной информации. Если вам есть, что терять, злоумышленникам есть, что украсть.

Смишинг

Сочетание слов "SMS" и "фишинг" означает отправку текстовых сообщений, замаскированных под надежные сообщения от таких компаний, как Amazon или FedEx. Люди особенно уязвимы для SMS–мошенников, поскольку текстовые сообщения – это обычный текст, который воспринимается более лично.

Вишинг

В кампаниях вишинга злоумышленники в мошеннических колл–центрах пытаются обманом заставить людей предоставить конфиденциальную информацию по телефону. Во многих случаях эти мошенники используют социальную инженерию, чтобы обмануть жертв и заставить их установить на свои устройства вредоносное ПО в виде приложения [15].

Преступления в сфере компьютерной информации – предусмотренные уголовным законом общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов.

К указанным преступлениям относятся: неправомерный доступ к компьютерной информации (ст. 272 Уголовного кодекса Российской Федерации (далее – УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей (ст. 274 УК).

Неправомерный доступ к компьютерной информации (ст. 272 УК) имеет предметом охраняемую законом компьютерную информацию, т.е. сведения

(сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (примечание 1 к данной статье).

Для признания информации охраняемой законом необходимо, чтобы:

а) закон (иной нормативный правовой акт) давал основание для защиты данных от несанкционированного доступа.

б) законный обладатель информации предпринимал меры по ее охране.

Доступ к компьютерной информации означает получение возможности знакомиться с информацией и использовать ее.

Принципиальным является доступ именно к информации, а не только к ее носителю. Получение сведений происходит посредством проникновения в ЭВМ, систему ЭВМ или их сеть (непосредственно или через удаленный доступ) либо путем перехвата компьютерной информации (подключение к коммуникационным каналам или узлам передачи данных; улавливание остаточного излучения монитора, принтера, других устройств).

Неправомерность доступа означает, что субъект не имеет права получать и использовать информацию. Наличие или отсутствие такого права может не зависеть от воли законного обладателя сведений. Например, разрешение банковского служащего на получение и использование информации о состоянии счетов клиентов не исключает ответственности за доступ к этим данным.

Деяние признается преступлением, если повлекло уничтожение компьютерной информации, ее блокирование, модификацию либо копирование. Под уничтожением компьютерной информации понимается ее исчезновение с носителя без возможности восстановления. Блокирование сведений предполагает невозможность законного доступа к ним при их сохранности. Модификацией информации являются любые ее изменения, кроме трансформации компьютерной программы или базы данных, осуществляемой в целях их функционирования на конкретных технических средствах пользователя или под управлением конкретных программ пользователя. Копирование данных означает их дублирование.

Физическое выражение и формат копии могут отличаться от оригинала. Это возможно при фотографировании сведений с монитора, переписывании от руки.

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

Можно выделить несколько видов несанкционированного доступа:

1. Человеческий. Информация может быть похищена путём 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.

Борьба с различными видами атак на информационную безопасность должна вестись на пяти уровнях, причём работа должна носить комплексный характер. Существует ряд методических разработок, которые позволят построить защиту образовательного учреждения на необходимом уровне [13].

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

Образовательный процесс в ГБПОУ «Челябинский радиотехнический техникум» реализуется в учебно–лабораторном корпусе общей площадью 4013 кв.м., который включает в себя современные учебные лаборатории и мастерские, 8 компьютерных классов, лаборатории виртуальных и цифровых измерительных

приборов, электронной техники, регулировки радиоэлектронной аппаратуры, компьютерных сетей и многие другие. Кроме того, техникум располагает современным оборудованным тренажерным залом, лыжной базой (спорткомплекс «Полет») и открытой спортивной площадкой.

Введен в эксплуатацию кластер серверов из девяти узлов Huawei FusionServer 2288H V5 на базе процессора Intel Xeon Gold 6148: 360 Cores/ 720 Threads/ 2.4 GHz/ 3456 Gb DDR4 RDIMM ECC/ и Система хранения данных Huawei OceanStorDorado5000 V3: 25x1.8TB SSD SAS Disk плюс Полка расширения для СХД Huawei Dorado V3 SSD SAS Disk EnclosureDV3–SDAE25U2–AC: 12x3.84TB SSD SAS Disk, а также СХД Huawei OceanStor 5110 V5 Backup Storage: 12x10TB NL SAS Disk

В процессе обучения используются лицензионные программные продукты, приобретенные по программам Open License, по подписке AzureDev Tools for Teaching, в рамках схемы лицензирования Classroom, Adobe Creative Cloud for Teams и 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях, либо используются в рамках лицензий свободного или открытого программного обеспечения.

Все компьютерные классы объединены в локальную сеть с использованием активного сетевого оборудования Huawei и HP (3Com). Персональные компьютеры используют современные технологии виртуализации. Вся локальная сеть использует гигабитные интерфейсы для поддержания высокого уровня производительности. Мобильный класс имеет собственную беспроводную сеть и может быть развернут в любом требуемом месте для проведения занятий. Для обеспечения необходимого качества и эффективности учебного процесса имеется подключение к сети интернет, со скоростью доступа 300 Мбит/сек (по данным http://pr–cy.ru/speed_test_internet/ 283 Мбит/сек). Подключение организуется по выделенной оптоволоконной линии связи. Фильтрация контента осуществляется при помощи универсального шлюза безопасности Ideco ICS,

Фильтрация по категориям. В качестве антивирусного решения используется Kaspersky EndpointSecurity для бизнеса расширенный.

