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»

«КОНЦЕПЦИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ И СИСТЕМ КОНТРОЛЯ ДОСТУПА ДЛЯ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ»

Магистерская диссертация
по направлению 44.04.04 «Профессиональное обучение»,
программа магистратуры «Управление информационной безопасности
в профессиональном образовании»

Проверка на объем заимствований:
74,99 % авторского текста
Работа рекомендована к защите
«13» мая 2023 г.
Зав. кафедрой АТ, ИТ и МОТД
_____ к.т.н., доцент, Руднев В.В.

Выполнил:
Магистрант группы ОФ-209/210-2-1
Никитин Юрий Владимирович
Научный руководитель:
Профессор кафедры
Белевитин Владимир Анатольевич

Челябинск, 2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На сегодняшний день, образовательные организации испытывают трудности в обеспечении информационной безопасности и контроля доступа к локальным вычислительным сетям. ЛВС являются основой для построения и функционирования всех информационных систем образовательных организаций.

Информационная безопасность – это поддержание инфраструктуры от намеренных либо случайных влияний искусственного или естественного характера, которые имеют все шансы причинить недопустимый вред субъектам информационных отношений.

В зарубежных и отечественных источниках на данный момент уделяется много внимания вопросам касающимся контроля доступа к локальным вычислительным сетям.

Вопрос исследования и изучения информационной политики, рост прогресса в развитии информационного пространства в РФ были объектом исследования в работах: К.В. Ветрова, А.И. Ракитова, М.С. Вершинина, С.Э. Зуева, В.Д. Попова. Особенный вклад в исследование и изучение информационной безопасности во всевозможных сферах культуры, общества, техники и науки привнесли такие исследователи и ученые, как А.С. Алексеев, Ю.М. Горский, А.М. Яновский, А.Б. Агапов, И.С. Даниленко, Г.Н. Горшенков, А.В. Возженников, Н.В. Данилов, Г.Г. Феоктистов, И.Л. Бачило, С.А. Дятлов и другие. В трудах, вышеперечисленных ученных сформулированы концептуальные утверждения о содержании категорий и сущности информационной безопасности, изучены их взаимосвязи, использованы рациональные способы и приемы исследования и обеспечения информационной безопасности и различных элементов системного подхода.

Существенное влияние, с точки зрения предмета и объекта исследования, имеют работы А.С. Рябцева, А.Б. Табакова, А.В. Кульбы, К.В. Станиславчика.

На данный момент в образовательных организациях имеются системы обработки и хранения данных, для которых обеспечение безопасности данных является первостепенным. А контроль доступа к ЛВС обеспечивает дополнительную защиту автоматизированных систем.

В настоящий период, невзирая на огромное количество трудов по проблеме информационной безопасности, необходимо отметить то, что изучение теоретических основ, очевидно, малоэффективно. А практические методы и технологии по обеспечению оптимальной работы механизмов информационной безопасности в организациях СПО не соответствуют нормам нашей действительности. В трудах западных и отечественных авторов преобладает односторонний подход в изучении вопросов по проблеме информационной безопасности, исследуется исключительно определенная область механизма информационной безопасности в организациях.

С целью того, чтобы показать подход в обеспечении защиты информационных ресурсов, организациям СПО следует создать политику информационной безопасности и контроля доступа к локальной вычислительной сети. При этом организация обязана осознать, что необходимо поддерживать соответствующие нормы в режиме обеспечения информационной безопасности и контроля доступа и при этом выделять значительные экономические ресурсы для решения этой проблемы.

Политика безопасности и контроль доступа к локальной вычислительной сети – это свод документов, рассматривающий вопрос стратегии, организации, процедур и способов в отношении безопасности конфиденциальных данных, доступности и целостности информационных ресурсов и автоматизированных систем организации. Политика безопасности и контроль доступа к ЛВС основывается на базе анализа рисков – процесса установления угроз безопасности в системе, а также в отдельных ее составляющих, установление их характеристик и возможного ущерба.

Заключительная цель разработки концепции в политике информационной безопасности – гарантировать доступность, конфиденциальность и целостность для каждого информационного ресурса, автоматизированных систем, востребованность в которых, в эпоху стремительно развивающегося мира и современной педагогики, только растет. Вследствие неуклонно продолжающегося роста информатизации среднего профессионального образования требуется внедрение и развитие новейших интерактивных форм и методов электронного обучения.

Особенность образовательных организаций заключается в нехватке стандартного подхода в осуществлении информатизации объектов СПО. Вследствие чего образовательная организация образует собственную корпоративную сеть, с присущей ей отличительной чертой, сформировавшуюся пользовательскими традициями, различной степенью обеспеченности специалистами, разными архитектурными и техническими характеристиками. Усовершенствование и развитие программно-аппаратного базиса корпоративной сети организации СПО в ряду с регулярно обновляющимися угрозами должно осуществляться с учетом особенности такой сети и согласно результативным трендам обеспечения информационной безопасности, используемым при едином подходе.

Необходимость в создании подходящей системы информационной безопасности с помощью реализации требований политики информационной безопасности при применении и создании ЭОР, а также проработка вопросов использования все более новых методов в обеспечении информационной безопасности и контроля доступа к ЛВС организаций СПО обусловили актуальность настоящего исследования.

Целью исследования

Является построение ЛВС образовательной организации в условиях обеспечения политики информационной безопасности и контроля доступа к ЛВС НОУ СПО «ЧЮК».

Объект исследования – формирование политики безопасности вычислительных сетей образовательной организации.

Предмет исследования – совершенствование политики безопасности и контроля доступа к локальной вычислительной сети образовательной организации НОУ СПО «ЧЮК»

Гипотеза исследования заключается в предложении о повышении эффективной защиты образовательных ресурсов в организации СПО при реализации комплексного подхода по обеспечению безопасности процесса обучения.

Для достижения поставленной цели в работе решались следующие **задачи:**

1) Проанализировать сущность понятия «концепция политики безопасности и контроль доступа к локальной вычислительной сети» и выявить основные требования к нему;
2) Изучить основные понятия, виды, функции и методику применения политик безопасности и системы контроля доступа к ЛВС;
3) Провести анализ существующих политик защищенность доступа к ЛВС в НОУ СПО «ЧЮК», выявить основные уязвимости;
4) Установить пути к усовершенствованию политик безопасности и контроля доступа к ЛВС НОУ СПО «ЧЮК»;
5) Разработать рекомендации по использованию АРМ студентами во время самостоятельной работы;
6) Провести апробацию на базе НОУ СПО «ЧЮК» и порекомендовать меры информационной защиты и контроля доступа.

Методологическую основу исследования составляют метод аналогии и сравнения, системный подход, метод моделирования, метод динамических испытаний и т.д.

Научная новизна проведенных исследований и полученных в работе результатов:

- Представлена возможность требуемого обновления имеющейся системы защиты и контроля доступа к ЛВС для организации образовательного процесса в системе среднего профессионального образования.

Практическая значимость работы заключается:

- В разработке концепции информационной безопасности и контроля доступа к ЛВС в НОУ СПО «ЧЮК», которая может найти применение в различных организациях СПО для дополнения существующих политик;
- Во внедрении и апробации политик безопасности и контроля доступа к ЛВС для обеспечения организованной самостоятельной работы студентов среднего профессионального образования;
- В обнаружении и устранении угроз информационной безопасности и контроля доступа к ЛВС.
- Повышение уровня квалификации сотрудников и преподавателей в сфере обеспечения информационной безопасности.

Апробация исследования: результаты исследования были внедрены в образовательной организации.

База исследования: НОУ СПО «Челябинский юридический колледж», г. Челябинск.

Структура работы: магистерская диссертация состоит из введения, трех глав, заключения, списка использованной литературы, состоящего из (57) наименований. Работа содержит (4) рисунков. Общий объем работы составляет (65) страниц.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАЗРАБОТКИ КОНЦЕПЦИИ ПОЛИТИКИ БЕЗОПАСНОСТИ И КОНТРОЛЯ ДОСТУПА К ЛВС

1.1 Основные цели информационной безопасности в локальных вычислительных сетях

Крайне важно понять, что безопасность это не продукт, который можно купить в магазине и быть уверенным в собственной защищенности. «Безопасность» — особая комбинация как технических, так и административных мер. Административные меры также включают в себя не только бумаги, рекомендации, инструкции, но и людей. Невозможно считать свою сеть «безопасной», если вы не доверяете людям, работающим с этой сетью.

Идеальная безопасность это недостижимый миф, который могут реализовать, в лучшем случае, только несколько профессионалов. Есть один фактор, который невозможно преодолеть на пути к идеальной безопасности это человек.

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основных целей обычно три представлены на рисунке 1.1:

1. Целостность данных;
2. Конфиденциальность данных;
3. Доступность данных.

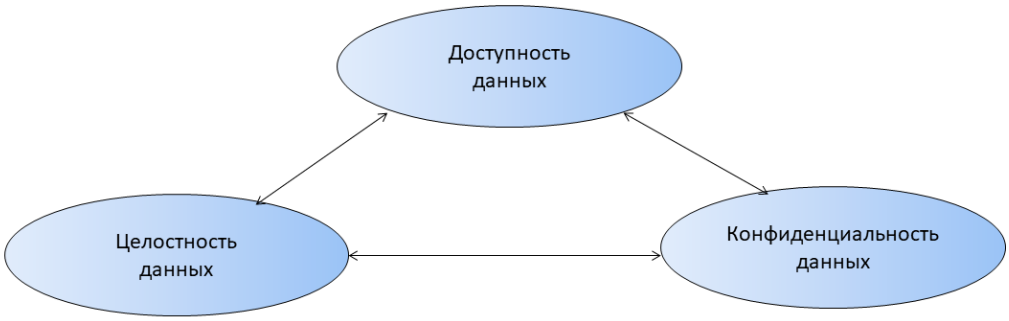

Рисунок 1.1 – Цели сетевой безопасности

Рассмотрим более подробно каждую из них.

Целостность данных

Одна из основных целей сетевой безопасности, гарантированность того, чтобы данные не были изменены, подменены или уничтожены. Целостность данных должна гарантировать их сохранность, как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных

Второй главной целью сетевой безопасности является обеспечение конфиденциальности данных. Не все данные можно относить к конфиденциальной информации. Существует достаточно большое количество информации, которая должна быть доступна всем. Но даже в этом случае обеспечение целостности данных, особенно открытых, является основной задачей. К конфиденциальной информации можно отнести следующие данные:

- личная информация пользователей;
- учетные записи (имена и пароли);
- данные о кредитных картах;
- данные о разработках и различные внутренние документы;
- бухгалтерская информация.

Доступность данных

Третьей целью безопасности данных является их доступность. Бесполезно говорить о безопасности данных, если пользователь не может работать с ними из-за их недоступности. Вот приблизительный список ресурсов, которые обычно должны быть «доступны» в локальной сети:

- принтеры;
- серверы;
- рабочие станции;
- данные пользователей;
- любые критические данные, необходимые для работы.

Рассмотрим угрозы и препятствия, стоящие на пути к безопасности сети. Все их можно разделить на две большие группы: технические угрозы и человеческий фактор.

Технические угрозы:

1. ошибки в программном обеспечении;
2. различные DoS- и DDoS-атаки;
3. компьютерные вирусы, черви, троянские кони;
4. анализаторы протоколов и прослушивающие программы («снифферы»);
5. технические средства съема информации.

Ошибки в программном обеспечении

Самое узкое место любой сети. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, следовательно, оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляет никакой опасности, некоторые же могут привести к трагическим последствиям, таким, как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (хранение ненужных данных на сервере, использование в качестве плацдарма для атаки и т.п.). Большинство таких уязвимостей устраняется с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких обновлений является необходимым условием безопасности сети.

