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

Формирование основ кибербезопасности у студентов профессиональных образовательных организаций при преподавании специальных дисциплин.

Выпускная квалификационная работа по направлению

44.04.04 Профессиональное обучение (по отраслям)

Направленность программы магистратуры

«Управление информационной безопасностью в профессиональном образовании»

Форма обучения заочная

Проверка на объем заимствований:
91,12 % авторского текста
Работа рекомендована к защите
«26» 01 2025 г.
Зав. кафедрой АТИТ и МОТД
_____ Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Поспелова Дарья Сергеевна
Научный руководитель:
к.п.н., старший преподаватель
кафедры АТ, ИТ и МОТД
Гафарова Елена Аркадьевна

Челябинск, 2026

Оглавление

Формирование основ кибербезопасности у студентов профессиональных образовательных организаций при преподавании специальных дисциплин.

ВВЕДЕНИЕ

*Актуальность исследования***.** Современное общество находится в постоянном движении и для его развития необходимо создание и использование качественно новой информации. Основная ее роль – это функционирование жизнедеятельности людей, общества и государства в целом. В настоящее время глобальная информационная среда имеет сильное влияние на человека, в результате чего он проходит информационную социализацию.

Информационная социализация – это социализация человека под воздействием нового социального института – информационного пространства, под которым понимают процесс усвоения индивидом из информационного пространства образцов поведения, психологических установок, социальных норм и ценностей, знаний, навыков, позволяющих ему успешно функционировать в обществе . Реальность сегодня – это рост экономической и технологической доступности интернет – сетей с существующими там ресурсами.

Информационно-коммуникационные системы, такие как, компьютер, телефон и т.д. пользуются спросом абсолютно во всех сферах деятельности субъекта общественной жизни. Данные системы используются в обеспечении государственной безопасности, здравоохранения, торговли, образования, и т.п.

Воздействие глобальной информационной среды на социальный и политический процесс развития государства весьма всесторонне, но в тоже время противоречиво.

Противоречие заключается в том, что информационная среда, с одной стороны, способствует многогранному развитию человека с помощью использования компьютерных игр, обучающих и развивающих программ, интерактивного телевидения, электронной прессы. Другой стороной

информационной среды является появление таких новых видов преступлений, как компьютерная преступность и компьютерный терроризм.

Сегодня в образовании приоритетной задачей является дальнейшая информатизация системы образования, создание условий для наращивания информационно-технологической базы образовательных учреждений, развитие современных методов обучения на базе информационных технологи. В связи с этим, возникает острый вопрос о защите учеников, которые проводят огромное количество времени за компьютером и в интернет-пространстве в процессе обучения и познания нового, от компьютерных (кибер) преступников и преступлений.

Важно осознать необходимость защиты детей от негативного информационного воздействия, осуществления педагогического контроля и надзора в сфере кибербезопасности.

Кибербезопасность (компьютерная безопасность) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Степень разработанности проблемы исследования. Изучением кибербезопасности занимались такие исследователи как Т. В. Воробьева, Л. В. Крапивская, В. П. Конецкий, К.Н.Дудкина, Б. Ф. Ломова, Н. И. Гендина, Н. В. Гутова, Л. С. Зазнобина др. Пересмотр методов организации учебного процесса, а также его кадрового обеспечения необходим в связи информатизацией общества, которая является одной из характеристик открытого образования.

Специалисты современного образования нуждаются в такой подготовке, которая даст им определенные компетенции и будет учитывать их постоянную изменяющуюся роль в учебном процессе. Педагог в открытом образовательном пространстве: больше занимается организацией деятельности обучающихся, чем дает им информацию; больше отвечает на вопросы обучающихся, чем излагает и рассказывает материал по теме; больше занимается обсуждением возможных путей решения задачи с обучающимися, чем предоставляет уже готовую инструкцию по выполнению задания.

В силу возрастных особенностей студенческой молодежи, обучающейся в учреждениях среднего профессионального образования, ее социально-психологической незрелости, податливости к информационным воздействиям в сочетании с ее активностью в киберпространстве решение задачи формирования культуры кибербезопасности обучающихся колледжа приобретает особую значимость.

Решение этой задачи осуществляется в специально организованной образовательной среде, обладающей потенциалом для эффективного формирования у обучающихся колледжа системы практико-ориентированных знаний основ кибербезопасного поведения, а также умений и навыков их реализации в киберпространстве. В связи с этим формирование культуры кибербезопасности должно стать важной составляющей профессиональной подготовки и неотъемлемой профессиональной компетенцией обучающихся колледжа.

Актуальность проблемы основы кибербезопасности при преподавании информатики для студентов на ступени средне-специального образования обуславливается ростом угроз и опасности, со стороны интернет-пространства и не умением учащихся их ликвидировать. Степень разработанности данной проблемы является крайне низкой, что требует тщательного изучения проблемы и поиск способов формирования основ кибербезопасности студентов средне-специального образования.

Проблема по формированию основ кибербезопасности при преподавании специальных дисциплин в колледже сегодня достаточно новая, поэтому возникает ряд противоречий между необходимостью у студентов формирования основ кибербезопасности, осмысления ими самостоятельных действий в сети Интернет и недостаточной разработанностью специфики преподавания Информатики с элементами обучения основам кибербезопасности сопровождения этого процесса в учебном учреждении.

Проблема исследования обусловлена противоречием открытой информационной среды и связана с необходимостью разработки системы для

защиты информации и от киберугроз в условиях цифровизации, содержащую совокупность эффективных методов и подходов.

В рамках частичного разрешения этой проблемы была сформулирована тема исследования: «Формирование основ кибербезопасти для студентов средне-профессиональных организаций при преподавании специальных дисциплин».

Объект исследования: образовательный процесс в профессиональной образовательной организации.

Предмет исследования: процесс формирования основ кибербезопасности обучающихся при преподавании спецдисциплин

Цель исследования: теоретически обосновать и практически проверить эффективность программы по формированию основ кибербезопасности учащихся на ступени средне-специального образования.

Гипотеза исследования: формирование основ кибербезопасности у студентов средне специального образования будет успешным, если:

• если будут внедряться обучающие занятия и лекции;

• если будут использоваться современные методы преподавания дисциплин;

Задачи исследования:

1. Раскрыть сущность основ кибербезопасности как педагогического феномена
2. Изучить и выявить особенности формирования личностных качеств студентов ПОО
3. Провести анализ учебно-методической документации спецдисплин и выявить содержание, на основе которого возможно формировать основы кибербезопасности
4. Проанализировать ИОС базы исследования и особенности образовательного процесса
5. Разработать методику формирования основ кибербезопасности студентов ПОО
6. Провести апробацию разработанной методики

Новизна исследования обусловлена разработкой программы по формированию основ кибербезопасности учащихся с помощью внедрения в процесс обучения методических рекомендаций опирающихся на новейшие знания.

В исследовании применялись следующие научные методы:

• *теоретические: изучение и анализ педагогической, научной литературы по проблеме исследования;*

• *эмпирические: анализ документов, тестирование, опрос.*

Теоретическая значимость исследования заключается в описании сущности кибербезопасности; рассмотрении основ кибербезопасности на ступени среднего образования; обосновании необходимости внедрения обучения основам кибербезопасности в процесс обучения студентов СПО.

Практическая значимость исследования заключается во внедрении, на основе проведенного исследования, разработанной программы по формированию основ кибербезопасности на ступени СПО. Результаты исследования могут быть использованы для индивидуальной и групповой работы, направленной на формирование основ кибербезопасности на ступени средне-специального образования.

База исследования: Челябинская область , г.Нязепетровск, Нязепетровский филиал Каслинского промышленно-гуманитарного техникума

Структура исследования. Выпускная квалификационная работа состоит из: введения, двух глав, 6 параграфов, заключения, списка используемой литературы и приложения.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ОСНОВАНИЯ ФОРМИРОВАНИЯ ОСНОВ КИБЕРБЕЗОПАСНОСТИ У СТУДЕНТОВ.

1.1 Сущность основ кибербезопасности как педагогического феномена

Педагогический феномен — это особое, значимое событие, свойство или состояние в образовательной системе, которое выходит за рамки обыденного, раскрывая глубинные процессы воспитания и обучения, часто связанное с уникальным взаимодействием педагога, ученика и социальной среды, например, возникновение мощной мотивации, нестандартное решение проблемы или эффект саморазвития личности, стимулированный педагогическим воздействием. Это может быть как явление в рамках урока, так и широкое социально-педагогическое взаимодействие, когда система образования интегрируется с внешним миром, формируя личность и профессиональные качества.

Сущность основ кибербезопасности как педагогического феномена — это формирование у обучающихся знаний, навыков и ценностей для безопасного поведения в цифровой среде, защиты от киберугроз, понимание рисков для личности и общества, и умение применять принципы конфиденциальности, целостности, доступности информации, превращая пассивного пользователя в ответственного цифрового гражданина, способного сохранять себя и свои данные в условиях цифровой цивилизации. Это комплексная подготовка к жизни в киберпространстве, включающая как технические аспекты, так и этико-правовые нормы, с целью минимизации вреда и максимальной реализации потенциала цифровых технологий. Кибербезопасность — это не только техническая дисциплина, но и образовательная задача по воспитанию «цифрового человека» в условиях повсеместного проникновения информации в жизнь.

Сущность основ кибербезопасности в педагогике — это создание системы обучения, которая трансформирует пользователя в защищенного, осведомленного и ответственного участника киберпространства. Это не просто набор правил, а фундаментальный элемент современного образования,

позволяющий индивиду жить, работать и развиваться в информационном обществе, минимизируя риски и используя возможности.

Сущность педагогического феномена заключается в следующем:

1. Формирование критического мышления: Кибербезопасность учит нас не принимать все на веру в интернете. Мы учимся анализировать информацию, распознавать фейки, мошеннические схемы и потенциально опасные ссылки. Это навык, который применим не только к цифровому миру, но и к реальной жизни.

2. Развитие навыков самозащиты: Это практическая сторона обучения. Мы осваиваем методы создания надежных паролей, распознавания фишинговых писем, безопасного использования социальных сетей, защиты личных данных и понимания рисков, связанных с загрузкой файлов и установкой программ.

3. Воспитание ответственности: Кибербезопасность – это не только о личной защите, но и о влиянии наших действий на других. Мы учимся понимать, как наши неосторожные действия могут навредить другим пользователям, и как важно соблюдать цифровую этику.

4. Понимание угроз и уязвимостей: Педагогический аспект заключается в том, чтобы сделать сложные технические понятия доступными и понятными. Мы узнаем о различных видах киберугроз (вирусы, хакерские атаки, кража данных) и о том, как они работают, чтобы лучше понимать, от чего именно мы защищаемся.

5. Формирование привычек безопасного поведения: Как и в случае с гигиеной или правилами дорожного движения, основы кибербезопасности должны стать частью наших повседневных привычек. Это означает постоянное обновление программного обеспечения, осторожность при работе с незнакомыми сетями и регулярное резервное копирование важных данных.

6. Адаптивность к меняющемуся миру: Цифровой мир постоянно развивается, появляются новые угрозы и технологии. Педагогический феномен кибербезопасности подразумевает обучение не только конкретным

инструментам, но и способности учиться, адаптироваться и оставаться в курсе последних тенденций.

Почему это важно как педагогический феномен? Недостаточная осведомленность в вопросах кибербезопасности делает людей уязвимыми для мошенничества, кражи личных данных, шантажа и других преступлений. Это наносит ущерб не только отдельным людям, но и обществу в целом. От безопасности каждого пользователя зависит общая безопасность цифровых систем, которыми мы пользуемся ежедневно – от банковских сервисов до государственных порталов. Современные профессии все больше требуют цифровой грамотности и понимания основ кибербезопасности. Обучение этим навыкам с раннего возраста – это инвестиция в будущее наших детей и молодежи. Кибербезопасность – это неотъемлемая часть формирования здоровой и безопасной цифровой культуры, где каждый участник осознает свои права и обязанности.

Важно подчеркнуть, что основы кибербезопасности как педагогический феномен не ограничиваются только техническими аспектами. Они тесно переплетаются с этическими и правовыми нормами цифрового мира**.** Обучение кибербезопасности – это также обучение цифровому гражданству**,** пониманию того, что в онлайн-пространстве действуют те же законы и моральные принципы, что и в реальной жизни, а иногда и с более серьезными последствиями. Мы учимся уважать чужую конфиденциальность, не распространять вредоносный контент, не участвовать в травле и не нарушать авторские права.

Более того, этот феномен требует постоянного обновления и адаптации**.** Киберугрозы эволюционируют с поразительной скоростью, и то, что было актуально вчера, сегодня может быть устаревшим. Поэтому педагогический подход к кибербезопасности должен быть динамичным и гибким**.** Он должен прививать не только знание конкретных инструментов защиты, но и способность к самообучению, умение находить достоверную информацию, анализировать новые угрозы и применять соответствующие меры

предосторожности. Это формирует у человека цифровую резильентность – способность не только противостоять угрозам, но и быстро восстанавливаться после возможных инцидентов.

С точки зрения педагогики, основы кибербезопасности – это фундамент для построения безопасного и продуктивного цифрового будущего. Это не просто предмет, который изучают в школе или университете, а непрерывный процесс формирования компетенций, который должен сопровождать человека на протяжении всей его жизни. От детей, которые только начинают осваивать интернет, до пожилых людей, которые сталкиваются с новыми технологиями, – каждый нуждается в понимании основ кибербезопасности.

Таким образом, сущность основ кибербезопасности как педагогического феномена заключается в формировании у человека целостной системы знаний, навыков и установок, позволяющих ему безопасно, ответственно и этично функционировать в цифровой среде, адаптироваться к ее изменениям и активно участвовать в построении безопасного цифрового общества. Это не просто защита от угроз, а развитие цифровой личности, готовой к вызовам и возможностям современного мира.

Этот процесс обучения и воспитания, по своей сути, является трансформационным. Он не просто передает информацию, а меняет мировоззрение человека, формируя у него новую парадигму взаимодействия с цифровым пространством. Если раньше интернет воспринимался как нечто абстрактное, далекое от реальных угроз, то теперь он становится полем, требующим постоянной бдительности и осознанных действий. Педагогический аспект здесь заключается в том, чтобы сделать эту бдительность не параноидальной, а рациональной и проактивной.

Важно подчеркнуть, что основы кибербезопасности как педагогический феномен не ограничиваются только техническими аспектами. Они тесно переплетаются с этическими и правовыми нормами цифрового мира. Обучение кибербезопасности – это также обучение цифровому гражданству, пониманию того, что в онлайн-пространстве действуют те же законы и моральные

принципы, что и в реальной жизни, а иногда и с более серьезными последствиями. Мы учимся уважать чужую конфиденциальность, не распространять вредоносный контент, не участвовать в травле и не нарушать авторские права. Это формирует у человека не только техническую грамотность, но и моральную ответственность за свои действия в сети.

В эпоху динамичных социокультурных изменений, когда система образования подвергается постоянной трансформации, вопрос формирования личностных качеств студентов приобретает особую актуальность. Современный специалист должен обладать не только профессиональными компетенциями, но и развитыми морально-этическими качествами, коммуникативными навыками и умением адаптироваться к новым условиям. Профессиональное образование, в свою очередь, является ключевым институтом социализации, оказывающим значительное влияние на становление личности будущего профессионала. Методологические подходы к изучению проблемы Исследование формирования личностных качеств студентов требует комплексного методологического подхода. Необходимо учитывать социально-психологические особенности студенческого возраста, специфику образовательной среды, а также влияние внеучебных факторов. Важным этапом является анализ существующих теоретических концепций и эмпирических данных, позволяющих определить ключевые факторы, влияющие на развитие личности студента. Практические аспекты формирования личностных качеств Результаты исследования могут быть использованы для разработки эффективных образовательных программ и технологий, направленных на развитие личностных качеств студентов. Важно создать условия для самореализации и творческой активности, стимулировать участие студентов в общественной жизни и волонтерских проектах. Особое внимание следует уделять формированию ценностных ориентаций, профессиональной этики и гражданской ответственности. Только комплексный подход, учитывающий индивидуальные особенности студентов и возможности образовательной среды, позволит успешно решать задачи формирования личности будущего

профессионала. В контексте профессионального образования, формирование личностных качеств неразрывно связано с развитием профессиональной идентичности. Студенты должны осознавать свою роль в обществе, понимать значимость своей будущей профессии и ощущать ответственность за результаты своей деятельности. Этому способствует активное вовлечение студентов в научно-исследовательскую работу, участие в профессиональных конкурсах и стажировках, а также взаимодействие с опытными специалистами-практиками. Важно, чтобы студенты имели возможность применять свои знания и навыки в реальных ситуациях, ощущая свою полезность и внося вклад в развитие своей профессиональной области.

В формировании личностных качеств ключевую роль играет преподаватель. Его задача не только передавать знания, но и формировать у студентов ценностное отношение к профессии, развивать критическое мышление и умение самостоятельно принимать решения. Преподаватель должен быть примером профессионализма, высокой морали и гражданской ответственности. Важно, чтобы в образовательном процессе создавалась атмосфера доверия и сотрудничества, где студенты могли бы свободно выражать свои мысли и идеи, не боясь критики и осуждения.

Необходимо также учитывать влияние информационных технологий на формирование личности студента. С одной стороны, они открывают широкие возможности для обучения и саморазвития. С другой стороны, могут негативно влиять на ценностные ориентации и социальное поведение. Поэтому важно развивать у студентов навыки критического анализа информации, умение отличать достоверные источники от недостоверных, а также формировать культуру использования информационных технологий.

Педагогический подход к кибербезопасности — это системное обучение цифровой гигиене и защите информации, превращающее

«Основы кибербезопасности» в педагогический феномен через формирование критического мышления, интерактивных методик и моделирование угроз, чтобы подготовить учащихся к безопасному поведению

в цифре. Ключевая задача — не просто дать знания, а воспитать осознанного пользователя, способного применять принципы конфиденциальности, целостности и доступности в реальной жизни, используя современные интерактивные формы обучения для будущих педагогов и школьников.

Таблица 1**.** Основные принципы педагогического подхода к кибербезопасности.

Аспект	Описание
Системность и последовательность	Постепенное введение понятий от простого к сложному.
Интерактивность	Использование игровых, практических, моделирующих задач для вовлечения.
Практическая направленность	Фокус на реальных угрозах и навыках поведения в цифровом мире (фишинг, пароли, личные данные).
Формирование критического мышления	Обучение анализу информации и оценке рисков.
Междисциплинарность	Интеграция с информатикой, обществознанием, психологией.

«Основы кибербезопасности» как педагогический феномен: Это не просто предмет, а воспитательный процесс, направленный на формирование новой культуры поведения в цифровой среде, где:

- Знания становятся навыками: Учащиеся не просто запоминают правила, а умеют их применять.
- Педагог — проводник: Учитель выступает как наставник, который обучает безопасному взаимодействию с информационными технологиями.
- Угрозы становятся учебными ситуациями: Моделирование кибератак (например, через симуляторы фишинга) помогает выработать иммунитет.
- Кибербезопасность — элемент цифровой грамотности: Становится частью общей культуры личности, наряду с чтением и письмом.

Таким образом, педагогический подход превращает кибербезопасность из технической дисциплины в социально-педагогическую проблему, решая которую, мы готовим граждан к жизни в цифровом обществе, где защита личных данных и критическая оценка информации — это новые базовые навыки.

Особенностью реализации образовательного процесса, направленного на формирование культуры кибербезопасного поведения, будет являться специфические особенности направления подготовки. Будущие программисты, помимо своих профессиональных навыков, должны освоить определенные умения и навыки, которые помогут им мобильно реагировать на информационные угрозы киберпространства как в реальной жизни, так и в ходе исполнения их рабочих обязанностей.

В связи с этим важно отметить, что помимо внедрения в образовательный процесс дополнительных элементов и комплексов, разработанных с учетом специфики образовательного направления «Информационные системы и программирование», важную роль необходимо уделить и воспитательному процессу, который оказывает значимое влияние на становление личности будущего программиста, и в последствии определяет его профессиональные качества и пути решения задач по защите от киберугроз.

Главным направлением реализации педагогических условий формирования культуры кибербезопасного поведения будущих программистов должны быть не только образовательные элементы, но и этические аспекты и понимание ответственности за свои действия. Обучающиеся должны иметь четкое понимание последствий своих действий, соответствие их нормам действующего законодательства в сфере безопасности данных.

Также достижения вышеперечисленных целей в области формирования культуры кибербезопасного поведения будущих программистов обязательным требованием к образовательному процессу колледжа будет являться реализация следующих педагогических условий:

1. Интеграция элементов кибербезопасности в рабочие программы. На сегодня в образовательном стандарте отсутствует отдельная дисциплина, посвященная кибербезопасности будущих программистов. Однако, внедрение лекций и практических занятий в дисциплины, связанные с изучением алгоритмов, разработки программного обеспечения и информационных технологий, может помочь в формировании у обучающихся базового опыта и знаний о кибербезопасности.

2. Практическое обучение на примерах реальных угроз и кейсах, а также использования ролевых игр. Здесь необходимо отметить важность присутствия реальных примеров атак, инцидентов и уязвимостей, связанных с киберугрозами. В практикум может входить решение ситуационных задач и выявления методов противодействия и защиты. Это направление деятельности может улучшить эффективность получения практического опыта для будущих программистов.

3. Развитие навыков критического мышления. Это важное педагогическое условие будет способствовать развитию у обучающихся умения быстро реагировать и принимать решения, осознавая при этом их последствия и риски, не только в процессе профессиональной деятельности, но и при различных жизненных ситуациях. Данный аспект будет играть ключевую роль при формировании кибербезопасного поведения будущих программистов, так как он в первую очередь ориентирован не только на защитную реакцию, но и на предотвращение возникновения уязвимых ситуаций на ранних этапах.

Предложенные педагогические условия могут способствовать формированию культуры кибербезопасного поведения будущих программистов, развивая навыки по проектированию безопасных информационных систем и своевременному выявлению киберугроз и способов защиты от них.

Сущность кибербезопасности как педагогического феномена заключается в формировании у обучающихся цифровой грамотности и культуры безопасного поведения в киберпространстве, превращая технические

и организационные меры защиты в осознанные, личностно значимые навыки для противодействия угрозам, осмысления рисков и ответственного участия в цифровой жизни, что критически важно для современного человека, а не просто набор правил, но и ценностный ориентир.

Таким образом, педагогический феномен кибербезопасности — это комплексный процесс воспитания ответственного цифрового гражданина, способного защищать себя и свои данные, а также осознавать социальные и этические последствия своих действий в цифровом мире.

1.2 Процесс формирования личностных качеств у студентов профессиональной образовательной организации

Формирование личностных качеств студентов профессионального образования — это сложный процесс, обусловленный возрастными особенностями такими как: переход к взрослости, самоопределение, кризисы, формирование собственного я, освоение профессиональных ролей и психическими факторами: развитие познавательных процессов, мотивации, воли, эмоциональной стабильности, где ключевую роль играют самовоспитание, учебно-профессиональная деятельность, общение и социальная среда, направленные на обретение зрелости, самостоятельности и профессиональной идентичности.

1) Возрастные особенности студентов в возрасте от 15-20 лет. Студенты получающие среднее специальное образование, как правило, находятся в периоде от ранней юности до взрослости, что характеризуется:
2) Кризисом выбора, который зачастую будет обусловлен такими психическо-эмоциональными особенностями как переоценка жизненных ценностей, неуверенность в том, что правильно выбрал профессию с которой сможешь связать свою жизнь, поиск жизненных ориентиров. Кризис профессионального выбора у студентов, характеризуется тревогой, неопределенностью и

сомнениями относительно правильности выбранной специальности и будущей карьеры. Этот кризис может проявляться на разных этапах обучения и имеет различные причины и пути решения.

3) Формированием идентичности**:** Поиск себя, своего места в мире, развитие чувства ответственности.
4) Освоением новых ролей: Переход к более независимому образу жизни, освоение профессиональных ролей.
5) Развитием самосознания: Погружение в «Я», стремление к самовыражению, формирование «больших» задач.
6) Психологические новообразования: Повышение общего уровня зрелости, устойчивости, развитие саморегуляции и самовоспитания.
7) Психические особенности и факторы:
8) Познавательные процессы: Формируется устойчивое внимание, развиваются воображение, память, интегрированность мышления.
9) Мотивация и направленность: Закрепляется профессиональная направленность, повышается значимость будущей профессии, растут притязания.
10) Воля и ответственность: Усиливается чувство долга и ответственности за свои действия и будущую работу.
11) Эмоциональная сфера: Время романтики, оптимизма, но и первых «взрослых» забот и переживаний.
12) Самостоятельность: Рост профессиональной самостоятельности, готовность к практической работе, активизация самовоспитания.

Влияние среды и деятельности

1) Учебно-профессиональная деятельность: Создает условия для формирования необходимых способностей и качеств.

2) Социальное окружение: Влияние группы, общественной работы, формирует организаторские навыки и позицию.

3) Самовоспитание: Ключевой фактор, когда студент сам работает над собой, преодолевает противоречия и достигает зрелости.

Таким образом, формирование личности студента ПОО — это переход от внешних требований к внутренней саморегуляции, где психические новообразования и возрастные задачи интегрируются в устойчивую профессиональную личность.

Почему это важно как педагогический феномен? Недостаточная осведомленность в вопросах кибербезопасности делает людей уязвимыми для мошенничества, кражи личных данных, шантажа и других преступлений. Это наносит ущерб не только отдельным людям, но и обществу в целом. От безопасности каждого пользователя зависит общая безопасность цифровых систем, которыми мы пользуемся ежедневно – от банковских сервисов до государственных порталов. Современные профессии все больше требуют цифровой грамотности и понимания основ кибербезопасности. Обучение этим навыкам с раннего возраста – это инвестиция в будущее наших детей и молодежи. Кибербезопасность – это неотъемлемая часть формирования здоровой и безопасной цифровой культуры, где каждый участник осознает свои права и обязанности.

Важно подчеркнуть, что основы кибербезопасности как педагогический феномен не ограничиваются только техническими аспектами. Они тесно переплетаются с этическими и правовыми нормами цифрового мира**.** Обучение кибербезопасности – это также обучение цифровому гражданству**,** пониманию того, что в онлайн-пространстве действуют те же законы и моральные принципы, что и в реальной жизни, а иногда и с более серьезными последствиями. Мы учимся уважать чужую конфиденциальность, не распространять вредоносный контент, не участвовать в травле и не нарушать авторские права.

Более того, этот феномен требует постоянного обновления и адаптации. Киберугрозы эволюционируют с поразительной скоростью, и то, что было актуально вчера, сегодня может быть устаревшим. Поэтому педагогический подход к кибербезопасности должен быть динамичным и гибким. Он должен прививать не только знание конкретных инструментов защиты, но и способность к самообучению, умение находить достоверную информацию, анализировать новые угрозы и применять соответствующие меры предосторожности. Это формирует у человека цифровую резильентность – способность не только противостоять угрозам, но и быстро восстанавливаться после возможных инцидентов.

С точки зрения педагогики, основы кибербезопасности – это фундамент для построения безопасного и продуктивного цифрового будущего. Это не просто предмет, который изучают в школе или университете, а непрерывный процесс формирования компетенций, который должен сопровождать человека на протяжении всей его жизни. От детей, которые только начинают осваивать интернет, до пожилых людей, которые сталкиваются с новыми технологиями, – каждый нуждается в понимании основ кибербезопасности.

Таким образом, сущность основ кибербезопасности как педагогического феномена заключается в формировании у человека целостной системы знаний, навыков и установок, позволяющих ему безопасно, ответственно и этично функционировать в цифровой среде, адаптироваться к ее изменениям и активно участвовать в построении безопасного цифрового общества. Это не просто защита от угроз, а развитие цифровой личности, готовой к вызовам и возможностям современного мира.