С 2017 года ГБПОУ «Челябинский радиотехнический техникум» является региональной Сетевой площадкой по Программе модернизации среднего профессионального образования Челябинской области на основе развития инновационной сети распространения лучших практик подготовки кадров по перечню наиболее востребованных, новых и перспективных профессий и специальностей среднего профессионального образования (Приказ Минобрнауки Челябинской области от 27.11.2017 № 01/3577) в области «Информационные и коммуникационные технологии», реализуемой в рамках Федеральной целевой программы развития образования на 2016–2020 годы. В рамках реализации данной программы планируется существенное укрепление материальной технической базы по всем реализуемым специальностям.

Учебный процесс в Техникуме, методическую и воспитательную работу осуществляет квалифицированный педагогический коллектив. Коллектив преподавателей и сотрудников отличается высоким профессионализмом, стабильностью и опытом практической работы, что позволяет максимально приблизить учебный процесс к требованиям производства и проводить занятия на высоком уровне. За последние годы существенно укрепилась материально–техническая база техникума, значительно усилена компьютерная база, что позволяет применять современные компьютерные обучающие технологии при изучении дисциплин.

Для проведения анализа уязвимостей существующей системы информационной безопасности ГБПОУ «Челябинский радиотехнический техникум» наиболее подходящим методом является разработка модели угроз.

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

– Федеральный закон №152–ФЗ «О персональных данных»:

Глава 1 Статья 2. Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Глава 2 Статья 19

«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 приказом ФСТЭК РФ от 11.02.2013 № 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"): «Формирование требований к защите информации… в том числе включает: …определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в 21 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 14.03.2014 N 31 (ред. от 15.03.2021) "Об утверждении Требований 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"): «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 25.12.2017 N 239 (ред. от 20.02.2020) "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"): «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 «Челябинский радиотехнический техникум» очевидна. Наполнение модели угроз описывается в приказе ФСТЭК РФ от 11.02.2013 № 17 "Об утверждении требований о защите информации, не составляющей

государственную тайну, содержащейся в государственных информационных системах": 22 «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 информационной безопасности 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».

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 «Челябинский радиотехнический техникум», она представлена в таблице 1.

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 «Челябинский радиотехнический техникум»

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные

1. По состоянию источника информации						
1.1 Вне зоны действия/видимости ИС (перехват данных во время прохождения каналами связи)	Низкая	Низкая	Средняя	Неактуальна		Ограничение доступа на охраняемый объект
1.2 В пределах видимости ИС (например, подслушивающие устройства)	Низкая	Низкая	Низкая	Неактуальна	Регулярный мониторинг функционирования рабочих станций	
2. По степени преднамеренного проявления						
2.1 Угрозы преднамеренного действия	Средняя	Средняя	Высокая	Неактуальна	Установка Защитного ПО	
2.2 Угрозы случайного действия и/или угрозы, вызванные халатностью персонала	Средняя	Низкая	Низкая	Неактуальна	Учет носителей Инструктаж персонала	
3. По непосредственному источнику угроз						
3.1 Угрозы, непосредственным источником,	Средняя	Средняя	Низкая	Неактуальна	Инструктаж персонала	

которого является человек					Резервное копирование информации	
3.2 Угрозы, непосредственным источником, которого являются санкционированные программно–аппаратные средства	Средняя	Средняя	Низкая	Неактуальна	Настройка средств защиты	
3.3 Угрозы, непосредственным источником, которого является природная среда	Низкая	Низкая	Низкая	Неактуальна		
4. По положению источника угроз						
4.1 Угрозы, источник которых находится вне контролируемой зоны	Средняя	Средняя	Низкая	Неактуальна	Настройка средств защиты	
4.2 Угрозы, источник которых находится в пределах контролируемой зоны	Средняя	Средняя	Низкая	Неактуальна	Резервное копирование информации	
5. По текущему месту расположения информации, хранимой и обрабатываемой в АС						
5.1. Угрозы доступа к информации на внешних запоминающих устройствах	Средняя	Средняя	Средняя	Неактуальна	Учет носителей	
5.2. Угрозы доступа к информации в	Средняя	Низкая	Средняя	Неактуальна	Хранение носителей, исключающих	

оперативной памяти					несанкцион ированный доступ	

Таким образом, нами проведен первичный аудит состояния защищенности информационной системы образовательной организации ГБПОУ «Челябинский радиотехнический техникум» на основании нормативных документов, рекомендованных ФСТЭК: были определены основные угрозы информационной безопасности, сделан предварительный анализ возможности реализации угроз, проанализированы существующие в ГБПОУ «Челябинский радиотехнический техникум» 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 ГБПОУ «Челябинский радиотехнический техникум»)

На сегодняшний день все имеющиеся модели угроз безопасности информации носят весьма условный характер. Нет единого принципа построения модели угроз. Существуют несколько подходов, и всем им присущи принципиальные недостатки, а именно: отсутствие четкого понятия «модели угроз», разительное отличие структур и принципов функционирования моделей, способов применения модели, избыточность модели в виде слияния с моделью нарушителя и многое другое.

Наличие этих и некоторых других пробелов в существующих подходах отрицательно сказывается на эффективности работы эксперта с самой моделью и на конечном результате, обусловленном отсутствием стандартизованных итоговых оценок одной модели угроз относительно другой. Поэтому задачей настоящего исследования является создание собственной модели угроз информации.