DoS- и DDoS-атаки

Denial Of Service (отказ в обслуживании) — особый тип атак, направленный на выведение сети или сервера из работоспособного состояния. При DoS-атаках могут использоваться ошибки в программном обеспечении или легитимные операции, но в больших масштабах (например, посылка огромного количества электронной почты). Новый тип

атак DDoS (Distributed Denial Of Service) отличается от предыдущего наличием огромного количества компьютеров, расположенных в большой географической зоне. Такие атаки просто перегружают канал трафиком и мешают прохождению, а зачастую и полностью блокируют передачу по нему полезной информации. Особенно актуально это для компаний, занимающихся каким-либо online-бизнесом, например, торговлей через Internet.

Компьютерные вирусы, троянские кони

Вирусы — старая категория опасностей, которая в последнее время в чистом виде практически не встречается. В связи с активным применением сетевых технологий для передачи данных вирусы все более тесно интегрируются с троянскими компонентами и сетевыми червями. В настоящее время компьютерный вирус использует для своего распространения либо электронную почту, либо уязвимости в ПО. А часто и то, и другое. Теперь на первое место вместо деструктивных функций вышли функции удаленного управления, похищения информации и использования зараженной системы в качестве плацдарма для дальнейшего распространения. Все чаще зараженная машина становится активным участником DDoS-атак. Методов борьбы достаточно много, одним из них является все та же своевременная установка обновлений.

Анализаторы протоколов и «снифферы»

В эту группу входят средства перехвата передаваемых по сети данных. Такие средства могут быть как аппаратными, так и программными. Обычно данные передаются по сети в открытом виде, что позволяет злоумышленнику внутри локальной сети перехватить их. Некоторые протоколы работы с сетью (POPS, FTP) не используют шифрование паролей, что позволяет злоумышленнику перехватить их и использовать самому. При передаче данных по глобальным сетям эта проблема встает наиболее остро. По возможности следует ограничить доступ к сети неавторизированным пользователям и случайным людям.

Технические средства съема информации

Сюда можно отнести такие средства, как клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т.д. Данная группа используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия спецтехники, требует доступа к сети и ее составляющим.

Человеческий факторы:

- уволенные или недовольные сотрудники;
- промышленный шпионаж;
- халатность;
- низкая квалификация.

Уволенные и недовольные сотрудники

Данная группа людей наиболее опасна, так как многие из работающих сотрудников могут иметь разрешенный доступ к конфиденциальной информации. Особенную группу составляют системные администраторы, зачастую недовольные своим материальным положением или несогласные с увольнением, они оставляют «черные ходы» для последующей возможности злонамеренного использования ресурсов, похищения конфиденциальной информации и т. д.

Промышленный шпионаж

Это самая сложная категория. Если ваши данные интересны кому-либо, то этот кто то найдет способы достать их. Взлом хорошо защищенной сети, не самый простой вариант. Очень может статься, что уборщица «тетя Глаша», моющая под столом и ругающаяся на непонятный ящик с проводами, может оказаться хакером весьма высокого класса.

Халатность

Самая обширная категория злоупотреблений: начиная с не установленных вовремя обновлений, неизмененных настроек «по умолчанию» и заканчивая несанкционированными модемами для выхода в

Internet, в результате чего злоумышленники получают открытый доступ в хорошо защищенную сеть.

Низкая квалификация

Часто низкая квалификация не позволяет пользователю понять, с чем он имеет дело; из-за этого даже хорошие программы защиты становятся настоящей морокой системного администратора, и он вынужден надеяться только на защиту периметра. Большинство пользователей не понимают реальной угрозы от запуска исполняемых файлов и скриптов и считают, что исполняемые файлы только файлы с расширением «exe». Низкая квалификация не позволяет также определить, какая информация является действительно конфиденциальной, а какую можно разглашать. В крупных компаниях часто можно позвонить пользователю и, представившись администратором, узнать у него учетные данные для входа в сеть. Выход только один обучение пользователей, создание соответствующих документов и повышение квалификации [7].

1.2 Модели безопасности

Рассмотрим некоторые известные модели безопасности.

Модель дискреционного доступа

В рамках модели контролируется доступ субъектов к объектам. Для каждой пары субъект-объект устанавливаются операции доступа (READ, WRITE и другие).

Контроль доступа осуществляется посредством механизма, который предусматривает возможность санкционированного изменения правил разграничения доступа. Право изменять правила предоставляется выделенным субъектам.

Модель дискретного доступа

В рамках модели рассматриваются механизмы распространения доступа субъектов к объектам.

Модель мандатного управления доступом Белла-Лападула

Формально записана в терминах теории отношений. Описывает механизм доступа к ресурсам системы, при этом для управления доступом используется матрица контроля доступа. В рамках модели рассматриваются простейшие операции READ и WRITE доступа субъектов к объектам, на которые накладываются ограничения.

Множества субъектов и объектов упорядочены в соответствии с их уровнем полномочий и уровнем безопасности, соответственно.

Состояние системы изменяется согласно правилам трансформации состояний.

Модели распределенных систем (синхронные и асинхронные)

В рамках моделей субъекты выполняются на нескольких устройствах обработки. Рассматриваются операции доступа субъектов к объектам READ и WRITE, которые могут быть удаленными, что может вызвать противоречия в модели Белла-Лападула.

В рамках асинхронной модели в один момент времени несколько субъектов могут получить доступ к нескольким объектам.

Переход системы из одного состояния в другое состояние в один момент времени может осуществляться под воздействием более, чем одного субъекта.

Модель безопасности военной системы передачи данных (MMS - модель)

Формально записана в терминах теории множеств. Субъекты могут выполнять специализированные операции над объектами сложной структуры. В модели присутствует администратор безопасности для управления доступом к данным и устройствам глобальной сети передачи данных. При этом для управления доступом используются матрицы контроля доступа. В рамках модели используются операции READ, WRITE, CREATE, DELETE доступа субъектов к объектам, операции над

объектами специфической структуры, а также могут появляться операции, направленные на специфическую обработку информации.

Состояние системы изменяется с помощью функции трансформации.

Модель трансформации прав доступа

Формально записана в терминах теории множеств. В рамках модели субъекту в данный момент времени предоставляется только одно право доступа. Для управления доступом применяются функции трансформации прав доступа.

Механизм изменения состояния системы основывается на применении функций трансформации состояний.

Схематическая модель

Формально записана в терминах теории множеств и теории предикатов. Для управления доступа используется матрица доступа со строгой типизацией ресурсов. Для изменения прав доступа применяется аппарат копирования меток доступа.

Иерархическая модель

Формально записана в терминах теории предикатов. Описывает управление доступом для параллельных вычислений, при этом управление доступом основывается на вычислении предикатов.

Модель безопасных спецификаций

Формально описана в аксиоматике Хоара.

Модель информационных потоков

Формально записана в терминах теории множеств. В модели присутствуют объекты и атрибуты, что позволяет определить информационные потоки. Управление доступом осуществляется на основе атрибутов объекта. Изменением состояния является изменение соотношения между объектами и атрибутами.

Вероятностные модели

В модели присутствуют субъекты, объекты и их вероятностные характеристики. В рамках модели рассматриваются операции доступа

субъектов к объектам READ и WRITE. Операции доступа также имеют вероятностные характеристики.

Модель элементарной защиты

Предмет защиты помещен в замкнутую и однородную защищенную оболочку, называемую преградой. Информация со временем начинает устаревать, т.е. цена ее уменьшается. За условие достаточности защиты принимается превышение затрат времени на преодоление преграды нарушителем над временем жизни информации. Вводятся вероятность не преодоления преграды нарушителем $P_{СЗИ}$, вероятность обхода преграды нарушителем $P_{обх}$, и вероятность преодоления преграды нарушителем за время, меньшее времени жизни информации $P_{нр}$. Для введенной модели нарушителя показано, что $P_{СЗИ}= min[(1 — P_{нр})(1-P_{обх})]$, что является иллюстрацией принципа слабейшего звена. Развитие модели учитывает вероятность отказа системы и вероятность обнаружения и блокировки действий нарушителя.

Модель системы безопасности с полным перекрытием

Отмечается, что система безопасности должна иметь по крайней мере одно средство для обеспечения безопасности на каждом возможном пути проникновения в систему. Модель описана в терминах теории графов. Степень обеспечения безопасности системы можно измерить, используя лингвистические переменные. В базовой системе рассматривается набор защищаемых объектов, набор угроз, набор средств безопасности, набор уязвимых мест, набор барьеров.

Модель гарантированно защищенной системы обработки информации

В рамках модели функционирование системы описывается последовательностью доступов субъектов к объектам. Множество субъектов является подмножеством множества объектов. Из множества объектов выделено множество общих ресурсов системы, доступы к которым не могут привести к утечке информации. Все остальные объекты

системы являются порожденными пользователями, каждый пользователь принадлежит множеству порожденных им объектов. При условиях, что в системе существует механизм, который для каждого объекта устанавливает породившего его пользователя; что субъекты имеют доступ только к общим ресурсам системы и к объектам, порожденным ими, и при отсутствии обходных путей политики безопасности модель гарантирует невозможность утечки информации и выполнение политики безопасности.

Субъектно-объектная модель

В рамках модели все вопросы безопасности описываются доступами субъектов к объектам. Выделены множество объектов и множество субъектов. Субъекты порождаются только активными компонентами (субъектами) из объектов. С каждым субъектом связан (ассоциирован) некоторый объект (объекты), т.е. состояние объекта влияет на состояние субъекта. В модели присутствует специализированный субъект, монитор безопасности субъектов (МБС), который контролирует порождение субъектов.

Из упомянутых моделей для нас наибольший интерес представляет дискреционные и мандатные механизмы разграничения доступа (как наиболее распространенные), модель гарантированно защищенной системы (в силу гарантированности) и субъектно-объектная модель (рассматривающая не только доступы, но и среду, в которой они совершаются).

Под сущностью понимается любая составляющая компьютерной системы.

Субъект определяется как активная сущность, которая может инициировать запросы ресурсов и использовать их для выполнения каких-либо вычислительных заданий.

Объект определяется как пассивная сущность, используемая для хранения и получения информации.

Доступ — взаимодействие между объектом и субъектом, в результате которого происходит перенос информации между ними.

Взаимодействие происходит при исполнении субъектами операций. Существуют две фундаментальные операции: операция чтения (перенос информации от объекта к субъекту) и операция записи (перенос информации от субъекта к объекту).

Данные операции являются минимально необходимым базисом для описания моделей, описывающих защищенные системы.

1.3 Виды угроз и методы защиты

Каждый ИТ-сервис или объект в совокупной инфраструктуре компании имеет определенный коэффициент риска, поэтому разработку концепции безопасности вашей корпорации следует начинать именно с всестороннего их анализа.

Другим немаловажным фактором при планировании концепции безопасности следует считать различные типы угроз каждому ключевому сервису ИТ-инфраструктуры. Эти аспекты напрямую соотносятся с факторами оценки объектов и позволяют получить информацию для последующих действий по мерам защиты. Важное правило эффективности мер — защита не должна быть избыточной!

Результаты всестороннего анализа типов угроз и оценки каждого объекта сетевой ИТ-инфраструктуры являются основой для разработки и внедрения политики безопасности. Она будет включать в себя политику управления конфигурациями и обновлениями, мониторинг и аудит систем, а также другие превентивные меры операционных политик и процедур. Обязательным условием является наличие тестовой лаборатории с уменьшенным аналогом типичной ИТ-среды корпорации. Накопленные знания и опыт, полученные при анализе угроз и уязвимостей систем, являются, по сути, уникальной базой знаний и будут служить фундаментом в построении надежной и защищенной инфраструктуры и последующем обучении персонала. Однако следует учесть, что при изменении (модернизации) инфраструктуры, добавлении новых объектов

необходимо произвести повторную оценку и анализ и впоследствии модифицировать политику безопасности.