Этот процесс обучения и воспитания, по своей сути, является трансформационным. Он не просто передает информацию, а меняет мировоззрение человека, формируя у него новую парадигму взаимодействия с цифровым пространством. Если раньше интернет воспринимался как нечто абстрактное, далекое от реальных угроз, то теперь он становится полем, требующим постоянной бдительности и осознанных действий. Педагогический

аспект здесь заключается в том, чтобы сделать эту бдительность не параноидальной, а рациональной и проактивной.

Важно подчеркнуть, что основы кибербезопасности как педагогический феномен не ограничиваются только техническими аспектами. Они тесно переплетаются с этическими и правовыми нормами цифрового мира. Обучение кибербезопасности – это также обучение цифровому гражданству, пониманию того, что в онлайн-пространстве действуют те же законы и моральные принципы, что и в реальной жизни, а иногда и с более серьезными последствиями. Мы учимся уважать чужую конфиденциальность, не распространять вредоносный контент, не участвовать в травле и не нарушать авторские права. Это формирует у человека не только техническую грамотность, но и моральную ответственность за свои действия в сети.

В эпоху динамичных социокультурных изменений, когда система образования подвергается постоянной трансформации, вопрос формирования личностных качеств студентов приобретает особую актуальность. Современный специалист должен обладать не только профессиональными компетенциями, но и развитыми морально-этическими качествами, коммуникативными навыками и умением адаптироваться к новым условиям. Профессиональное образование, в свою очередь, является ключевым институтом социализации, оказывающим значительное влияние на становление личности будущего профессионала. Методологические подходы к изучению проблемы Исследование формирования личностных качеств студентов требует комплексного методологического подхода. Необходимо учитывать социально-психологические особенности студенческого возраста, специфику образовательной среды, а также влияние внеучебных факторов. Важным этапом является анализ существующих теоретических концепций и эмпирических данных, позволяющих определить ключевые факторы, влияющие на развитие личности студента. Практические аспекты формирования личностных качеств Результаты исследования могут быть использованы для разработки эффективных образовательных программ и технологий, направленных на

развитие личностных качеств студентов. Важно создать условия для самореализации и творческой активности, стимулировать участие студентов в общественной жизни и волонтерских проектах. Особое внимание следует уделять формированию ценностных ориентаций, профессиональной этики и гражданской ответственности. Только комплексный подход, учитывающий индивидуальные особенности студентов и возможности образовательной среды, позволит успешно решать задачи формирования личности будущего профессионала. В контексте профессионального образования, формирование личностных качеств неразрывно связано с развитием профессиональной идентичности. Студенты должны осознавать свою роль в обществе, понимать значимость своей будущей профессии и ощущать ответственность за результаты своей деятельности. Этому способствует активное вовлечение студентов в научно-исследовательскую работу, участие в профессиональных конкурсах и стажировках, а также взаимодействие с опытными специалистами-практиками. Важно, чтобы студенты имели возможность применять свои знания и навыки в реальных ситуациях, ощущая свою полезность и внося вклад в развитие своей профессиональной области.

В формировании личностных качеств ключевую роль играет преподаватель. Его задача не только передавать знания, но и формировать у студентов ценностное отношение к профессии, развивать критическое мышление и умение самостоятельно принимать решения. Преподаватель должен быть примером профессионализма, высокой морали и гражданской ответственности. Важно, чтобы в образовательном процессе создавалась атмосфера доверия и сотрудничества, где студенты могли бы свободно выражать свои мысли и идеи, не боясь критики и осуждения.

Необходимо также учитывать влияние информационных технологий на формирование личности студента. С одной стороны, они открывают широкие возможности для обучения и саморазвития. С другой стороны, могут негативно влиять на ценностные ориентации и социальное поведение. Поэтому важно развивать у студентов навыки критического анализа информации, умение

отличать достоверные источники от недостоверных, а также формировать культуру использования информационных технологий.

В заключение следует отметить, что формирование личностных качеств студентов в процессе профессионального образования — это сложный и многогранный процесс, требующий комплексного подхода и совместных усилий преподавателей, студентов и общества в целом. Только в этом случае можно подготовить высококвалифицированных специалистов, обладающих не только профессиональными компетенциями, но и развитыми морально-этическими качествами, готовых к решению сложных задач и внесению вклада в развитие общества.

Формирование личностных качеств у студентов профессиональной образовательной организации является важным и многогранным процессом, который напрямую влияет на их будущую профессиональную деятельность и успешную социализацию в обществе. Этот процесс включает в себя не только передачу профессиональных знаний и навыков, но и развитие таких качеств, как ответственность, самостоятельность, коммуникабельность, критическое мышление и способность к саморазвитию.

Основу формирования личностных качеств составляет образовательная среда, в которой студент находится на протяжении всего периода обучения. В профессиональных образовательных организациях создаются условия для активного взаимодействия студентов с преподавателями, наставниками и сверстниками, что способствует развитию эмоционального интеллекта и навыков командной работы. Важную роль играют практические занятия, стажировки и проекты, которые позволяют применять теоретические знания на практике и формируют профессиональную этику и дисциплину.

Значительное влияние оказывает воспитательная работа, направленная на формирование ценностных ориентиров и мотивации к профессиональному росту. Психолого-педагогическая поддержка помогает студентам осознать свои сильные стороны и зоны развития, что способствует формированию позитивной самооценки и уверенности в своих силах.

Процесс формирования личностных качеств у студентов в профессиональной образовательной организации является комплексным и требует системного подхода, включающего образовательные, воспитательные и психологические компоненты. Только при условии гармоничного развития этих аспектов можно подготовить квалифицированных специалистов, готовых к вызовам современного профессионального мира.

Современный рынок труда требует от специалистов не только глубоких профессиональных знаний, но и гибкости мышления, умения анализировать информацию, прогнозировать последствия своих действий и эффективно взаимодействовать с коллегами и клиентами.

Важным аспектом формирования личностных качеств является создание условий для самореализации студентов, что достигается через внедрение инновационных образовательных технологий и методов, ориентированных на активное участие обучающихся в учебном процессе. Проектная деятельность, исследовательские работы, участие в конкурсах и профессиональных сообществах способствуют развитию инициативности, творческого подхода и ответственности за конечный результат.

Не менее значима роль педагогического коллектива, который выступает не только источником знаний, но и наставником, примером для подражания, поддержкой в сложных ситуациях. Профессионализм преподавателей, их умение мотивировать и вдохновлять студентов, создавать атмосферу доверия и взаимопонимания способствует формированию у обучающихся позитивных личностных установок и стремления к постоянному совершенствованию.

Кроме того, интеграция внеучебной деятельности, включая культурные, спортивные и волонтерские инициативы, расширяет кругозор студентов, способствует развитию социальной ответственности, эмпатии и умению работать в коллективе. Участие в таких мероприятиях помогает студентам осознать значимость своего вклада в общественную жизнь, формирует чувство принадлежности к профессиональному сообществу и укрепляет навыки лидерства.

Особое значение приобретает создание системы обратной связи, позволяющей студентам получать конструктивную оценку своей деятельности и личностного роста. Регулярное обсуждение результатов учебной и внеучебной работы с преподавателями и наставниками способствует формированию рефлексивных умений, что является важным условием для осознанного саморазвития и профессионального становления.

В современных условиях цифровизации образования важным инструментом формирования личностных качеств становится использование информационно-коммуникационных технологий. Виртуальные образовательные платформы, интерактивные тренажёры и онлайн-курсы расширяют возможности для самостоятельного обучения, стимулируют развитие критического мышления и творческого подхода к решению профессиональных задач.

Необходимо также учитывать индивидуальные особенности каждого студента, что требует дифференцированного подхода в образовательном процессе. Психолого-педагогическое сопровождение помогает выявить уникальные способности и интересы обучающихся, что позволяет создавать персонализированные траектории развития и повышать мотивацию к обучению и профессиональному росту.

Таким образом, формирование личностных качеств у студентов профессиональной образовательной организации представляет собой сложный и многоаспектный процесс, требующий интеграции различных педагогических, психологических и социальных факторов. Только при условии комплексного и системного подхода возможно создание условий, способствующих всестороннему развитию личности, формированию профессиональной идентичности и готовности к эффективной деятельности в условиях современного общества.

Особое внимание следует уделять развитию мотивационной сферы обучающихся, поскольку именно внутренняя мотивация является движущей силой личностного роста и профессионального становления. В этом контексте

важна организация учебного процесса таким образом, чтобы он не только передавал знания, но и стимулировал интерес к предмету, побуждал к самостоятельному поиску информации и творческому решению профессиональных задач. Использование активных и интерактивных методов обучения, таких как проблемное обучение, кейс-стади, деловые игры и тренинги, способствует формированию у студентов навыков критического мышления, умения работать в команде и принимать ответственные решения.

Не менее значима роль социального окружения, в котором развивается студент. Создание благоприятной образовательной среды, поддерживающей открытость, уважение и сотрудничество, способствует формированию позитивных личностных качеств. Взаимодействие с разными социальными группами и культурными сообществами расширяет горизонты восприятия студентов, формирует у них способность к межличностному диалогу и адаптации в многообразном профессиональном и социальном пространстве.

Особое значение приобретает развитие эмоциональной компетентности, которая включает умение распознавать и управлять своими эмоциями, а также понимать эмоциональное состояние других людей. Эмоциональный интеллект способствует эффективному разрешению конфликтов, укреплению командного духа и созданию позитивной атмосферы в коллективе, что является неотъемлемой частью профессиональной деятельности в современных условиях.

Важным направлением является также формирование у студентов навыков самоорганизации и тайм-менеджмента, что позволяет им эффективно планировать учебную и внеучебную деятельность, справляться с нагрузками и сохранять баланс между профессиональным развитием и личной жизнью. Эти умения способствуют развитию ответственности и дисциплинированности, что положительно сказывается на качестве подготовки будущих специалистов.

Необходимо отметить, что процесс формирования личностных качеств должен быть непрерывным и сопровождаться регулярной рефлексией. Создание условий для самоанализа и критической оценки собственного опыта

помогает студентам осознанно подходить к своему развитию, выявлять достижения и зоны для улучшения, а также корректировать образовательные и профессиональные навыки.

1.3 Возможность формирования основ кибербезопасности на содержании специальных дисциплин профессиональной образовательной организации

В формировании личностных качеств ключевую роль играет преподаватель. Его задача не только передавать знания, но и формировать у студентов ценностное отношение к профессии, развивать критическое мышление и умение самостоятельно принимать решения. Преподаватель должен быть примером профессионализма, высокой морали и гражданской ответственности. Важно, чтобы в образовательном процессе создавалась атмосфера доверия и сотрудничества, где студенты могли бы свободно выражать свои мысли и идеи, не боясь критики и осуждения.

Необходимо также учитывать влияние информационных технологий на формирование личности студента. С одной стороны, они открывают широкие возможности для обучения и саморазвития. С другой стороны, могут негативно влиять на ценностные ориентации и социальное поведение. Поэтому важно развивать у студентов навыки критического анализа информации, умение отличать достоверные источники от недостоверных, а также формировать культуру использования информационных технологий.

В заключение следует отметить, что формирование личностных качеств студентов в процессе профессионального образования — это сложный и многогранный процесс, требующий комплексного подхода и совместных усилий преподавателей, студентов и общества в целом. Только в этом случае можно подготовить высококвалифицированных специалистов, обладающих не только профессиональными компетенциями, но и развитыми морально-этическими качествами, готовых к решению сложных задач и внесению вклада в развитие общества.

Анализ учебно-методической документации информационно-цифровых дисциплин для выявления тех дисциплин, на основе которых возможно внедрить в процесс обучения основы кибербезопасности. В условиях стремительного роста цифровизации всех сфер жизни, вопросы кибербезопасности приобретают первостепенное значение. Подготовка квалифицированных специалистов, обладающих знаниями и навыками в этой области, является одной из ключевых задач современного образования. Интеграция основ кибербезопасности в учебные программы информационно-цифровых дисциплин представляется эффективным способом достижения этой цели. Настоящий анализ направлен на выявление тех дисциплин, в рамках которых наиболее целесообразно внедрение модулей и тем, посвященных кибербезопасности. В качестве основы для анализа служат учебно-методические комплексы (УМК) дисциплин, охватывающие различные аспекты информационных технологий, программирования, сетевых технологий и управления данными. Критериями отбора дисциплин для интеграции основ кибербезопасности являются: Наличие в содержании дисциплин тем, связанных с обработкой, хранением и передачей информации. Акцент на практическое применение изучаемых технологий и инструментов. Направленность на формирование у студентов навыков анализа и решения проблем. Результаты анализа позволяют определить перечень дисциплин, в рамках которых возможно наиболее эффективно интегрировать основы кибербезопасности. Среди них могут быть выделены курсы по операционным системам, компьютерным сетям, базам данных, веб-разработке и прикладному программированию. Внедрение соответствующих модулей и тем в учебные программы позволит повысить уровень осведомленности студентов о существующих угрозах, методах защиты информации и нормативно-правовом регулировании в сфере кибербезопасности. Для каждой отобранной дисциплины необходимо разработать или адаптировать существующие учебные материалы с учетом специфики кибербезопасности. Это может включать в себя добавление новых лекций, практических заданий, кейсов и

лабораторных работ, направленных на изучение угроз, уязвимостей, методов защиты и инструментов обеспечения кибербезопасности. Важно интегрировать практические примеры и сценарии, отражающие реальные случаи из практики специалистов по кибербезопасности, чтобы максимально приблизить обучение к реальным условиям.

При интеграции кибербезопасности в дисциплины необходимо учитывать уровень подготовки студентов и сложность предлагаемых материалов. Рекомендуется начинать с основ, постепенно переходя к более сложным и специализированным темам. Важно также обеспечить баланс между теоретическими знаниями и практическими навыками, чтобы студенты могли не только понимать основные концепции, но и применять их на практике для решения конкретных задач.

Оценка эффективности внедрения основ кибербезопасности в учебные программы должна проводиться на основе различных методов, включая тестирование, опрос студентов и преподавателей, анализ успеваемости и оценку практических навыков. Полученные результаты позволят выявить сильные и слабые стороны внедрения, а также внести необходимые корректировки в учебные программы и методические материалы.

В заключение, интеграция основ кибербезопасности в учебно-методическую документацию информационно-цифровых дисциплин является важным шагом в подготовке квалифицированных специалистов, способных решать задачи обеспечения безопасности в современном цифровом мире. Тщательный анализ существующих дисциплин, разработка и адаптация учебных материалов, а также оценка эффективности внедрения позволят создать образовательную среду, способствующую формированию у студентов необходимых знаний, навыков и компетенций в области кибербезопасности.

Цель выявить в учебно-методической документации (УМД) дисциплин, связанных с информационными сетями, программированием, информатикой и смежными областями, содержание, которое может служить основой для проведения занятий по кибербезопасности.

Современный мир немыслим без информационных технологий. Вместе с их развитием растет и актуальность кибербезопасности – защиты наших цифровых активов от угроз. Для эффективного обучения основам кибербезопасности необходимо опираться на уже существующую базу знаний, заложенную в учебных программах по информатике, программированию и сетям. Данный анализ призван систематизировать и выявить те разделы и темы, которые могут быть трансформированы и дополнены для формирования компетенций в области кибербезопасности.

Для проведения анализа учебно-методической документации по дисциплинам, связанным с информационными сетями, программированием, информатикой и смежными областями, с целью выявления содержания, на основе которого возможно организовать занятия по кибербезопасности, необходимо выполнить несколько ключевых этапов.

1. Сбор и систематизация документации

Первым шагом является сбор учебных планов, программ, методических рекомендаций и учебных материалов по дисциплинам: информационные сети, программирование, информатика, базы данных, операционные системы и др. Важно охватить как базовые, так и профильные курсы, чтобы получить полное представление о содержании и структуре обучения.

2. Анализ содержания дисциплин

Далее проводится детальный анализ программ и учебных материалов с целью выявления тем и разделов, которые напрямую или косвенно связаны с вопросами кибербезопасности. Например:

- Основы сетевых технологий и протоколов (TCP/IP, DNS, DHCP) — понимание работы сетей необходимо для изучения угроз и методов защиты.
- Программирование и разработка ПО — изучение безопасного кодирования, предотвращение уязвимостей (SQL-инъекции, XSS и др.).

- Операционные системы — управление правами доступа, работа с файлами и процессами, защита от вредоносного ПО.
- Криптография — основы шифрования, цифровые подписи, аутентификация.
- Администрирование и управление информационными системами — настройка безопасности, мониторинг и реагирование на инциденты.
- Выделение ключевых тем для занятий по кибербезопасности На основе анализа можно выделить следующие направления для формирования учебного курса или отдельных занятий по кибербезопасности:
- Введение в кибербезопасность: основные понятия, актуальные угрозы и риски.
- Безопасность сетей: методы защиты
- Безопасность сетей: методы защиты, включая использование межсетевых экранов (firewalls), систем обнаружения и предотвращения вторжений (IDS/IPS), VPN-технологий, а также принципы сегментации сети и контроля доступа. Особое внимание уделяется анализу сетевого трафика и выявлению аномалий, что является ключевым элементом в предотвращении атак.
- Безопасное программирование: изучение принципов разработки защищённого кода, предотвращение распространённых уязвимостей, таких как буферные переполнения, инъекции, межсайтовый скриптинг (XSS), а также применение практик код-ревью и статического анализа кода. Важно рассмотреть жизненный цикл разработки программного обеспечения с учётом аспектов безопасности (Secure SDLC).
- Операционные системы и безопасность: управление правами пользователей и групп, настройка политик безопасности, использование систем аутентификации и авторизации, защита от

вредоносного ПО, а также мониторинг системных журналов и событий безопасности. Рассматриваются особенности безопасности различных ОС (Windows, Linux, macOS) и их уязвимости.

- Криптография и её применение: базовые понятия шифрования, симметричные и асимметричные алгоритмы, цифровые подписи, сертификаты и инфраструктура открытых ключей (PKI).
- Управление инцидентами и реагирование: методы обнаружения и анализа инцидентов безопасности, организация процессов реагирования, восстановление после атак и минимизация ущерба. Важно включить практические аспекты работы с системами логирования, SIEM-платформами и инструментами форензики.
- Социальная инженерия и человеческий фактор: понимание методов социальной инженерии, фишинга, методов манипуляции и способов повышения осведомлённости пользователей. Включение тренингов по информационной гигиене и формирование культуры безопасности среди пользователей.
- Законодательство и этика в кибербезопасности: обзор нормативных актов, регулирующих информационную безопасность, вопросы конфиденциальности данных, ответственность за нарушение безопасности, а также этические аспекты деятельности специалистов в области ИБ.

4. Интеграция кибербезопасности в учебные дисциплины

Для эффективного усвоения материала рекомендуется интегрировать темы кибербезопасности непосредственно в соответствующие дисциплины, а не рассматривать их изолированно. Например, при изучении сетевых технологий уделять внимание не только протоколам, но и их уязвимостям и методам защиты; при программировании — внедрять практики безопасного кодирования; при изучении операционных систем — рассматривать механизмы контроля доступа и защиты.

5. Разработка учебных модулей и материалов, включающих теоретические и практические задания по кибербезопасности, с использованием современных инструментов и кейсов. Важно обеспечить регулярное обновление содержания с учётом новых угроз и технологий. Рекомендуется внедрять междисциплинарный подход и активные методы обучения, такие как лабораторные работы, симуляции атак и защитных мер. Таким образом, формируется комплексное понимание кибербезопасности и навыки её применения в профессиональной деятельности.

Методология анализа. Анализ будет проводиться путем изучения рабочих программ дисциплин, учебных планов, методических указаний, фондов оценочных средств и других релевантных документов. Особое внимание будет уделено следующим аспектам:

- Структура и содержание дисциплин: Изучение тем, разделов, ключевых понятий и навыков, которые формируются в рамках каждой дисциплины.
- Связь с практикой: Оценка наличия практических заданий, лабораторных работ, проектов, которые могут быть адаптированы для демонстрации уязвимостей и методов защиты.
- Терминология и концепции: Выявление терминов и концепций, которые напрямую или косвенно связаны с вопросами безопасности.

Выявленное содержание и его потенциал для кибербезопасности:

В результате анализа учебно-методической документации по дисциплинам, связанным с информационными сетями, программированием и информатикой, можно выделить следующие ключевые направления, которые станут прочным фундаментом для занятий по кибербезопасности:

1. Информационные сети:

1) Протоколы и архитектура сетей (TCP/IP, OSI):
   - Потенциал для кибербезопасности: Понимание работы протоколов на разных уровнях позволяет выявлять уязвимости, связанные с некорректной реализацией, перехватом трафика, атаками типа "отказ в обслуживании" (DoS/DDoS). Изучение механизмов аутентификации и шифрования на уровне протоколов (например, TLS/SSL) является основой для понимания безопасной передачи данных.
   - Примеры тем для занятий: Анализ сетевого трафика с помощью Wireshark, основы сетевой сегментации для изоляции угроз, понимание принципов работы VPN.
2) Сетевое оборудование (маршрутизаторы, коммутаторы, межсетевые экраны):
   - Потенциал для кибербезопасности: Изучение настроек и конфигураций сетевого оборудования позволяет понять, как правильно его защищать, какие уязвимости могут быть в стандартных настройках, и как использовать межсетевые экраны для фильтрации трафика и предотвращения несанкционированного доступа.
   - Примеры тем для занятий: Базовая настройка межсетевого экрана, принципы работы NAT, понимание ролей сетевых устройств в защите периметра.
3) Беспроводные сети (Wi-Fi):

- Потенциал для кибербезопасности: Изучение стандартов шифрования (WEP, WPA, WPA2, WPA3) и уязвимостей, связанных с ними, является критически важным. Понимание принципов работы точек доступа и методов аутентификации позволяет проводить аудит безопасности беспроводных сетей.
- Примеры тем для занятий: Анализ безопасности Wi-Fi сетей, методы перехвата паролей (в образовательных целях), настройка безопасных беспроводных сетей.

4) Сетевая безопасность (основы):
   - Потенциал для кибербезопасности: Часто в рамках дисциплин по сетям уже присутствуют вводные темы по сетевой безопасности, такие как типы атак, основы криптографии, принципы аутентификации. Эти темы являются прямым продолжением и углублением в контексте кибербезопасности.
   - Примеры тем для занятий: Классификация сетевых атак, основы шифрования и хеширования, методы аутентификации пользователей.

2. Программирование:
   1) Алгоритмы и структуры данных:
      - Потенциал для кибербезопасности: Понимание эффективности алгоритмов и их уязвимостей (например, переполнение буфера, уязвимости в работе с памятью) является основой для написания безопасного кода. Знание структур данных помогает понять, как злоумышленники могут манипулировать данными для достижения своих целей.
   2) Примеры тем для занятий: Анализ уязвимостей в простых алгоритмах, демонстрация переполнения буфера на примере C/C++, понимание принципов работы хеш-таблиц и их потенциальных проблем.
   3) Языки программирования (Python, C++, Java и др.):

- Потенциал для кибербезопасности: Изучение синтаксиса, семантики и особенностей конкретных языков позволяет выявлять и предотвращать распространенные уязвимости, такие как SQL-инъекции, межсайтовый скриптинг (XSS), небезопасная десериализация. Понимание работы с файлами, базами данных и сетевыми сокетами в контексте программирования является критически важным.
- Примеры тем для занятий: Разработка простых веб-приложений с учетом безопасности, написание скриптов для автоматизации задач безопасности, анализ уязвимостей в коде на Python (например, использование небезопасных функций).

4) Объектно-ориентированное программирование (ООП):
   - Потенциал для кибербезопасности: Понимание принципов инкапсуляции, наследования и полиморфизма помогает создавать более модульный и безопасный код. Изучение паттернов проектирования, в том числе и тех, которые направлены на повышение безопасности, также является важным.
   - Примеры тем для занятий: Применение принципов ООП для создания безопасных компонентов ПО, анализ уязвимостей, связанных с некорректным использованием наследования.
5) Разработка веб-приложений (основы):
   - Потенциал для кибербезопасности: Изучение клиент-серверной архитектуры, HTTP-протокола, работы с базами данных (SQL, NoSQL) и языков разметки/скриптов (HTML, CSS, JavaScript) является прямым путем к пониманию уязвимостей веб-приложений.
   - Примеры тем для занятий: Основы OWASP Top 10 (SQL-инъекции, XSS, CSRF), безопасная разработка форм ввода

данных, аутентификация и авторизация пользователей в веб-приложениях.

3. Информатика (общие дисциплины):

1) Основы операционных систем (Windows, Linux):
   - Потенциал для кибербезопасности: Понимание файловой системы, управления процессами, прав доступа, сетевых служб и механизмов безопасности операционных систем является фундаментом для защиты компьютеров и серверов. Изучение командной строки и скриптовых языков (Bash, PowerShell) открывает возможности для автоматизации задач безопасности и анализа систем.
   - Примеры тем для занятий: Управление пользователями и группами в Linux, настройка прав доступа к файлам, мониторинг процессов и сетевых соединений, основы работы с журналами событий.
2) Базы данных (SQL, NoSQL):
   - Потенциал для кибербезопасности: Понимание структуры баз данных, языка SQL и уязвимостей, связанных с доступом к данным (SQL-инъекции), является критически важным. Изучение механизмов резервного копирования и восстановления данных также относится к аспектам безопасности.
   - Примеры тем для занятий: Основы SQL-инъекций и методы их предотвращения, безопасное проектирование схем баз данных, управление доступом к данным.
3) Архитектура компьютера:
   - Потенциал для кибербезопасности: Понимание работы процессора, памяти, шин данных и периферийных устройств может помочь в осознании низкоуровневых уязвимостей, таких как эксплойты, использующие особенности аппаратной архитектуры, или атаки на целостность данных на уровне памяти.

4) Примеры тем для занятий: Основы работы кэш-памяти и ее влияние на безопасность, понимание принципов работы аппаратных ускорителей и их потенциальных уязвимостей.
5) Информационная безопасность (вводные курсы):
   - Потенциал для кибербезопасности: Если в рамках общих курсов информатики присутствуют вводные разделы по информационной безопасности, то они являются прямым мостом к более специализированным знаниям. Это могут быть темы, касающиеся конфиденциальности, целостности и доступности информации, основных угроз и уязвимостей, а также базовых мер защиты.
   - Примеры тем для занятий: Концепции CIA (Confidentiality, Integrity, Availability), основные типы вредоносного ПО (вирусы, черви, трояны), основы криптографии (шифрование, хеширование), принципы аутентификации и авторизации.
6) Теория информации и кодирование:
   - Потенциал для кибербезопасности: Понимание принципов сжатия данных, обнаружения и исправления ошибок, а также основ криптографических примитивов, таких как шифрование и хеширование, закладывает теоретическую базу для более глубокого изучения криптографии и стеганографии.
   - Примеры тем для занятий: Основы теории кодирования для обнаружения ошибок в передаваемых данных, принципы работы алгоритмов сжатия данных и их влияние на безопасность.

4. Смежные дисциплины (например, системное администрирование, разработка ПО):

1) Системное администрирование:
   - Потенциал для кибербезопасности**:** Управление учетными записями, настройка служб, мониторинг систем, резервное копирование и восстановление – все эти задачи являются неотъемлемой частью обеспечения безопасности систем. Понимание уязвимостей, связанных с неправильной конфигурацией, является ключевым.
   - Примеры тем для занятий**:** Безопасная настройка веб-серверов (Apache, Nginx), управление службами в Linux, основы мониторинга систем на предмет аномальной активности, политики паролей.
2) Разработка программного обеспечения (общие принципы):
   - Потенциал для кибербезопасности: Любая разработка ПО должна учитывать аспекты безопасности. Изучение жизненного цикла разработки ПО (SDLC) с учетом безопасности (Secure SDLC), принципов безопасного кодирования и тестирования на уязвимости является основой для создания надежных приложений.
   - Примеры тем для занятий: Принципы безопасного кодирования (например, OWASP Secure Coding Practices), тестирование на проникновение (пентестинг) на базовом уровне, использование инструментов статического и динамического анализа кода.