В статье Грибановой–Подкиной М.Ю. представлен подход к построению модели угроз информационной безопасности информационной системы с использованием методологии объектно–ориентированного проектирования.

Данный подход предполагает активное использование UML–диаграмм при описании концептуальной модели угроз информационной безопасности, способов реализации угроз, сценариев реализации угрозы и сценариев защиты. В русле данного подхода с помощью языка UML и CASE–средства Enterprise Architect разработана и описана объектно–ориентированная модель угроз информационной безопасности для распределенной информационной системы. Полученная модель может быть органично встроена в комплект документации по информационной безопасности информационной системы.

Разработанные с помощью нотации UML модели угроз и сценариев позволят эффективнее взаимодействовать информационным аналитикам и специалистам по информационной безопасности с целью обеспечения защиты информационных систем от угроз информационной безопасности [9].

Согласно исследованиям О.А. Козлов, Л.А. Гузикова комплекс мер по обеспечению информационной безопасности должен включать:

- правовые (законодательные) меры;
- технологические меры;
- организационные (административные и процедурные) меры; технические (физические, аппаратные и программные) средства;
- морально–этические нормы;
- средства мониторинга эффективности.

При создании системы информационной безопасности в образовательной организации необходимо учитывать ключевые характеристики информационной среды, в рамках которой реализуется сетевое взаимодействие.

Такая среда обладает следующими свойствами:

- она создана и поддерживается для конкретных целей;
- она является динамичной;

- она является быстрой;
- она относительно безгранична;
- она имеет низкие входные барьеры;
- она быстро растет;
- ее можно рассматривать с позиций различных структур, которые неизбежно формируют представления о соответствующем поведении и ценностях [14].

В статье Жарникова, Ю. С. Угрозы информационной безопасности образовательного учреждения информационную безопасность образовательного учреждения рассматривают, как состояние защищенности персональных данных субъектов образовательного процесса, обучающихся от информации, причиняющей вред их здоровью и развитию, информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. При создании системы защиты информации в образовательном учреждении обязательно необходимо учитывать те угрозы, которые могут возникнуть.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

- По природе возникновения (естественные и искусственные)

Естественные – это те угрозы, которые возникли в результате какого–либо природного катаклизма (землетрясения, наводнения и др.);

Искусственные – результат деятельности человека.

- По степени преднамеренности:

Случайные – угрозы, вызванные ошибками или халатностью персонала; Преднамеренные – возникают в результате целенаправленной деятельности злоумышленников.

- По аспекту информационной безопасности:

Угрозы конфиденциальности, угрозы целостности, угрозы доступности.

- По компонентам, на которые нацелена угроза:

Данные, программное обеспечение, аппаратное обеспечение [10].

В статье Золотарева В.В. и Лапиной М.А. Модель и алгоритм управления информационной безопасностью образовательной организации высшего образования с учетом требований управления на основе данных приведенная автором модель сосредоточена на формировании пригодных в практике рекомендаций по построению процессной модели управления информационной безопасности, учитывающей как традиционные рассматриваемые уровни управления инфраструктурой информационной системы и управления организационными процессами, так и новые, расширяющие модель уровень данных, рассмотренный в настоящей работе, и уровень знаний.

Подобное расширение может быть полезно при развертывании разных типов экспертных и советующих систем, систем поддержки принятия решений, ситуационных центров и особенно интересно для задач переходных состояний, которые возможно рассмотреть в отдельных исследования.

В исследовании предлагается использовать измеряемые количественные признаки, пригодные для оценки устойчивых связей поддерживающих процессов управления информационной безопасностью. Уровень управления данными будет рассмотрен с использованием требований программ цифровой трансформации, разработанных в университетах в 2021 году.

Каждая из таких моделей, к примеру, должна включать уровень управления данными, что может создать основу для решаемых в настоящем исследовании задач управления информационной безопасностью, и при этом генерирует множественные вариации этой задачи в переходных состояниях, некоторые примеры которых будут рассмотрены ниже.

В целом, для дальнейшего рассмотрения можно учесть следующее. Согласно программе цифровой трансформации, «целевой моделью университета, с позиций цифровой трансформации, является формирование единого цифрового образовательного и научного пространства. При этом глобально университет должен представлять комплекс цифровых возможностей, транслирующих идею

цифровой трансформации всем участникам образовательного процесса и заинтересованным сторонам через цифровые сервисы, элементы цифровой среды, инфраструктуру и исследовательские задачи». Но это, как видно из формулировки, требует пересборки как поддерживающих процессов на уровне самого университета, так и на уровне заинтересованных в участии в таком взаимодействии сторон.

Управление информационной безопасностью, безусловно, часть указанного процесса трансформации. В основе своей это является следствием продолжающейся цифровой трансформации образовательного процесса.