Идентификация угроз

Повышение привилегий — Получение системных привилегий через атаку с переполнением буфера, незаконное получение административных прав.

Фальсификация — Модификация данных, передаваемых по сети, модификация файлов.

Имитация — Подделка электронных сообщений, подделка ответных пакетов при аутентификации.

Раскрытие информации — Несанкционированный доступ или незаконная публикация конфиденциальной информации.

Отречение — Удаление критичного файла или совершение покупки с последующим отказом признавать свои действия.

Отказ в обслуживании — Загрузка сетевого ресурса большим количеством поддельных пакетов.

Защита на всех уровнях

Чтобы уменьшить возможность успешного вторжения в ИТ-среду корпорации, надо создать комплексные меры защиты на всех возможных уровнях. Такая концепция информационной безопасности подразумевает, что нарушение одного уровня защиты не скомпрометирует всю систему в целом.

Проектирование и построение каждого уровня безопасности должны предполагать, что любой уровень может быть нарушен злоумышленником. Кроме того, каждый из уровней имеет свои специфические и наиболее эффективные методы защиты. Из перечня доступных и разработанных многими известными вендорами технологий можно выбрать наиболее подходящую по техническим и экономическим факторам. Например:

- *защита данных* — списки контроля доступа, шифрование;

- **приложения** — защищенные приложения, антивирусные системы;
- *компьютеры* — защита операционной системы, управление обновлениями, аутентификация, система обнаружения вторжений на уровне хоста;
- *внутренняя сеть* — сегментация сети, IP Security, сетевые системы обнаружения вторжений;
- *периметр* — программные и программно-аппаратные межсетевые экраны, создание виртуальных частных сетей с функциями карантина;
- *физическая защита* — охрана, средства наблюдения и разграничения доступа;
- *политики и процедуры* — обучение пользователей и технического персонала.

Таким образом, в результате комплексных мер защиты на всех уровнях упрощается процесс обнаружения вторжения и снижаются шансы атакующего на успех.

Человеческий фактор

Многие уровни защиты имеют в своей основе программно-аппаратные средства, однако влияние “человеческого фактора” вносит в общую картину серьезные коррективы.

Уровень физической защиты

Требования физической защиты являются базовыми и первоочередными для внедрения.

Имея физический доступ к оборудованию, злоумышленник может легко обойти последующие уровни защиты. Для доступа могут использоваться телефоны компании или карманные устройства. Особо уязвимыми с точки зрения утечки важной информации являются портативные компьютеры, которые могут находиться за пределами корпорации.

В некоторых случаях фактор доступа нацелен на нанесение вреда. Однако при наличии физического доступа можно устанавливать программные средства контроля и мониторинга за особо важной корпоративной информацией, которые будут накапливать ее в течение длительного времени.

Для обеспечения безопасности уровня физической защиты можно использовать любые доступные средства, которые позволит бюджет компании. Элементы защиты должны охватывать все компоненты ИТ-инфраструктуры. Например, инженер сервисной службы заменил вышедший из строя дисковый массив уровня RAID 10, содержавший важные данные пользователей корпорации. После этого диск может быть отправлен в сервисный центр, где его можно восстановить и получить доступ к данным. В таком случае уровень физической защиты корпорации можно считать скомпрометированным.

Первым шагом в обеспечении надежного уровня защиты является физическое разнесение серверной и пользовательской инфраструктуры. Обязательным при этом становится наличие отдельного, надежно закрытого помещения, с процедурами жесткого контроля доступа и мониторинга. Наличие персонифицированного доступа на основе магнитных карт или биометрических устройств резко уменьшает шансы злоумышленника. Серверная комната должна быть оснащена автоматическими системами пожаротушения и климат-контроля. Доступ можно дополнительно контролировать с помощью системы видеонаблюдения с возможностью записи событий.

Удаленный доступ к консолям серверов также подлежит тщательному контролю. Имеет смысл выделять административную группу в отдельный физический сегмент сети с постоянным мониторингом доступа и на сетевом уровне управляемых коммутаторов и хостов, и на логическом уровне персональной идентификации.

Последующие меры по обеспечению полного спектра физической защиты должны быть направлены на удаление и изъятие устройств ввода (приводов флоппи- и компакт-дисков) из тех компьютеров, где в них нет необходимости. Если это невозможно, обязательно следует использовать программные средства блокировки доступа к съемным носителям. В конечном итоге следует обеспечить гарантию физической защиты активного сетевого оборудования (коммутаторы, маршрутизаторы) в специальных шкафах с контролем доступа. Кроме этого, необходимо обеспечить коммутацию только тех устройств и розеток, которые действительно необходимы.

Периметр информационной системы является той частью сетевой инфраструктуры, которая наиболее открыта для атак извне. В периметр входят подключения к:

- интернету;
- филиалам;
- сетям партнеров;
- мобильным пользователям;
- беспроводным сетям;
- интернет-приложениям.

Важно рассматривать безопасность данного уровня в целом, а не только для конкретного направления. Возможные направления атак через периметр:

- на сеть организации;
- на мобильных пользователей;
- со стороны партнеров;
- со стороны филиалов;
- на сервисы интернета;
- из интернета.

Традиционно считается, что наиболее уязвимым является направление из интернета, однако угроза из других направлений не менее

существенна. Важно, чтобы все входы и выходы в (из) вашей сети были надежно защищены. Нельзя быть уверенным в отношении мер защиты в сетевых инфраструктурах бизнес-партнеров или филиалов, поэтому данному направлению также следует уделить пристальное внимание.

Обеспечение безопасности периметра достигается, прежде всего, использованием межсетевых экранов. Их конфигурация, как правило, технически достаточно сложна и требует высокой квалификации обслуживающего персонала, а также тщательного документирования настроек. Современные операционные системы позволяют легко блокировать неиспользуемые порты, чтобы уменьшить вероятность атаки.

Трансляция сетевых адресов (NAT) позволяет организации замаскировать внутренние порты. При передаче информации через незащищенные каналы надо использовать методы построения виртуальных частных сетей (VPN) на основе шифрования и туннелирования.

Угрозы и защита локальной сети

Атаки могут производиться не только из внешних источников. По статистике, очень большой процент удачных атак принадлежит вторжениям изнутри сетевой среды. Очень важно построить внутреннюю сетевую безопасность, чтобы остановить злонамеренные и случайные угрозы. Неконтролируемый доступ к внутренней сетевой инфраструктуре позволяет атакующему получить возможность доступа к важным данным корпорации, контролировать сетевой трафик. Полностью маршрутизируемые сети позволяют злоумышленнику получить доступ к любому ресурсу из любого сегмента сети. Сетевые операционные системы имеют множество установленных сетевых сервисов, каждый из которых может стать объектом атаки (рисунок 1.2).

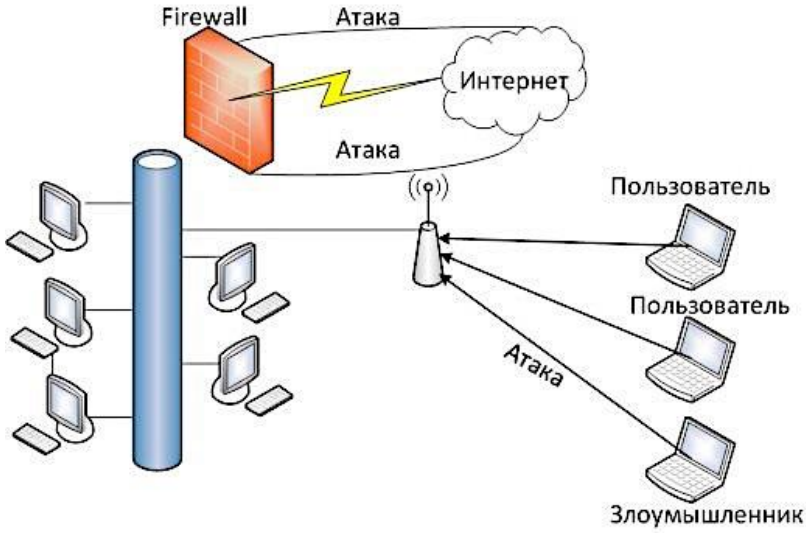

Рисунок 1.2 – Угрозы локальной сети

Для защиты внутреннего сетевого окружения надо обеспечить механизмы надежной аутентификации пользователей в глобальной службе каталогов (едином центре входа). Взаимная аутентификация на уровне сервера и сетевой рабочей станции значительно поднимает качество сетевой безопасности. Современные требования подразумевают наличие управляемой коммутируемой сетевой среды и разделение на логические сегменты (VLAN). Для администрирования удаленных устройств надо всегда использовать подключение по защищенному протоколу (например SSH). Трафик Telnet-подключений может быть легко перехвачен, а имена и пароли передаются в открытом виде. Максимум внимания — защите резервных копий конфигураций сетевых устройств, — они могут многое рассказать о топологии сети злоумышленнику.

Защищать сетевой трафик следует даже после проведения сегментации сети. И для проводных, и для беспроводных подключений можно использовать протокол 802.1X, чтобы обеспечить зашифрованный и аутентифицированный доступ. Это решение может использовать учетные записи и пароли в глобальной службе каталогов (Microsoft Active Directory, Novell e-Directory и т. п.) либо цифровые сертификаты. Технология цифровых сертификатов обеспечивает очень высокий уровень защиты сетевого транспорта, однако требует развертывания

инфраструктуры публичных ключей (Public Key Infrastructure) в виде сервера и хранилища сертификатов.

Внедрение технологий шифрования и цифровых подписей типа IPSec или Server Message Block (SMB) Signing воспрепятствует перехвату сетевого трафика и его анализу.

Компьютерные системы в сетевой среде выполняют некоторые задачи, которые и определяют требования защиты. Сетевые хосты могут подвергаться нападению, поскольку они является публично доступными. Злоумышленники могут распространять вредоносный код (вирусы) для осуществления распределенной атаки. Установленное на рабочих станциях и серверах программное обеспечение может иметь уязвимости в программном коде, поэтому своевременная установка обновлений — один из важных шагов в общей концепции защиты.

Настройки политики защиты уровня компьютера необходимо обеспечивать и контролировать централизованно, например, с помощью групповой политики (Group Policy). Защита серверных систем на этом уровне будет включать в себя установку атрибутов безопасности для файловых систем, политики аудита, фильтрации портов и других мер в зависимости от роли и назначения сервера.

Наличие всех доступных обновлений для операционной системы и программного обеспечения кардинально улучшает общий уровень обеспечения безопасности. Можно использовать любые способы автоматической установки и контроля обновлений, от самых простых — Windows Update, Software Update Service (SUS), Windows Update Service (WUS) до наиболее сложных и мощных — Systems Management Server (SMS).

Использование антивирусного пакета с актуальными обновлениями, персональных брандмауэров с фильтрацией портов позволит резко сократить шансы на атаку.

Защита компьютеров:

- взаимная аутентификация пользователей, серверов и рабочих станций;
- защита операционной системы;
- установка обновлений безопасности;
- аудит успешных и неуспешных событий;
- отключение неиспользуемых сервисов;
- установка и обновление антивирусных систем;
- защита приложений.

Сетевые приложения дают возможность пользователям получать доступ к данным и оперировать ими. Сетевое приложение — это точка доступа к серверу, где это приложение выполняется. В этом случае приложение обеспечивает определенный уровень сетевого сервиса, который должен быть устойчив к атакам злоумышленников. Следует провести тщательное исследование как собственных разработок, так и используемых коммерческих продуктов на наличие уязвимостей. Целью атаки может быть и разрушение кода приложения (как следствие — его недоступность), и исполнение вредоносного кода. Нападавший также может применить тактику распределенной атаки, направленной на перегрузку производительности приложения. Результатом может стать отказ в облуживании (Denial of Service).