Анализ учебно-методической документации информационно-цифровых дисциплин для выявления тех дисциплин, на основе которых возможно внедрить в процесс обучения основы кибербезопасности. В условиях стремительного роста цифровизации всех сфер жизни, вопросы кибербезопасности приобретают первостепенное значение. Подготовка квалифицированных специалистов, обладающих знаниями и навыками в этой области, является одной из ключевых задач современного образования. Интеграция основ кибербезопасности в учебные программы информационно-цифровых дисциплин представляется эффективным способом достижения этой

цели. Настоящий анализ направлен на выявление тех дисциплин, в рамках которых наиболее целесообразно внедрение модулей и тем, посвященных кибербезопасности. В качестве основы для анализа служат учебно-методические комплексы (УМК) дисциплин, охватывающие различные аспекты информационных технологий, программирования, сетевых технологий и управления данными. Критериями отбора дисциплин для интеграции основ кибербезопасности являются: Наличие в содержании дисциплин тем, связанных с обработкой, хранением и передачей информации. Акцент на практическое применение изучаемых технологий и инструментов. Направленность на формирование у студентов навыков анализа и решения проблем. Результаты анализа позволяют определить перечень дисциплин, в рамках которых возможно наиболее эффективно интегрировать основы кибербезопасности. Среди них могут быть выделены курсы по операционным системам, компьютерным сетям, базам данных, веб-разработке и прикладному программированию. Внедрение соответствующих модулей и тем в учебные программы позволит повысить уровень осведомленности студентов о существующих угрозах, методах защиты информации и нормативно-правовом регулировании в сфере кибербезопасности. Для каждой отобранной дисциплины необходимо разработать или адаптировать существующие учебные материалы с учетом специфики кибербезопасности. Это может включать в себя добавление новых лекций, практических заданий, кейсов и лабораторных работ, направленных на изучение угроз, уязвимостей, методов защиты и инструментов обеспечения кибербезопасности. Важно интегрировать практические примеры и сценарии, отражающие реальные случаи из практики специалистов по кибербезопасности, чтобы максимально приблизить обучение к реальным условиям.

При интеграции кибербезопасности в дисциплины необходимо учитывать уровень подготовки студентов и сложность предлагаемых материалов. Рекомендуется начинать с основ, постепенно переходя к более сложным и специализированным темам. Важно также обеспечить баланс между

теоретическими знаниями и практическими навыками, чтобы студенты могли не только понимать основные концепции, но и применять их на практике для решения конкретных задач.

Оценка эффективности внедрения основ кибербезопасности в учебные программы должна проводиться на основе различных методов, включая тестирование, опрос студентов и преподавателей, анализ успеваемости и оценку практических навыков. Полученные результаты позволят выявить сильные и слабые стороны внедрения, а также внести необходимые корректировки в учебные программы и методические материалы.

Интеграция основ кибербезопасности в учебно-методическую документацию информационно-цифровых дисциплин является важным шагом в подготовке квалифицированных специалистов, способных решать задачи обеспечения безопасности в современном цифровом мире. Тщательный анализ существующих дисциплин, разработка и адаптация учебных материалов, а также оценка эффективности внедрения позволят создать образовательную среду, способствующую формированию у студентов необходимых знаний, навыков и компетенций в области кибербезопасности.

Основы кибербезопасности успешно формируются на специальных дисциплинах в профессионально-образовательных организациях через изучение прикладных модулей по защите информации, программно-аппаратных методов защиты, криптографии, антивирусной защите и управлению доступом, что обеспечивает практические навыки и компетенции для защиты IT-систем, а также формирует понимание угроз, принципов конфиденциальности, целостности и доступности данных в рамках ФГОС.

Таблица 2. Принципы формирования основ кибербезопасности.

Категория	Описание
Специальные дисциплины	- Программно-аппаратные методы защиты информации

	- Установка, наладка и обслуживание средств ИБ
Практико-ориентированный подход	- Обнаружение и защита от атак - Шифрование данных - Межсетевые экраны - Резервное копирование - Контроль доступа
Формирование ключевых компетенций	1. Понимание объектов защиты: - Информация - Пользователи - Системы - Сети 2. Освоение принципов ИБ: - Защита конфиденциальности - Целостности - Доступности данных 3. Знание основных угроз: - Вирусы - Фишинг - Хакерские атаки
Соответствие ФГОС	Программа соответствует Федеральным государственным образовательным стандартам (ФГОС)

Таким образом, профессиональные образовательные огранизации готовят специалистов, которые понимают как теоретические основы кибербезопасности, так и практические методы противодействия киберугрозам.

Анализ учебных планов среднего профессионального образования — это процесс оценки и корректировки документа, определяющего структуру, содержание и организацию образовательной программы в колледже или техникуме, основанный на требованиях ФГОС, с целью обеспечения соответствия современным стандартам и формирования требуемых компетенций у выпускников, что включает проверку графиков, часов, дисциплин и практики, и может автоматизироваться с помощью специализированного ПО.

Цели анализа:

1. Обеспечить системность и логичность образовательного процесса.
2. Выявить «узкие места» и несоответствия.
3. Оптимизировать распределение нагрузки.
4. Подготовить документацию для аккредитации и лицензирования.

Таким образом, анализ УП СПО — это комплексная работа по совершенствованию образовательного процесса в СПО, направленная на повышение качества подготовки квалифицированных кадров в соответствии с требованиями ФГОС.

1.3.1 Анализ УП базы

Нязепетровский филиал государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум».

Адрес организации: 456970, Челябинская область, г. Нязепетровск, ул. Ленина, д.97.

Лицензия на осуществление образовательной деятельности №11758 от «02» октября 2015года. Основной государственный регистрационный номер юридического лица 1027400728695. Идентификационный номер налогоплательщика 7409001380.

Государственная аккредитация: бессрочная.

Наименование укрупненных групп профессий, специальностей и направлений подготовки: техника и технологии строительства, информатика и вычислительная техника, машиностроение, технология материалов, сервиз и туризм, образование и педагогические науки.

ГБПОУ «Каслинский промышленно-гуманитарный техникум» был основан 20 мая 1944 года, организатором стал А. К. Соболевский. В 1946 году были выпущены 110 человек, которые получили такие специальности как: токарь, слесарь, столяр и формовщик.

Силами учащихся и работников училища были возведены слесарные мастерские, сварочный, кузнечный и формовочные участки, технологическое отделение и спортивный городок. В 1976 году было проведено много работы по расширению и укреплению материальной базы.

В настоящее время техникум выпускает таких специалистов как: техник, повар кондитер, воспитатель детей дошкольного возраста, штукатур, системный администратор.

Выводы по 1 главе

Формирование личностных качеств студентов профессиональных образовательных организаций (ПОО) — это многогранный и сложный процесс, тесно связанный с возрастными и психическими особенностями молодого

человека в период перехода к взрослости. Важную роль в этом процессе играют самовоспитание, учебно-профессиональная деятельность и социальная среда, которые способствуют развитию зрелости, самостоятельности и профессиональной идентичности.

Педагогический подход к формированию основ кибербезопасности рассматривается как системное и последовательное обучение, направленное не только на передачу знаний, но и на воспитание осознанного пользователя цифровых технологий. Использование интерактивных методов, моделирование угроз и развитие критического мышления позволяют превратить кибербезопасность в важный элемент цифровой культуры личности.

Основы кибербезопасности эффективно интегрируются в содержание специальных дисциплин ПОО, что обеспечивает студентам как теоретические знания, так и практические навыки защиты информации и IT-систем. Это соответствует требованиям Федеральных государственных образовательных стандартов (ФГОС) и способствует подготовке квалифицированных специалистов, готовых к противодействию современным киберугрозам.

Анализ учебных планов среднего профессионального образования является необходимым инструментом для обеспечения соответствия образовательных программ современным стандартам, оптимизации учебного процесса и повышения качества подготовки специалистов. Использование автоматизированных систем и компетентностного подхода способствует системности, логичности и эффективности образовательной деятельности в ПОО.

В целом, интеграция формирования личностных качеств, педагогических подходов к кибербезопасности и системного анализа учебных планов способствует подготовке всесторонне развитых, профессионально компетентных и социально ответственных выпускников, готовых к вызовам цифрового общества и профессиональной деятельности.

Важным аспектом дальнейшего развития системы профессионального образования является усиление междисциплинарного взаимодействия, что

позволяет не только углубить профильные знания студентов, но и расширить их кругозор, повысить адаптивность и гибкость мышления. В частности, интеграция дисциплин, связанных с кибербезопасностью, с гуманитарными и социальными науками способствует формированию комплексного понимания цифровой среды как социального пространства, где технические навыки дополняются этическими нормами и правовыми аспектами.

Кроме того, значительное внимание следует уделять развитию метапредметных компетенций, таких как критическое мышление, коммуникация, умение работать в команде и принимать решения в условиях неопределённости. Эти навыки становятся особенно актуальными в условиях быстрого технологического прогресса и постоянных изменений на рынке труда. Формирование таких компетенций возможно через проектную деятельность, кейс-методы, а также через внедрение современных образовательных технологий, включая дистанционные и смешанные формы обучения.

Особое значение приобретает поддержка и развитие мотивации студентов, что требует создания благоприятной образовательной среды, учитывающей индивидуальные особенности обучающихся. Психолого-педагогическое сопровождение, наставничество и организация внеучебной деятельности способствуют укреплению внутренней мотивации, формированию устойчивых ценностных ориентиров и профессиональной идентичности.

В контексте цифровизации образования необходимо также развивать цифровую компетентность педагогов, что позволит им эффективно использовать современные инструменты и методики обучения, адаптировать образовательные программы под актуальные требования и обеспечивать высокий уровень взаимодействия с обучающимися. Повышение квалификации преподавателей, обмен опытом и внедрение инновационных практик становятся ключевыми факторами успешной реализации образовательных задач.

Немаловажным направлением является развитие системы оценки качества образования, которая должна быть комплексной, объективной и ориентированной на достижение планируемых результатов. Внедрение современных средств контроля и мониторинга, включая автоматизированные системы, позволяет своевременно выявлять проблемные зоны, корректировать учебные планы и повышать эффективность образовательного процесса.

В перспективе особое внимание следует уделять развитию партнерских отношений между образовательными организациями, работодателями и научными учреждениями. Такое сотрудничество способствует актуализации содержания образования, расширению возможностей для практической подготовки студентов, а также интеграции научных достижений и инноваций в учебный процесс.

Таким образом, дальнейшее совершенствование профессионального образования требует комплексного подхода, включающего развитие личностных и профессиональных компетенций, внедрение современных педагогических технологий, повышение квалификации педагогов и активное взаимодействие с социальными и профессиональными институтами.

ГЛАВА 2. РАЗРАБОТКА МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО ФОРМИРОВАНИЮ ОСНОВ КИБЕРБЕЗОПАСНОСТИ У СТУДЕНТОВ ПОО НА БАЗЕ НЯЗЕПЕТРОВСКОГО ФИЛИАЛА ГБПОУ «КАСЛИНСКИЙ ПРОМЫШЛЕННО ГУМАНИТАРНЫЙ ТЕХНИКУМ».

В современном цифровом мире, где образовательные организации активно внедряют информационные технологии в учебный процесс, вопросы кибербезопасности приобретают особую актуальность. Студенты профессиональных образовательных организаций (ПОО), будущие специалисты в различных областях, должны обладать базовыми знаниями и навыками для защиты себя и организации от киберугроз.

Целью методических рекомендаций является предоставление педагогам ПОО практического инструмента для обучения студентов основам кибербезопасности. Рекомендации разработаны с учетом специфики образовательной среды ПОО и ориентированы на формирование у студентов критического мышления, умения оценивать риски и предпринимать необходимые меры для защиты информации.

Методические рекомендации включают в себя:

1. Обзор основных киберугроз и методов защиты от них.
2. Рекомендации по организации учебных занятий по кибербезопасности.
3. Примеры практических заданий и кейсов для закрепления полученных знаний.
4. Перечень ресурсов для самостоятельного изучения кибербезопасности.
5. Лабораторные работы для оттачивания полученных навыков.

Важно подчеркнуть, что формирование основ кибербезопасности – это не однократное мероприятие, а непрерывный процесс, требующий постоянного обновления знаний и навыков в соответствии с изменяющимися угрозами. Предлагаемые методические рекомендации призваны стать отправной точкой для педагогов ПОО в создании эффективной системы обучения

кибербезопасности, способствующей подготовке компетентных и ответственных специалистов.

Для эффективного внедрения основ кибербезопасности в образовательный процесс необходимо учитывать возрастные особенности и уровень подготовки студентов ПОО. Рекомендуется начинать с ознакомления с основными понятиями и принципами кибербезопасности, постепенно переходя к более сложным темам, таким как защита персональных данных, безопасное использование социальных сетей и электронной почты, а также основы защиты от вредоносного программного обеспечения.

Важным аспектом является интеграция вопросов кибербезопасности в различные учебные дисциплины, а не выделение их в отдельный курс. Это позволит студентам увидеть практическое применение знаний и навыков кибербезопасности в своей будущей профессиональной деятельности. Например, при изучении информационных технологий можно рассматривать вопросы защиты данных и конфиденциальности, а при изучении экономики – вопросы финансовой безопасности в интернете.

Для закрепления полученных знаний рекомендуется использовать интерактивные методы обучения, такие как деловые игры, кейс-стади, онлайн-тесты и викторины. Это позволит вовлечь студентов в активный учебный процесс и проверить их понимание материала. Также полезно организовывать встречи с экспертами в области кибербезопасности, которые смогут поделиться своим опытом и ответить на вопросы студентов.

В заключение, методические рекомендации по формированию основ кибербезопасности у студентов ПОО – это важный инструмент для подготовки компетентных и ответственных специалистов, способных эффективно защищать себя и организацию от киберугроз. Реализация этих рекомендаций позволит повысить уровень осведомленности студентов о кибербезопасности и сформировать у них необходимые навыки для безопасной работы в цифровой среде.

2.1 Информационно-образовательная среда Нязепетровского филиала Каслинского промышленно-гуманитарного техникума (ГБПОУ «КПГТ»)

Цель выявить в учебно-методической документации (УМД) дисциплин, связанных с информационными сетями, программированием, информатикой и смежными областями, содержание, которое может служить основой для проведения занятий по кибербезопасности.

Современный мир немыслим без информационных технологий. Вместе с их развитием растет и актуальность кибербезопасности – защиты наших цифровых активов от угроз. Для эффективного обучения основам кибербезопасности необходимо опираться на уже существующую базу знаний, заложенную в учебных программах по информатике, программированию и сетям. Данный анализ призван систематизировать и выявить те разделы и темы, которые могут быть трансформированы и дополнены для формирования компетенций в области кибербезопасности.

Для создания полноценных занятий по кибербезопасности необходимо:

- Акцентировать внимание на уязвимостях: При изучении любого аспекта (протокола, алгоритма, функции ОС) необходимо целенаправленно рассматривать, какие уязвимости могут быть связаны с его некорректным использованием или реализацией.
- Вводить специфическую терминологию: Дополнить существующую терминологию понятиями из области кибербезопасности (например, эксплойт, руткит, фишинг, социальная инженерия).
- Разрабатывать практические задания с фокусом на безопасность: Адаптировать существующие лабораторные работы или создавать новые, где студенты будут сталкиваться с реальными или смоделированными угрозами, учиться их выявлять и нейтрализовать.
- Использовать специализированные инструменты: Включать в учебный процесс инструменты, используемые в кибербезопасности (например,

Wireshark, Nmap, Metasploit, Burp Suite – в образовательных целях и с соблюдением этических норм).

- Интегрировать кейс-стади: Анализировать реальные инциденты кибербезопасности, чтобы студенты понимали последствия уязвимостей и важность защитных мер.
- Развивать критическое мышление: Стимулировать студентов к анализу информации, поиску неочевидных решений и прогнозированию потенциальных угроз.
- Включать этические аспекты: Обсуждать вопросы этики в области кибербезопасности, ответственность за свои действия в цифровом пространстве и правовые аспекты.

Примеры трансформации конкретных тем:

- Из "Протоколы TCP/IP" в "Анализ сетевого трафика и уязвимости протоколов": Вместо простого описания работы протоколов, акцентировать внимание на том, как можно перехватывать и анализировать трафик (например, с помощью Wireshark), выявлять незашифрованные данные, понимать, как работают атаки типа "человек посередине" (Man-in-the-Middle), и как протоколы могут быть использованы злоумышленниками.
- Из "Основы языка C++" в "Безопасное программирование на C++ и уязвимости управления памятью": Изучать не только синтаксис и возможности языка, но и распространенные уязвимости, такие как переполнение буфера, использование освобожденной памяти (use-after-free), гонки данных (data races). Практические задания могут включать написание кода с умышленными уязвимостями и последующее их исправление.
- Из "Основы операционной системы Linux" в "Администрирование Linux с фокусом на безопасность": Вместо общих команд, сосредоточиться на настройке прав доступа к файлам и каталогам, управлении пользователями и группами с учетом принципа наименьших привилегий, настройке межсетевого экрана (iptables/firewalld), мониторинге системных журналов на предмет

подозрительной активности, а также на безопасной установке и обновлении программного обеспечения.

- Из "Базы данных SQL" в "Безопасность баз данных и предотвращение SQL-инъекций": Изучать не только синтаксис SQL, но и различные типы SQL-инъекций, методы их обнаружения и предотвращения (например, параметризованные запросы, экранирование специальных символов). Практические задания могут включать создание уязвимого веб-приложения и последующую его защиту.
- Из "Разработка веб-приложений" в "Безопасная разработка веб-приложений (OWASP Top 10)": Целенаправленно изучать наиболее распространенные уязвимости веб-приложений согласно списку OWASP Top 10, такие как инъекции, небезопасная аутентификация, кросс-сайтовый скриптинг (XSS), кросс-сайтовая подделка запроса (CSRF), небезопасная десериализация. Практические задания могут включать поиск и эксплуатацию (в контролируемой среде) этих уязвимостей, а также разработку защищенных веб-приложений.

Учебно-методическая документация по дисциплинам, связанным с информационными сетями, программированием и информатикой, содержит богатый потенциал для формирования компетенций в области кибербезопасности. Путем целенаправленной трансформации и дополнения существующего содержания, с акцентом на уязвимости, специфическую терминологию и практические аспекты, можно создать эффективные учебные программы, которые подготовят специалистов, способных противостоять современным киберугрозам. Важно помнить, что кибербезопасность – это динамично развивающаяся область, поэтому учебные программы должны регулярно обновляться и адаптироваться к новым вызовам. Интеграция практических навыков, этических принципов и понимания правовых аспектов является залогом успешной подготовки квалифицированных кадров в сфере кибербезопасности.

Информационная образовательная среда Нязепетровского филиала Каслинского промышленно-гуманитарного техникума: взгляд на особенности образовательного процесса.

Нязепетровский филиал ГБПОУ "Каслинский промышленно-гуманитарный техникум" – это не просто стены, где проходят занятия, а целая экосистема, в которой переплетаются информационные технологии, педагогические подходы и потребности студентов. Анализ информационной образовательной среды (ИОС) позволяет нам понять, как именно здесь строится образовательный процесс, какие у него сильные стороны и где есть потенциал для развития.

Что такое ИОС и почему она важна?

Информационная образовательная среда – это совокупность технических, программных, информационных и методических ресурсов, а также организационных условий, которые обеспечивают доступ к информации, ее обработку, хранение и передачу в процессе обучения. Проще говоря, это все, что помогает студентам и преподавателям получать знания, общаться, выполнять задания и оценивать результаты.

В современном мире ИОС играет ключевую роль. Она позволяет:

- Расширить доступ к знаниям: Онлайн-курсы, электронные библиотеки, образовательные платформы делают информацию доступной в любое время и в любом месте.
- Персонализировать обучение: ИОС может адаптироваться к индивидуальным потребностям студентов, предлагая материалы разного уровня сложности и в разных форматах.
- Повысить эффективность обучения**:** Интерактивные задания, симуляторы, системы автоматической проверки знаний делают процесс более увлекательным и результативным.
- Развить цифровые компетенции: Студенты, активно использующие ИОС, приобретают навыки, необходимые для успешной карьеры в современном мире.

Применительно к Нязепетровскому филиалу, анализ ИОС позволяет выявить следующие особенности образовательного процесса:

1. Техническая база и доступность ресурсов:

Важно оценить количество и оснащенность компьютерных классов. Современные компьютеры, стабильный доступ в Интернет, наличие необходимого программного обеспечения – все это фундамент для эффективного использования ИОС. Скорость и стабильность интернет-соединения в аудиториях и общежитиях (если есть) напрямую влияют на возможность использования онлайн-ресурсов, участия в вебинарах и скачивания учебных материалов. Для профессионального образования важно наличие оборудования, которое может быть интегрировано в ИОС (например, станки с ЧПУ, лабораторное оборудование с возможностью подключения к компьютеру).

2. Информационные и программные ресурсы:

Наличие и актуальность электронной библиотечной системы, доступ к учебникам, методическим пособиям, научным статьям – это основа для самостоятельной работы студентов. Важно, чтобы элетроная библиотека была удобной в использовании и содержала материалы по всем преподаваемым дисциплинам. Используются в филиале платформы Moodle, Google Classroom или другие. Эти системы позволяют преподавателям размещать учебные материалы, создавать задания, проводить тестирование, отслеживать успеваемость студентов и организовывать дистанционное обучение. Для технических специальностей это могут быть CAD/CAM системы, программы для моделирования, симуляторы. Для гуманитарных – программы для работы с текстом, базами данных, презентациями. Наличие доступа к видеолекциям, интерактивным тренажерам, виртуальным лабораториям, онлайн-курсам от других образовательных учреждений.

3. Методическое обеспечение и педагогические подходы:

В филиале преподавателями разработаны электронные учебники, презентации, интерактивные задания, видеоуроки, которые соответствуют современным требованием и потребностям студентов. Преподаватели интегрируют ИОС в свои занятия. Используя элементы смешанного обучения, проектной деятельности с использованием цифровых инструментов и онлайн-дискуссий. Проводятся курсы повышения квалификации для преподавателей по использованию новых технологий и платформ, что критически важно для эффективного внедрения ИОС. Студентам предоставляется помощь в освоении цифровых инструментов, осуществляется работа с платформами и даются напутствия в поиске информации.

4. Организационные аспекты:

Политика использования информационной образовательной среды в каслинском промышленно гуманитарном техникуме существуют четкие правила и рекомендации по использованию ИОС для студентов и преподавателей. Есть специалисты технической поддержки, которые могут оперативно решить технические проблемы, связанные с работой ИОС. Обеспечивается защита персональных данных студентов и преподавателей, а также конфиденциальность учебной информации.

Исходя из вышеперечисленных аспектов, можно выделить ряд особенностей образовательного процесса в Нязепетровском филиале, которые напрямую связаны с его информационной образовательной средой.

Если информационная образовательная среда гибкая и доступная для обучающихся, студенты получают возможность учиться в удобное для них время и в любом месте, где есть доступ к сети Интернет. Это особенно актуально для студентов, которые совмещают учебу с работой или имеют другие обязательства. Возможность повторного просмотра лекций, доступа к дополнительным материалам и выполнения заданий в онлайн-режиме делает процесс обучения более гибким. Современная образовательная среда должна побуждать студентов к самостоятельной работе с информацией, поиску решений, критическому осмыслению полученных данных. Преподаватель из

роли единственного источника знаний трансформируется в наставника, направляющего и консультирующего. Это требует от студентов большей самоорганизации и ответственности за свой учебный процесс. Современные цифровые инструменты позволяют сделать занятия более динамичными и интересными. Использование интерактивных презентаций, онлайн-тестов, виртуальных лабораторий, образовательных игр способствует лучшему усвоению материала и повышает мотивацию студентов. Возможность участвовать в онлайн-дискуссиях и форумах также способствует активному вовлечению в учебный процесс. При наличии соответствующих инструментов ИОС может быть адаптирована под индивидуальные потребности каждого студента. Преподаватели могут предлагать дифференцированные задания, дополнительные материалы для тех, кто испытывает трудности, или более сложные задачи для тех, кто опережает программу. Это позволяет каждому студенту двигаться в своем темпе и максимально раскрывать свой потенциал. Активное использование ИОС в процессе обучения неизбежно приводит к развитию у студентов цифровых навыков, которые являются неотъемлемой частью современного рынка труда. Они учатся работать с различными программами, искать и анализировать информацию в сети, создавать цифровой контент, безопасно использовать интернет-ресурсы. Эти компетенции становятся конкурентным преимуществом при трудоустройстве. Хорошо развитая ИОС является основой для организации дистанционного обучения, что может быть особенно важно в условиях непредвиденных обстоятельств (например, пандемии). Также она позволяет эффективно реализовывать модели смешанного обучения, сочетая традиционные аудиторные занятия с онлайн-компонентами. ИОС может значительно упростить и ускорить коммуникацию между студентами и преподавателями, а также между самими студентами. Электронная почта, мессенджеры, форумы, системы обмена сообщениями в LMS позволяют оперативно решать возникающие вопросы, обмениваться информацией и координировать совместную работу.

Несмотря на очевидные преимущества, эффективное функционирование ИОС в Нязепетровском филиале может сталкиваться с определенными проблемами такими как: неравномерность технического оснащения, необходимость постоянного обновления контента, цифровое неравенство, педагогическая адаптация. Разберем каждую проблему более подробно:

1. Неравномерность технического оснащения: Важно обеспечить равный доступ к современным технологиям для всех студентов и преподавателей.

2. Необходимость постоянного обновления контента: Цифровые ресурсы быстро устаревают, поэтому требуется регулярное обновление учебных материалов и программного обеспечения.

3. Цифровое неравенство: Не все студенты могут иметь одинаковый уровень цифровой грамотности или доступ к необходимым устройствам вне стен техникума.

4. Педагогическая адаптация: Преподавателям необходимо постоянно совершенствовать свои навыки и методики, чтобы эффективно использовать возможности ИОС.

В целом, информационная образовательная среда Нязепетровского филиала ГБПОУ " Каслинский промышленно-гуманитарный техникум" является динамично развивающимся компонентом образовательного процесса. Ее дальнейшее совершенствование, направленное на обеспечение доступности, актуальности и интерактивности, будет способствовать повышению качества образования, подготовке конкурентоспособных специалистов и успешной адаптации выпускников к требованиям современного мира. Анализ и постоянная оптимизация ИОС – это залог успешного будущего техникума и его студентов.

Для более глубокого понимания особенностей образовательного процесса в Нязепетровском филиале, обусловленных ИОС, необходимо также рассмотреть роль административного и методического руководства**.** Эффективность ИОС невозможна без четкой стратегии ее развития, которая

должна быть интегрирована в общую концепцию образовательной деятельности техникума. Это включает в себя: планирование, бюджетирование, разработка нормативно-правовой базы, мониторинг и оценка, мониторинг и оценка.