Управление информационной безопасностью в целом должно генерировать базовые процессы, применимые в задаче, такие как:

- управление требованиями к безопасности хранения, обработки, синтеза и анализа данных образовательного контента и цифрового следа;
- реализация процедур и сценариев обеспечения непрерывности образовательного контента, включая сценарии нарушения работоспособности при развертывании виртуальных стендов и контроля целостности цифровых двойников рабочих программ дисциплин;
- обучающие сценарии и сценарии оповещения при администрировании организационной и технической части образовательного процесса, в том числе и обучение действиям на основе стресс–тестов;
- управление уязвимостями используемого программного обеспечения для виртуальных лабораторий и виртуальной инфраструктуры в целом;
- управление рисками, включая правовые и юридические моменты, при формировании и использовании цифровых двойников дисциплин, рабочих программ, лабораторий и программных (программно–аппаратных) средств защиты информации (в рамках рассматриваемой проблематики); для иных областей образования – программных (программно–аппаратных) средств, используемых для формирования образовательного контента цифрового двойника дисциплины;

- управление инцидентами;
- целостное и непрерывное управление изменениями образовательного контента и цифровых двойников, включая процедуры синхронизации.–

Далее будет показан план развертывания поддерживающих процессов в различных моделях управления информационной безопасностью.

К примеру, акцентируя внимание на управляющих системах индустриального типа, изучают отличия подхода к построению систем управления информационной безопасностью промышленных систем от стандартного подхода, как на уровне свойств безопасности, так и на уровне стандартных требований.

Интересным в плане настоящего исследования в упомянутой работе является отслеживание типового информационного потока и сопоставление различных требований безопасности по областям их применения.

В исследовании проводится анализ стандартов безопасности для улучшения их управления информационной безопасностью.

Дедуктивный метод был применен для обзора и анализа соответствующих стандартов для государственных учреждений.

В результате была получена информация о различных политиках безопасности, стандартах и руководствах, которые применяются национальными и международными общественными организациями.

Приведена схема мероприятий по принятию стандартов для организаций, модель управления информационной безопасностью, основанная на стандартах и матрица управления информационной безопасностью, на основе которой был рассчитан процент снижения риска.

Получены результаты, что поддержание высокого уровня безопасности в организациях требует принятия стандартов контроля в разных сферах и взаимодействия различных организационно–иерархических уровней организаций.

Формируя модель управления информационной безопасностью, сосредоточились на оптимизационной задаче, отталкиваясь от ограниченности ресурсов. Подход авторов статьи заключается в возможности многоуровневой

(отличающейся по сложности и ресурсоемкости) системы защиты и риск–ориентированном порядке действий.

В статье изучаются требования к сервис–ориентированным платформам с позиций управления безопасностью. Для информационных систем образовательных учреждений это имеет значение с позиций изучения управляющих механизмов безопасности центрального ядра электронно–информационной образовательной среды и развернутой в ней цифровых сервисов.

В работе показано, каким образом, возможно, учесть для управляющих механизмов безопасности информационной среды, дестабилизирующие факторы в условиях неопределенности, что может быть применено и для переходных состояний различного типа, и для ситуаций (сценариев) с неполной информацией. Авторы же сосредоточились на задачах оценки зрелости организаций (и организационных структур).

Даже краткие обзоры работ показывают, что, к примеру, нормой при развертывании системы управления информационной безопасностью является конфликт интересов, дублирование задач, снижение эффективности использования ресурсов, а учет движения данных и задач работы с ними, не говоря уже о более абстрактных уровнях приложения управляющих воздействий, остается в тени инфраструктурных и организационных задач.

Следовательно, такие модели управления информационной безопасностью, которые могут учитывать и требования к работе с данными, и более высокие уровни абстракции, могут быть востребованы на практике при дальнейшем росте уровня зрелости организаций в области информационной безопасности. Далее авторами и показаны особенности работы с процессами управления информационной безопасности с учетом нового слоя процессов управления данными.

Уровни модели управления информационной безопасностью. Начнем рассмотрение с общей схемы, учитывающей особенности цифровой трансформации ООВО, представленной на рисунке 1.

Принципиальные изменения, декларируемые в ней, следующие:

1. Появляется отдельный класс систем управления на основе данных, которые необходимо использовать в работе.

2. Появляются множественные информационные потоки, ранее не представленные (или представленные фрагментарно) в системах управления ООВО.

Управления знаниями здесь нет, но создаются предпосылки для массового использования одной или нескольких агрегированных баз данных, что генерирует задачи управления информационной безопасностью как самих этих баз, так и доступом к ним.

Поддерживающие процессы

Рисунок 1 – Схема функционирования университета по завершению цифровой трансформации (КЦЭ – компетенция цифровой экономики, ОП -образовательный процесс)

Рассмотрим общую модель управления информационной безопасностью образовательной организации высшего образования с учетом требований управления данными на схеме ниже (рис. 2)

Рисунок 2- Модель управления информационной безопасностью образовательной организации высшего образования с учетом требований управления данных

Итак, в данном случае требования к управлению данными должны быть дополнены требованиями управления информационной безопасностью для агрегированных баз, используемых для принятия решений. Далее на основе современного стандарта, регламентирующего практические правила управления информационной безопасностью, показаны применимые (и недостающие) процессы управления ИБ (табл. 2).

Акцентирование внимание на четырех основных процессах – сбора, валидации, верификации и использования данных позволяет как использование принципа, который можно сформулировать так: все данные, собираемые внутри систем и процессов ООВО, должны быть доступны для использования в любых процессах, в которых они могут понадобиться (принцип максимальной полезности), так и особенность самой деятельности по сбору, анализу и использованию данных, которая предполагает агрегирование, но не обязательно требует централизации (синхронизированные децентрализованные базы данных и некоторые другие решения также применимы). Таким образом, далее описано управление ИБ универсальных процессов уровня управления данными [11].