Приложение также может быть использовано в непредусмотренных задачах, например маршрутизация почтовых сообщений (открытый почтовый релей). Приложения должны быть установлены и настроены только с необходимым уровнем функциональности и сервиса, а работу программного кода можно контролировать системами мониторинга и антивирусными пакетами. Чтобы уменьшить уровень угроз, выполнение приложения следует ограничить минимальными сетевыми привилегиями.

Копрометация и защита приложений:

- использование только необходимых служб и функций приложений;

- настройка параметров защиты приложений;
- установка обновлений безопасности;
- запуск приложений в контексте с минимальными привилегиями;
- установка и обновление антивирусных систем;
- защита данных.

Финальный уровень — это защита данных, которые могут располагаться и на серверных хостах, и на локальных. На этом уровне следует защитить информацию, используя современные файловые системы с контролем атрибутов доступа на уровне томов, папок и файлов. Расширенные функции файловой системы, такие как аудит и шифрование, позволят более надежно построить систему разграничения доступа и осуществить надежную сохранность данных. Злоумышленник, получивший доступ к файловой системе, может причинить огромный ущерб в виде хищения, изменения или удаления информации. Особое внимание следует уделить файловым системам главной сетевой опорной архитектуры — глобальным службам каталогов. Похищение или удаление этой информации может иметь печальные последствия.

Шифрованная файловая система является еще одним важным элементом надежного бастиона защиты. Однако следует помнить, что файлы только хранятся в зашифрованном виде, а передаются через сеть открыто. Кроме того, шифрование защищает от неправомерного чтения, а защиты от удаления оно не дает. Чтобы предотвратить несанкционированное удаление, следует использовать атрибуты доступа.Например, служба каталогов Active Directory использует для хранения своей информации файлы. По умолчанию эти файлы располагаются в известном каталоге, имя которого указывается по умолчанию при генерации контроллера домена. Изменив месторасположение данных файлов путем перенесения на другой том, можно возвести огромный барьер для атакующего.

Поскольку данные являются основой современных информационных процессов, очень важно предусмотреть процедуры резервного копирования и восстановления. Важно также обеспечить регулярность проведения этих действий. Но следует учесть, что резервные копии являются ценным источником и лакомым куском для хищения, поэтому их сохранности нужно уделить внимание на уровне безопасности серверной комнаты.

После переноса файлов на другой, например сменный, носитель атрибуты доступа теряются. Есть, правда, технология контроля доступа к цифровым документам Windows Rights Management Services (RMS), которая обеспечивает уровень защиты независимо от месторасположения документа. RMS обладает расширенными возможностями, такими как, например, возможность просмотра документа, но запрет печати или копирования содержимого, запрет пересылки содержимого письма другому адресату, если речь идет о почтовых сообщениях.

Выводы по Главе I

Результат всестороннего анализа типов угроз и оценки каждого объекта сетевой инфраструктуры, должен стать основой для разработки и внедрения переработанной концепции политики безопасности и контроля доступа к ЛВС НОУ СПО «ЧЮК». Концепция будет включать в себя политику управления конфигурациями и обновлениями, мониторинг и аудит систем, а также другие превентивные меры операционных политик и процедур. Обязательным условием является наличие тестовой лаборатории с уменьшенным аналогом типичной ИТ-среды корпорации. Накопленные знания и опыт, полученные при анализе угроз и уязвимостей систем, являются, по сути, уникальной базой знаний и будут служить фундаментом в построении надежной и защищенной инфраструктуры и последующем обучении персонала, а также самостоятельной работы студентов в лабораториях. Однако следует учесть, что при изменении (модернизации) инфраструктуры, добавлении новых объектов необходимо

произвести повторную оценку и анализ и впоследствии модифицировать политику безопасности. Так же нужно проводить оценку модели угроз и модернизировать политику безопасности в связи с постоянными вызовами с которыми сталкиваются образовательная организация в процессе своей деятельности. Проводится такая оценка, и переработка политик, не реже раз в пять лет.

Проектирование и построение каждого уровня безопасности должны предполагать, что любой уровень может быть нарушен злоумышленником. Кроме того, каждый из уровней имеет свои специфические и наиболее эффективные методы защиты.

ГЛАВА 2 ПРОЕКТИРОВАНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

2.1 Основные направления политики информационной безопасности НОУ СПО «ЧЮК»

На сегодняшний день, в условиях повсеместной информатизации образовательных организаций, становится явной проблема противоречия между возможностью использования информационных образовательных ресурсов, предлагаемых организацией СПО, и потребностями студентов и преподавателей во взаимодействии в образовательном процессе. Информационно-образовательные ресурсы и информационное взаимодействие в этих условиях должно быть не только доступным, но и должны обладать достаточной защищенностью, гарантирующей высокий уровень обеспечения конфиденциальности и целостности всех компонентов ЭОР [4].

Чтобы решить данную задачу организации СПО формируют концепции ИБ (информационной безопасности), описывающие соответствующие методы, объекты и меры защиты.

Структура концепции ИБ содержит ряд тематических сегментов:

- Понятийный (терминологический) аппарат;
- Нормативно-правовая база;
- Описание объектов защиты;
- Принципы реализации защиты;
- Организационные и административные методы и меры;
- Программно-аппаратные методы и меры [7].

Терминологический аппарат концепций фактически совпадает с терминологическим аппаратом перечисленных правовых актов.

Нормативно-правовой базой, являются законы федерального уровня, например федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ [48], федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ

[49], федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 №436-ФЗ [50], нормативно-методические документы ФСБ и ФСТЭК, а также стратегические документы РФ, характеризующие политическую деятельность государства в сфере защиты конституционных прав и конфиденциальной информации граждан и ряд других документов.

К основным объектам защиты в организации СПО причисляют персональные данные студентов и сотрудников, данные информационные сведения являются более ценными и нуждаются в более интенсивной защите. Но подобная точка зрения не считается правильной, так как в защите нуждаются и такие ресурсы как: электронно-образовательные, материально-технические и информационные системы организации в целом [54].

В работах О.А. Шемяков справедливо подчеркнуто, что образовательная организация должна обеспечить:

- Организацию системы безопасного доступа к образовательным ресурсам, вне зависимости от времени и места;
- Защиту информационных ресурсов с ограниченным доступом (индивидуальные сведения об участниках образовательного процесса, коммерческая тайна и т.д.);
- Защиту интеллектуальной собственности;
- Соблюдение требований прописанных в законодательных актах в области защиты информации (защита от негативной информации обучаемых, защита персональных данных и т.д.) [51].

Принцип обеспечения и реализации защищенной среды разработан в теории информационной защиты, и в значительной степени не отличается от концепций других организаций среднего профессионального образования: непрерывность, системность, комплексность, открытость алгоритмов, простота применения, персональная ответственность, минимизирование полномочий [46].

Организационные меры складываются из процедурных мер по информационной безопасности и административных процедур. Базой административных процедур выступает совокупность из управленческих решений, нацеленных на защиту информационных ресурсов и совокупных с ней данных [30].

Согласно статистики по анализу интернет-ресурсов организаций СПО, лишь небольшая часть исследуемых сайтов, это менее 12% согласно мониторингу, обладают документально оформленной политикой информационной безопасности, которая включает такие составные единицы, как политику защиты от несанкционированного доступа, политику по предоставлению доступа к информационным системам сотрудникам, политику по предоставлению доступа к ресурсам интернет-сети, политику по управлению паролями, политику по использованию электронной почты и другие программные и политехнические положения по использованию информационных ресурсов учебной организации.

Высокой степенью проработки обладает программно-аппаратная защита информации. Что обусловлено мощной нормативно методической базой ФСБ и ФСТЭК, вследствие чего если даже организация СПО не пройдет процедуру аттестации, степень подготовки специалистов по информационной защите будет на весьма высоком уровне [28].

Кроме описания разделов в концепции информационной защиты существует порядок подразделения защищаемой информации на соответствующие категории, порядок взаимодействия с информационными системами и распределение ответственных лиц, что, бесспорно, способствует усилению степени защиты данных организации, а также контроля доступа к ней.

Более подробное описание системы информационной защиты представлено в концепции информационной безопасности образовательной организации, все это обусловлено современными требованиями необходимыми для защиты информационных ресурсов.

Концепция по информационной безопасности закреплена в «Политике информационной безопасности организации», которая представляет свод локальных документов и правил, регулирующих защиту, управление и распределение информационных данных в образовательной организации [25].

Зачастую политику информационной безопасности трактуют как комплекс задокументированных административных решений, нацеленных на обеспечение ИБ информационного ресурса.

Показателем результативности в политике по обеспечению информационной безопасности является создание высокоуровневого документа, который представляет систематизировано изложенные цели, задачи, принципы и способы достижения в защите информации.

В данном документе подробно описана методология по практическому применению процедур и мер по реализации защиты информации. Он включает следующие категории сведений:

1) Основные положения по обеспечению защиты информации;
2) Области применения;
3) Задачи и цели по обеспечению защиты информации;
4) Разделение ролей и ответственности;
5) Общие обязательства [29].

Основные положения устанавливают значимость обеспечения защиты информации, общие проблемы по обеспечению защиты информационных ресурсов, тенденции их решения, нормативно-правовые основы, а также распределение ролей сотрудников.

Сферой использования политики информационной безопасности являются основные подсистемы и активы автоматизированной ИС организации, которые подлежат защите. Стандартными активами считаются информационное обеспечение и программно-аппаратные средства автоматизированных ИС. Персонал администрирования, в свою

очередь, можно причислить к информационной инфраструктуре образовательной организации [5].

А особенности информационных активов диктуют соответствующие задачи, цели и критерии по обеспечению информационной безопасности.

Стандартные цели прописаны в национальном стандарте РФ «Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности» ГОСТ Р 57628-2017 от 01.01.2018 [12]. Данный стандарт определяет основные принципы оценки и понятия информационной безопасности, устанавливает основную модель оценки характеристик ИБ будущих продуктов информационных систем организации.

В вышеназванном стандарте прописано краткое описание и обзор всех элементов систем обеспечения безопасности информации, выбраны термины, определено основное понятие оцениваемого объекта, определена целевая аудитория, которой направлены критерии оценки информационной безопасности и представлены способы и меры по реализации безопасности информационных систем. Данным стандартам придерживаются все учебные заведения СПО и другие образовательные организации в частности.

Несомненно то, что любая организация определяет собственную стратегию в формировании политики ИБ, основываясь на собственных особенностях и специфике иерархической лестницы организационной структуры, которая имеет собственную инфраструктуру, тенденции и требования официальных документов и иные аспекты [9].

Политика информационной безопасности затрагивает всех сотрудников и студентов, пользующихся компьютером в образовательной организации. По этой причине немаловажно решить политический вопрос, связанный с вопросом наделения всех пользователей определенными правами, обязанностями и привилегиями. С этой целью определяют лиц, которые имеют доступ к сервисам и подсистемам автоматизированной

системы. Для этого каждого пользователя, имеющего определенный статус в системе, наделяют правами доступа или отказа в доступе использования ресурсов. На этом уровне определяются регламентация доступа соответствующих лиц [10].

А также необходимо отметить, что существует правило умолчания на пользование ресурсами. Звучит оно следующим образом: «Обязанности и полномочия пользователей формируются согласно безопасного использования сервисов и подсистем АС. При установлении обязанностей и полномочий администраторам следует учитывать баланс на право пользователя на тайну, а также на обязанность оператора вести контроль нарушений информационной безопасности».

Значимым компонентом политики является ранжирование ответственности пользователей. В политике по обеспечению безопасности невозможно предусмотреть абсолютно все, но необходимо для любого вида проблем определить ответственного.