Выделение достаточных средств на приобретение и обновление оборудования, лицензирование программного обеспечения, подписку на электронные ресурсы и обучение персонала. Создание внутренних положений, регламентирующих использование ИОС, правила доступа, ответственность пользователей и порядок технической поддержки. Регулярный анализ эффективности использования ИОС, сбор обратной связи от студентов и преподавателей, выявление проблемных зон и принятие мер по их устранению. Это может включать опросы, фокус-группы, анализ статистики использования платформ и ресурсов. Особое внимание следует уделить тому, как ИОС способствует формированию именно профессиональных компетенций, что критически важно для промышленно-гуманитарного техникума. Практико-ориентированное обучение позволяет интегрировать в учебный процесс виртуальные тренажеры, симуляторы производственных процессов, цифровые модели оборудования. Это дает студентам возможность отрабатывать практические навыки в безопасной и контролируемой среде, прежде чем приступить к работе с реальным оборудованием. Например, будущие сварщики могут использовать VR-тренажеры, а механики – программы для диагностики неисправностей. Работа с реальными данными и проектами облегчает доступ к отраслевым базам данных, статистике, технической документации. Студенты могут использовать эти ресурсы для выполнения курсовых и дипломных проектов, максимально приближенных к реальным производственным задачам. Возможность удаленного доступа к таким данным расширяет горизонты проектной деятельности. Развитие навыков командной работы в цифровой среде: Многие современные проекты реализуются распределенными командами. ИОС предоставляет инструменты для совместной работы над документами, презентациями, кодом, что позволяет студентам осваивать

навыки эффективного взаимодействия в цифровом пространстве, что является ценным качеством для будущего специалиста. Непрерывное профессиональное развитие открывает доступ к огромному количеству онлайн-курсов, вебинаров, профессиональных сообществ. Это формирует у студентов понимание необходимости постоянного самообразования и развития в течение всей карьеры, что особенно актуально в быстро меняющемся мире профессий. Многие промышленные предприятия активно внедряют цифровые технологии, автоматизацию, "умное" производство. ИОС техникума, если она отражает эти тенденции, готовит студентов к работе в условиях цифровой трансформации, обучая их взаимодействию с автоматизированными системами, анализу больших данных, использованию специализированного ПО.

Нельзя игнорировать и социально-психологические аспекты влияния ИОС на образовательный процесс. Современные студенты, выросшие в цифровой среде, ожидают использования технологий в обучении. Интерактивные элементы, мультимедийный контент, геймификация могут значительно повысить их мотивацию и интерес к учебе. Возможность повторного просмотра материалов, выполнения заданий в своем темпе, а также доступ к дополнительным ресурсам для самоподготовки может снизить уровень тревожности у студентов, особенно у тех, кто испытывает трудности с усвоением материала. Помимо формальной коммуникации, ИОС может способствовать развитию неформального общения между студентами, созданию учебных групп, обмену знаниями и опытом.

Развитие коммуникативных навыков (продолжение): Помимо формальной коммуникации, ИОС может способствовать развитию неформального общения между студентами, созданию учебных групп, обмену знаниями и опытом. Форумы, чаты и совместные онлайн-проекты становятся площадками для формирования дружеских связей и развития навыков командной работы, что важно для будущей профессиональной деятельности. Однако, важно помнить и о потенциальных рисках, таких как кибербуллинг или чрезмерная зависимость от онлайн-общения, что требует внимания со стороны

педагогического коллектива и разработки соответствующих правил поведения в цифровой среде.

1.Формирование самодисциплины и самоконтроля: Гибкость ИОС требует от студентов высокого уровня самоорганизации. Умение планировать свое время, ставить цели, отслеживать прогресс и самостоятельно находить мотивацию для обучения – это те качества, которые развиваются в процессе активного использования цифровых образовательных ресурсов. Преподаватели, в свою очередь, могут использовать инструменты ИОС для мониторинга активности студентов и предоставления своевременной обратной связи, помогая им развивать эти важные навыки.

2. Инклюзивность и доступность: Хорошо спроектированная ИОС может стать мощным инструментом для обеспечения инклюзивного образования. Студенты с ограниченными возможностями здоровья могут получить доступ к адаптированным учебным материалам, использовать вспомогательные технологии, участвовать в занятиях в дистанционном формате. Это способствует созданию равных возможностей для всех обучающихся и формированию толерантного отношения в коллективе.

Учитывая современные тенденции в образовании и стремительное развитие технологий, Нязепетровский филиал имеет значительный потенциал для дальнейшего развития своей информационной образовательной среды. Ключевыми направлениями могут стать:

1. Углубленная интеграция искусственного интеллекта (ИИ): ИИ может быть использован для персонализации образовательных траекторий, автоматической проверки сложных заданий, предоставления индивидуальных рекомендаций по обучению, а также для анализа больших данных об успеваемости студентов с целью выявления закономерностей и прогнозирования возможных трудностей.

2. Развитие виртуальной и дополненной реальности (VR/AR): Для технических специальностей VR/AR могут предложить революционные возможности для практического обучения. Создание виртуальных лабораторий,

симуляторов сложных производственных процессов, возможность "побывать" на реальном производстве – все это может значительно повысить эффективность обучения и сделать его более наглядным и запоминающимся.

3. Создание собственной образовательной платформы или расширение функционала существующей: Разработка или адаптация платформы, максимально отвечающей специфике техникума, его образовательным программам и потребностям студентов, может стать стратегическим шагом. Это позволит более гибко управлять контентом, интегрировать различные сервисы и обеспечить единое информационное пространство.

4. Активное вовлечение в сетевое взаимодействие: Сотрудничество с другими образовательными учреждениями, предприятиями-партнерами, ведущими экспертами в отрасли через ИОС может обогатить образовательный процесс. Это может включать совместные онлайн-курсы, мастер-классы, стажировки, участие в профессиональных конкурсах и проектах.

5. Развитие системы непрерывного мониторинга и обратной связи: Создание эффективных механизмов сбора и анализа обратной связи от всех участников образовательного процесса (студентов, преподавателей, работодателей) позволит оперативно реагировать на изменения, выявлять "узкие места" и постоянно совершенствовать ИОС.

Информационная образовательная среда Нязепетровского филиала ГБПОУ "Каслинский промышленно-гуманитарный техникум" является неотъемлемой частью современного образовательного процесса. Ее анализ показывает, что она не только обеспечивает доступ к информации и технологиям, но и активно формирует особенности образовательного процесса, способствуя развитию самостоятельности, ответственности, цифровых компетенций и профессиональных навыков студентов. Дальнейшее целенаправленное развитие ИОС, с учетом современных технологических трендов и потребностей рынка труда, позволит техникуму оставаться конкурентоспособным, готовить высококвалифицированных специалистов и

успешно отвечать на вызовы времени. Инвестиции в ИОС – это инвестиции в будущее студентов и в развитие региональной экономики.

В эпоху динамичных социокультурных изменений, когда система образования подвергается постоянной трансформации, вопрос формирования личностных качеств студентов приобретает особую актуальность. Современный специалист должен обладать не только профессиональными компетенциями, но и развитыми морально-этическими качествами, коммуникативными навыками и умением адаптироваться к новым условиям. Профессиональное образование, в свою очередь, является ключевым институтом социализации, оказывающим значительное влияние на становление личности будущего профессионала. Методологические подходы к изучению проблемы Исследование формирования личностных качеств студентов требует комплексного методологического подхода. Необходимо учитывать социально-психологические особенности студенческого возраста, специфику образовательной среды, а также влияние внеучебных факторов. Важным этапом является анализ существующих теоретических концепций и эмпирических данных, позволяющих определить ключевые факторы, влияющие на развитие личности студента. Практические аспекты формирования личностных качеств Результаты исследования могут быть использованы для разработки эффективных образовательных программ и технологий, направленных на развитие личностных качеств студентов. Важно создать условия для самореализации и творческой активности, стимулировать участие студентов в общественной жизни и волонтерских проектах. Особое внимание следует уделять формированию ценностных ориентаций, профессиональной этики и гражданской ответственности. Только комплексный подход, учитывающий индивидуальные особенности студентов и возможности образовательной среды, позволит успешно решать задачи формирования личности будущего профессионала. В контексте профессионального образования, формирование личностных качеств неразрывно связано с развитием профессиональной идентичности. Студенты должны осознавать свою роль в обществе, понимать

значимость своей будущей профессии и ощущать ответственность за результаты своей деятельности. Этому способствует активное вовлечение студентов в научно-исследовательскую работу, участие в профессиональных конкурсах и стажировках, а также взаимодействие с опытными специалистами-практиками. Важно, чтобы студенты имели возможность применять свои знания и навыки в реальных ситуациях, ощущая свою полезность и внося вклад в развитие своей профессиональной области.

В формировании личностных качеств ключевую роль играет преподаватель. Его задача не только передавать знания, но и формировать у студентов ценностное отношение к профессии, развивать критическое мышление и умение самостоятельно принимать решения. Преподаватель должен быть примером профессионализма, высокой морали и гражданской ответственности. Важно, чтобы в образовательном процессе создавалась атмосфера доверия и сотрудничества, где студенты могли бы свободно выражать свои мысли и идеи, не боясь критики и осуждения.

Необходимо также учитывать влияние информационных технологий на формирование личности студента. С одной стороны, они открывают широкие возможности для обучения и саморазвития. С другой стороны, могут негативно влиять на ценностные ориентации и социальное поведение. Поэтому важно развивать у студентов навыки критического анализа информации, умение отличать достоверные источники от недостоверных, а также формировать культуру использования информационных технологий.

В заключение следует отметить, что формирование личностных качеств студентов в процессе профессионального образования — это сложный и многогранный процесс, требующий комплексного подхода и совместных усилий преподавателей, студентов и общества в целом. Только в этом случае можно подготовить высококвалифицированных специалистов, обладающих не только профессиональными компетенциями, но и развитыми морально-этическими качествами, готовых к решению сложных задач и внесению вклада в развитие общества.

Анализ учебно-методической документации информационно-цифровых дисциплин для выявления тех дисциплин, на основе которых возможно внедрить в процесс обучения основы кибербезопасности. В условиях стремительного роста цифровизации всех сфер жизни, вопросы кибербезопасности приобретают первостепенное значение. Подготовка квалифицированных специалистов, обладающих знаниями и навыками в этой области, является одной из ключевых задач современного образования. Интеграция основ кибербезопасности в учебные программы информационно-цифровых дисциплин представляется эффективным способом достижения этой цели. Настоящий анализ направлен на выявление тех дисциплин, в рамках которых наиболее целесообразно внедрение модулей и тем, посвященных кибербезопасности. В качестве основы для анализа служат учебно-методические комплексы (УМК) дисциплин, охватывающие различные аспекты информационных технологий, программирования, сетевых технологий и управления данными. Критериями отбора дисциплин для интеграции основ кибербезопасности являются: Наличие в содержании дисциплин тем, связанных с обработкой, хранением и передачей информации. Акцент на практическое применение изучаемых технологий и инструментов. Направленность на формирование у студентов навыков анализа и решения проблем. Результаты анализа позволяют определить перечень дисциплин, в рамках которых возможно наиболее эффективно интегрировать основы кибербезопасности. Среди них могут быть выделены курсы по операционным системам, компьютерным сетям, базам данных, веб-разработке и прикладному программированию. Внедрение соответствующих модулей и тем в учебные программы позволит повысить уровень осведомленности студентов о существующих угрозах, методах защиты информации и нормативно-правовом регулировании в сфере кибербезопасности. Для каждой отобранной дисциплины необходимо разработать или адаптировать существующие учебные материалы с учетом специфики кибербезопасности. Это может включать в себя добавление новых лекций, практических заданий, кейсов и

лабораторных работ, направленных на изучение угроз, уязвимостей, методов защиты и инструментов обеспечения кибербезопасности. Важно интегрировать практические примеры и сценарии, отражающие реальные случаи из практики специалистов по кибербезопасности, чтобы максимально приблизить обучение к реальным условиям.

При интеграции кибербезопасности в дисциплины необходимо учитывать уровень подготовки студентов и сложность предлагаемых материалов. Рекомендуется начинать с основ, постепенно переходя к более сложным и специализированным темам. Важно также обеспечить баланс между теоретическими знаниями и практическими навыками, чтобы студенты могли не только понимать основные концепции, но и применять их на практике для решения конкретных задач.

Оценка эффективности внедрения основ кибербезопасности в учебные программы должна проводиться на основе различных методов, включая тестирование, опрос студентов и преподавателей, анализ успеваемости и оценку практических навыков. Полученные результаты позволят выявить сильные и слабые стороны внедрения, а также внести необходимые корректировки в учебные программы и методические материалы.

В заключение, интеграция основ кибербезопасности в учебно-методическую документацию информационно-цифровых дисциплин является важным шагом в подготовке квалифицированных специалистов, способных решать задачи обеспечения безопасности в современном цифровом мире. Тщательный анализ существующих дисциплин, разработка и адаптация учебных материалов, а также оценка эффективности внедрения позволят создать образовательную среду, способствующую формированию у студентов необходимых знаний, навыков и компетенций в области кибербезопасности.

2.1.1 БИОП СПО Касли информационная образовательная среда СПО Касли , специальности переподготовки / описание базы исследования.

Нязепетровский филиал государственного бюджетного профессионального образовательного учреждения «Каслинский промышленно-гуманитарный техникум».

Адрес организации: 456970, Челябинская область, г. Нязепетровск, ул. Ленина, д.97.

Лицензия на осуществление образовательной деятельности №11758 от «02» октября 2015года. Основной государственный регистрационный номер юридического лица 1027400728695. Идентификационный номер налогоплательщика 7409001380.

Государственная аккредитация: бессрочная.

Наименование укрупненных групп профессий, специальностей и направлений подготовки: техника и технологии строительства, информатика и вычислительная техника, машиностроение, технология материалов, сервиз и туризм, образование и педагогические науки.

ГБПОУ «Каслинский промышленно-гуманитарный техникум» был основан 20 мая 1944 года, организатором стал А. К. Соболевский. В 1946 году были выпущены 110 человек, которые получили такие специальности как: токарь, слесарь, столяр и формовщик.

Силами учащихся и работников училища были возведены слесарные мастерские, сварочный, кузнечный и формовочные участки, технологическое отделение и спортивный городок. В 1976 году было проведено много работы по расширению и укреплению материальной базы.

В настоящее время техникум выпускает таких специалистов как: техник, повар кондитер, воспитатель детей дошкольного возраста, штукатур, системный администратор.

Информационная образовательная среда Нязепетровского филиала ГБПОУ "Каслинский промышленно-гуманитарный техникум" – это не просто набор технических средств и программ, а живой организм, который постоянно

развивается и адаптируется к меняющимся условиям. Анализ этой среды позволяет нам не только понять текущее состояние образовательного процесса, но и наметить пути его дальнейшего совершенствования, делая акцент на тех особенностях, которые делают обучение в филиале уникальным и эффективным.

Ключевые особенности образовательного процесса, обусловленные ИОС:

Как уже было отмечено, ИОС оказывает прямое влияние на то, как студенты учатся и как преподаватели преподают. Рассмотрим эти особенности более детально, подчеркивая их значимость для Нязепетровского филиала:

1. Гибкость и доступность обучения как основа для профессионального роста: В условиях, когда студенты часто совмещают учебу с работой или имеют другие жизненные обстоятельства, гибкость, предоставляемая ИОС, становится не просто удобством, а необходимостью. Возможность доступа к учебным материалам в любое время, повторный просмотр лекций, выполнение заданий в удобном темпе – все это позволяет студентам более эффективно управлять своим временем и глубже погружаться в изучаемый материал. Для техникума, ориентированного на подготовку специалистов для реального сектора экономики, такая гибкость означает, что выпускники будут более подготовлены к динамичной рабочей среде, где требуется постоянная адаптация и самообучение.
2. Развитие самостоятельности и ответственности – фундамент для будущих профессионалов: ИОС, по своей сути, требует от студента активной позиции. Переход от пассивного потребления информации к самостоятельному поиску, анализу и синтезу знаний формирует критически важное качество – ответственность за собственное обучение. Преподаватель становится не столько транслятором знаний, сколько наставником, проводником в мире информации. Это формирует у будущих специалистов умение самостоятельно решать проблемы, принимать решения и нести за них ответственность, что является основой для успешной карьеры в любой отрасли.

3. Интерактивность и вовлеченность – путь к глубокому пониманию и запоминанию: Современные цифровые инструменты, интегрированные в ИОС, превращают обучение из монотонного процесса в увлекательное приключение. Интерактивные симуляторы, виртуальные лаборатории, образовательные игры, онлайн-квизы – все это делает процесс усвоения материала более наглядным, динамичным и запоминающимся. Для техникума, где важно не только теоретическое знание, но и практическое применение, интерактивные методы обучения позволяют студентам лучше понять сложные концепции и отработать навыки в безопасной среде, что напрямую влияет на качество их профессиональной подготовки.

4. Персонализация образовательного пути – раскрытие потенциала каждого студента: ИОС открывает возможности для индивидуализации обучения. Преподаватели могут использовать различные инструменты для дифференциации заданий, предоставления дополнительных материалов для тех, кто нуждается в поддержке, или более сложных задач для тех, кто демонстрирует высокие результаты. Это позволяет каждому студенту двигаться в своем темпе, максимально раскрывая свой потенциал и развивая те навыки, которые наиболее важны для его будущей профессии. Для техникума это означает возможность выпускать специалистов, чьи компетенции максимально соответствуют их индивидуальным способностям и интересам.

5. Формирование цифровых компетенций – ключ к успешной карьере в XXI веке: В современном мире цифровые навыки являются не просто преимуществом, а необходимостью. Активное использование ИОС в процессе обучения, начиная от работы с офисными программами и заканчивая освоением специализированного программного обеспечения, формирует у студентов комплекс цифровых компетенций. Они учатся эффективно искать и обрабатывать информацию в сети, создавать цифровой контент, безопасно использовать онлайн-ресурсы, работать с различными платформами. Эти навыки становятся критически важными для трудоустройства и дальнейшего профессионального роста в любой сфере.

Нязепетровский филиал ГБПОУ «Каслинский промышленно-гуманитарный техникум» представляет собой важное образовательное учреждение, обеспечивающее подготовку специалистов в различных технических и гуманитарных направлениях. Анализ информационной образовательной среды данного филиала позволяет выявить ключевые особенности организации учебного процесса и использования современных технологий в обучении.

Во-первых, информационная образовательная среда филиала характеризуется интеграцией цифровых ресурсов и традиционных методов преподавания. В учебном процессе активно применяются электронные образовательные платформы, мультимедийные материалы и интерактивные технологии, что способствует повышению мотивации студентов и улучшению усвоения учебного материала. Наличие доступа к электронным библиотекам и специализированным базам данных расширяет возможности для самостоятельной работы и научных исследований.

Во-вторых, филиал уделяет внимание развитию компетенций, необходимых для успешной профессиональной деятельности. Образовательный процесс построен с учетом современных требований рынка труда, что отражается в использовании практикоориентированных заданий, проектной деятельности и сотрудничестве с предприятиями региона. Такая направленность способствует формированию у студентов не только теоретических знаний, но и практических навыков.

Кроме того, важной особенностью является поддержка взаимодействия между преподавателями и студентами через цифровые коммуникационные средства. Использование электронных дневников, платформ для дистанционного обучения и мессенджеров обеспечивает оперативную обратную связь и способствует более гибкому и индивидуализированному подходу к обучению.

Таким образом, информационная образовательная среда Нязепетровского филиала ГБПОУ «Каслинский промышленно-гуманитарный техникум»

представляет собой современную, технологически оснащенную систему, ориентированную на эффективное обучение и подготовку квалифицированных специалистов. Особенности образовательного процесса включают сочетание цифровых и традиционных методов, практическую направленность и активное использование коммуникационных технологий, что в целом способствует повышению качества образования и формированию конкурентоспособных выпускников.

Особое внимание в образовательной среде филиала уделяется созданию условий для непрерывного профессионального развития как студентов, так и преподавателей. Регулярное проведение методических семинаров, тренингов и курсов повышения квалификации способствует обновлению педагогических компетенций и внедрению инновационных образовательных технологий. Это позволяет преподавателям эффективно адаптировать учебные программы под изменяющиеся требования отрасли и использовать современные инструменты обучения.

Кроме того, филиал активно развивает инфраструктуру, обеспечивающую доступ к современному оборудованию и программному обеспечению, необходимому для освоения профессиональных навыков. Лаборатории и мастерские оснащены техническими средствами, которые позволяют студентам на практике закреплять теоретические знания и осваивать современные технологии производства и управления.

Важным аспектом является также формирование в образовательной среде условий для развития критического мышления, творческих способностей и самостоятельности студентов. Использование проектной деятельности, кейс-методов и групповых форм работы способствует развитию аналитических навыков и умению работать в команде, что является неотъемлемой частью профессиональной подготовки.

Не менее значимой составляющей является поддержка инклюзивного образования и создание комфортной среды для студентов с различными образовательными потребностями.

2.2 Методика формирования основы кибербезопасности на базе Нязепетровского филиала Каслинского промышленно-гуманитарного техникума.

Методика формирования основ кибербезопасности студентов профессионального обучения: разработка и апробация. В эпоху цифровой трансформации, когда киберпространство становится неотъемлемой частью профессиональной деятельности в любой отрасли, формирование компетенций в области кибербезопасности у студентов профессионального образования приобретает особую актуальность. Данная работа посвящена разработке и апробации методики, направленной на формирование основ кибербезопасности у студентов профессионального обучения. В рамках разработки методики были определены ключевые компоненты: теоретический блок, включающий в себя изучение основных понятий и угроз кибербезопасности; практический блок, предполагающий выполнение лабораторных работ и решение кейсов, моделирующих реальные ситуации; и блок контроля, включающий в себя тестирование и оценку приобретенных знаний и навыков. Особое внимание уделено интеграции интерактивных методов обучения, таких как хакатоны и ролевые игры, для повышения мотивации студентов и развития их практических навыков. Апробация методики проводилась на базе Нязепетровского филиала ГБПОУ «Каслинский промышленно-гуманитарный техникум» и включала в себя оценку эффективности по нескольким критериям: уровень усвоения теоретического материала, способность применять полученные знания на практике, а также уровень сформированности навыков защиты информации. Результаты апробации показали значительное повышение уровня кибербезопасности среди студентов, прошедших обучение по разработанной методике. Внедрение данной методики в образовательный процесс позволит повысить уровень защищенности критической инфраструктуры и обеспечить конкурентоспособность выпускников на рынке труда. Для обеспечения устойчивого и эффективного формирования основ кибербезопасности у студентов профессионального обучения, методика была

разработана с учетом специфики различных направлений подготовки. Это предполагает адаптацию содержания и форм обучения к конкретным профессиональным задачам, с которыми выпускники столкнутся в своей будущей деятельности. Например, для студентов, обучающихся по направлениям, связанным с информационными технологиями, акцент делается на углубленное изучение технических аспектов защиты информации, в то время как для студентов гуманитарных направлений больше внимания уделяется вопросам социальной инженерии и кибергигиены.

Важным элементом разработанной методики является использование современных образовательных технологий, таких как онлайн-платформы, интерактивные симуляторы и системы управления обучением. Это позволяет обеспечить гибкость и доступность обучения, а также создать персонализированную траекторию обучения для каждого студента. Кроме того, применение современных технологий способствует повышению вовлеченности студентов в учебный процесс и формированию у них устойчивой мотивации к изучению вопросов кибербезопасности.

В процессе апробации методики была выявлена необходимость постоянного мониторинга и актуализации учебных материалов, чтобы они соответствовали современным угрозам и тенденциям в области кибербезопасности. Для этого предусмотрен регулярный анализ новых видов кибератак, изменений в законодательстве и нормативных актах, а также внедрение лучших практик в области защиты информации.

В заключение, разработанная и апробированная методика формирования основ кибербезопасности у студентов профессионального обучения представляет собой эффективный инструмент для подготовки квалифицированных специалистов, обладающих необходимыми знаниями и навыками для защиты информации в цифровой среде. Внедрение данной методики в образовательный процесс позволит не только повысить уровень защищенности критической инфраструктуры, но и обеспечить конкурентоспособность выпускников на рынке труда.

Ожидаемые результаты исследования включают в себя разработку учебно-методического комплекса, обеспечивающего эффективное формирование основ кибербезопасности у студентов профессионального образования. Данный комплекс будет включать в себя: программу курса, методические рекомендации для преподавателей, учебные материалы для студентов, а также систему контроля знаний.

Предлагаемая методика формирования основ кибербезопасности базируется на принципах проблемно-ориентированного обучения и активного вовлечения студентов в учебный процесс. Использование интерактивных методов обучения, таких как деловые игры, моделирование кибератак и разбор реальных инцидентов, позволит повысить интерес студентов к изучаемому материалу и сформировать у них практические навыки в области кибербезопасности.

Важным аспектом разработанной методики является ее ориентированность на формирование не только теоретических знаний, но и практических навыков, необходимых для защиты информации в различных сферах профессиональной деятельности. В рамках практических занятий студенты будут изучать методы защиты от вредоносного программного обеспечения, способы обеспечения безопасности веб-приложений и баз данных, а также принципы работы средств криптографической защиты информации.

Оценка эффективности разработанной методики будет проводиться на основе анализа успеваемости студентов, результатов тестирования и выполнения практических заданий, а также на основе их отзывов о качестве обучения. Полученные результаты позволят внести необходимые корректировки в методику и повысить ее эффективность. Результаты исследования могут быть использованы для совершенствования образовательных программ в системе профессионального образования и повышения уровня подготовки специалистов в области кибербезопасности.

Внедрение разработанного учебно-методического комплекса позволит систематизировать процесс обучения основам кибербезопасности в профессиональном образовании, обеспечив единообразие требований к знаниям и навыкам выпускников. Это, в свою очередь, повысит их конкурентоспособность на рынке труда и будет способствовать снижению рисков, связанных с киберугрозами, в различных отраслях экономики.

Особое внимание в учебно-методическом комплексе будет уделено формированию у студентов навыков анализа и оценки рисков в области кибербезопасности, а также умениям разрабатывать и реализовывать меры по их минимизации. Это включает в себя изучение стандартов и нормативных правовых актов в области кибербезопасности, а также освоение современных инструментов и технологий защиты информации.

Перспективы дальнейших исследований в данной области связаны с разработкой адаптивных образовательных технологий, учитывающих индивидуальные особенности и потребности каждого студента. Это позволит повысить эффективность обучения и обеспечить более глубокое усвоение материала. Кроме того, необходимо проводить постоянный мониторинг актуальных киберугроз и оперативно вносить изменения в учебно-методический комплекс, чтобы он соответствовал современным требованиям.

В конечном итоге, реализация результатов исследования будет способствовать формированию кадрового резерва специалистов в области кибербезопасности, способных эффективно решать задачи по защите информации и обеспечению безопасности критической инфраструктуры. Это имеет важное значение для национальной безопасности и устойчивого развития экономики в условиях цифровой трансформации.

Дальнейшее развитие учебно-методического комплекса предполагает интеграцию практико-ориентированных заданий и кейсов, моделирующих реальные ситуации в сфере кибербезопасности. Это позволит студентам применить полученные теоретические знания на практике, развить навыки командной работы и принятия решений в условиях неопределенности.

Планируется также активное взаимодействие с представителями индустрии для получения обратной связи и актуализации содержания учебных материалов.

Важным аспектом является создание системы оценки качества обучения, включающей как традиционные формы контроля (тестирование, экзамены), так и оценку практических навыков и умений. Это позволит не только оценить уровень подготовки студентов, но и выявить пробелы в знаниях и скорректировать образовательный процесс. Также необходимо разработать систему повышения квалификации для преподавателей, чтобы они могли быть в курсе последних тенденций и технологий в области кибербезопасности.

В перспективе, результаты исследования могут быть использованы для разработки образовательных программ в области кибербезопасности для различных уровней образования, от среднего профессионального до высшего. Это позволит создать непрерывную систему подготовки специалистов, способных эффективно противостоять киберугрозам и обеспечивать информационную безопасность в различных сферах деятельности.