Таблица 2 – Применимые (и недостающие) процессы управления ИБ для уровня данных

Процесс	Назначение	Требование	Примечание
Сбор данных	Назначение ролей и обязанностей	Ограничение доступа к данным (не все	ГОСТ Р ИСО/МЭК 27002–2021, п.6.1.1,6.1.2,6.1.5 (применимо)

	по контролю, анализу и технологии безопасного сбора данных Разделение обязанностей в области безопасного сбора и анализа данных Минимизация полномочий Обеспечение информационной безопасности при управлении проектами	данные должны подлежать автоматическому или автоматизированному сбору), ограниченные по ролям и обязанностям Срок хранение и место хранения, а также условия хранения должны быть определены	
Верификация данных	Назначение ролей и обязанностей по контролю, анализу и технологии безопасной	Ограничение доступа к источникам вспомогательных данных для верификации (записям, документам,	ГОСТ Р ИСО/МЭК 27002–2021, п.6.1.1,6.1.3,6.1.4 (применимо)

	верификации данных Разделение обязанностей в области безопасной верификации данных Минимизация полномочий Обеспечение информационной безопасности при взаимодействии с органами власти и профессиональными сообществами	регистрационным данным) Ограничение доступа к данным для случая запроса внешних заинтересованных лиц Ограничения доступа к данным для случая запроса внутренних заинтересованных лиц	
Валидация данных	Назначение ролей и обязанностей по безопасной валидации данных Разделение обязанностей в	Ограничения доступа к тестовым и имитационным моделям управления качеством	ГОСТ Р ИСО/МЭК 27002–2021, п.6.1.1 (применимо)

	области безопасного анализа данных Минимизация полномочий	Ограничение доступа к источникам вспомогательных данных для валидации (записям, документам, регистрационным данным)	
Использование данных	Разделение обязанностей в области безопасного использования данных Минимизация полномочий Обеспечение информационной безопасности при взаимодействии с органами власти и профессиональными сообществами	Управление доступом к данным на всех этапах жизненного цикла	ГОСТ Р ИСО/МЭК 27002–2021, п.6.1.1,6.1.3,6.1.4 (применимо)

Общие процессы	Моделирование бизнес–процессов в области информационной безопасности (ИБ) для уровня данных Реализация политики управления данными в части ИБ Оценка и контроль защищенности уровня данных модели управления ИБ Управление активами, связанными с данными Управление доступом к данным Резервное копирование	Ограничение доступа к данным используемым для формирования моделей чувствительных процессов ООВО Учет требований при формировании руководящих указаний в части ИБ	ГОСТ Р ИСО/МЭК 27002–2021,п.5.1,п.6.2,п.8,п.9,п.12.3,п.13,п.14.3,п.18 (применимо)

	Управление коммуникациями Управление тестовыми данными		

Выводы по главе I

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

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

В понятие информационной безопасности образовательного учреждения 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.

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

В ГБПОУ «Челябинском радиотехническом техникуме» Kaspersky EndpointSecurity для бизнеса расширенный.

С 2017 года ГБПОУ «Челябинский радиотехнический техникум» является региональной Сетевой площадкой по Программе модернизации среднего профессионального образования Челябинской области на основе развития инновационной сети распространения лучших практик подготовки кадров по перечню наиболее востребованных, новых и перспективных профессий и

специальностей среднего профессионального образования (Приказ Минобрнауки Челябинской области от 27.11.2017 № 01/3577) в области «Информационные и коммуникационные технологии», реализуемой в рамках Федеральной целевой программы развития образования на 2016–2020 годы. В рамках реализации данной программы планируется существенное укрепление материальной технической базы по всем реализуемым специальностям.

Для проведения анализа уязвимостей существующей системы информационной безопасности ГБПОУ «Челябинского радиотехнического техникума» наиболее подходящим методом является разработка модели угроз.

В третьем параграфе первой главы была представлена в общем виде модель причинения вреда информационной системе образовательной организации ГБПОУ «Челябинский радиотехнический техникум».

2 ГЛАВА ОПЫТНО–ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО ПРИМЕНЕНИЮ МОДЕЛИ ПРИЧИНЕНИЯ ВРЕДА ИНФОРМАЦИОННОЙ СИСТЕМЕ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

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

Информация играет важную роль в информационных технологиях и имеет большое значение в современном мире. Она является основным ресурсом, который обрабатывается и передается с помощью технологий и информационных систем.

Значение информации в информационных технологиях можно выделить в нескольких составляющих:

- Хранение и передача данных. Информация хранится в компьютерных системах и базах данных, которые обеспечивают ее доступность и сохранность. С помощью информационных технологий данные предоставляются в разных форматах в виде данных и по разным каналам связи.
- Обработка и анализ данных. С помощью информационных технологий можно исследовать и анализировать большие объёмы данных, выделять важную информацию и выявлять полезные знания. Это позволяет делать различные прогнозы, принимать взвешенные решения и оптимизировать бизнес–процессы.
- Коммуникация и обмен информацией. Информационные технологии обеспечивают возможность коммуникации и обмена информацией между людьми, организациями и компьютерными системами. С помощью интернета и сетей связи мы можем общаться, передавать файлы, делиться знаниями и информацией.
- Автоматизация и оптимизация процессов.

Информационные технологии позволяют автоматизировать различные процессы и управлять ими с помощью компьютерных программ. Это значительно увеличивает эффективность и точность работы, снижает вероятность ошибок и позволяет реагировать на изменения в реальном времени.