Как правило, существует несколько ступеней ответственности. На первой сотрудники обязаны работать согласно политике безопасности, действовать согласно распоряжениям, отвечающим за определенные аспекты безопасности, сообщать руководству об абсолютно всех сомнительных или подозрительных ситуациях. Системный администратор отвечает за сохранность информационно-вычислительных систем. Сетевой администратор обеспечивает реализацию по обеспечению организационно-технических мер, которые необходимы при формировании политики информационной безопасности автоматизированных систем. В свою очередь руководитель подразделения несет ответственность за контроль и доработку политики безопасности [31].

С точки зрения практики, политику информационной безопасности рационально делить на несколько уровней.

Высший уровень определяет организационную политику в целом и несет общий характер. Здесь акцент внимания нацелен на: пересмотр политики информационной безопасности и порядок ее создания; цели, которые преследует образовательная организация в области формирования безопасной среды; вопросы распределения и выделения ресурсов; принципы технической политики, определение средств и методов информационной защиты; организацию мер по защите данных; стратегический контроль и планирование; внешние взаимодействия и другие вопросы, которые имеют общий организационный характер. На данном уровне определяется главная цель в области безопасности: доступность, целостность и конфиденциальность.

На среднем уровне политики безопасности поднимаются сложные вопросы, связанные со структурой организации или при необходимости создаются специфические подсистемы, которые решают проблемы организационного уровня безопасной среды. Что непосредственно относится к многообещающим, еще не апробированным технологиям. К примеру, реализация новейших сервисов в интернет - среде, организация удаленного доступа к информационным ресурсам с компьютера домашнего пользования, уровень соблюдения положений, связанных с компьютерным правом и т.д. Помимо этого, средний уровень отвечает за автоматизированные системы обработки критически важной (секретной) информации.

За реализацию и разработку политики среднего и высшего уровня несет ответственность руководитель службы безопасности, администратор информационной безопасности автоматизированных систем, и, непосредственно, администратор по обслуживанию корпоративной сети.

К низшему уровню политики информационной безопасности принадлежат конкретные подразделения и службы организации, которые детализируют деятельность высшего уровня политики. Деятельность данного уровня необходима не только для технического уровня, но и для

решения вопросов, требующих решения на уровне управления. Подразделения этого уровня определяют конечные цели, частные показатели и критерии в области безопасности информации, определяют полномочия конкретных пользователей, формулируют надлежащие требования доступа к информационным ресурсам и т.д. На этом уровне вытекают конкретные цели правил безопасности, которые определяют условия, при которых пользователь имеет право на доступ или не имеет. Это гарантирует, что более детальный подход в формировании правил может упростить настройку средств обеспечения информационной безопасности и внедрение системы. На данном уровне подробно описаны механизмы защиты и используемые программные средства (безусловно, в рамках уровня управления, а не технического). За деятельность низшего уровня несет ответственность системный администратор [8,21,22].

В рамках формирования политики информационной безопасности ведется анализ рисков. Это обеспечивает минимизацию на затраты по обеспечению безопасности. Эта данность в свою очередь характеризует основной принцип информационной безопасности, который гласит, что расходы на средства обеспечения защиты не должны быть выше цены на сам объект. По этой причине, если политика оформляется в виде документа, реализуемого на высоком уровне, который описывает общую стратегию, в таком случае анализ риска оформляют в виде перечня активов, требующих защиту данных [41].

Основополагающий список по формированию политики информационной безопасности образовательной организации можно найти в национальном стандарте РФ «Методы и средства обеспечения безопасности» ГОСТ Р ИСО/МЭК ТО 13335-3-2007.

Согласно анализу нормативной документации Челябинского юридического колледжа можно сделать вывод, что общая концепция информационной безопасности и контроля доступа к локальной вычислительной сети разработана в недостаточной мере. Существуют

только отдельные документы, которые относятся к высшему, среднему и низшему уровню безопасности.

К высшему уровню политики информационной безопасности можно отнести «Программу развития профессиональной образовательной организации среднего профессионального образования на 2014-2018 г». Документ содержит только задачу по обеспечению комплексной безопасности в образовательном процессе.

На среднем уровне политики информационной безопасности можно выделить следующий ряд документов: «Положение по защите и обработке персональной информации НОУ СПО «ЧЮК», «Положение по обеспечению безопасности в образовательном процессе НОУ СПО «ЧЮК», «Политика информационной безопасности в отношении персональной информации в НОУ СПО «ЧЮК». В данной документации определен основополагающий путь по развитию защиты персональных данных, по реализации и формированию комплексной защиты образовательного процесса [54].

К низшему уровню политики информационной безопасности можно отнести должностные обязанности специалистов по безопасности, системных администраторов и инженеров по информатизации.

В данной ситуации, если учитывать, что в образовательной организации существует разработанный комплекс документов, который определяет политику информационной безопасности, но отсутствует регламентация действий по использованию информационных образовательных ресурсов, что в свою очередь является неотъемлемой составляющей информационного ресурса образовательного процесса, отсутствует четкий алгоритм присвоения ролей доступа к информационным образовательным ресурсам. Этот факт является угрозой информационной системы. Кроме того не проработан и не определён порядок соответствующих действий при проведении итоговой и промежуточной аттестации.

2.2 Особенности и ограничения на ИОР согласно требованиям обеспечения информационной безопасности и контроля доступа

В разработке и применении электронного образовательного ресурса в образовательном процессе, обладающего актуальной степенью защиты данных в условиях стремительного прогресса, существует проблема. В независимости от существующих методов и средств обеспечения безопасности, с течением времени информационная безопасность становится не актуальной и уязвимость ее увеличивается. Данный факт дает почву для размышления в вопросе по осознанию опережающего или передового противодействия угрозам информационной безопасности учебного заведения.

Найти решение в данной проблеме можно только при условии, что будет соответствующая финансовая, нормативная и научно-методическая поддержка со стороны организации, и работа будет производиться достаточно компетентным персоналом, способным гарантировать достаточный уровень защищенности от всевозможных воздействий, которые могут привести к нежелательным последствиям [49].

Нормативной основой в организации СПО на пользование электронными образовательными ресурсами являются правила по работе сотрудников и студентов в локальной сети учебного заведения и правила по работе в интернет - сети, которые входят в концепцию ИБ колледжа, соответствующие требованиям обеспечения политики безопасности.

Правила по работе с интернет-ресурсами, включая также образовательные ресурсы.

1.1 Интернет - сеть предоставляет возможность доступа к различным ресурсам любого направления и содержания. Информационный отдел организации в праве на ограничения доступа к информационным ресурсам, которые не относятся к исполнению должностных обязанностей, а также имеют право ограничить и заблокировать доступ к интернет-

ресурсам, направленность и содержание которых противоречит международному и Российскому законодательству. Это информация угрожающего, непристойного, вредоносного и злоязычного характера, в том числе информация, которая оскорбляет достоинство и честь иных лиц, материалы, которые способствуют провоцированию национальных междоусобиц, призывающие к насилию, подстрекающие на совершение противоправных деяний, а также объясняющие процедуру изготовления и применения оружия и взрывчатых веществ и т.д.

1.2 При работе с информационными ресурсами в интернет-сети недопустимо:

1.2.1 Оглашать служебную и коммерческую информацию учебного учреждения, которая стала известна сотруднику по должностной обязанности или другим путем;

1.2.2 Распространять материалы, защищенные авторскими правами или затрагивающие патент на авторское изобретение, и прочую информацию, которая может нарушить авторское право или право собственности;

1.2.3 Распространение и загрузка ресурсов, которые содержат вредоносные программные продукты или прочие компьютерные программные коды, а также файлы, назначение которых ликвидировать, нарушить или лимитировать функциональность телекоммуникационного или компьютерного оборудования, с целью осуществить неправомерный доступ;

1.2.4 Копирование и распространение серийных номеров коммерческих программных продуктов и программ для последующей их генерации, недопустимо разглашение паролей, логинов и прочей информации, предоставляющей доступ к коммерческим или платным ресурсам в сети Интернет, кроме того недопустимо размещать ссылки на данную информацию.

1.3 При работе с информационными ресурсами в интернет-сети запрещено:

1.3.1 Загружать на сервер и запускать исполняемые файлы или другие программные продукты без соответствующей проверки на наличие вредоносного кода, установленным антивирусным программным обеспечением;

1.3.2 Политикой информационной безопасности строго запрещено применять аппаратные и программные средства, которые позволяют получить удаленный доступ к информационным или программным ресурсам образовательной организации;

1.4 Возможность получения доступа к информационным ресурсам не является залогом того, что данный затребованный ресурс разрешен политикой информационной безопасности колледжа.

1.5 Все сведения о запрошенных ресурсах, посещаемых студентами и сотрудниками сайтах, может быть продублирована и предоставлена администрации учебного заведения, а также непосредственным руководителям подразделения для подробных выяснений.

Правила по работе сотрудников и студентов организации СПО в локальной сети.

1. Данный свод правил регулирует полномочия и обязанности студентов, сопряженные с работой в локальной сети учебного учреждения и интернет-сети в частности, как и главные правила по работе и права всех сотрудников организации. Эти требования служат для организации и обеспечения образовательного потенциала компьютерной сети в целом в сочетании с системой мер по обеспечению безопасной интеллектуальной детальности обучающихся.

2. Основными принципами в организации политики информационной безопасности по работе в локальной и интернет-сети учебного заведения, являются:

– Равный одноименный доступ к ресурсам для всех студентов колледжа;

– Использование локальной и интернет-сети исключительно в образовательных целях;

– Обеспечение защиты студентов от вредоносных или незаконных информационных ресурсов, которые пропагандируют терроризм или насилие, наркотики, азартные игры, религиозную или этническую нетерпимость и т.д.

3. Полномочия сотрудников образовательной организации.

3.1. Начальник отдела информационной безопасности:

– Обеспечивает руководство и организацию по всей деятельности в реализации правил по работе в локальной и интернет-сети;

– Гарантирует свободный и равнозначный доступ студентов к локальной и интернет-сети в соответствии с возможностью учебного заведения и учебной программы;

– Является руководителем организационных мер, в том числе сотрудничеством с интернет-провайдером по лимитации доступа студентов к информационным ресурсам вредоносного или противозаконного характера в интернет-сети согласно действующем законодательным актам;

– Обеспечивает надзор в области соблюдения правил по работе студентов в локальной и интернет-сети;

– Обеспечивает поддержку и контроль по обновлению информационных и образовательных ресурсов организации. Размещает информационные материалы, одобренные и утвержденные директором;

– Незамедлительно информирует директора о выявленных угрозах и немедленно принимает меры по их устранению.

3.2 Преподаватели, имеющие компьютерную технику или закрепленный за ними учебный класс, обязаны:

– Проводить инструктаж техники безопасности студентам по работе в локальной сети колледжа и в интернет-сети;

– Использовать возможности интернет-технологий для расширения и обогащения образовательного процесса, по средствам выполнения конкретных заданий;

– Осуществлять постоянный надзор за деятельностью студентов в сети во время учебного процесса;

– Осуществлять незамедлительные меры в прекращении доступа студентам к информационным ресурсам запрещенного и неприемлемого содержания в интернет-сети;

– Незамедлительно информировать руководителя отдела по информационной безопасности о нарушениях;

– Не оставлять учебный кабинет без надзора во время занятий, а также не допускать студентов во время перерыва к работе в сети;

3.3 Преподаватели обязаны нести ответственность за целостность учебного оборудования организации СПО, прикрепленного к учебному кабинету, в котором проводится занятие.

3.4 Администратор сети обязан:

– Обеспечить эффективность и общую безопасность работы в локальной и интернет-сети;

– Предлагать нововведения и реализовывать меры в ограничении доступа студентов к вредоносным или противоправным информационным ресурсам в сети учебной организации, во избежание всевозможных рисков и угроз безопасности обучающихся;

– Незамедлительно информировать руководителя по информационной безопасности о нарушении правил или о наличии противозаконного контента в сети организации.