2.3 Опыто-экспериментальная работа Нязепетровского филиала Каслинского промышленно-гуманитарного техникума

Среди перечисленных возможных компонентов модернизации содержательной составляющей отечественной системы подготовки специалистов по информационной безопасности (переориентация профессиональной подготовки в области информационной безопасности (по «открытым» образовательным программам) от потребностей, в большей степени, государственных органов на потребности, в том числе, «открытого» бизнессообщества; фрагментарное изменение содержания образовательных программ; интеграция образовательных программ с дополнительными образовательными курсами отечественных и зарубежных вендоров) для проведения опытно-экспериментальной работы был выбран третий компонент в виду объективных сложностей опытно-экспериментальной проверки механизмов совершенствования по первому и второму компоненту. Для проверки результатов обучения по одному из внедренных механизмов была проведена опытно-экспериментальная работа по оценке влияния разработаной методической рекомендации, готовность студентов противостоянию цифровым угрозам.

Опытно-экспериментальная работа по интеграции образовательных программ с разработанным учебным курсом проводилась на базе Нязепетровского филиала государственного бюджетного профессионального образовательного учереждения «Каслинский промышленно-гуманитарный техникум». В исследовании приняли участие 81 обучающийся, среди которых студенты 2-го и 3-го курсов направления подготовки 10.03.01 «Информационная безопасность», в течение 2023-2024, 2024-2025 и 2025- 2026 учебных лет. Исследование по интеграции учебного курса было проведено на примере курса «Формирование основ кибербезопасности у студентов СПО».

Студенты обучались по программе с внедрением учебного курса среднего уровня «Формирование основ кибербезопасности у студентов СПО» в дисциплину «Системы защиты информации в мире». Данная дисциплина изучается студентами образовательных программ 10.03.01 «Информационная безопасность» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» в течение трех семестров (5-7 семестры). Пятый семестр изучается тематический блок «История становления системы обеспечения безопасности в информационной сфере в России», в шестой – «Современная система защиты информации за рубежом» и в седьмой – «Зарубежный взгляд на обеспечение кибербезопасности». В рамках третьего блока предполагается изучение разработанного учебного курса.

Группы обучающихся были поделены на две подгруппы: первая изучала третий блок дисциплины с внедрением «Формирование основ кибербезопасности у студентов СПО» и выполнением лабораторных работ с совместными дискуссиями, вторая – продолжила обучение по тем же темам, что и в курсе, но не выполняла лабораторные работы. Таким образом, в экспериментальную группу (ЭГ) вошли 49 студентов, в контрольную (КГ) – 32.

Целью проведения опытно-экспериментальной работы стало изучение уровня готовности студентов к будущему противодействию киберугрозам в будущей профессиональной деятельности. Л.С. Моцарь понятие готовность студента к профессиональной деятельности рассматривает «как результат накопления качественных личностных изменений и обретения профессиональной компетентности субъектом будущей профессиональной деятельности» [64, с.111].

В работе Т.А. Лавиной и Л.А. Ильиной уточняется, что «готовность к осуществлению профессиональной деятельности стали оценивать, используя понятия «компетенция» и «компетентность», а их формирование посредством знаний, умений, навыков, свойств личности и т.д.» [49, с.114]. Подробный анализ подходов к трактовке понятия «готовность к профессиональной деятельности» представлен в диссертации М.В. Храмовой, где автор приходит

к выводу, что «все исследователи рассматривают готовность как необходимую предпосылку успешной деятельности специалиста, которая 131 предполагает наличие профессионально значимых качеств и свойств личности» [109, с.47-48].

Мы рассматриваем готовность студентов к будущей профессиональной деятельности как комплекс, включающий мотивационный, когнитивный, деятельностный, эмоционально-оценочный компоненты.

Таким образом, уровни готовности (низкий, средний и высокий) характеризуются по выделенным компонентам (критериям): мотивационный (проявление интереса к учебно-познавательной и профессиональной деятельности и осознание значимости изучения курсов), когнитивный (уровень теоретической подготовки), деятельностный (способность к решению задач информационной безопасности в условиях существования угроз), эмоциональнооценочный (сформированность профессиональной и личностной компетентности) [2, с.95].

Методики, по которым были проведены диагностические исследования, представлены в таблице 3.

Таблица 3 – Критерии и диагностический инструментарий уровня готовности студентов к будущей профессиональной деятельности.

Критерии	**Показатели**	**Методики диагностики**
Мотивационный	Осознание значимости изучения вендорского курса для повышения личностной конкурентоспособности студента	Экспресс-диагностика личностной конкурентоспособности (Фетискин Н.П.)
	Проявление интереса к профессиональной деятельности	Методика для диагностики учебной мотивации студентов (А.А.Реан и В.А.Якунин, модификация Н.Ц.Бадмаевой)
	Проявление интереса к учебно-познавательной деятельности	
Когнитивный	Уровень теоретической подготовки	Вводное тестирование Итоговое тестирование
Деятельностный	Способность к решению задач информационной безопасности в условиях существования угроз	Самооценка студентов профессиональных умений и навыков
Эмоционально-оценочный	Представление о процессе обучения	Профессиональный личностный опросник (Филиппова К.А.)
	Видение перспектив профессионального и карьерного роста	
	Уверенность в себе и в своей будущей профессиональной эффективности	

Характеристики компонентов готовности студентов к будущей профессиональной деятельности на низком, среднем и высоком уровнях ее сформированности в таблице 4.

Таблица 4 – Характеристика компонентов готовности студентов к будущей профессиональной деятельности на низком, среднем и высоком уровнях ее сформированности

1	2	3	4
Показатель Сформированности	**Уровни выраженности**		
	Низкий	**Средний**	**Высокий**
Мотивационный компонент			
Осознание значимости изучения курса для повышения личностной конкурентоспособности студента	Незначительный интерес к изучению вендорских курсов, не развита личностная конкурентоспособность	Фрагментарный интерес к изучению курсов, частично развита личностная конкурентоспособность	Устойчивый интерес к изучению курсов, развита личностная конкурентоспособности
Проявление интереса к профессиональной деятельности	Слабо выраженная профессиональная мотивация	Ситуативная профессиональная и мотивация	Ярко выраженная профессиональная и мотивация
Проявление интереса к учебнопознавательной деятельности	Слабо выраженная учебнопознавательная мотивация	Ситуативная учебнопознавательная мотивация	Ярко выраженная учебнопознавательная мотивация

Таблица 3. Продолжение

1	2	3	4
Показатель Сформированности	**Уровни выраженности**		
	Низкий	**Средний**	**Высокий**
Когнитивный компонент			
Уровень теоретической подготовки	Фрагментарные знания принципов обеспечения защиты информации, источников угроз, современных методов и сред	Достаточный объем знаний о принципах обеспечения защиты информации, источников угроз, современных методов и средств защиты от угроз	Систематизированные , глубокие и полные знания принципов обеспечения защиты информации, источников угроз, современных методов и средств защиты от угроз
Деятельностный компонент			
Способность к решению задач информационной безопасности в условиях существования угроз	Фрагментарные умения и навыки применения современных подходов к технологиям и методам обеспечения информационной безопасности	Достаточный уровень сформированности навыков применения современных подходов к технологиям и методам обеспечения информационной безопасности	Высокий уровень сформированности навыков применения современных подходов к технологиям и методам обеспечения информационной безопасности
Эмоционально-оценочный компонент			
Представление о процессе обучения	Негативная направленность представлений о целях обучения в вузе, в целом недостаточная для наполнения ценностносмыслового содержания учебнопрофессиональной деятельности	Нейтральная направленность представления о целях обучения в вузе, в целом достаточная для наполнения ценностносмыслового содержания учебнопрофессиональной деятельности студента	Позитивная направленность представления о целях обучения в вузе, адекватная для наполнения ценностносмыслового содержания учебнопрофессиональной деятельности студента

Видение перспектив профессионального и карьерного роста	Смутное представление о перспективах и планах относительно личной профессиональной карьеры	Частичное видение перспектив и планов относительно личной профессиональной карьеры	Четкое видение перспектив и выраженная способность планировать личную профессиональную карьеру
Уверенность в себе и в своей будущей профессиональной эффективности	Профессиональное будущее представляется неопределенным, существует ее неоднозначность, даже в виде представления.	Представление о своей будущей профессиональной эффективности в целом оптимистичны, но имеются сомнения	Устойчивое оптимистическое представление о своей будущей профессиональной эффективности

Констатирующий этап опытно-экспериментальной работы.

На констатирующем этапе опытно-экспериментальной работы в каждом учебном году диагностировался исходный уровень готовности студентов к будущей профессиональной деятельности. Опишем полученные данные по использованным в ходе эксперимента методикам в ЭГ и КГ.

Перейдем к анализу исходного уровня развития мотивационного критерия.

Методика «Экспресс-диагностика личностной конкурентоспособности» (Н.П. Фетискин)[105, с. 272-273].

В рамках нашего исследования данный показатель рассматриваем в ключе осознания значимости изучения образовательной программы для повышения личностной конкурентоспособности студентов старших курсов, в том числе при будущем трудоустройстве.

Обучающимся предлагалось оценить степень проявления 11 психологических качеств по шкале от -3 до +3 (в левой части качество, которым свойственны баллы с отрицательным, а в правой – с положительным знаком). При обработке результатов выяснилось, что градация, предлагаемая в интерпретации, не совсем корректна. Поэтому нами была разработана собственная шкала, максимально приближенная к предлагаемой автором.

Данное исследование показало, что 21,9 % студентов КГ и 31,35 % студентов ЭГ имеют средний уровень личностной конкурентоспособности, незначительным уровнем обладают по 56,3 % в обеих группах. У 21,9 % студентов КГ и 12,5 % ЭГ – незначительное преобладание свойств, препятствующих проявлению личностной конкурентоспособности [2, с.95-96].

В рамках оценки готовности студентов к будущей профессиональной деятельности будем считать, что у студента не развита личностная конкурентоспособность и он проявляет незначительный интерес к изучению курса и в случае, если у него будут преобладать свойства, препятствующие проявлению личностной конкурентоспособности в любой степени; частично развита, если у испытуемого обнаружили незначительный уровень; и, что личностная конкурентоспособность развита, а студент проявляет устойчивый интерес к изучению курсов, в случае, если у студента обнаружили средний или высокий уровень личностной конкурентоспособности.

Соответственно, личностная конкурентоспособность развита у 21,9 % студентов КГ и 31,35 % студентов ЭГ. Продемонстрировали частично развитую конкурентоспособность 56,3 % студентов в КГ и ЭГ. Низкий уровень по данному показателю обнаружился у 21,9 % студентов КГ и 12,5 % ЭГ [2, с.95-96].

Проведенная диагностика показывает, что показатель – осознание значимости изучения курсов для повышения личностной конкурентоспособности студента – мотивационного критерия в КГ и ЭГ имеет средний уровень развития.

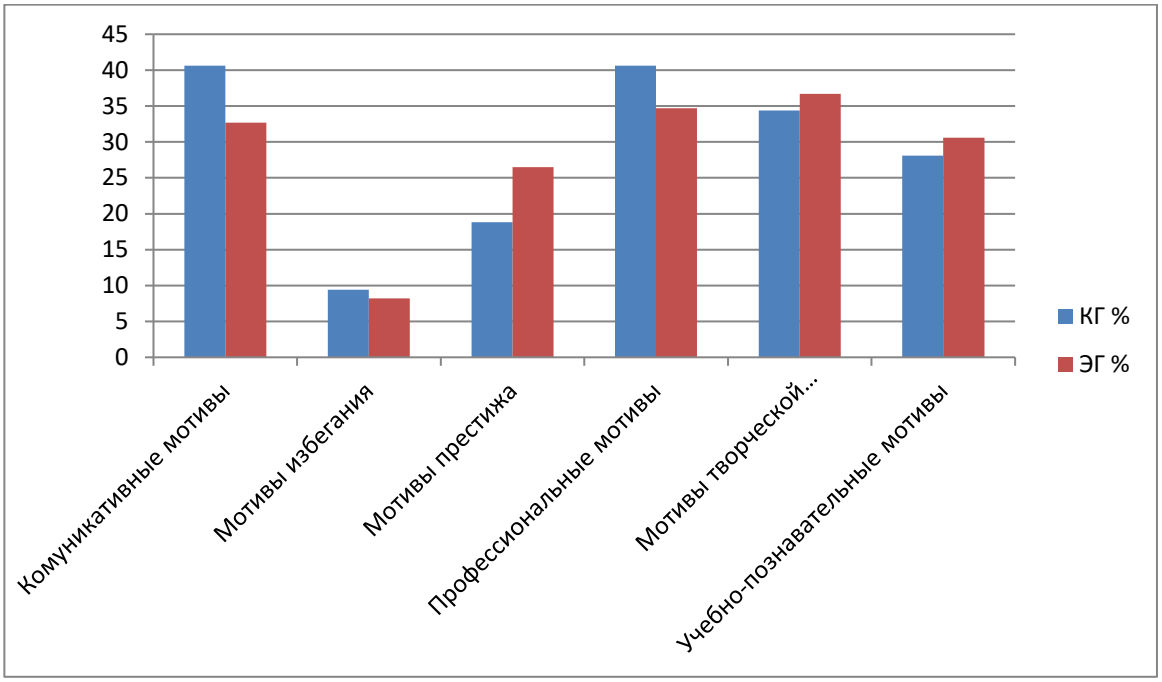
Методика для диагностики учебной мотивации студентов (А.А. Реан и В.А. Якунин, модификация Н.Ц. Бадмаевой) [20, с.151-154].

Студентам предлагалось оценить 34 мотива учебной деятельности по 5-балльной системе. Результат обрабатывался подсчетом среднего значения по каждой шкале опросника.

Целью проведения диагностики по данной методике в рамках нашего исследования является изучение уровня профессиональной и учебнопознавательной мотивации студентов [2, с.96]. Будем считать, что у обучающихся слабо выраженная профессиональная или учебно-познавательная мотивация (низкий уровень), если средний балл по соответствующем шкале будет менее 2,3333; ситуативная профессиональная или учебно-познавательная (средний уровень) мотивация средний балл в диапазоне от 2,3333 до 3,6666; ярко выраженная профессиональная или учебно-познавательная мотивация (высокий уровень) – более 3,66666.

На рисунке 1 представлено процентное соотношение по семи шкалам мотивов в КГ и ЭГ, в выборку вошли обучающиеся, у которых соответствующий мотив имеет средний балл выше 4,0.

Рисунок 1 - Распределение мотивов по шкалам в КГ и ЭГ на контатирующем этапе эксперемента, %



Определение уровня профессиональной мотивации показывает, что у 18,8 % КГ и 24,5 % ЭГ мотивация выражена слабо, ситуативная мотивация присуща 25,0 % КГ и 34,7 % ЭГ. Ярко выраженной профессиональной мотивацией обладают 56,2 % студентов КГ и 40,8 % ЭГ [2, с.96]. Таким образом, усредненное значение по группе данного показателя мотивационного критерия в ЭГ и КГ находится на среднем уровне.

Схожая ситуация складывается по итогам диагностики учебнопознавательных мотивов. Низкий уровень имеют 25 % студентов ЭГ и 21,9 % КГ, мотивация на среднем уровне – у 37,5 % ЭГ и 40,6 % КГ и на высоком – у 37,5 % в обеих группах [2, с.96]. Следовательно, показатель «проявление интереса к учебно-познавательной деятельности» мотивационного критерия в ЭГ и КГ, в целом по группам, до проведения изучения вендорского учебного курса имеет средний уровень.

Это может говорить о том, что студенты исходно, в целом, заинтересованы в выбранной специальности и считают изучаемые дисциплины значимыми для своей будущей профессиональной деятельности, однако около половины 40.6 9.4 18.8 40.6 34.4 28.1 21.9 32.7 8.2 26.5 34.7 36.7 30.6 28.6 0 5 10 15 20 25 30 35 40 45 Коммуникативные мотивы Мотивы избегания Мотивы престижа Профессиональные мотивы Мотивы творческой самореализации Учебно-познавательные мотивы Социальные мотивы КГ % ЭГ % 138 обучающихся, не имеющих выраженной учебно-познавательной и профессиональной мотивации, сомневаются, что получаемые знания

пригодятся в будущей профессии или вообще не уверены, что хотят стать специалистами по защите информации. С целью выявления исходного уровня когнитивного критерия студентам КГ и ЭГ предлагалось пройти вводное тестирование (приложение Р) для определения уровня теоретических знаний. Данные результатов тестирования показали, что знания принципов обеспечения защиты информации, источников угроз, современных методов и средств защиты от угроз информационной безопасности на низком уровне обнаружились у 18,8 % обучающихся КГ и 12,2 % ЭГ, средний уровень продемонстрировали значительная часть студентов КГ и КГ – 68,8 % и 75,5 % соответственно. Высоким уровнем знаний основ информационной безопасности обладают чуть более 12 % студентов обеих групп [2, с.97]. Результаты проведенной диагностики уровня когнитивного критерия на констатирующем этапе показали, что и в КГ и в ЭГ данный показатель находится на среднем уровне. Для определения уровня развития показателя деятельностного критерия обучающимся была предложена анкета самооценки умений и навыков применения современных подходов к технологиям и методам обеспечения информационной безопасности (приложение С), среди которых: навыки использования многофакторной аутентификации для защиты личной учетной записи, навыки исключения несанкционированного доступа к личной учетной записи и проверки активности учетной записи, умение применять методы стеганографии, умение выяснить пароль пользовательских учетных записей с помощью специальных утилит, навык проверки электронного документа и цифровой подписи и других. Собственные умения и навыки обучающимся необходимо было оценить по 10-бальной шкале.

В таблице 5 представлен средний балл по каждому умению и навыку в КГ и ЭГ.

Таблица 5 – Результат самооценки студентов умений и навыков на констатирующем этапе эксперимента.

	Умения и навыки применения современных подходов к технологиям и методам обеспечения информационной безопасности	КГ	ЭГ
1	Навыки поискка вакансий в сфере информационной безопасности.	5,3	5,2
2	Умение оценить угрозы, исходящие от кибератак	5,9	5,9
3	Навыки использования многофакторной аутентификации для защиты личной учетной записи	7,0	6,8

4	Навыки исключения несанкционированного доступа к личной учетной записи и проверки активности учетной записи	7,3	7,3
5	Навыки применения мер обеспечения безопасности на хостовой машине методом создания и проверки групп, пользователей и паролей	7,0	6,2
6	Навыки применения мер обеспечения безопасности на хостовой машине методом создания и проверки групп, пользователей и паролей	5,7	5,6
7	Умение выявлять угрозы и уязвимости в системе с помощью средства для анализа топологии сетевой инфраструктуры (сканера портов	5,5	5,8
8	Умение применять методы стеганографии (сокрытия документа внутри графического файла)	5,1	5,1
9	Умение выяснить пароль пользовательских учетных записей с помощью специальных утилит	5,6	5,8
10	Навыки использования цифровых подписей для подписания юридического документа	5,9	5,8
11	Навыки проверки электронного документа и цифровой подписи	5,9	6,1
12	Умение создать собственную цифровую подпись	6,8	6,5
13	Умение использовать протокол SSH для удаленного подключения к хосту	5,9	5,6
14	Умение использовать протокол Telnet для удаленного подключения к хосту	6,2	5,6
15	Умение использовать инструменты повышения надежности операционной системы	7,1	7,1
16	Навыки анализа примененных инструментов повышения надежности операционной системы и интерпретации предупреждений и рекомендаций системы	6,3	6,8

Будем считать, что студент обладает фрагментарными умениями и навыками применения современных подходов к технологиям и методам обеспечения информационной безопасности (низкий уровень) в случае если средний балл его оценки собственных способностей был менее или равен 4,9, средний уровень сформированности умений и навыков – в диапазоне 5-7,4 баллов, а высокий уровень –7,5 баллов и более.

Исследование по данному показателю деятельностного критерия выявило, что в КГ 15,6 % обучающихся обладают фрагментарным уровнем сформированности умений и навыков, 75 % – средним и 9,4 % студентов имеют высокий уровень сформированности соответствующих умений и навыков. В ЭГ показатель низкого уровня – у 20,4 %, среднего – у 73,5 %, высокого – у 6,1 % студентов [2, с.97].

Результаты анкетирования показали, что уровень показателя деятельностного критерия в КГ и ЭГ примерно одинаковый и находится на среднем уровне.

С целью выявления уровня показателя эмоционально-оценочного критерия была использована методика, разработанная К.А. Филипповой [106, с. 172-179]. В соответствии с авторской методикой профессиональная и личностная компетентность исследуется с помощью профессионального личностного опросника.

Анкета представлена 50 вопросами, сгруппированными в 5 групп по 10 вопросов. В рамках нашего исследования уровня сформированности профессиональной и личностной компетентности обучающихся были отобраны три наиболее подходящие группы: «Представление о процессе обучения», «Профессиональная карьера» и «Я-реальное в будущем», соответствующие выделенными нами трем показателям эмоционально-оценочного критерия: представление о процессе обучения, видение перспектив профессионального и карьерного роста, уверенность в себе и в своей будущей профессиональной эффективности [2, с.98].

Результаты тестирования по каждой из трех групп обрабатывались отдельно и интерпретировались в соответствии с рекомендацией автора методики: – суммарный балл более 70% характеризуется автором как сформированность учебно-профессиональной деятельности (высокий уровень);

– суммарный балл в диапазоне 50-70% – характеризуется как 141 оптимальный показатель (средний уровень);

– суммарный балл 49% и менее будет соответствовать низкому уровню по соответствующим показателям.

По первому показателю критерия «представление о процессе обучения» были получены следующие результаты.

Негативная направленность представлений о целях обучения в вузе, в целом недостаточная для наполнения ценностно-смыслового содержания учебно-профессиональной деятельности студента (низкий уровень) обнаружилась у 28,1 % студентов КГ и 16,3 % ЭГ. Нейтральная направленность (средний уровень) у 50,0 % КГ и 42,9 % ЭГ. Позитивная направленность представления о целях обучения в вузе, адекватная для наполнения ценностно-смыслового содержания учебно-профессиональной деятельности студента (высокий уровень) по результатам тестирования соответствует 21,9 % КГ и 40,8 % обучающимся ЭГ [2, с.98].

Таким образом, обе группы по первому показателю эмоциональнооценочного критерия имеют средний уровень сформированности.

По второму исследуемому показателю «видение перспектив профессионального и карьерного роста» эмоционально-оценочного критерия были получены следующие результаты.

21,9% обучающихся КГ и 14,3% ЭГ имеют смутное представление о перспективах и планах относительно личной профессиональной карьеры, то есть в данном случае будем говорить о низком уровне сформированности показателя. Средний уровень (частичное видение перспектив и планов относительно личной профессиональной карьеры) демонстрируют 56,3% студентов КГ и 49,0% ЭГ. Высокий уровень, соответствующий четкому видение перспектив и выраженной способности планировать личную профессиональную карьеру, у 21,9% КГ и 36,7% ЭГ [2, с.98].

ЭГ и КГ по второму показателю эмоционально-оценочного критерия исходно имеют средний уровень сформированности.

Третий показатель эмоционально-оценочного критерия «уверенность в себе и в своей будущей профессиональной эффективности» диагностировался группой вопросов профессионального личностного опросника «Я-реальное в будущем» [2, с.98].

Профессиональное будущее представляют неопределенным и имеют низкий уровень сформированности показателя у 25,0 % КГ и 18,4 % ЭГ. Представление о своей будущей профессиональной эффективности в целом оптимистичны, но имеются сомнения (средний уровень) у 40,6% в КГ и 40,8% в ЭГ. Устойчивое оптимистическое представление о своей будущей профессиональной эффективности (высокий уровень) демонстрируют 34,4% в КГ и 40,8% в ЭГ [2, с.98]. Таким образом, обе группы по третьему показателю эмоциональнооценочного критерия исходно имеют средний уровень сформированности.

Обобщая результаты исследования на констатирующем этапе мотивационного, когнитивного, деятельностного и эмоционально-оценочного критериев, мы обнаружили следующие показатели уровня готовности студентов старших курсов к будущей профессиональной деятельности: низкий у 15,6% студентов КГ и 18,4% ЭГ; средний – у 68,8% КГ и 63,3% ЭГ; высокий – 15,6% КГ и 18,4% ЭГ (таблица 4).

Таблица 4 - Результаты оценки уровней готовности студентов к будущей профессиональной деятельности по критериям на констатирующем этапе

Критерии	Уровни	Результаты			
		КГ		ЭГ	
		Кол-во обучающихся	%	Кол-во обучающихся	%
Мотивационный	Низкий	7	21,9	6	12,2
	Средний	13	40,6	28	59,2
	Высокий	12	37,5	14	28,6
Когнитивный	Низкий	6	18,8	6	12,2
	Средний	22	68,8	36	75,5
	Высокий	4	12,5	6	12,2
Деятельностный	Низкий	5	15,6	10	20,4
	Средний	24	75,0	35	73,5
	Высокий	3	9,4	3	6,1
Эмоционально-оценочный	Низкий	8	25,0	11	22,4
	Средний	17	53,1	20	42,9
	Высокий	7	21,9	17	34,7
Уровни готовности студентов к будущей профессиональной деятельности					
	Низкий	5	15,6	9	18,4
	Средний	21	68,8	31	63,3
	Высокий	5	15,6	9	18,4

Таким образом, на констатирующем этапе распределение студентов по уровням готовности к будущей профессиональной деятельности примерно одинаковое в КГ и ЭГ с выраженным преобладанием среднего уровня.

Контрольный этап опытно-экспериментальной работы:

Оценка достигнутого уровня готовности студентов к будущей профессиональной деятельности также осуществлялась с использованием показателей мотивационного, когнитивного, деятельностного и эмоциональнооценочного критериев.

Применение методики экспресс-диагностики личностной конкурентоспособности (Н.П. Фетискин) по окончании эксперимента показало, что в ЭГ существенно сократилось количество студентов с преобладанием свойств, препятствующих проявлению личностной конкурентоспособности – 4,1 % (на констатирующем этапе – 12,5 %). Незначительный уровень личностной конкурентоспособности продемонстрировали 51 % студентов. Средний уровень обнаружился у 42,9 % (на 12 % больше начального уровня). У одного студента был диагностирован высокий уровень личностной конкурентоспособности.

В КГ экспресс-диагностика выявила следующие показатели: 12,5 % – преобладание свойств, препятствующих проявлению личностной

конкурентоспособности, 59,4 % обучающихся – незначительный, 28,1 % – средний уровень личностной конкурентоспособности.

Результаты исследования показывают, что, в целом, личностная конкурентоспособность в ЭГ повысилась.

С помощью методики для диагностики учебной мотивации студентов (А.А. Реан и В.А. Якунин, модификация Н.Ц. Бадмаевой) снова были исследованы два показателя мотивационного критерия: проявление интереса к профессиональной деятельности и проявление интереса к учебно-познавательной деятельности.

Напомним, что при первичном анализе результатов по данной методике, мы просчитывали, какое количество обучающихся высоко оценили данные мотивы по значимости, то есть средний балл по шкале был от 4,0 до 5,0 баллов.