Таким образом, информация является ценным ресурсом и одним из главных компонентов информационных технологий. Она обеспечивает доступ к знаниям, позволяет делать взвешенные решения и оптимизировать различные процессы.

В современном мире умение работать с информацией и использовать ее в информационных технологиях становится все более важным и востребованным навыком.

А самой главной проблемой информационной безопасности является несанкционированный доступ.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Основными причинами осуществления несанкционированного доступа выступают ошибки конфигурации, слабая защищенность средств авторизации, злоупотребление служебными полномочиями, ошибки в программном обеспечении.

Несанкционированный доступ к информации может повлечь за собой множество последствий. Наиболее часто происходят утечка персональных данных, служебной переписки, коммерческой или государственной тайны.

Несанкционированный доступ к информации (НСД) может быть получен разными способами. Прямое хищение документов или взлом операционных систем компьютеров составляют лишь малую часть возможных вариантов. Наиболее уязвимыми считаются электронные средства хранения информации, так как для них могут быть использованы удаленные методы управления и контроля.

Возможные варианты получения незаконного доступа:

- подключение к системам связи (телефонные линии, интеркомы, проводные переговорные устройства);
- хищение документации, в том числе ее копирование (тиражирование) с враждебными целями;
- непосредственное использование компьютеров, внешних накопителей или иных устройств, содержащих информацию;
- внедрение в операционную систему через Интернет, в том числе с использованием шпионских программ, вирусов и прочего вредоносного программного обеспечения;

- использование сотрудников компании (инсайдеров) в качестве источников сведений.

Основные принципы защиты от НСД

1.Защита средства вычислительной техники (СВТ) и автоматизированные системы (АС) основывается на положениях и требованиях существующих законов, стандартов и нормативно–методических документов по защите от НСД к информации.

2.Защита СВТ обеспечивается комплексом программно–технических средств.

3.Защита АС обеспечивается комплексом программно–технических средств и поддерживающих их организационных мер.

4.Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

5.Программно–технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

6.Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

Классификация автоматизированных систем и требования по защите информации» [4]:

1.подсистема управления доступом;

2.подсистема регистрации и учета;

3.подсистема обеспечения целостности.

Методика защиты конфиденциальной информации в АС от НСД состоит из трех основных этапов [18]:

1. Планирование;

2. Тестирование;

3. Анализ результатов.

На этапе планирования проводится анализ всех исходных данных и документации по АС, в частности анализ защищаемых информационных ресурсов, структуры АС, а также целей и задач системы защиты конфиденциальной информации в АС от НСД. Перед началом тестирования необходимо установить, что в документации на объект испытаний декларируется соответствие АС требованиям 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.
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. 2. 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). 3. 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. 4. 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	1. Провести идентификацию программ путем их запуска (через «Проводник») и проверить их соответствие заданным параметрам.

средствами ОС и средствами установленных на СЗИ от НСД	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).
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 режим	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.
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.
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 5.

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 [19].

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 Применение модели причинения вреда на базе ГБПОУ «Челябинский радиотехнический техникум».

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.[12].

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 [6].

Адаптируем предложенную в методику для условий нашей экспериментальной работы, планируем работы по следующим этапам [16].

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

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	Происходит доступ в систему с правильно введенным логином и паролем Вход в ОС с неправильно введенным идентификатором (логином) и паролем – система сообщает об ошибке и предлагает повторно ввести идентификатор При многократном вводе неправильного идентификатора и пароля система временно блокируется и выдается сообщение о несанкционированных действиях(может быть и незаметно для пользователя)
Проверка соблюдения требований к паролю (длина пароля должна быть не менее 6 символов, пароль должен включать буквы и цифры)	Установку первичного пароля производит IT–специалист при создании новой учётной записи. Ответственность за сохранность первичного пароля лежит на администраторе, установившим данный пароль. При создании первичного пароля IT–специалист обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учётной записи о необходимости произвести смену пароля. Первичный пароль не используется при сбросе забытого пароля на учётную запись, необходима смена пароля. Установку основного пароля производит пользователь при первом входе в систему с новой учётной записью. Личные пароли должны выбираться

	администраторами и пользователями с учётом следующих требований: – длина пароля не менее шести символов; – пароль не должен включать ч себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, числа, сочетания цифр и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.); – пароль не должен содержать имени учётной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков; – содержать знаки трёх из четырёх перечисленных категорий: латинские заглавные буквы (от A до Z), латинские строчные буквы (от a до z), цифры (от 0 до 9), отличающиеся от букв и цифр знаки (например, !, $, #, %); – при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4–х позициях.
Проверка механизма идентификации внешних устройств по именам	Попытки загрузки с внешних носителей информации 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) 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 6

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 режим	Произведен выход из системы, а также вход в систему. Вход в ОС с неправильно введенным идентификатором (логином) и паролем – система сообщает об ошибке и предлагает повторно ввести идентификатор При выходе из спящего режима требуется ввести пароль. В журнале событий все фиксируется.
Проверка регистрации запуска и завершения программ	В журнале событий зафиксированы запуск и завершение программ, используемые для обработки защищаемой информации. .
Проверка регистрации попыток доступа к защищаемым файлам и каталогам	В журнале событий зафиксировано открытие и закрытие файлов и папок, содержащих защищаемую информацию, а 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 мусорное ведро.
Проверка регистрации и учета носителей защищаемой информации	Учет носителей защищаемой информации не проводится в журнале и не регистрируются. Носители защищаемой информации не уничтожаются, и не фиксируется записью об этом в журнале учета.