4. Полномочия и обязанности студентов

4.1 Обучающиеся вправе:

– На равноправный доступ к локальной и интернет-сети в соответствии с политикой информационной безопасности колледжа;

– Пользоваться интернет-соединениям во время обучения (только под надзором преподавателя);

– Быть проинформированными о правилах по работе в сети;

– На добросовестное и качественное обучение работе в локальной и интернет-сети.

4.2 Студенты обязаны придерживаться соблюдения соответствующих правил безопасности:

– Использовать интернет-соединение исключительно в образовательных целях;

– Запрещено входить в информационные ресурсы, не указанные преподавателем;

– Незамедлительно информировать преподавателя при обнаружении подозрительных материалов, содержание которых пропагандирует насилие или терроризм, религиозную и этническую нетерпимость, пропаганду наркотиков и азартных игр, и т.д.;

– Запрещено осуществлять деятельность, угрожающую целостности сети образовательной организации или провоцирующую на атаки прочей системы;

– Запрещается применение нелицензионных программных продуктов, материалов, защищенных авторским правом;

– Запрещена деятельность, нарушающая авторское право;

5. Ответственность при несоблюдении положения правил безопасности

5.1 Студенты за несоблюдение или нарушение положения утвержденных правил безопасности привлекаются к дисциплинарной ответственности согласно правилам внутреннего распорядка организации СПО.

5.2 Сотрудники за несоблюдение или нарушение положения утвержденных правил безопасности несут ответственность согласно трудовому кодексу или привлекаются к дисциплинарной ответственности.

5.3 За преступную деятельность или административные правонарушения, причиняющие ущерб собственности учебного учреждения, нарушители несут ответственность согласно закону РФ.

В соответствии с этим, для обеспечения ИБ информационных образовательных ресурсов в организации СПО, следует соблюдать соответствующие меры:

– Необходимо обеспечить достоверность и целостность образовательных информационных ресурсов с целью поступательного формирования личности студентов и педагогического состава;

– Необходимо обеспечить конфиденциальность образовательных информационных ресурсов для обеспечения защиты от несанкционированного доступа;

– Необходимо обеспечить доступность образовательных информационных ресурсов для предоставления возможности обратиться к материалу независимо от времени и места;

– Необходимо поддерживать вспомогательную инфраструктуру в оптимальном состоянии для её корректной работы и обеспечения сохранности концепции в целом [30].

2.3 Разработка концепции политики безопасности и контроля доступа к ЛВС НОУ СПО «ЧЮК».

Существует множество различных протоколов и устройств, которые позволяют ограничить доступ к ЛВС или контролировать подключение. Протокол **802.1X -** это стандарт IEEE для контроля доступа к сети на основе портов (PNAC) в точках доступа к проводным и беспроводным сетям. 802.1X определяет элементы аутентификации для любого пользователя или устройства, которые пытаются получить доступ к локальным или беспроводным сетям.

Локальная вычислительная сеть – совокупность кабельной системы, серверов, сетевого оборудования, программного обеспечения и средств вычислительной техники, обеспечивающая реализацию информационных технологий.

Локальная вычислительная сеть, как составная часть информационной системы, является активом любого предприятия, который имеет ценность и должен быть надежно защищен. Ценность представляет собой как оборудование локальной вычислительной сети (ЛВС), так и информация, хранящаяся в ЛВС.

В целях информационной безопасности в образовательной организации, рабочие станции имеют определенный и постоянный набор характеристик

То есть пользователь не может самостоятельно изменить их, для этого нужно разрешение отдела информационной безопасности (все устройства опечатаны и разграничен доступ к информации).

Основную опасность составляет «атака подмены устройства», ведь так или иначе, злоумышленнику придется преодолевать пусть недостаточные, но примененные средства защиты, а идентификация конкретного устройства, которое подключается к серверу, проводится редко. Идентификация – процесс присвоения объекту уникального идентификатора. Таким образом, злоумышленник может принести портативный компьютер и, переключив сетевой адаптер легитимного устройства на свое, (или подключив устройство непосредственно к роутеру, сможет обойти физические ограничения, принятые администратором). Иначе говоря, необходим комплексный подход к реализации процедуры идентификации состояний активного сетевого оборудования как динамического объекта с использованием методов распознавания образов.

Концепция предполагает создание процесса идентификации рабочих станций сети, а также пользователей. Практическое использование данного

подхода позволяет повысить качество администрирования и уровень защищенности данных

Для начала, администратор записывает сигнатуры всех рабочих станции в базу данных (которая в последующих ситуациях будет выступать в роли «базы знаний» для нашей интеллектуальной системы).

Данная база будет использоваться для дальнейшей настройки сервера доступа (RADIUS, в нашем случае NAP от Microsoft). Сервер NAP будет отвечать за идентификацию устройств подключенных к сети. Политикой будет определен ряд параметров рабочей станции, которые в совокупности определят текущий статус подключения.

Статус подключения это состояние порта к которому подключена станция, он может быть 3х видов:

1. Залокирован. Рабочая станция не выполнила ни одного условия политики.
2. Ограниченное подключение. Рабочая станция подключена к сети и может получить доступ к обновлению антивирусного ПО
3. Разрешен. Рабочая станция может работать в рамках ограничений учетной записи пользователя.

Описанная выше концепция обеспечит управление сложным динамическим многопараметрическим активным сетевым оборудованием и повышенный уровень информационной безопасности оборудования локальной сети, и защитит информацию, а также предоставит интеллектуальную поддержку механизма администрирования ЛВС.

При построении сети использовалось сетевое оборудование, которое позволяет задействовать протокол безопасности 802.1X AAA. Данный протокол позволяет настроить физический доступ к локальной вычислительной сети, с использованием RADIUS сервера.

Для обеспечения образовательного процесса, преподаватели и студенты имеют привязанные к учетной записи пользователя сетевые каталоги. Эти каталоги расположены на файловых серверах организации,

Структура организована таким образом, чтобы преподаватели видели каталоги студентов и могли просматривать результаты самостоятельных работ, а студенты могли видеть только свой каталог и каталог преподавателей, откуда они могут брать лекционные материалы и задания от преподавателей. Такая структура позволяет избежать переписывания и подмену результатов самостоятельных работ.

Сами сервера защищены антивирусным программным обеспечением, которое своевременно обновляется.

На каждом компьютере произведены базовые настройки безопасности Uefi-Bios, установлен пароль на изменение параметров загрузки и конфигурирование самого Uefi-Bios, отключены неиспользуемые устройства. Установлена сертифицированная ОС, и регламентированный набор ПО в зависимости от специфики аудитории. В базовый состав обязательно включены все форматы архиваторов, программы чтения PDF и антивирусное ПО, которое управляется централизованно через сервер администрирования. Антивирусная защита подразумевает использование политик, которые могут оперативно применятся в зависимости от регламента безопасности и конкретной ситуации. Например, во время Экзаменов отключается доступ к интернет ресурсам за исключением белого списка адресов. Отключается возможность подключения внешних запоминающих устройств и т.д.

То есть разработанная концепция безопасности и контроля доступа к ЛВС, подразумевает многоуровневую проверку устройств и пользователей. Прежде чем предоставить те или иные права к сети передачи данных, а также к самим данным, и уже на основе выданных прав средствами файловой системы разграничиваем доступ к данным на серверах организации, где дополнительную защиту обеспечивает антивирусное ПО и сетевые настройки оборудования, исключающие возможность подключения к сети неавторизованных устройств.

2.4 Информационная безопасность образовательного информационного ресурса в НОУ СПО «ЧЮК»

Основная цель деятельности НОУ СПО «ЧЮК» направлена на повышение качества усвоения профессиональных компетенций за счет внедрения новаторских электронно-образовательных технологий в образовательный процесс учебного учреждения. Электронное обучение и основанные на ней формы и технологии способны качественно повысить профессиональную подготовку будущих специалистов и преумножить востребованность у работодателей.

В образовательной организации активно ведется работа по разработке и развитию средств современного обучения на базе системы ЭОР, формируются новые программы подготовки обучающихся, различного уровня, отвечающие требованиям рынка труда, открываются новые специализации и специальности по всевозможным направлениям промышленности. Динамично развиваются системы дистанционного, дополнительного и непрерывного образования, внедряется система трудоустройства на основе взаимодействия организации и предприятий.

В Челябинском юридическом колледже реализована технология электронного обучения на базе системы виртуальной образовательной среды Elearning 4G

Elearning 4G (модульная ориентированно-объектная динамическая среда для обучения) – это среда управления, с помощью которой можно организовать взаимодействие между студентом и преподавателем. Данная система подходит также для организации традиционного дистанционного обучения и годится в качестве дополнительного источника информации очного обучения.

Краткие системные возможности:

1. Общедоступна с любого компьютерного устройства, где присутствует возможность выхода в Интернет.

2. Обеспечивает персональный доступ к информационным ресурсам. Эта данность означает, что управление работами происходит в одностороннем порядке, и что работа студентов независима от других лиц. За каждым обучаемым закреплен личный электронный журнал, который заполняется по результат выполненных работ;

3. Существует система автоматического контроля выполнения различных заданий. Данный инструмент облегчает работу с одаренными студентами, самостоятельно изучающими образовательную программу, также с обучаемыми, которые отстают по учебной программе.

4. Различные инновационные инструменты дают возможность более продуктивно организовывать учебную работу и осуществлять контроль за выполнением контрольных и курсовых работ, семинаров и т.д. Тем самым более эффективно и рационально использовать учебное время студентов и преподавателей [2].

Применяя систему Elearning 4G, преподаватель способен разрабатывать и внедрять различные курсы, наполняя их теоретическим материалом в виде текста, презентаций, тестов и т.д. Для использования учебной среды Elearning 4G достаточно обладать любым браузером, благодаря этому свойству пользование данной средой удобно как преподавателям, так и студентам. Согласно итогам выполненных студентами заданий, преподаватель способен выставить соответствующую оценку и написать комментарий.

С точки зрения информационной безопасности учебная среда Elearning 4G обладает достаточной защитой от всевозможных угроз из вне, хакерских атак и спама. Для того чтобы оградить образовательный курс от несанкционированного доступа, достаточно в настройках убрать галочку «разрешить» в окне самостоятельной регистрации пользователя.

Но определенные опции безопасности данных могут быть весьма полезными для комфортной работы пользователей и при администрировании системы.

Политика информационной безопасности образовательной среды Elearning 4G:

Здесь мы проанализируем только определенные опции безопасности, на которых необходимо сосредоточить внимание администратора. Другие опции рекомендуется сохранить без изменений.

Чтобы пройти в раздел политики безопасности сайта, необходимо пройти в раздел администрирования и найти вкладку «Настройки», а после пройти по соответствующей ссылке рисунке 2.1.