Таблица 5 - Распределение мотивов по шкалам КГ и ЭГ до и после проведения опытно-экспериментальной работы

Шкала мотивов	КГ		ЭГ	
	До %	После %	До %	После %
Коммуникативные	40,6	43,8	32,7	38,8
Избегания	9,4	12,5	8,2	10,2
Престижа	18,8	18,8	26,5	30,6
Профессиональные	40,6	56,3	34,7	55,1
Творческой самореализации	34,4	40,6	36,7	51,0
Учебно-познавательные	28,1	28,1	30,6	49,0
Социальной	21,9	21,9	28,6	21,9

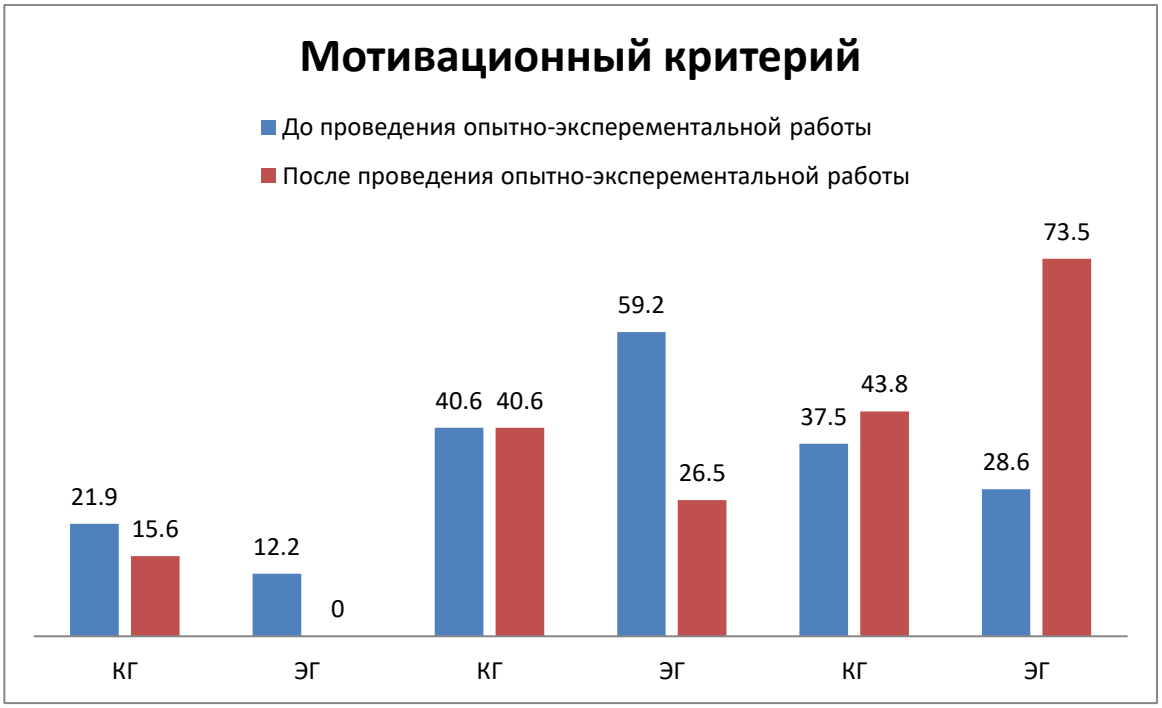
Однако подобный анализ не дает нам полное представление об изменениях по профессиональным и учебно-познавательным мотивам, потому отдельно проанализируем уровень сформированности по второму и третьему показателю. Оказалось, что в ЭГ больше не осталось студентов со слабо выраженной профессиональной мотивацией (на констатирующем этапе данный уровень обнаруживался у 24,5 %), ситуативную профессиональную мотивацию демонстрируют 22,4 %, а ярко выраженной мотивацией в профессиональной сфере обладают 77,6 % студентов ЭГ (ранее – 40,8 %) [2, с.96].

В КГ значимо данный показатель не изменился. Низкий уровень – у 12,5 % студентов (ранее 18,8 %), средний – 28,1 % (ранее 25,0 %) и высокий уровень – 59,4 % студентов (ранее 56,3 %).

Распределение по уровням третьего показателя (проявление интереса к учебно-познавательной деятельности) следующее: аналогично предыдущему показателю в ЭГ не осталось студентов с низкой мотивацией (до изучения курса низкий уровень был у 26,5 % студентов). Средний уровень сформированности по данному показателю имеют 26,5 % студентов, а высокий

уровень увеличился в 2 раза – 73,5 % [2, с.96]. Уровень сформированности мотивационного критерия заметно повысился в ЭГ: высокий уровень после опытно-экспериментальной работы наблюдается у 73,5 % студентов (ранее – 28,6 %), а низкий уровень не обнаружился ни у одного студента ЭГ. В КГ значимых различий не наблюдается. На рисунке 2 показан уровень мотивационного критерия до и после опытно-экспериментальной работы в КГ и ЭГ [2, с.96].

Рисунок 2 - Уровень развития мотивационного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %

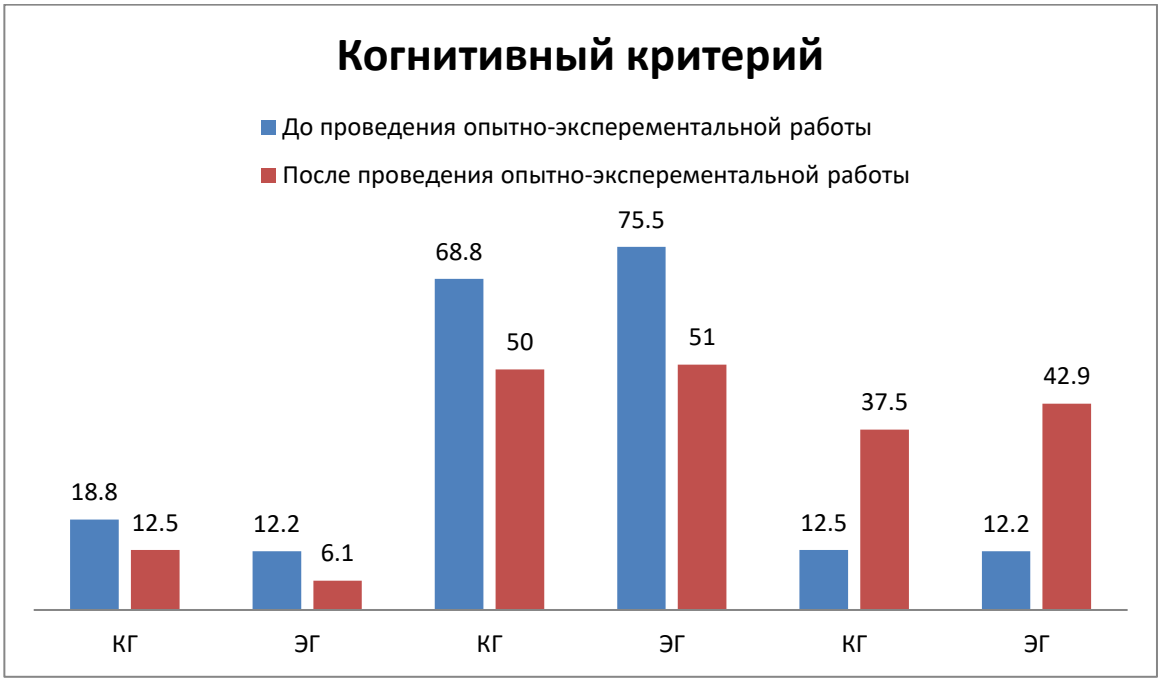


Исследование динамики уровня развития мотивационного критерия обнаружило, что в КГ остался на прежнем среднем уровне, в ЭГ – поднялся до высокого уровня.

Уровень сформированности когнитивного критерия был проанализирован с помощью итогового тестирования вендорского курса Сетевой академии Cisco «Основы кибербезопасности», состоящего из 50 вопросов. Так как студенты КГ изучали аналогичные темы, что и студенты ЭГ мы сочли возможным провести одинаковую диагностику по данному критерию в обеих группах.

Результаты тестирования показали, что уровень развития когнитивного критерия после опытно-экспериментальной работы повысился в КГ и ЭГ [2, с.97] .

Рисунок 3 - Уровень развития когнитивного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %



Аналогичную картину можем наблюдать и по результатам самооценки студентов своих знаний и умений, характеризующим уровень развития деятельностного критерия. Результаты самооценки студентов умений и навыков в КГ и ЭГ до и после опытно-экспериментальной работы проиллюстрированы в таблице 8: средний балл самооценки по навыкам и умениям несколько повысился, причем повышение произошло равномерно и в КГ и в ЭГ [2, с.97].

Таблица 6 - Результат самооценки студентов умений и навыков в КГ и ЭГ до и после опытно- экспериментальной работы.

	Умения и навыки применения современных подходов к технологиям и методам обеспечения информационной безопасности	**КГ**	**ЭГ**		
		До	После	До	После
1	Навыки поискка вакансий в сфере информационной безопасности.	5,3	6,4	5,2	5,9
2	Умение оценить угрозы, исходящие от кибератак	5,9	6,4	5,9	6,4
3	Навыки использования многофакторной аутентификации для защиты личной учетной записи	7,0	7,1	6,8	7,2

4	Навыки исключения несанкционированного доступа к личной учетной записи и проверки активности учетной записи	7,3	7,3	7,3	7,6
5	Навыки применения мер обеспечения безопасности на хостовой машине методом создания и проверки групп, пользователей и паролей	7,0	7,0	6,2	7,1
6	Навыки применения мер обеспечения безопасности на хостовой машине методом создания и проверки групп, пользователей и паролей	5,7	6,4	5,6	6,6
7	Умение выявлять угрозы и уязвимости в системе с помощью средства для анализа топологии сетевой инфраструктуры (сканера портов	5,5	6,4	5,8	6,3
8	Умение применять методы стеганографии (сокрытия документа внутри графического файла)	5,1	6,2	5,1	5,9
9	Умение выяснить пароль пользовательских учетных записей с помощью специальных утилит	5,6	6,6	5,8	6,5
10	Навыки использования цифровых подписей для подписания юридического документа	5,9	6,4	5,8	6,6
11	Навыки проверки электронного документа и цифровой подписи	5,9	6,3	6,1	6,9
12	Умение создать собственную цифровую подпись	6,8	6,8	6,5	7,0
13	Умение использовать протокол SSH для удаленного подключения к хосту	5,9	6,6	5,6	6,4
14	Умение использовать протокол Telnet для удаленного подключения к хосту	6,2	6,6	5,6	6,6
15	Умение использовать инструменты повышения надежности операционной системы	7,1	7,2	7,1	7,6
16	Навыки анализа примененных инструментов повышения надежности операционной системы и интерпретации предупреждений и рекомендаций системы	6,3	6,6	6,8	7,2

Полученный результат по когнитивному и деятельностному критерию может объясняться тем, что студенты обеих групп изучали схожий теоретический материал и выполняли аналогичные практические и лабораторные работы, соответственно уровень теоретических знаний, а также умений и навыков повысился примерно одинаково и у студентов, изучающих вендорский курс, и у студентов, занимающихся с преподавателем традиционными методами [2, с.97].

Последняя методика диагностики – профессиональный личностный опросник – была применена с целью определения уровня сформированности трех показателей эмоционально-оценочного критерия.

Таким образом, уровень сформированности по первому показателю эмоционально-оценочного критерия в ЭГ стал высоким, а уровень в КГ остался на прежнем среднем уровне. Определение представления у студентов перспектив их профессионального и карьерного роста в ЭГ показало, что 69,4 % обучающихся ЭГ стали четко видеть перспективу и имеют выраженную способность планировать личную профессиональную карьеру. При этом один студент, по-прежнему, имеет смутное представление о перспективах и планах относительно своей карьеры.

Мы видим причину подобных позитивных изменений в том, что студент, изучая курс популярной и авторитетной отечественной или зарубежной ИТ компании, как бы выходит за рамки образовательной среды вуза и интегрируется в общемировое профессиональное сообщество. Это убеждает будущего специалиста в области информационной безопасности в актуальности и значимости своих сформированных способностей и дает ему возможность иметь оптимистическое представление о своей будущей профессиональной деятельности [2, с.100].

Обоснование полученных результатов методом математической статистики.

Проведем статистическую проверку полученных результатов полученных результатов после проведения опытно-экспериментальной работы. Все расчеты будем производить с использованием программы для статистической обработки данных IBM SPSS Statistics.

С помощью непараметрического U-критерия Манна-Уитни для независимых выборок проверялась статистическая гипотеза о равенстве средних значений в КГ и ЭГ до и после проведения опытно-экспериментальной работы. Проверка проводилась для каждого критерия (мотивационный, когнитивный, деятельностный и эмоционально-оценочный) и общего уровня готовности студентов к будущей профессиональной деятельности. Данные проверки гипотез представлены в сводной Таблице 7, где x1 и x2 – среднее

значение выборки КГ и ЭГ соответственно, U – U-критерий Манна-Уитни для независимых выборок, p – асимптотическая значимость (2-сторонний критерий) [2, с.99].

Таблица 7 - Результаты статистической обработки данных до и после проведения опыто-эксперементальной работы

Критерии	x1	x2	U	p	Вывод
До проведения опытно-эксперементальной работы					
Мотивационный	1,156	1,163	791,500	0,936	p>0,1, следовательно, статистически достоверные различия не обнаружены
Когнитивный	0,937	1,000	741,000	0,594	p>0,1, следовательно, статистически достоверные различия не обнаружены
Деятельностный	0,938	0,857	839,500	0,484	p>0,1, следовательно, статистически достоверные различия не обнаружены
Эмоциональнооценочный	0,969	1,122	693,000	0,343	p>0,1, следовательно, статистически достоверные различия не обнаружены
Уровень готовности студентов к будущей проф. деятельности	4,000	4,143	712,500	0,480	p>0,1, следовательно, статистически достоверные различия не обнаружены

После проведения опытно-эксперементальной работы					
Мотивационный	1,281	1,734	518,500	0,003	p≤0,01, следовательно, различия обнаружены на высоком уровне статистической значимости
Когнитивный	1,250	1,367	716,000	0,463	p>0,1, следовательно, статистически достоверные различия не обнаружены
Деятельностный	1,156	1,244	720,000	0,479	p>0,1, следовательно, статистически достоверные различия не обнаружены
Эмоциональнооценочный	1,031	1,796	321,000	0,000	p≤0,01, следовательно, различия обнаружены на высоком уровне статистической значимости
Уровень готовности студентов к будущей проф. деятельности	4,719	6,143	362,500	0,000	p≤0,01, следовательно, различия обнаружены на высоком уровне статистической значимости

Анализ данных таблицы 7 позволяет заключить:

– студенты ЭГ и КГ до проведения опытно-экспериментальной работы имели примерно одинаковый уровень готовности к будущей профессиональной деятельности (по данным выборкам статистически достоверные различия не обнаружены);

– повышение уровня развития по когнитивному и деятельностному критериям в ЭГ и КГ после проведения опытно-экспериментальной работы произошло примерно в равной степени (по данным выборкам статистически достоверные различия не обнаружены);

– имеются значимые различия по уровням развития мотивационного и эмоционально-оценочного критериев, а также по общему уровню готовности студентов к будущей профессиональной деятельности после проведения опытноэкспериментальной работы между КГ и ЭГ (различия обнаружены на высоком уровне статистической значимости) [2, с.99].

Таким образом, по окончании апробирования внедрения вендорского учебного курса уровень готовности студентов к будущей профессиональной деятельности в ЭГ вырос, что следует из результатов диагностики, полученных в начале и конце опытно-экспериментальной работы.

Выводы по главе II

В данной главе на основе анализа актуальных киберугроз и специфики поведения студенческой молодежи в цифровой среде были разработаны комплексные методические рекомендации для преподавателей.

Основные результаты этапа проектирования заключаются в следующем:

1. Определены ключевые блоки компетенций, на формирование которых направлено обучение: от базовой цифровой гигиены (управление паролями, двухфакторная аутентификация) до навыков распознавания социальной инженерии и защиты персональных данных.
2. Сформулированы педагогические принципы обучения, среди которых приоритетными являются практикоориентированность, использование интерактивных методов (кейсов, симуляций кибератак) и регулярность актуализации знаний в условиях быстро меняющегося ландшафта угроз.
3. Предложен комплекс оценочных средств (тесты, теоритические материалы, лабораторные работы), позволяющий преподавателям объективно измерять уровень сформированности навыков безопасного поведения студентов в сети.

Предложенные рекомендации представляют собой готовый инструментарий для преподавателей, позволяющий систематизировать процесс обучения информационной безопасности и минимизировать риски вовлечения

студентов в противоправную деятельность или их становления жертвами киберпреступлений.

Рекомендации адаптированы под разные профили подготовки. Актуальность подтверждена тем, что содержание соответствует вызовам 2026 года (защита данных в ИИ-сервисах, противодействие дипфейкам).

ЗАКЛЮЧЕНИЕ.

В заключение, проведенное исследование позволило углубить понимание основ кибербезопасности как значимого педагогического феномена в контексте профессионального образования. Выявлены ключевые личностные качества, необходимые студентам для успешной адаптации к цифровой среде и защиты от киберугроз. Анализ учебно-методической документации дисциплин профессионального цикла позволил определить потенциал для интеграции аспектов кибербезопасности в существующие образовательные программы. Исследование информационно-образовательной среды учебного заведения выявило возможности и ограничения для реализации разработанной методики. Результатом работы стала разработка методики формирования основ кибербезопасности у студентов профессиональных образовательных организаций. Данная методика, интегрирующая теоретические знания и практические навыки, направлена на формирование у студентов осознанного и ответственного подхода к вопросам кибербезопасности. Апробация разработанной методики позволит оценить ее эффективность и внести необходимые корректировки для дальнейшего совершенствования процесса обучения. Предлагаемая методика формирования основ кибербезопасности базируется на принципах систематичности, наглядности и практико-ориентированности. Она предусматривает использование интерактивных лекций, кейс задач, практических занятий и моделирования реальных ситуаций, связанных с киберугрозами. Особое внимание уделяется развитию критического мышления и способности к анализу информации, что позволяет студентам самостоятельно оценивать риски и принимать обоснованные решения в области кибербезопасности.

Для оценки эффективности разработанной методики планируется проведение серии педагогических экспериментов с участием студентов различных профессиональных направлений. В ходе экспериментов будут оцениваться уровень знаний и навыков студентов в области кибербезопасности, их способность выявлять и предотвращать киберугрозы, а также их мотивация

к дальнейшему изучению данной области. Результаты экспериментов будут тщательно проанализированы и использованы для внесения необходимых корректировок в методику.

Дальнейшие исследования будут направлены на разработку специализированных образовательных ресурсов и инструментов, поддерживающих процесс формирования основ кибербезопасности. Планируется создание интерактивных учебных пособий, мультимедийных презентаций и виртуальных лабораторий, позволяющих студентам в безопасной среде приобретать практические навыки работы с современными средствами защиты информации.

Внедрение разработанной методики в образовательный процесс будет способствовать повышению уровня кибербезопасности в профессиональных образовательных организациях и подготовке квалифицированных специалистов, способных эффективно защищать информацию в цифровой среде. Данный вклад является важным шагом на пути к созданию безопасного и устойчивого цифрового общества.

Список использованных источников.

1. Алексеев А. А. Основы кибербезопасности. – М.: Инфра-М, 2023. – 256 с.
2. Белов В. А. Кибербезопасность в образовании: проблемы и решения. – СПб.: Питер, 2022. – 320 с.
3. Волков С. П. Формирование цифровой грамотности и основ кибербезопасности у студентов. – М.: Юрайт, 2023. – 288 с.
4. Григорьев И. Н. Кибербезопасность: учебное пособие. – М.: Форум, 2022. – 352 с.
5. Иванов Д. С. Современные угрозы кибербезопасности и методы защиты. – М.: Академия, 2023. – 272 с.
6. Козлов П. М. Основы информационной безопасности и киберзащиты. – М.: Проспект, 2022. – 304 с.
7. Лебедев О. В. Кибербезопасность: теория и практика. – М.: КноРус, 2023. – 240 с.
8. Петров А. И. Методические подходы к обучению кибербезопасности студентов. – М.: Лань, 2022. – 208 с.
9. Сидоров Е. Г. Кибербезопасность: актуальные вопросы и перспективы. – М.: Альфа-Пресс, 2023. – 288 с.
10. Смирнов В. Н. Основы кибербезопасности для студентов высших учебных заведений. – М.: Риор, 2022. – 224 с.
11. Тихонов А. А. Кибербезопасность: учебник. – М.: Дашков и К°, 2023. – 336 с.
12. Ушаков И. В. Цифровая безопасность и защита информации. – СПб.: Нева, 2022. – 280 с.
13. Федоров М. А. Основы защиты информации в компьютерных сетях. – М.: БИНОМ. Лаборатория знаний, 2023. – 256 с.
14. Хуснутдинов Р. Р. Кибербезопасность: практическое руководство. – М.: Эксмо, 2022. – 312 с.
15. Чернов А. А. Угрозы и защита в цифровом мире. – М.: АСТ, 2023. – 272 с.

16. Шевченко В. А. Информационная безопасность и киберугрозы. – СПб.: Питер, 2022. – 304 с.

17. Щербаков И. А. Основы кибербезопасности для начинающих. – М.: Инфра-М, 2023. – 240 с.

18. Юдин А. А. Кибербезопасность: современные вызовы и решения. – М.: Юрайт, 2022. – 288 с.

19. Яковлев П. А. Цифровая грамотность и кибербезопасность в современном обществе. – М.: Форум, 2023. – 256 с.

20. Ярцев В. А. Кибербезопасность: учебное пособие. – М.: Академия, 2022. – 320 с.

21. Зайцев О. В. Информационная безопасность и защита данных. – М.: Проспект, 2023. – 296 с.

22. Ковалев С. Д. Кибербезопасность: основы и принципы. – М.: КноРус, 2022. – 264 с.

23. Михайлов Г. В. Практическая кибербезопасность. – М.: Лань, 2023. – 312 с.

24. Новиков Д. А. Кибербезопасность в условиях цифровой трансформации. – М.: Юрайт, 2022. – 272 с.

25. Орлов Е. П. Защита информации в информационных системах. – М.: Инфра-М, 2023. – 280 с.

26. Павлов В. С. Основы кибергигиены. – М.: Питер, 2022. – 200 с.

27. Романов А. Б. Кибербезопасность: от теории к практике. – М.: Форум, 2023. – 304 с.

28. Соколов И. Н. Информационная безопасность: учебник. – М.: Дашков и К°, 2022. – 368 с.

29. Трофимов К. В. Кибербезопасность: вызовы и решения. – М.: Академия, 2023. – 296 с.

30. Филиппов Л. М. Основы кибербезопасности для пользователей. – М.: Эксмо, 2022. – 240 с.

ПРИЛОЖЕНИЯ А

Оглавление

Предисловие.

Учебное пособие «Формирование основ кибербезопасности у студентов спо» разработано для студентов направлений подготовки и специальностей «Информационная безопасность». Пособие может также использоваться студентами других направлений и специальностей при изучении вопросов, связанных с защитой информации.

В пособии рассмотрена терминология кибербезопасности, основные виды угроз, способы защиты информации, личная информация и приватность, кибербулинг и этика общения, контент и информация, техническая безопасность, разграниченный доступ как способ защиты информации.

Знание основ теории информационной безопасности будет способствовать умелым действиям в решении практических вопросов защиты информации в профессиональной деятельности.

Используйте современные образовательные ресурсы, такие как видеоролики, онлайн-игры и интерактивные платформы, для повышения осведомленности о кибербуллинге. Организуйте встречи с психологами, юристами и другими специалистами, которые могут рассказать о различных аспектах этой проблемы и предложить практические советы.

Обучайте студентов медиаграмотности, чтобы они могли критически оценивать информацию, поступающую из интернета, и распознавать манипуляции и фейки. Научите их проверять источники информации и не распространять неподтвержденные сведения, которые могут причинить вред другим людям.

Подчеркивайте, что цифровая репутация играет важную роль в жизни человека. Объясните, что все, что публикуется в интернете, может остаться там навсегда и повлиять на будущую карьеру, отношения и личную жизнь. Поощряйте студентов к осознанному и ответственному использованию социальных сетей и других онлайн-платформ.

Создавайте возможности для открытого и доверительного общения. Поддерживайте в классе атмосферу, где студенты не боятся говорить о своих

проблемах и обращаться за помощью, если они стали жертвами или свидетелями кибербуллинга. Разработайте четкий и понятный механизм сообщения о случаях кибербуллинга, который гарантирует конфиденциальность и защиту потерпевших. Важно, чтобы студенты знали, что они не одиноки и что им окажут необходимую поддержку.

Активно вовлекайте родителей в процесс профилактики кибербуллинга. Организуйте родительские собрания и семинары, на которых можно обсудить риски, связанные с использованием интернета, и предложить стратегии защиты детей от онлайн-агрессии. Предоставьте родителям информацию о полезных ресурсах и инструментах, которые помогут им контролировать онлайн-активность детей и вовремя реагировать на возникающие проблемы.

Помните, что профилактика кибербуллинга – это непрерывный процесс, требующий постоянных усилий и внимания со стороны всех участников образовательного процесса. Важно не только реагировать на уже произошедшие случаи, но и активно работать на опережение, создавая в классе культуру уважения, эмпатии и ответственности. Только совместными усилиями мы сможем сделать интернет безопасным и полезным пространством для наших детей.

Внедрение позитивных онлайн-практик также играет ключевую роль. Поощряйте студентов к использованию интернета для обучения, творчества и общения с друзьями и семьей. Подчеркивайте важность создания позитивного контента и поддержки других пользователей в сети. Развивайте в студентах навыки конструктивного общения и разрешения конфликтов онлайн, чтобы они могли эффективно справляться с негативными ситуациями и предотвращать кибербуллинг.

Для эффективной защиты студентов СПО от опасного контента в сети интернет необходимо комплексный подход, включающий в себя образовательные программы, направленные на развитие критического мышления и медиаграмотности, а также создание поддерживающей и

безопасной онлайн-среды, где студенты могут обращаться за помощью и поддержкой в случае столкновения с деструктивным контентом.

Важную роль в профилактике распространения опасного контента играет взаимодействие образовательных учреждений с родителями и законными представителями студентов. Регулярные информационные кампании, посвященные вопросам интернет-безопасности, могут помочь повысить осведомленность о существующих рисках и способах их предотвращения. Кроме того, необходимо развивать культуру ответственного использования интернета, подчеркивая важность уважительного отношения к другим пользователям и соблюдения этических норм поведения в онлайн-пространстве.

Внедрение эффективных механизмов мониторинга и фильтрации контента в образовательных учреждениях также является важным шагом в защите студентов от опасного контента. Однако важно помнить, что технологические решения не являются панацеей, и необходимо сочетать их с образовательными и воспитательными мерами. Кроме того, важно обеспечить конфиденциальность и защиту персональных данных студентов, чтобы предотвратить их использование в злонамеренных целях.

Психологическая поддержка студентов, столкнувшихся с опасным контентом, является неотъемлемой частью комплексного подхода к обеспечению их безопасности в сети. Квалифицированные психологи и педагоги должны быть готовы оказать помощь и поддержку студентам, пережившим кибербуллинг, онлайн-харассмент или другие формы деструктивного воздействия. Важно создать атмосферу доверия и открытости, в которой студенты будут чувствовать себя комфортно, обращаясь за помощью в случае необходимости.

Защита студентов СПО от опасного контента в сети интернет требует совместных усилий образовательных учреждений, родителей, студентов и других заинтересованных сторон. Только комплексный и осознанный подход

позволит создать безопасную и благоприятную онлайн-среду, способствующую гармоничному развитию и социализации молодых людей.

❶Основные понятия теории информационной безопасности

Теория информационной безопасности — это область знаний, изучающая концепции, принципы, методы и средства защиты информации от несанкционированного доступа, искажения, уничтожения и утечки, с ключевыми целями обеспечения конфиденциальности, целостности и доступности данных, а также устойчивости самих информационных систем к угрозам. Она включает как технические, так и организационные меры, охватывает вопросы психологии, права и управления рисками, формируя комплексную систему защиты информации.

Задачи рассматриваемые в теории информационной безопасности: анализ угроз и уязвимостей, идентификация потенциальных рисков. разработка моделей и политик безопасности, методология защиты, обеспечение непрерывности бизнеса.