Проверка качества очистки освобождаемых областей памяти внешних накопителей и оперативной памяти	Очистка (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.

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 при помощи специализированных средств контроля защищенности.
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. 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 отсутствует.
Порядок проверки наличия средств восстановления	Средства восстановления программной среды компьютера имеются в наличии. Средства восстановления СЗИ от НСД имеются в наличии.
Проверка наличия средств антивирусной защиты	Средства антивирусной защиты имеются в наличии.

Заключительный этап

В пункте 1.3. была описана модель причинения вреда информационной системе образовательной организации.

Данная модель позволила нам рассмотреть необходимые действия по защите информационных ресурсов, такие как создание механизма быстрого реагирования на угрозы, своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, создание методов управления системой информационной безопасности, эффективное устранение незаконных атак на информацию ресурсы, создание методов обеспечения контроля за системой информационной безопасности.

На стадии применения модели были проведены все этапы согласно описанной модели, описанной в п.2.1. Анализ результатов проведенной методики представлено в виде таблице 10.

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

Проверяемое требование	Порядок действий при проверке	Соответствие норме
Проверка механизма идентификации и аутентификации субъектов доступа при входе в систему	Происходит доступ в систему с правильно введенным логином и паролем Вход в ОС с неправильно введенным идентификатором (логином) и паролем – система сообщает об ошибке и предлагает повторно ввести идентификатор При многократном вводе неправильного идентификатора и пароля система временно блокируется и выдается сообщение о несанкционированных действиях(может быть и незаметно для пользователя)	Соответствует норме

Проверка соблюдения требований к паролю (длина пароля должна быть не менее 6 символов, пароль должен включать буквы и цифры)	Установку первичного пароля производит IT–специалист при создании новой учётной записи. Ответственность за сохранность первичного пароля лежит на администраторе, установившим данный пароль. При создании первичного пароля IT–специалист обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учётной записи о необходимости произвести смену пароля. Первичный пароль не используется при сбросе забытого пароля на учётную запись, необходима смена пароля. Установку основного пароля производит пользователь при первом входе в систему с новой учётной записью. Личные пароли должны выбираться администраторами и пользователями с учётом следующих требований: – длина пароля не менее шести символов; – пароль не должен включать ч себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, числа, сочетания цифр и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.); – пароль не должен содержать имени учётной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков; – содержать знаки трёх из четырёх перечисленных	Соответствует норме

	категорий: латинские заглавные буквы (от A до Z), латинские строчные буквы (от a до z), цифры (от 0 до 9), отличающиеся от букв и цифр знаки (например, !, $, #, %); – при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4–х позициях.	
Проверка механизма идентификации внешних устройств по именам	Попытки загрузки с внешних носителей информации 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) 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 6	Соответствует норме
Проверка регистрации входа (выхода) пользователя в (из) ОС, входа (выхода) компьютера из спящего режим	Произведен выход из системы, а также вход в систему. Вход в ОС с неправильно введенным идентификатором (логином) и паролем –	Соответствует норме

	система сообщает об ошибке и предлагает повторно ввести идентификатор При выходе из спящего режима требуется ввести пароль. В журнале событий все фиксируется.	
Проверка регистрации запуска и завершения программ	В журнале событий зафиксированы запуск и завершение программ, используемые для обработки защищаемой информации. .	Соответствует норме
Проверка регистрации попыток доступа к защищаемым файлам и каталогам	В журнале событий зафиксировано открытие и закрытие файлов и папок, содержащих защищаемую информацию, а также создание файлов и папок.	Соответствует 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	Бракованные листы должны уничтожатся с помощью шредера в отдельном помещении.

	сотрудником, ответственным за вывод документов из АС. Бракованные листы выбрасываются в мусорное ведро.	
Проверка регистрации и учета носителей защищаемой информации	Учет носителей защищаемой информации проводится в журнале и регистрируется. Носители защищаемой информации уничтожаются, и фиксируются записью об этом в журнале учета.	Соответствует норме
Проверка качества очистки освобождаемых областей памяти внешних накопителей и оперативной памяти	Очистка (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.	Соответствует норме
Проверка обеспечения целостности программных СЗИ от НСД	Проверка обеспечения целостности программных СЗИ от НСД и неизменности программной среды не производится.	Проверка обеспечения целостности программных СЗИ от НСД и неизменности программной среды должна производится при помощи специализированных средств контроля защищенности
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. Возможность периодического тестирования СЗИ путем анализа применяемых разработчиком средств контроля целостности компонентов системного ПО,	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,

	реализующих функции СЗИ от НСД и наборов данных, используемых этими средствами отсутствует.	используемых этими средствами.
Порядок проверки наличия средств восстановления	Средства восстановления программной среды компьютера имеются в наличии. Средства восстановления СЗИ от НСД имеются в наличии.	Соответствует норме
Проверка наличия средств антивирусной защиты	Средства антивирусной защиты имеются в наличии.	Соответствует норме

Проведя анализ таблицы 10, мы можем утверждать, что есть необходимость в 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.

Таким образом, использованный метод позволил, наряду с потенциальным вероятностной моделью угроз, рассмотреть необходимые действия для защиты и предотвращения утечки информационных ресурсов, оценить текущее состояние безопасности и спланировать механизмы защиты.