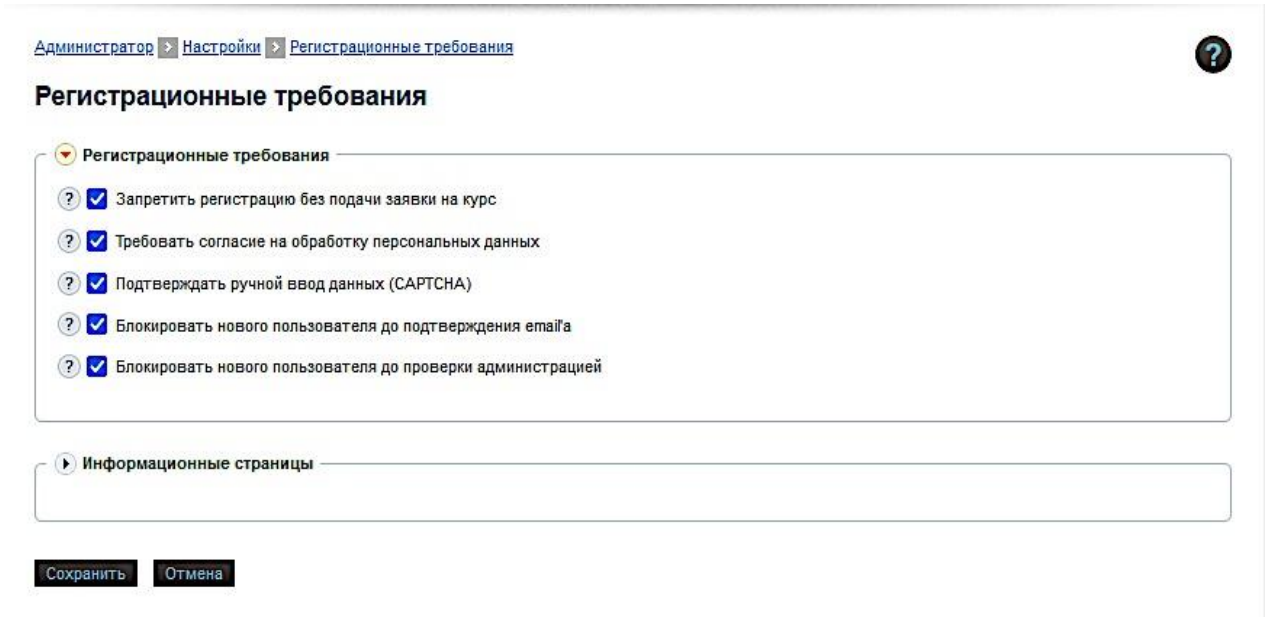

Рисунок 2.1 – Политика информационной безопасности сайта Elearning 4G

Политика паролей определяет уровень сложности при входе для пользователя. Согласно настройке «по умолчанию» — это достаточно непростое сочетание символов и знаков, для комфортного входа в систему доступ можно упростить.

Данных настроек достаточно для безопасной работы информационного ресурса на сайте (рисунок 2.2). С иными настройками необходимо обращаться с осторожностью, так как при неверной регулировке можно нанести ущерб курсу. Согласно настройке «по умолчанию» в системе Elearning 4G предусмотрена только ручная регистрация. Что, в свою очередь, обязывает администратора системы самостоятельно регистрировать студентов на сайте.

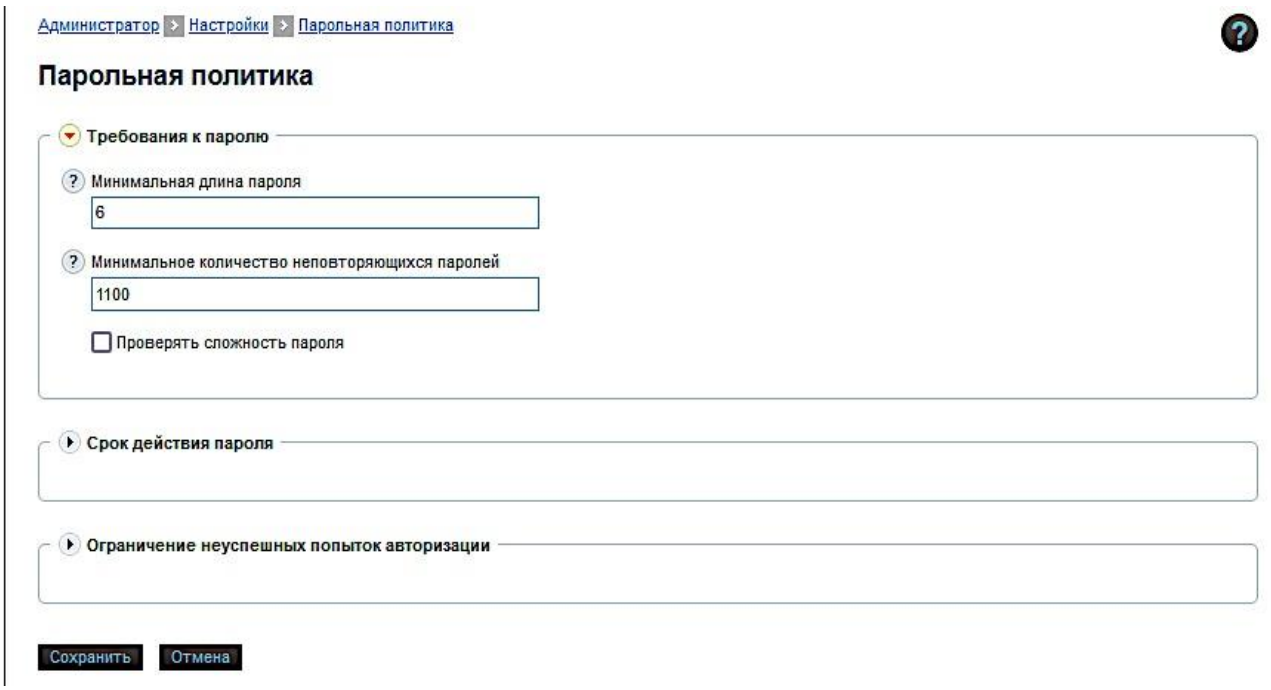

Рисунок 2.2 – Окно политики безопасности пароля

Однако эта мера весьма эффективна с точки зрения информационной безопасности сайта. Регистрация потусторонних лиц станет невозможна. Это означает, что на сайте будут отсутствовать заброшенные аккаунты и различный спам.

Помимо данного способа регистрации существуют и другие. В первую очередь стоит отметить самостоятельную регистрацию пользователя по электронной почте. В случае если этот тип регистрации разрешен со стороны администратора сайта, то пользователь может самостоятельно пройти регистрацию на сайте с дальнейшим его подтверждением, которое осуществляется при переходе по гиперссылке в e-mail.

Данный вид регистрации является абсолютно приемлемым.

Среда Elearning 4G обладает несколькими вариантами записи на электронные курсы. Наиболее популярный и востребованный это тот, который включен по умолчанию – ручная запись и гостевой доступ.

В том случае, если гостевой доступ разрешен, зарегистрироваться в системе может абсолютно любой пользователь, и тем самым сможет

просматривать информационные материалы курса. Однако в гостевом режиме нет возможности работы с тестами, заданиями и т.д.

При ручной регистрации пользователя преподаватель должен самостоятельно записывать студентов на свои курсы, производя работу по поиску обучающихся в списке зарегистрированных пользователей сайта.

Из этого можно сделать вывод, что обеспечение информационной безопасности ЭОР напрямую зависит от политики информационной безопасности образовательной среды Elearning 4G.

ВЫВОДЫ ПО ГЛАВЕ II

Во второй главе проведен анализ концепции информационной безопасности организации СПО. Подробно проанализировали каждый из сегментов концепции информационной безопасности. Определили, по каким направлениям образовательная организация должна обеспечивать защиту и т.д.

Проанализировали нормативно-правовую базу на различных уровнях политики ИБ в НОУ СПО «ЧЮК».

К высшему уровню политики информационной безопасности можно отнести «Программу развития профессиональной образовательной организации среднего профессионального образования на 2021-2024 г.г.».

На среднем уровне политики информационной безопасности можно выделить следующий ряд документов: «Положение по защите и обработке персональной информации НОУ СПО «ЧЮК» «Положение по обеспечению безопасности в образовательном процессе НОУ СПО «ЧЮК», «Политика информационной безопасности в отношении персональной информации в НОУ СПО «ЧЮК».

К низшему уровню политики информационной безопасности можно отнести должностные обязанности специалистов по безопасности, системных администраторов и инженеров по информатизации.

Согласно анализу нормативной документации НОУ СПО «ЧЮК» можно сделать вывод, что общая концепция информационной

безопасности разработана в недостаточной мере. Отсутствие регламентации действий по использованию информационных образовательных ресурсов, что в свою очередь является неотъемлемой составляющей информационного ресурса образовательного процесса и т.д.

Также в рамках исследовательской работы были изучены основные ограничения и особенности по работе с электронными образовательными ресурсами. Были проанализированы правила по работе с образовательными интернет-ресурсами и правила по работе в локальной сети СПО, а также степень ответственности за несоблюдение прописанных норм.

В ходе работы выяснили, что в Челябинском юридическом колледже реализована технология электронного обучения на базе системы виртуальной образовательной среды Elearning 4G

Elearning 4G (модульная ориентированно-объектная динамическая среда для обучения) – это свободная и независимая среда управления, с помощью которой можно организовать взаимодействие между студентом и преподавателем. Данная система подходит также для организации традиционного дистанционного обучения, и годится в качестве дополнительного источника информации очного обучения.

С точки зрения информационной безопасности учебная среда Elearning 4G обладает достаточной защитой от всевозможных угроз из вне, хакерских атак и спама. Для того чтобы оградить образовательный курс от несанкционированного доступа достаточно в настройках убрать галочку «разрешить» в окне самостоятельной регистрации пользователя.

Но определенные опции безопасности данных могут быть весьма полезными для комфортной работы пользователей и при администрировании системы.

ЗАКЛЮЧЕНИЕ

Вследствие анализа многочисленных информационных источников по теме магистерской диссертации можно сделать вывод о практической важности разработки и внедрении политики безопасности образовательной организации.

В первой главе магистерской диссертации проведен всесторонний анализ типов угроз и оценки каждого объекта сетевой инфраструктуры, который стал основой для разработки и внедрения переработанной концепции политики безопасности и контроля доступа к ЛВС НОУ СПО «ЧЮК». Концепция будет включать в себя политику управления конфигурациями и обновлениями, мониторинг и аудит систем, а также другие превентивные меры операционных политик и процедур. Обязательным условием является наличие тестовой лаборатории с уменьшенным аналогом типичной ИТ-среды корпорации. Накопленные знания и опыт, полученные при анализе угроз и уязвимостей систем, являются, по сути, уникальной базой знаний и будут служить фундаментом в построении надежной и защищенной инфраструктуры и последующем обучении персонала, а также самостоятельной работы студентов в лабораториях. Однако следует учесть, что при изменении (модернизации) инфраструктуры, добавлении новых объектов необходимо произвести повторную оценку и анализ и впоследствии модифицировать политику безопасности. Так же нужно проводить оценку модели угроз и модернизировать политику безопасности в связи с постоянными вызовами с которыми сталкиваются образовательная организация в процессе своей деятельности. Проводится такая оценка, и переработка политик, не реже раз в пять лет.

Проектирование и построение каждого уровня безопасности должны предполагать, что любой уровень может быть нарушен злоумышленником. Кроме того, каждый из уровней имеет свои специфические и наиболее эффективные методы защиты.

Во второй главе магистерской диссертации изучены основные направления политики информационной безопасности в образовательной организации НОУ СПО «ЧЮК». Подробно проанализировали каждый из сегментов концепции информационной безопасности. Определили, по каким направлениям образовательная организация должна обеспечивать защиту и контролировать доступ к ЛВС. Согласно анализу нормативной документации колледжа можно сделать вывод, что общая концепция информационной безопасности разработана в недостаточной мере и требует определенной доработки. Были изучены основные ограничения и особенности по работе с образовательными ресурсами. Проанализированы правила по работе с образовательными Интернет-ресурсами и правила по работе в локальной сети СПО, а также степень ответственности за несоблюдение прописанных норм.

В ходе работы выяснено, что в Челябинском юридическом колледже реализована технология электронного обучения на базе системы виртуальной образовательной среды Elearning 4G. С точки зрения информационной безопасности данная среда обладает достаточной защитой от всевозможных угроз.