Теория информационной безопасности постоянно развивается, адаптируясь к новым технологиям и типам киберугроз, и лежит в основе создания безопасных информационных систем для государств, предприятий и частных лиц.

Активная атака – это атака приводящая к изменению функций и параметров системы или изменению данных, к нарушению интерактивных операций и взаимодействий в сети.

Аутентификация – это проверка подлинности субъекта или объекта доступа, а также проверка того, что именно ему принадлежит предъявленный идентификатор доступа и аутентификационная информация.

Антивирус – специальное программное обеспечение для обнаружения вредоносных программ и восстановления поврежденных ими файлов.

База данных – то набор упорядоченной информации, хранящийся в электронном виде.

Вирус – это вредоносная программа или код.

Вишинг или телефонное мошенничество – это один из видов фишинга. Злоумышленники звонят потенциальной жертве и с помощью методов социальной инженерии пытаются выведать личные данные либо заставляют сделать перевод.

Генератор случайных паролей — это программа, которая создает случайные пароли на основе выбранных правил (длина пароля, наличие специальных символов и так далее).

Доступность – это возможность своевременного и надежного использования информации или сервисов.

Двухфакторная аутентификация – метод аутентификации пользователя в онлайн сервисе (например, СберБанк Онлайн) при помощи запроса данных двух разных типов.

ЕСИА – федеральная государственная система, котороя в предусмотренных законодательством случаях обеспечивает санкционированный доступ к информации, содержащейся в информационных системах. Порядок использования ЕСИА устанавливается Правительством РФ.

Идентификация – это проверка схожести объектов по определенным признакам. Этим признаками – идентификаторами – могут быть имя, номер телефона, логин и так далеее.

Информационная безопасность – это состояние информации, при котором обеспечены её конфиденциальность, доступность и целостность.

Информация ограниченного доступа – это сведения,доступ к которым ограничен по требованием закона или согласно внутренним правилам организации.

Искусственный интеллект – это компьютерная технология, которая с помощью алгоритмов, математических моделей и наборов данных учит программы и системы «думать» и «решать» как люди.

Теория информационной безопасности постоянно развивается это обусловлено постоянным развитием информационной среды, регулярно сталкиваемся с необходимостью решать новые задачи по обеспечению информационной безопасности.

Сложно поспорить с тем что на сегодняшний момент это одна из самых активно развивающихся наук. Регулярно появляются новые перспективные направления исследований, а уже существующие получают еще более детальную научную проработку.

Вопросы

1. Что обеспечивает конфиденциальность, доступность и целостность?
2. Что такое активная атака?
3. Для чего используется антивирус?
4. Что такое ЕСИА?
5. Сколько факторов требует двухфакторная аунтификация?
6. Как называется телефонный вид фишинга?
7. Что проверяет аунтификация?
8. Какая задача включает анализ угроз и уязвимостей?
9. Что создает генератор случайных паролей?
10. Назовите одно из трех ключевых свойств информационной безопасности.

❷Вредоносное программное обеспечению (вирусы, ransomware)

Вредоносные программы, враждебные, навязчивые и намеренно неприятные, стремятся вторгнуться в компьютеры, компьютерные системы, сети, планшеты и мобильные устройства, нанести им ущерб или вывести их из строя, зачастую частично контролируя работу устройства. Подобно человеческому гриппу, они мешают нормальному функционированию.

Мотивы, стоящие за вредоносным ПО, различны. Вредоносные программы могут быть направлены на то, чтобы заработать на вас деньги, нарушить вашу способность выполнять работу, сделать политическое заявление или просто похвастаться своими правами. Хотя вредоносные программы не могут повредить физическое оборудование системы или сетевое оборудование (за одним известным исключением - см. раздел о Google Android ниже), они могут красть, шифровать или удалять ваши данные, изменять или перехватывать основные функции компьютера, а также шпионить за вашей работой без вашего ведома или разрешения.

Вы знаете, что каждый год медицинское сообщество призывает всех сделать прививку от гриппа? Это потому, что у вспышек гриппа обычно есть сезон - время года, когда они начинают распространяться и заражать людей. В отличие от этого, для ПК, смартфонов, планшетов и корпоративных сетей не существует предсказуемых сезонных инфекций. Для них сезон гриппа наступает всегда. Но вместо озноба и ломоты в теле пользователи могут заболеть от разновидности машинной болезни - вредоносного ПО.

Вредоносное ПО может проявлять себя самыми разными способами. Вот несколько признаков того, что в вашей системе есть вредоносное ПО:

- Ваш компьютер замедляется. Одним из побочных эффектов вредоносного ПО является снижение скорости работы вашей операционной системы (ОС), независимо от того, работаете ли вы в Интернете или просто используете локальные приложения, использование ресурсов системы кажется ненормально высоким. Вы

даже можете заметить, что вентилятор вашего компьютера жужжит на полной скорости - верный признак того, что что-то отнимает системные ресурсы в фоновом режиме. Как правило, это происходит, когда ваш компьютер попал в ботнет, то есть сеть порабощенных компьютеров, используемых для DDoS-атак, рассылки спама или добычи криптовалюты.

- Ваш экран наводнен назойливой рекламой. Неожиданные всплывающие объявления - типичный признак заражения вредоносным ПО. Особенно часто они связаны с разновидностью вредоносного ПО, известной как рекламное. Более того, всплывающие окна обычно сопровождаются другими скрытыми вредоносными программами. Поэтому, если вы увидите во всплывающем окне что-то вроде "CONGRATULATIONS, You've won a free psychic reading!", не нажимайте на него. Какой бы бесплатный приз ни сулила реклама, он обойдется вам очень дорого.
- Ваша система дает сбой. Это может произойти в виде зависания или BSOD (Blue Screen of Death - синий экран смерти), последний возникает в системах Windows после фатальной ошибки.
- Вы заметили загадочную потерю дискового пространства. Это может быть связано с раздутым вредоносным ПО, скрывающимся на вашем жестком диске под названием bundleware.
- В вашей системе наблюдается странное увеличение активности в Интернете. Возьмем, к примеру, троянцев. Как только троянец попадает на целевой компьютер, он тут же связывается с командно-контрольным сервером злоумышленника (C&C), чтобы загрузить вторую инфекцию, часто вымогательскую. Этим можно объяснить всплеск активности в Интернете. То же самое относится к ботнетам, шпионским программам и любым другим угрозам, требующим обмена данными с серверами C&C.
- Меняются настройки браузера. Если вы заметили, что изменилась домашняя страница или установлены новые панели инструментов, расширения или плагины, то, возможно, вы заразились вредоносным ПО.

Причины могут быть разными, но обычно это означает, что вы нажали на всплывающее окно "Поздравляем", которое загрузило нежелательное программное обеспечение.

- Ваш антивирусный продукт перестает работать, и вы не можете включить его снова, оставаясь незащищенным от коварного вредоносного ПО, которое его отключило.
- Вы теряете доступ к своим файлам или всему компьютеру. Это симптом инфицирования программой-вымогателем. Злоумышленники уведомляют вас, оставив записку с требованием выкупа на рабочем столе или изменив обои рабочего стола на саму записку с требованием выкупа (см. GandCrab). В записке злоумышленники обычно сообщают, что ваши данные зашифрованы и требуют выкуп за их расшифровку.

Даже если кажется, что в вашей системе все работает нормально, не успокаивайтесь, потому что отсутствие новостей - это не обязательно хорошие новости. Мощные вредоносные программы могут прятаться глубоко в вашем компьютере, ускользая от обнаружения и занимаясь своими грязными делами, не вызывая никаких тревожных сигналов. Мы привели краткое руководство по обнаружению вредоносных программ, но на самом деле для обнаружения вредоносного ПО в вашей системе требуется неусыпный взор хорошей программы кибербезопасности (подробнее об этом позже).

Вопросы.

1. Как переводится термин malware?
2. Что означает аббревиатура C&C?
3. Как называется вредоносная программа, требующая выкупа?
4. Какая разновидность ПО вызывает назойливые всплывающие объявления?
5. Как называется сеть порабощенных компьютеров?
6. Что означает аббревиатура BSOD?

7. Как называется скрывающееся на диске ПО под названием bundleware?
8. Какой признак проявляется громкой работой вентилятора компьютера?
9. Перечислите признаки вредоносного ПО.

❸Программы-вымогатели

Программы-вымогатели – это разновидность вредоносных программ, используемых киберпреступниками. Если компьютер или сеть заражены программой-вымогателем, происходит блокировкадоступа к системе или шифрованиеданных. Киберпреступники требуют от своих жертв выкуп в обмен на предоставление доступа к данным. Чтобы защититься от заражения программами-вымогателями, рекомендуется сохранять бдительность и использовать программы безопасности. У жертв программ-вымогателей есть три варианта действий после заражения: можно заплатить выкуп, попытаться удалить вредоносную программу или перезагрузить устройство. Векторы атак, используемые троянами-вымогателями, включают, в основном, протокол удаленного рабочего стола, фишинговые сообщения электронной почты и уязвимости программного обеспечения. Таким образом, атака программ-вымогателей может быть нацелена как на частных лиц, так и на компании.

Наиболее популярны два типа программ-вымогателей:

- Программы-блокировщики с требованием выкупа. Этот тип вредоносных программ блокирует основные функции компьютера. Например, может быть ограничен доступ к рабочему столу, а мышь и клавиатура могут быть частично отключены, что позволяет взаимодействовать с окном, содержащим требование выкупа, и произвести платеж. Кроме того, может быть выведен из строя компьютер. Но есть и хорошие новости:

вредоносные программы-блокировщики обычно не нацелены на важные файлы; их цель – просто заблокировать ваше устройство. Поэтому полное уничтожение ваших данных маловероятно.

- Вредоносные программы-шифровальщики. Цель таких программ-вымогателей – зашифроватьважные данные, такие как документы, изображения и видео, но не вмешиваться в основную работу компьютера. Это часто вызывает панику, поскольку пользователи видят файлы, но не могут получить к ним доступ. Разработчики таких программ часто добавляют к требованию выкупа обратный отсчет: «Если вы не заплатите выкуп до установленного срока, все ваши файлы будут удалены». Учитывая количество пользователей, не знающих о необходимости создания резервных копий данных в облачных хранилищах или на внешних физических устройствах, атаки программ-шифровальщиков могут иметь крайне негативные последствия. Поэтому многие жертвы платят выкуп просто для того, чтобы вернуть свои файлы.

Теперь вы знаете, что такое программы-вымогатели, и каких основных двух типов они бывают. Далее приведены несколько примеров известных программ-вымогателей, показывающих, чем они опасны.

- *Locky*

Locky – это программа-вымогатель, атака с применением которой была впервые совершена группой организованных хакеров в 2016 году. С использованием Locky было зашифровано более 160 типов файлов. Программа распространялась с помощью писем, содержащих зараженные вложения. Пользователи попались на уловку с сообщениями электронной почты и установили программу-вымогатель на свои компьютеры. Этот метод распространения называется фишингом и представляет собой один из методов социальной инженерии. Программа-вымогатель Locky нацелена на типы файлов, часто используемые дизайнерами, разработчиками, инженерами и тестировщиками.

- *WannaCry*

WannaCry – это атака программы-вымогателя, в 2017 году имевшая место в более чем 150 странах. Она была разработана для использования уязвимости в системе безопасности Windows, созданной АНБ и ставшей известной в результате действий группы хакеров Shadow Brokers. Атаке WannaCry подверглись 230 000 компьютеров по всему миру, в том числе треть больниц Национальной службы здравоохранения Великобритании, что повлекло ущерб в 92 миллиона фунтов стерлингов. Пользователи были заблокированы, и у них требовали выкуп в биткойнах. Это атака вскрыла проблему устаревших систем: хакеры использовал уязвимость операционной системы, для которой на момент атаки уже в течение продолжительного времени существовал патч. Мировой финансовый ущерб, нанесенный WannaCry, составил около 4 миллиардов долларов США.

- *Bad Rabbit*

Bad Rabbit – это атака с использованием программ-вымогателей, которая распространялась с 2017 года посредством так называемой скрытой загрузки. Для выполнения таких атак используются незащищенные веб-сайты. При атаке с использованием скрытой загрузки пользователь посещает настоящий веб-сайт, не подозревая, что он был взломан. Для большинства атак с использованием скрытой загрузки от пользователя требуется только открыть взломанную страницу. В этом случае запуск установщика, содержащего скрытую вредоносную программу, ведет к заражению. Это называется распространением вредоносных программ. Bad Rabbit просит пользователей запустить поддельную установку Adobe Flash, тем самым заражая компьютер вредоносной программой.

- *Ryuk*

Ryuk – это троян-шифровальщик, распространившийся в августе 2018 года. Он отключаетфункцию восстановления операционных систем Windows, что делает невозможным восстановление зашифрованных данных без внешней резервной копии. Вирус Ryuk также шифрует сетевые жесткие диски. Атака

имела масштабные последствия; многие американские компании, подвергшиеся нападению, выплатили требуемые суммы выкупа. Общий ущерб оценивается более чем в 640 000 долларов.

- *Shade/Troldesh*

Атака программы-вымогателя Shade (также известной как Troldesh) произошла в 2015 году. Она распространялась через спам-сообщения, содержащие зараженные ссылки или вложенные файлы. Интересно, что исполнители атаки Troldesh общались непосредственно со своими жертвами по электронной почте. Жертвы, с которыми у них сложились «хорошие отношения», получали скидки. Однако такое поведение – скорее исключение, чем правило.

- *Jigsaw*

Атака программы-вымогателя Jigsaw началась в 2016 году. Она получила свое название из-за изображения известной куклы из франшизы фильма «Пила». С каждым часом, пока выкуп оставался невыплаченным, программа-вымогатель Jigsaw удаляла все больше файлов. Дополнительный стресс у пользователей вызвало использование изображения из фильма ужасов.

- CryptoLocker

CryptoLocker – это программа-вымогатель, впервые обнаруженная в 2007 году, распространяемая через зараженные вложения электронной почты. Она выполняла поиск важных данных на зараженных компьютерах и зашифровывала их. Пострадало около 500 000 компьютеров. Правоохранительным органам и компаниям по обеспечению безопасности в конечном итоге удалось получить контроль над сетью взломанных домашних компьютеров, используемых для распространения CryptoLocker по всему миру. Это позволило агентствам и компаниям перехватывать данные, передаваемые по сети, незаметно для злоумышленников. В конечном итоге это привело к созданию онлайн-портала, на котором жертвы могли получить ключ для

разблокировки своих данных. Это позволило им получить свои данные без необходимости платить преступникам выкуп.

- *Petya*

Petya (не путать с ExPetr) – это атака программы-вымогателя, впервые произошедшая в 2016 году, а затем повторившаяся как GoldenEye в 2017 году. Вместо шифрования отдельных файлов эта вредоносная программа-вымогатель шифровала целиком жесткие диски жертв. Это достигалось путем шифрования основной таблицы файлов (MFT), что сделало невозможным доступ к файлам на жестком диске. Программа-вымогатель Petya распространялась по корпоративным отделам кадров с посредством поддельного приложения, содержащего зараженную ссылку Dropbox.

Существует другой вариант вируса Petya – Petya 2.0, отличающийся некоторыми ключевыми особенностями. Однако с точки зрения осуществления атаки, оба вируса одинаково опасны для устройства.

- *GoldenEye*

Повторное появление вируса Petya под именем GoldenEye привело к мировому заражению программами-вымогателями в 2017 году. Вирус GoldenEye, также известный как "смертоносный брат" WannaCry, поразил более 2000 целей, в том числе несколько известных российских нефтяных компаний и банков. В результате атаки вируса GoldenEye на Чернобыльскую АЭС, сотрудники были вынуждены вручную проверять уровень радиации, поскольку их компьютеры с Windows были отключены от сети.

- *GandCrab*

GandCrab – это скандальная программа-вымогатель, угрожающаяраскрыть увлечения своих жертв порнографией. Злоумышленники утверждали, что взломали веб-камеру жертвы и требовали выкуп. В случае неуплаты выкупа они грозились опубликовать материалы, компрометирующие жертву. После первого упоминания в 2018 году,

появлялись различные версии программы-вымогателя GandCrab. В рамках проекта «No More Ransom» производители систем безопасности и органы полиции разработали инструмент для расшифровки данных, зашифрованных программами-вымогателями, чтобы помочь жертвам восстановить конфиденциальные данные из GandCrab.

- *B0r0nt0k*

B0r0nt0k – это использующая шифрование программа-вымогатель, предназначенная для серверов на базе Windows и Linux. Эта программа-вымогатель шифруетфайлы на серверах Linux и добавляет к ним расширение .rontok. Она представляет опасность не только для файлов, но также меняет параметры запуска программ, отключает функции и приложения и добавляет записи реестра, файлы и программы.

- *Dharma Brrr*

Brrr – новая программа-вымогатель от Dharma, устанавливается вручную хакерами, взломавшими подключенные к Интернету службы рабочего стола. Как только хакер активирует программу-вымогатель, начинается шифрование обнаруженных файлов. Зашифрованным файлам присваивается расширение .id-[id].[email].brrr.

- *FAIR RANSOMWARE*

FAIR RANSOMWARE – это программа-вымогатель, выполняющая шифрование данных. С помощью мощного алгоритма шифруются все личные документы и файлы жертвы. Файлы, зашифрованные с помощью этой вредоносной программы, имеют расширение .FAIR RANSOMWARE.

- *MADO*

Программа-вымогатель MADO – это еще один вид программы-шифровальщика. Данные, зашифрованные этой программой, имеют расширение mado и больше не открываются.

- *Атаки с использованием программ-вымогателей*

Как описано выше, программы-вымогатели используются в абсолютно разных сферах. Обычно требуемый размер выкупа составляет от 100 до 200 долларов. Однако в некоторых случаях злоумышленники требуют гораздо больший выкуп, особенно если понимают, что блокировка данных может повлечь значительные финансовые потери для атакуемой компании. Таким образом, это позволяет киберпреступникам зарабатывать существенные суммы денег. В двух приведенных ниже примерах обратите внимание на жертв кибератаки, а не на тип используемых программ-вымогателей.

- *WordPress*

Программа-вымогатель WordPress, как следует из названия, нацелена на файлы веб-сайтов WordPress. У жертв вымогают выкуп, что типично для программ-вымогателей. Чем более востребован сайт на платформе WordPress, тем выше вероятность его атаки с применением программ-вымогателей.

- *Дело компании Wolverine*

Компания Wolverine Solutions Group (предоставляющая медицинские услуги) стала жертвой атаки программ-вымогателей в сентябре 2018 года. Большое количество файлов компании было зашифровано вредоносной программой, в результате чего сотрудники не смогли их открыть. К счастью, эксперты-криминалисты смогли расшифровать и восстановить данные 3 октября. Однако в результате атаки были скомпрометированы данные многих пациентов. Имена, адреса, медицинские данные и другая личная информация могла попасть в руки киберпреступников.

Услуги по предоставлению программ-вымогателей позволяют киберпреступникам с низкими техническими возможностями осуществлять атаки с использованием этих программ. Вредоносные программы предоставляется покупателям, что снижает риск и повышает выгоду для разработчиков.

Атаки программ-вымогателей имеют различные проявления и масштабы. Вектор атаки – это важный фактор, зависящий от типа используемой

программы-вымогателя. Чтобы оценить серьезность и масштабы атаки, необходимо учитывать потенциальный ущерб, то есть какие данные могут быть удалены или опубликованы. Независимо от типа программы-вымогателя, предварительное резервное копирование данных и использование программ безопасности может значительно снизить последствия атаки.

Вопросы.

1. Почему жертвы программ-вымогателей обычно соглашаются на выплату выкупа?
2. Как атака Bad Rabbit использует скрытую загрузку для заражения устройств?
3. Для чего программа Ryuk отключает функцию восстановления операционных систем Windows?
4. Как обеспечивалась коммуникация между исполнителями атаки Troldesh и их жертвами?
5. Почему программа-вымогатель Jigsaw вызывает дополнительный стресс у пользователей?

❹Что такое «фишинг»

Фишинг (англ. phishing, от *fishing* — рыбная ловля, выуживание и *password* — пароль) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Причины могут называться различные. Это может быть утеря данных, поломка в системе и прочее.

Атаки фишеров становятся все более продуманными, применяются методы социальной инженерии. Но в любом случае клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении («если вы не сообщите ваши данные в течение недели, ваш счет будет заблокирован»). Забавно, но часто в качестве причины, по которой пользователь якобы должен выдать конфиденциальную информацию, фишеры называют необходимость улучшить антифишинговые системы («если хотите обезопасить себя от фишинга, пройдите по этой ссылке и введите свой логин и пароль»).

Фишинговые сайты, как правило, живут недолго (в среднем — 5 дней). Так как анти-фишинговые фильтры довольно быстро получают информацию о новых угрозах, фишерам приходится регистрировать все новые и новые сайты. Внешний же вид их остается неизменен — он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники.

Зайдя на поддельный сайт, пользователь вводит в соответствующие строки свой логин и пароль, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, в худшем — к электронному счету. Но не все фишеры сами обналичивают счета жертв. Дело в том, что обналичивание счетов сложно осуществить практически, к тому же человека, который занимается обналичиванием, легче засечь и привлечь мошенников к ответственности. Поэтому, добыв персональные данные, некоторые фишеры продают их другим мошенникам, у которых, в свою очередь, есть отработанные схемы снятия денег со счетов.

Наиболее частые жертвы фишинга — банки, электронные платежные системы, аукционы.

Наиболее частые жертвы фишинга — банки, электронные платежные системы, аукционы. То есть мошенников интересуют те персональные данные, которые дают доступ к деньгам. Но не только. Также популярна кража личных

данных от электронной почты — эти данные могут пригодиться тем, кто рассылает вирусы или создает зомби-сети.

Характерной особенностью фишинговых писем является очень высокое качество подделки. Адресат получает письмо с логотипами банка / сайта / провайдера, выглядящее в точности так же, как настоящее. Ничего не подозревающий пользователь переходит по ссыке «Перейти на сайт и залогиниться», но попадает на самом деле не на официальный сайт, а на фишерский его аналог, выполненный с высочайшей точностью.

Еще одной хитростью фишеров являются ссылки, очень похожие на URL оригинальных сайтов. Ведь достаточно наблюдательный пользователь может обратить внимание на то, что в командной строке браузера высвечивается ссылка, совершенно отличная от легитимного сайта. Такие «левые» ссылки тоже встречаются, но рассчитаны они на менее искушенного пользователя. Часто они начинаются с IP-адреса, хотя известно, что настоящие солидные компании давно не используют подобные ссылки.

Поэтому фишинговые URL часто похожи на настоящие. Они могут включать в себя название настоящего URL, дополненное другими словами (например, вместо www.examplebank.com стоит www.login-examplebank.com). Также в последнее время популярный фишинговый прием — ссылка с точками вместо слешей, внешне очень похожая на настоящую (вместо www.examplebank.com/personal/login стоит www.examplebank.com.personal.login). Можно привести еще такой фишерский вариант: www.examplebank.com-personal.login.

Также в самом теле письма может высвечиваться ссылка на легитимный сайт, но реальный URL, на который она ссылается, будет другим. Бдительность пользователя притупляется еще тем, что в письме может быть несколько второстепенных ссылок, ведущих на официальный сайт, но основная ссылка, по которой пользователю надо пройти и залогиниться, ведет на сайт мошенников.

Иногда личные данные предлагается ввести прямо в письме. Надо помнить, что никакой банк (либо другая организация, запрашивающая конфиденциальную информацию) не будет этого делать подобным образом.

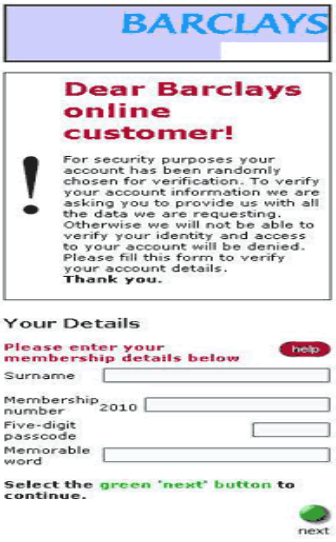


Рис. 3. Пример фишингового письма (подделка под уведомление online-банка

Атаки фишеров становятся все более продуманными, применяются методы социальной инженерии. Но в любом случае клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении («если вы не сообщите ваши данные в течение недели, ваш счет будет заблокирован»). Забавно, но часто в качестве причины, по которой пользователь якобы должен выдать конфиденциальную информацию, фишеры называют необходимость улучшить антифишинговые системы («если хотите обезопасить себя от фишинга, пройдите по этой ссылке и введите свой логин и пароль»).

Иногда личные данные предлагается ввести прямо в письме. Надо помнить, что никакой банк (либо другая организация, запрашивающая конфиденциальную информацию) не будет этого делать подобным образом.

Технологии фишеров совершенствуются. Так, появилось сопряженное с фишингом понятие — фарминг.

Технологии фишеров совершенствуются. Так, появилось сопряженное с фишингом понятие — *фарминг*. Это тоже мошенничество, ставящее целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNS цифровые адреса легитимных веб-сайтов на адреса поддельных, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид мошенничества еще опасней, так как заметить подделку практически невозможно.

Наиболее популярные фишерские мишени — аукцион Ebay и платежная система PayPal. Также страдают различные банки по всему миру. Атаки фишеров бывают случайными и целевыми. В первом случае атака производится «наобум». Атакуются наиболее крупные и популярные объекты — такие как аукцион Ebay — так как вероятность того, что случайный получатель имеет там учетную запись, довольно высока. Во втором случае мошенники узнают, каким именно банком, платежной системой, провайдером, сайтом пользуется адресат. Этот способ более сложен и затратен для фишеров, зато больше шансов, что жертва купится на провокацию.

Вопросы.

1. Что такое фишинг?
2. Какие методы использует фишинг?
3. Как узнать фишинговое письмо?
4. Какие бывают атаки фишеров?
5. Перечислите характерные особенности фишинговых писем.

❺Что такое DDoS-атака?

Существует множество киберугроз, которых следует опасаться интернет-пользователям и сетевым администраторам, но для организаций, чьи сервисы в основном работают в режиме онлайн, одной из самых важных атак, о которой следует знать, ввиду ее растущей распространенности, являются атаки типа «распределенный отказ в обслуживании» (DDoS). Как они работают и есть ли способы их предотвратить.

DDoS-атака - это отправка большого количества запросов на веб-ресурс, в результате чего может произойти прекращение работы ресурса – «отказ в обслуживании» или DoS (Denial-of-service).

- *DDoS-атаки (распределенный отказ в обслуживании)*

Этот тип кибератак, который иногда называют распределенными сетевыми атаками, использует определенные ограничения пропускной

способности, которые применяются к любым сетевым ресурсам, например, к инфраструктуре, обеспечивающей работу веб-сайта компании. DDoS-атака будет отправлять множественные запросы на атакуемый веб-ресурс с целью превышения возможностей веб-сайта по обработке множественных запросов и воспрепятствования его корректной работе. Типичными целями DDoS-атак являются сайты электронной коммерции и любые организации, предлагающие онлайн-услуги.

Сетевые ресурсы, такие как веб-серверы, имеют конечное ограничение на количество запросов, которые они могут обслуживать одновременно. Помимо ограничения емкости сервера, канал, соединяющий сервер с Интернетом, также будет иметь конечную пропускную способность или емкость. Всякий раз, когда количество запросов превышает пределы пропускной способности любого компонента инфраструктуры, уровень обслуживания, скорее всего, пострадает.