2.3 Рекомендации на основе модели причинения вреда информационной системе образовательной организации ГБПОУ «Челябинский радиотехнический техникум»

В России принята «Национальная стратегия действий в интересах детей», определяющая степень угроз и меры защиты их безопасности. Действия по ограничению агрессивного воздействия на сознание ребёнка должны стать

основными. На втором месте должно оказаться обеспечение безопасности баз данных.

Защита информации опирается на действующие в этой сфере законы, определяющие отдельные её 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.

1.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 ребёнка», определяющие его права на защиту от сведений, которые могут причинить моральную травму. Необходимо создавать перечни документов, программ и иных источников, которые могут травмировать психику детей, в целях недопущения их проникновения на территорию учебного заведения. Это станет одной из основ информационной безопасности.

2.Административно–организационные меры

Этот комплекс мер целиком построен на создании внутренних правил и регламентов, определяющих порядок работы с информацией и её 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 ребёнка, запрет на пользование собственными носителями информации. Должно быть предусмотрено использование системы родительского контроля над ресурсами сети Интернет.

3.Физические меры

За данную систему мер и её 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 с 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.

4.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 разрешённых 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 ребёнка 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 ребёнок может получить дома. Необходимо просматривать страницы, посещаемые ребёнком. На основании анализа его поиска можно вносить изменения в перечень сайтов, доступ к которым ограничен с компьютеров, установленных в учебном заведении.

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 применению модели причинения вреда информационной системы образовательной организации.

Информация играет важную роль в информационных технологиях и имеет большое значение в современном мире. Она является основным ресурсом, который обрабатывается и передается с помощью технологий и информационных систем.

Дано определение понятию несанкционированный доступ — доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

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 применения 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 нужные средства и способы защиты необходим более детальный анализ угроз.

Рассмотрены дополнительные технические средства защиты информации.

Проанализированы уровни защиты от несанкционированного доступа к информационной системе.

Была применена 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.

ЗАКЛЮЧЕНИЕ

В ходе выполненного исследования были изучены аспекты безопасности информационной системы образовательной организации, обеспечение безопасности информационных систем образовательных организаций – важная задача, которая сегодня становится все более актуальной. Современные технологии не только помогают и ускоряют процессы обучения, но и повышают уровень угроз информационной безопасности.

Был проведен анализ актуального состояния защищенности информационной безопасности системы образовательной организации.

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.

Приведено применение модели причинения вреда информационной системы образовательной организации при несанкционированных доступах.

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.

Целью исследования было: теоретико–методическое обоснование и применение 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.

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.).

6) 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.pd f (дата обращения: 08.01.2024).

7) Бабаш А., Баранова Е., Ларин Д."Информационная безопасность. История защиты информации в России" (2015)

8) 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

9) Грибанова-Подкина М.А. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования //Научный журнал: вопросы безопасности. 2017.– URL: https://cyberleninka.ru/article/n/postroenie-modeli-ugroz-informatsionnoy-bezopasnosti-informatsionnoy-sistemy-s-ispolzovaniem-metodologii-obektno-orientirovannogo/viewer

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

11) Золотарев В.В., Лапина М.А. МОДЕЛЬ И АЛГОРИТМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ С УЧЕТОМ ТРЕБОВАНИЙ УПРАВЛЕНИЯ НА ОСНОВЕ ДАННЫХ//Прикаспийский журнал: управление и высокие технологии,№4 (60). 2022. – URL: https://cyberleninka.ru/article/n/model-i-algoritm-upravleniya-informatsionnoy-bezopasnostyu-obrazovatelnoy-organizatsii-vysshego-obrazovaniya-s-uchetom-trebovaniy/viewer

12) 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-zaschischennostiavtomatizirovannyh-sistem-ot-nesanktsionirovannogo-dostupa (дата обращения: 10.01.2024)

13) Кирьянов Д. Ю., Литвиненко А. А. Информационная безопасность: защита информации от несанкционированного доступа".М:2015

14) Козлов О.А., Гузиков Л.А. Информационная безопасность как условие деятельности образовательных организаций//Вопросы методики преподавания в вузе. 2017. Том 6. No 22 .– URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-uslovie-deyatelnosti-obrazovatelnyh-organizatsiy/viewer

15) Лэнс Джеймс Фишинг. Техника компьютерных преступлений : настольная книга программистов, сотрудников правоохранительных органов и

специалистов по компьютерной безопасности, методы обнаружения и защиты от сложнейших фишинговых атак, разоблачение методов высокоорганизованных фишинговых бандитов / Лэнс Джеймс ; [пер. с англ. Р. В. Гадицкого]. - Москва : NT Preaa, [2008]. - 314 с. : ил.; 24 см.

16) Михайловская, А. С. Методика контроля защищенности конфиденциальной информации в автоматизированной системе от несанкционированного доступа / А. С. Михайловская. — // Молодой ученый. — 2016. — № 12 (116). — С. 327- 331. — URL: https://moluch.ru/archive/116/31904/ (дата обращения: 14.01.2024)

17) Нестеров С. А. Н Основы информационной безопасности: Учебное пособие. — 3е изд., стер. — СПб.: Издательство «Лань», 2017. — 324 с. — (Учебники для вузов. Специальная литература).

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

19) Носкова, Т. Н. Проблемы воспитания средствами информационной образовательной среды [Текст]: Известия Российского 85 государственного педагогического университета им. А. И. Герцена / Т.Н. Носкова. – 2015. – № 177. – С. 61-69