В рамках исследования спроектирована и испытана концепция политики безопасности и контроля доступа к ЛВС для организации самостоятельной работы студентов НОУ СПО «ЧЮК», а также сотрудников. Разработали комплекс мер по защите данных, которые могут ограничить доступ к информационным ресурса, обеспечить контроль за деятельность студентов во время проведения занятий и существенно повысить компетентность и квалификацию преподавателей в вопросе ИБ при работе с информационными ресурсами колледжа.

Таким образом, цель работы достигнута, задачи выполнены, гипотезы нашего исследования подтверждены.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. iSpringSuite. База знаний [Электронный ресурс]// Режим доступа: https://www.ispring.ru/ispring-suite/knowledge. Дата обращения 17.04.2023.

2. Андреев, А.В. Практика электронного обучения с использованием Moodle [Текст] / А.В. Андреев, С.В. Андреева, И.Б. // Доценко. Изд-во. ТТИ ЮФУ, 2018. - 146 с.

3. Абдулина, Е.Л. Общесистемные требования к электронным учебным материалам: лекция [Электронный ресурс] /Е.Л. Абдулина / Режим доступа: http: //www.cctpu.edu.ru/conf/sec7/tez02.htm. Дата обращения 12.03.2023.

4. Бадарчев, Д.А. Информационные и коммуникационные технологии в образовании [Текст] / Д.А Бадарчев – М.: ИИТО ЮНЕСКО, 2017 – 318 с.

5. Баранова, Ю.Ю. Методика использования электронных учебников в образовательном процессе [Текст] / Ю.Ю. Баранова // Информатика и образование. - 2016. - 47 с.

6. Бекетов, Н. Информационная безопасность развития государства [Текст] / Н. Бекетов // Информационные ресурсы России, № 8, 2017. – 35 с.

7. Белов, Е.Б. Основы информационной безопасности. [Текст] // Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов.– М.: Горячая линия – Телеком, 2016. – 534 с.

8. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс. -2018. - 454 с.

9. Белов, Е.Б. Основы информационной безопасности. //Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком. - 2016. – 243 с.

10. Галатенко, В.А. Стандарты информационной безопасности: курс лекций [Текст] / В.А. Галатенко //. Учебное пособие. - 2-ое издание. М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий». - 2017. - 264 с.

11. Гафарова Е.А. К вопросу проектирования онтологий предметной области при подготовке магистров по направлению информационная безопасности [Текст] / Е.А. Гафарова, Ф.В. Синицын // Сборник научных трудов. 2016. С. 54-57.

12. ГОСТ Р 57628-2017 «Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности». [Электронный ресурс] / Режим доступа: http://docs.cntd.ru/ document/1200146707 Дата обращения 24.04.2020.

13. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. [Электронный ресурс] / Режим доступа: http://docs.cntd.ru/document/1200146707 Дата обращения 17.03.2020.

14. ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». [Электронный ресурс] / Режим доступа: http://docs.cntd.ru/document/1200146707 Дата обращения 10.03.2020.

15. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий». [Электронный ресурс] / Режим доступа: http://docs.cntd.ru/document/1200146707 Дата обращения 21.04.2023.

16. Диниц, Г.Д. Самостоятельная работа как средство профессиональной подготовки студента. [Текст]/ Г.Д Диниц. – Высш. образование в России. 2015. – 176с.

17. Доктрина информационной безопасности Российской Федерации. [Электронный ресурс] / Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html Дата обращения 29.04.2023.

18. Дьяченко, В.К. Организационная структура учебного процесса и ее развитие. [Текст]/ В.К. Дьяченко. - М.: Педагогика, 2018. - 160 с.

19. Зеер, Э.Ф. Психология профессионального образования [Электронный ресурс] / Э.Ф. Зеер. Учеб. пособие. – М.: Академия, 2016. - 416 с. – URL:http://www.academiamoscow.ru/ftp_share/_books/fragments /fragment_23598.pdf. Дата обращения 14.03.2023.

20. Зимняя, И. А. Педагогическая психология. Учебник для вузов. Изд. второе. [Текст]/ И. А. Зимняя. – М.: Издательская корпорация «Логос», 2014. -384 с.

21. Информационная безопасность: Учебное пособие [Текст] / В.В. Гафнер. - Рн/Д: Феникс, 2016. - 324 с.

22. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности. [Электронный ресурс] / Режим доступа: http://citforum.ru /security/articles/categorizing/3.shtml**.** Дата обращения: 02.05.2020.

23. Кириллов А.В. Организационно-педагогические условия совершенствования самостоятельной работы в профессиональном образовании государственных служащих. [Текст] / А.В. Кириллов - М.: СПБ.: БХВ-Петербург, - 2018. - 16 с.

24. Коджаспирова, Г. М. Педагогический словарь [Текст] / Г. М. Коджаспирова, А. Ю. Коджаспиров. — М.: Academia, 2016. - 176 с.

25. Лукацкий А. Обеспечение информационной безопасности современного ВУЗа. [Электронный ресурс] / А. Лукацкий // Режим доступа: http://www.comprice.ru/articles/detail Дата обращения 9.03.2020.

26. Нильсон О.А. Самостоятельная работа. [Текст] / О.А. Нильсон // Российская педагогическая энциклопедия. Т. 2. М.: Педагогика, 2018. - 308 с.

27. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. №149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 01.03.2020.

28. Обеспечение информационной безопасности в образовательной организации. [Электронный ресурс] / Режим доступа: http://www.iccwbo.ru/blog/2016/obespehenie-informatsionnoy-bezopasnosti/. Дата обращения: 10.04.2020.

29. Особенности защиты информации в образовательном учреждении. [Электронный ресурс] / Режим доступа: http://pandia.ru/text/79/076/98286.php. Дата обращения: 13.05.2020.

30. Партыка Т.Л. Информационная безопасность: Учебное пособие [Текст] / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2016. - 432 с.

31. Петров С.В. Информационная безопасность: Учебное пособие [Текст] / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2017. – 296 с.

32. Пилкасинского П. И. Педагогика: учеб. пособие для студентов пед. вузов и пед. колледжей [Текст] / П. И. Пилкасинского. – М.: Пел. О-во России, 2018. – 640с.

33. Письменная, Е.Е. Самостоятельная работа студентов: методические рекомендации. [Текст]/ Г.Г. Силласте, Е.Е. Письменная, Н.М. Белгарокова. – М.: Финансовый университет, кафедра «Теоретическая социология». 2017. –35с.

34. Полат Е.С. Новые педагогические и информационные технологии в системе образования: учебное пособие [Электронный ресурс] / Е.С. Полат, М. Ю. Бухаркина, М.В. Моисеева, А.Е. Петров // Под ред. Е.

С. Полат. -6-е изд. — М.: Академия, 2019. 252 с. – Режим доступа: http://library.kpi.kharkov.ua/NEW/NewPiITvSO. Дата обращения 17.03.2020.

35. Положение об организации работы по охране труда, обеспечению безопасности образовательного процесса в ГБПОУ [Электронный ресурс] / Режим доступа: SUOT-PP-02-01-Ob-organizacii-raboty-po-OT-obespecheniyu-bezopasnosti-obrazovatelnogo-processa. Дата обращения 17.03.2020

36. Прессман, Л.П. Методика и техника эффективного использования средств обучения в учебно-воспитательном процессе. [Текст] / Л.П. Прессман. - СПб.: СПбГУП, 2016. - 219 с.

37. Программа развития ЮУрГТК [Электронный ресурс] / Режим доступа: [http://sustec.ru/svedeniya-o-kolledzhe/dokumenty/PROGRAMMA-RAZVITIYA-YUUrGTK-na-2014-2018gg-dlya-chirpo.pdf/ Дата обращения 26.03.2020.

38. Ранних В.Н. Электронный практикум как дидактическое средство повышения качества образования в вузе [Электронный ресурс] / В.Н. Ранних/ Режим доступа:http://cyberleninka.ru/article. Дата обращения 02.03.2020.

39. Роберт И. Современные информационные технологии в образовании: дидактические проблемы; перспективы использования [Текст] / И. Роберт. - М: Школа-Пресс, 2018 -292 с.

40. Роберт, И.В. Теория и методика информатизации образования (психолого-педагогические и технологические аспекты). [Текст] / И.В. Роберт. - М.: ИИО РАО, 2017. - 234с.

41. Сабанов А.Г. О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии [Электронный ресурс] / А.Г. Сабанов / Режим доступа: https://cyberleninka.ru/article/n/o-probleme-dostovernosti-identifikatsii-polzovatelya-pri-udalennom-elektronnom-vzaimodeystvii. Дата обращения 12.04.2020.

42. Селевко Г.К. Современные образовательные технологии [Текст] / Г.К. Селевко. - М: Народное образование, 2016 -255 с.

43. Сенашенко, В.С. Самостоятельная работа студентов: актуальные проблемы [Текст] / В. С. Сенашенко, Н. В. Жалнина. - Высш. образование в России. — 2016. – 109 с.

44. Терехова, Н.Р. Методические рекомендации по организации самостоятельной работы студентов. [Электронный ресурс] / Н.Р. Терехова. / Режим доступа: http://www.miu-iv.ru/. Дата обращения 04.02.2020.

45. Тихомиров, А.А. Компьютерные технологии в науке, практике и образовании. [Электронный ресурс] / А.А. Тихомиров. / Режим доступа: http://нэб.рф/catalog/ Дата обращения 19.03.2020.

46. Тихонов В.А. Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты [Текст] /В.А. Тихонов, В.В. Райх // Гелиос АРВ.- 2019г. - 528 с.

47. Федорова, А.М. Модель организации внеаудиторной самостоятельной работы [Текст] / А.М. Федорова, Л.П. Якушина // Высш. образование в России. — 2019. – 90 с.

48. Хестер, Н. Microsoft Front Page для Windows. [Текст] / Н. Хестер - М.: ДМК Пресс. – 2017. – 450с.

49. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений/ П.Б. Хорев.–М.:Издательский центр «Академия», 2017.–256 с.

50. Черногаева, Н.А. Методическое обеспечение при осуществлении контроля самостоятельной работы студентов: методическая разработка зам. директора по УМР ФГОУ СПО «Донской техникум информатики и вычислительной техники». [Текст] / Н.А. Черногаева. - М.: Педагогическое общество России, - 2018 -41 с.

51. Шемяков О.А. Научно-методический аппарат оценки уязвимости системы обеспечения безопасности информации в современном вузе - диссертация на соискании степени канд. техн. наук,

2013 Серпухов. [Электронный ресурс] / О.А. Шемяков. / [Электронный ресурс]: http://www.dissercat.com/content/nauchno-metodicheskii-apparat-otsenki-uyazvimosti-sistemy-obespecheniya-bezopasnosti-informa Дата обращения 03.03.2020.

52. Щеголева, О. Н. Роль и место самостоятельной контролируемой работы в новой парадигме образования [Текст] / О. Н. Щеголева. - СПб.: СПбГУП, - 2017. – 71 с.

53. Явич, М.П. Концепции обучения информационных технологий ElMI- metodikjournal. [Текст] / М.П. Явич, Ц.Г. Мишеладзе, М.Т. Тхелидзе. Азербаджанский педагогический университет. 2016.-42 с.

54. «Южно-Уральский государственный колледж» Официальный сайт ГБПОУ [Электронный ресурс]: / Режим доступа: http://sustec.ru. Дата обращения 27.03.2020.

55. Герасименко В. А. Защита информации в автоматизированных системах обработки данных: развитие, итоги, перспективы. Зарубежная радиоэлектроника, 2003, № 3.

56. Закер К. Компьютерные сети. Модернизация и поиск неисправностей. СПб.: БХВ-Петербург, 2001.

57. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети — анализ технологий и синтез решений. М.: ДМК Пресс, 2004. — 616 с.