Обычно целью злоумышленника в любом примере DDoS-атаки является перегрузка сервера веб-ресурса, что приведет к невозможности его нормальной работы и полному отказу в обслуживании. Злоумышленник также может потребовать плату за прекращение атаки. В некоторых случаях ддос-атака может даже представлять собой попытку дискредитировать или нанести ущерб бизнесу конкурента.

Для осуществления атаки злоумышленник захватывает контроль над сетью или устройством, заражая его вредоносным ПО , создавая ботнет . Затем они инициируют атаку, отправляя ботам определенные инструкции. В свою очередь, ботнет начинает отправлять запросы на целевой сервер через его IP-адрес , перегружая его и вызывая отказ в обслуживании его обычного трафика.

- *Примеры DDoS-атак*

Изучение значения DDoS-атак и принципов их работы — это один из шагов к их предотвращению, но также важно понимать, что существуют различные типы DDoS-атак. Для этого необходимо сначала описать, как формируются сетевые соединения.

Модель взаимодействия открытых систем (OSI), разработанная Международной организацией по стандартизации, определяет семь отдельных уровней, из которых состоят сетевые соединения в Интернете.

К ним относятся физический уровень, уровень канала передачи данных, сетевой уровень, транспортный уровень, сеансовый уровень, уровень представления и прикладной уровень.

Многочисленные примеры DDoS-атак различаются в зависимости от того, на какой уровень соединения они нацелены. Ниже приведены некоторые наиболее распространенные примеры.

- *Атаки на уровне приложений*

Иногда их называют атакой уровня 7 (потому что они нацелены на 7-й (прикладной) уровень модели OSI). Такие атаки истощают ресурсы целевого сервера с помощью DDoS-сайтов. На 7-м уровне сервер генерирует веб-страницы в ответ на HTTP-запрос. Злоумышленники выполняют многочисленные HTTP-запросы, перегружая целевой сервер, поскольку он отвечает за загрузку многочисленных файлов и выполнение запросов к базе данных, необходимых для создания веб-страницы.

- *HTTP-флуд*

Представьте себе эти DDoS-атаки как многократное обновление веб-браузера на многих компьютерах. Это создает «поток» HTTP-запросов, вызывающий отказ в обслуживании. Реализация этих атак может быть простой — с использованием одного URL-адреса с узким диапазоном IP-адресов — или сложной, с использованием массива IP-адресов и случайных URL-адресов.

- *Атаки на протоколы*

Эти DDoS-атаки, часто называемые атаками истощения состояния, используют уязвимости на 3-м и 4-м уровнях модели OSI (сетевой и транспортный уровни). Эти атаки приводят к отказу в обслуживании за счет перегрузки ресурсов сервера или сетевого оборудования, например брандмауэров . Существует несколько типов атак на протоколы, включая SYN-флуд. Они используют протокол TCP (протокол управления

передачей), который позволяет двум устройствам установить сетевое соединение, отправляя неуправляемое количество «начальных запросов на подключение» TCP с поддельных IP-адресов.

- *Объемные атаки*

Эти примеры DDoS-атак создают отказ в обслуживании, используя всю доступную полосу пропускания на целевом сервере путем отправки огромных объемов данных для создания всплеска трафика на сервере.

- *DNS-амплификация*

Это атака на основе отражения, при которой запрос отправляется на DNS-сервер с поддельного IP-адреса (целевого сервера), побуждая DNS-сервер «перезвонить» цели для проверки запроса. Это действие усиливается за счет использования ботнета, который быстро перегружает ресурсы целевого сервера.

DDoS-атаки бывает сложно обнаружить, поскольку они могут имитировать обычные проблемы с обслуживанием и становятся все более изощренными. Однако существуют определенные признаки, которые могут указывать на то, что система или сеть стала жертвой DDoS-атаки. Перечислим некоторые из этих приложений и продуктов.

- Внезапный всплеск трафика, исходящего с неизвестного IP-адреса
- Поток трафика от многочисленных пользователей, имеющих определенные сходства, например, геолокацию или версию веб-браузера.
- Необъяснимый рост запросов на одну страницу
- Необычные схемы движения
- Нетипично замедленная работа в сети.
- Служба или веб-сайт, который внезапно и без причины отключается

- *Предотвращение и смягчение последствий DDoS-атак*

Хотя DDoS-атаки сложно обнаружить, можно реализовать ряд мер, чтобы попытаться предотвратить подобные типы кибератак и смягчить любой ущерб в случае атаки. Для пользователей, интересующихся тем, как предотвратить

DDoS-атаки, главное — создать план действий по защите систем и минимизации ущерба в случае атаки. В целом, для предприятий полезно внедрить такое решение, как защита от DDoS-атак Kaspersky , которое постоянно анализирует и перенаправляет вредоносный трафик. Кроме того, следующие общие советы могут помочь еще больше усилить вашу защиту:

- Оцените текущую настройку системы, включая программное обеспечение, устройства, серверы и сети, чтобы выявить риски безопасности и потенциальные угрозы, а затем примите меры по их снижению; проводите регулярные оценки рисков.
- Поддерживайте все программное обеспечение и технологии в актуальном состоянии, чтобы быть уверенными в наличии последних исправлений безопасности.
- Разработать эффективную стратегию предотвращения, обнаружения и смягчения последствий ддос-атак.
- Убедитесь, что все участники плана по предотвращению атак понимают значение DDoS-атаки и свои назначенные роли.
- В случае атаки эти действия могут обеспечить некоторое смягчение последствие.
- Сети Anycast: использование сети Anycast для перераспределения трафика может помочь сохранить работоспособность сервера во время устранения проблемы, гарантируя, что сервер не придется полностью отключать.
- Маршрутизация по принципу «черной дыры». В этом сценарии сетевой администратор интернет-провайдера перенаправляет весь трафик с целевого сервера на маршрут «черной дыры» (целевой IP-адрес), исключая его из сети и сохраняя его целостность. Однако это может оказаться слишком радикальным шагом, поскольку он также блокирует легитимный трафик.

- Ограничение скорости: ограничивает количество запросов, которые сервер может принять в любой момент времени. Хотя само по себе это не будет очень эффективным, оно может быть полезным как часть более крупной стратегии.
- Межсетевые экраны: организации могут использовать межсетевые экраны веб-приложений (WAF) в качестве обратного прокси-сервера для защиты своих серверов. WAF можно настроить с помощью правил фильтрации трафика, и администраторы могут изменять их в режиме реального времени, если подозревают DDoS-атаку.

Вопросы.

1. Как называется описанная в тексте атака?
2. Как называется сеть заражённых устройств, используемая для атаки?
3. Какую основную цель преследует злоумышленник при DDoS?
4. Какие запросы генерируют веб-страницы на 7-м уровне OSI?
5. Сколько уровней содержит модель OSI?
6. На какой уровень модели OSI нацелены атаки уровня приложений?
7. Что может требовать злоумышленник за прекращение атаки?
8. Через что ботнет отправляет запросы на целевой сервер?
9. Какой вид ресурса часто является целью DDoS?
10. Как называется ПО, которым заражают устройства для создания ботнета?

❻Атака с использованием SQL инъекции

Возможно, вы не знаете, что такое атака с использованием SQL инъекции (SQLI) или как она работает, но вы точно знаете жертв. Target, Yahoo, Zappos, Equifax, Epic Games, TalkTalk, LinkedIn и Sony Pictures — все эти компании подверглись атакам киберпреступников с использованием SQL инъекций.

SQLI — это тип атаки, при которой киберпреступники эксплуатируют уязвимости ПО в веб-приложениях с целью кражи, удаления или модификации данных, или получения административного контроля над системами, на которых запущены эти приложения.

Исследователи в области кибербезопасности считают SQLI одной из наименее сложных, легко защищаемых киберугроз. Malwarebytes Labs поставила SQLI на третье место в рейтинге "Топ-5 самых глупых киберугроз, которые все равно работают", сославшись на то, что SQLI - это известная, предсказуемая атака с легко реализуемыми контрмерами.

Атаки с использованием SQL инъекций настолько просты, что злоумышленники могут находить уязвимые сайты с помощью продвинутых поисков Google, называемых Google Dorking. Найдя подходящую цель, злоумышленники могут использовать автоматизированные программы для выполнения атаки. Все, что им нужно, — это ввести URL сайта-цели и наблюдать, как потекут украденные данные.

Тем не менее атаки SQLI происходят каждый день и везде. Фактически, если у вас есть сайт или онлайн-бизнес, киберпреступники уже могли попытаться взломать его с помощью SQLI. Исследование Ponemon Institute на тему угроз SQL инъекций и недавно взломанных ритейлеров показало, что 65% опрошенных компаний стали жертвами атаки SQLI.

Наиболее часто атакуемые веб-приложения включают: социальные сети, интернет-магазины и университеты. Малый и средний бизнес особенно уязвим, так как часто не знаком с методами, которые киберпреступники используют в атаках SQLI, и, соответственно, не знают, как от них защититься.

В связи с этим, давайте начнем с первого шага по защите от SQL инъекций - обучению этой теме. Вот ваше введение в мир SQL инъекций.

"SQLI - это тип атаки, в ходе которой злоумышленники используют уязвимости программного обеспечения в веб-приложениях с целью кражи,

удаления или изменения данных, а также получения административного контроля над системами, на которых работают затронутые приложения."

- *Как работает SQL инъекция?*

Разработанный в начале 70-х годов, SQL (сокращение от structured query language) является одним из старейших языков программирования, который до сих пор используется для управления базами данных в Интернете. Эти базы данных содержат такие данные, как цены и уровень запасов на сайтах интернет-магазинов. Когда пользователю нужно получить доступ к информации из базы данных, SQL используется для доступа и представления этих данных пользователю. Но эти базы данных могут содержать и более чувствительные и ценные данные, такие как имена пользователей и пароли, информация о кредитных картах и номера социального страхования. Именно в таких случаях в дело вступают SQL-инъекции.

Проще говоря, SQL инъекция — это когда злоумышленники вводят вредоносные команды в веб-формы, такие как поле поиска, логина или URL небезопасного сайта, чтобы получить несанкционированный доступ к конфиденциальным и ценным данным.

Вот пример. Представьте, что вы заходите на ваш любимый сайт по продаже одежды онлайн. Вы ищете носки и погружаетесь в мир ярких носков, которые можно купить одним нажатием мыши. Чудеса технологии! Каждый носок, который вы видите, существует в базе данных на каком-то сервере. Когда вы находите носок, который вам нравится и нажимаете на него, вы отправляете запрос в базу данных носков, и сайт магазина отвечает информацией о выбранном вами носке. Теперь представьте, что ваш любимый сайт создан небрежно, с множеством эксплуатируемых уязвимостей SQL.

Киберпреступник может манипулировать запросами к базе данных таким образом, что запрос на информацию о паре носков вернет номер кредитной карты какого-нибудь неудачливого покупателя. Повторяя этот процесс снова и снова, киберпреступник может проникнуть в глубины базы данных и

похитить конфиденциальную информацию о каждом покупателе, который когда-либо совершал покупки на вашем любимом сайте онлайн-одежды, включая вас. Если пойти еще дальше, представьте, что вы - владелец этого сайта одежды. У вас на руках огромная утечка данных.

В результате одной атаки SQLI киберпреступники могут получить персональные данные, электронную почту, логины, номера кредитных карт и номера социального страхования миллионов пользователей. Затем киберпреступники могут продать эту личную информацию в самых мрачных уголках темной паутины, чтобы использовать ее во всевозможных незаконных целях.

Украденные электронные письма могут использоваться для фишинговых и вредоносных атак. В свою очередь, спам-атаки могут использоваться для заражения жертв всевозможными вредоносными программами, такими как ransomware, рекламное ПО, криптоджекеры, троянцы (например, Emotet) и т. д. Украденные телефонные номера для Android и iOS могут быть использованы для рассылки робозвонков и текстового спама.

Украденные логины из социальных сетей можно использовать даже для рассылки спама и кражи еще большего количества логинов для дополнительных сайтов. Malwarebytes Labs ранее сообщала о том, что взломанные аккаунты LinkedIn использовались для рассылки спама другим пользователям с помощью сообщений InMail, содержащих поддельные URL-адреса, выглядящие как страница входа в Google Docs, с помощью которых злоумышленники могли собирать имена пользователей и пароли Google.

"Киберпреступник может манипулировать запросами к базе данных таким образом, что запрос на информацию о паре носков вернет номер кредитной карты какого-нибудь несчастного покупателя".

- *Какова история SQL инъекций?*

Эксплойт для SQL-инъекций был впервые задокументирован в 1998 году исследователем кибербезопасности и hacker Джефф Форристал. Его находки были опубликованы в давно выходящем hacker журнале Phrack. Под псевдонимом Rain Forest Puppy Форристал объяснил, как человек с базовыми навыками кодирования может наложить несанкционированные SQL-команды на легитимные SQL-команды и извлечь конфиденциальную информацию из базы данных незащищенного веб-сайта.

Когда Форристал уведомил Microsoft о том, как уязвимость повлияла на их популярный продукт SQL Server, они не восприняли это как проблему. Как выразился Форристал: «По их [Microsoft] мнению, то, о чем вы сейчас читаете, не является проблемой, так что не беспокойтесь и не поступайте никак, чтобы это пресечь.»

Что делает вялую реакцию Microsoft столь шокирующей, так это то, что многие отрасли и учреждения всерьез полагались (как тогда, так и сейчас) на технологии управления базами данных этой компании для поддержания своего бизнеса, включая розничную торговлю, образование, здравоохранение, банки и отделы человеческих ресурсов. Это приводит нас к следующему событию в истории SQLI — первой серьезной атаке.

В 2007 году крупнейшая сеть магазинов шаговой доступности в США, 7-Eleven, стала жертвой атаки SQLI. Российские хакеры использовали SQL инъекции, чтобы взломать сайт 7-Eleven и использовать это как трамплин, чтобы проникнуть в базу дебетовых карт клиентов магазина. Это позволило хакерам затем снимать деньги у себя дома, в России. Как сообщило издание Wired, в итоге преступники унесли с собой два миллиона долларов.

Не все атаки SQLI преследуют корыстные цели. В другом примечательном примере из 2007 года киберпреступники использовали SQLI для получения административного контроля над двумя сайтами, связанными с армией США, и перенаправления посетителей на сайты с антиамериканской и антиизраильской пропагандой.

Утечка данных MySpace в 2008 году является одной из крупнейших атак на сайт потребителей. Киберпреступники похитили электронные адреса, имена и частичные пароли почти 360 миллионов учетных записей. И вот почему мы не используем одни и те же пароли на нескольких сайтах.

Звание компании с самым вопиющим отсутствием безопасности получает Equifax. Утечка данных в Equifax в 2017 году привела к разглашению крайне личной информации (такие как имена, номера социального страхования, даты рождения и адреса) о 143 миллионах потребителей. Для организации, которая является хранителем информации для каждого американца, за исключением тех, кто живет вне системы, можно было бы ожидать, что они примут меры предосторожности против основных атак SQLI. До того, как произошла утечка данных, исследовательская фирма в области кибербезопасности даже предупредила Equifax, что она уязвима к атаке SQLI, однако кредитное бюро не предприняло никаких действий до тех пор, пока было уже слишком поздно.

В 2015 году SQLI-атака на производителя игрушек Vtech, ставшая самым жутким взломом в истории, привела к утечке данных почти пяти миллионов родителей и 200 000 детей. В беседе с мультимедийным онлайн-изданием Motherboard hacker , ответственный за hacker , заявил, что у него не было планов по использованию этих данных и он не публиковал их нигде в сети. С другой стороны, hacker также объяснил, что данные было очень легко украсть, и кто-то другой мог добраться до них первым. Действительно, холодное утешение.

Если перенестись в сегодняшний день, то атака SQLI по-прежнему актуальна. Каждые три года Open Web Application Security Project (OWASP) составляет рейтинг 10 наиболее критичных рисков безопасности веб-приложений. В последнем выпуске 2017 года атака SQLI заняла первое место.

Помимо долголетия атак SQLI, интересно заметить, что они никак не изменились и не эволюционировали. Атаки SQLI работают и будут продолжать работать, пока люди не изменят свое отношение к кибербезопасности. Будьте этими изменениями.

Вопросы.

1. Как расшифровывается SQLI?
2. Наиболее часто атакуемые веб-приложения?
3. Как работает SQL инъекция?
4. Атака на какую компанию в 2008 году является одной из крупнейших атак на сайт потребителей?
5. Какие способы защиты от SQLI атак можно предложить?

❼Кража данных и как ее избежать

Кража данных, также называемая кражей информации – это незаконная передача или хранение личной, конфиденциальной и финансовой информации: паролей, программных кодов и алгоритмов, а также авторских процессов и технологий. Кража данных считается серьезным нарушением безопасности и конфиденциальности с потенциально неблагоприятными последствиями как для частных лиц, так и для организаций.

Кража данных – это кража цифровой информации, хранящейся на компьютерах, серверах и электронных устройствах, с целью получения не подлежащих разглашению данных или нарушения конфиденциальности. Украденные данные могут включать информацию о банковском счете, пароли от онлайн-сервисов, номера паспортов, номера водительских прав, номера социального страхования, медицинские записи, онлайн-подписки и прочее. Получив доступ к личной или финансовой информации, неавторизованные пользователи могут удалять и изменять ее без разрешения владельца, или даже запретить к ней доступ.

Частой причиной кражи данных является стремление злоумышленников продать эту информацию или использовать ее для кражи других личных данных. В случае, если в руки злоумышленников попадет достаточно информации, они могут получить доступ к защищенным учетным записям, воспользоваться кредитными картами жертвы или иным образом использовать

эти данные в своих интересах. Раньше кража данных в первую очередь являлась проблемой компаний и организаций, но, к сожалению, сейчас она все более серьезно встает для частных лиц.

Несмотря на слово «кража» в определении, кража данных не означает изъятие информации у жертвы в буквальном смысле – злоумышленники просто копируют или дублируют информацию для собственного использования.

В контексте кражи данных термины «утечка данных» и «нарушение целостности данных» могут использоваться как синонимы. Однако они отличаются:

- *Утечка данных* происходит в результате случайного раскрытия конфиденциальных данных либо в интернете, либо в результате потери жестких дисков или устройств. Это позволяет киберпреступникам получить несанкционированный доступ к конфиденциальным данным без каких-либо усилий с их стороны.
- *Нарушение целостности данных*, напротив, происходит в результате умышленных кибератак.

Кража данных или цифровая кража может осуществляться различными способами. Ниже приведены наиболее распространенные их них.

- *Социальная инженерия*

Самая распространенная форма социальной инженерии – это фишинг. Фишинг имеет место, когда злоумышленники, выдавая себя за доверенное лицо или надежный источник, обманом вынуждают пользователя открыть электронное письмо или текстовое сообщение. Пользователи, ставшие жертвами фишинговых атак, часто подвергаются краже данных.

- *Ненадежные пароли*

Использование пароля, который можно легко угадать, или одного и того же пароля для нескольких учетных записей может позволить злоумышленникам получить доступ к данным. Также причиной кражи данных

могут стать «вредные привычки» при обращении с паролями, например, записывать пароль на бумаге или сообщать его другим пользователям.

- *Уязвимости в системе*

Некачественно разработанные программные приложения или недостаточно внимательно спроектированные и реализованные сетевые системы создают уязвимости, которые могут использоваться злоумышленниками для кражи данных. Устаревшее антивирусное программное обеспечение также может стать источником уязвимостей.

- *Кадровые риски*

Сотрудники, работающие в компании, имеют доступ к личной информации клиентов. Недобросовестные сотрудники или недовольные подрядчики могут скопировать, изменить или украсть эти данные. Однако внутренние угрозы не обязательно связаны с действиями сотрудников, работающих в настоящее время. Их причиной могут также стать действия бывших сотрудников, подрядчиков или партнеров, имеющих доступ к системам компании и к конфиденциальной информации. Сообщается о постоянном росте кадровых рисков.

- *Ошибки, вызванные человеческим фактором*

Утечки данных не всегда являются следствием злонамеренных действий, иногда они могут произойти в результате человеческой ошибки. Самые распространенные ошибки – отправка конфиденциальной информации не тому человеку, например, на ошибочный адрес электронной почты, прикрепление неправильного документа или передача физического файла лицу, у кого не должно быть доступа к информации. Также человеческие ошибки могут включать неправильную конфигурацию, например, если сотрудник не установил защитный пароль для базы данных, содержащей конфиденциальную информацию.

Пользователи могут загрузить программы и данные с взломанных веб-сайтов, зараженных вирусами, червями или вредоносными программами,

предоставляя тем самым злоумышленникам несанкционированный доступ к своим устройствам, и позволяя им красть данные.

Некоторые случаи кражи данных происходят не в результате киберпреступлений, а становятся следствием физических действий. К ним относится кража документов или устройств: ноутбуков, телефонов, запоминающих устройств. С распространением удаленной работы увеличивается вероятность пропажи и кражи устройств. Если вы работаете в общественном месте, например в кафе, злоумышленник, наблюдая за вашим экраном и клавиатурой, может получить ваши данные для входа. Еще один способ кражи данных – скимминг – позволяет злоумышленникам получать информацию о платежных картах посредством установки специальных устройств в считыватели банковских карт и банкоматы.

Если компания, хранящая персональные данные, подвергнется атаке из-за проблем с базой данных или сервером, злоумышленники смогут получить доступ к личной информации клиентов.

Большой объем информации находится в открытом доступе, ее можно найти посредством поиска в интернете или просматривая посты пользователей в социальных сетях.

- *Типы данных, которые крадут чаще всего*

Любая информация, хранимая частными лицами или компаниями, может стать потенциальной целью для похитителей данных. Например:

- Записи о клиентах.
- Финансовые данные, такие как информация о кредитных и дебетовых картах.
- Исходные коды и алгоритмы.
- Запатентованные описания процессов и методики работы.
- Сетевые учетные данные, такие как имена пользователей и пароли.
- Кадровые записи и данные сотрудников.
- Личные документы, хранящиеся на компьютерах.

Последствия кражи данных

Последствия утечки данных для организаций могут оказаться достаточно серьезными:

- Возможные судебные иски со стороны клиентов, информация которых была раскрыта.
- Требования выкупа от программ-вымогателей, запущенных злоумышленниками.
- Затраты на восстановление, например, исправление или обновление взломанных систем.
- Репутационный ущерб и потеря клиентов.
- Штрафы и пени от регулирующих органов (в зависимости от отрасли).
- Простой на период восстановления данных.

Для частных лиц, чьи данные подверглись утечке, основным последствием является возможная кража личных данных, влекущая за собой финансовые потери и эмоциональное расстройство.

Чтобы предотвратить кражу данных злоумышленниками, можно предпринять следующие действия.

Злоумышленники с легкостью могут взламывать пароли, особенно ненадежные. Надежный пароль состоит не менее чем из 12 символов: заглавных и строчных букв, специальных символов и цифр. Чем короче и проще пароль, тем легче киберпреступникам будет его взломать. Следует избегать выбора очевидных паролей, например последовательных цифр (1234) и личной информации, которую может угадать тот, кто вас знает, например, не следует использовать дату рождения или имя домашнего животного.

Для усложнения пароля можно использовать кодовую фразу. Для формирования кодовой фразы выбирается легко запоминающаяся значимая фраза, а затем из первых букв каждого слова этой фразы составляется пароль.

- *Не используйте один и тот же пароль для нескольких учетных записей.*

Если один и тот же пароль используется для нескольких учетных

записей, и злоумышленникам удастся взломать его на одном из сайтов, они получат доступ ко всем остальным учетным записям. Не забывайте регулярно менять пароли, желательно приблизительно каждые шесть месяцев.

- *Не записывайте пароли.* Пароль, записанный в любом месте: на бумаге, в электронной таблице Excel или в приложении Notes на телефоне – становится уязвимым для злоумышленников. Если нужно запоминать слишком много паролей, подумайте об использовании менеджера паролей – он позволит контролировать все ваши пароли.
- *Многофакторная аутентификация.* Многофакторная аутентификация – это инструмент, предоставляющий пользователям интернета дополнительный уровень защиты учетных записей, помимо стандартной комбинации адреса электронной почты / имени пользователя и пароля. Наиболее распространенной является двухфакторная аутентификация. Двухфакторная аутентификация требует двух отдельных, различных форм идентификации для доступа к чему-либо. Первый фактор – это пароль, а второй – это обычно код, отправляемый на номер телефона, или биометрические данные: отпечаток пальца, снимок лица или сетчатки глаза. По возможности включите многофакторную аутентификацию для своих учетных записей.
- *Будьте осторожны при распространении личной информации.* Постарайтесь ограничить доступ к своим данным по принципу крайней необходимости, как в интернете, так и в реальной жизни. Например, если кто-то запрашивает вашу личную информацию: номер социального страхования, номер кредитной карты, номер паспорта, дату рождения, данные об опыте работы, кредитный статус и прочую информацию – задумайтесь, зачем им нужна эта информация и как они будут ее использовать. Какие меры безопасности они предпринимают, чтобы обеспечить конфиденциальность вашей личной информации?

- *Ограничьте публикации в социальных сетях.* Ознакомьтесь с параметрами безопасности каждой социальной сети и убедитесь, что они настроены на комфортном для вас уровне. Избегайте раскрытия личной информации, например, адреса и даты рождения, в биографии в социальной сети: по этим данным злоумышленники могут сформировать о вас представление.
- *Удалите неиспользуемые учетные записи.* Большинство сначала подписываются на онлайн-сервисы, а затем больше не используют их. Сервисы, в которых все еще существуют эти учетные записи, могут содержать ваши личные и идентификационные данные и номера кредитных карт – все это ценная информация для киберпреступников. Хуже того, если вы используете один и тот же пароль для нескольких учетных записей, что крайне не рекомендуется, то в случае утечки пароля на одном из сайтов, злоумышленники могут получить доступ к вашим учетным записям на других сайтах. Чтобы сохранить конфиденциальность, рекомендуется удалить личные данные из неиспользуемых сервисов. Для этого необходимо удалить устаревшие учетные записи, не следует просто бросать их.
- *Уничтожьте личную информацию.* Измельчайте письма, содержащие личные данные: имя, дату рождения или номер социального страхования. Обращайте внимание на содержимое почтового ящика: оно может предупредить о незамеченной утечке данных. Например, признаком взлома может стать получение документов о посещении врача, которого вы на самом деле не посещали. В этом случае пора принимать меры.
- *Своевременно обновляйте системы и программы.* Поддерживайте все операционные системы и программы в актуальном состоянии, регулярно, по мере появления, устанавливайте обновления систем безопасности, веб-браузеров, операционных систем и программ.

- *Следите за банковскими счетами.* Регулярно проверяйте свой банковский счет, выписки по кредитной карте и другие счета. Это позволяет контролировать, имели ли место какие-либо несанкционированные платежи или другие аномалии. Если компания, с которой вы совершаете транзакции, подверглась утечке данных, вы можете не получать уведомления о списании средств, поэтому рекомендуется проявлять бдительность.
- *Остерегайтесь бесплатных сетей Wi-Fi.* Использование бесплатного общедоступного Wi-Fi вошло для многих в повседневную жизнь, но такие точки доступа не всегда обеспечивают безопасное и надежное соединение. Общедоступные точки доступа Wi-Fi могут оказаться легкой целью для киберпреступников, использующих их для кражи данных. Чтобы сохранить безопасность при работе в общедоступных сетях Wi-Fi, не открывайте и не отправляйте конфиденциальные данные, отключите Bluetooth и общий доступ к файлам, используйте VPN и сетевой экран. Также необходимо наличие надежного антивируса. Ознакомьтесь с рекомендациями по соблюдению безопасности при использовании общедоступных сетей Wi-Fi.
- *Следите за новостями.* Следите как за общими новостями, так и за новостями безопасности, чтобы быть в курсе, если компания, с которой вы взаимодействуете, подвергнется утечке данных.

Один из лучших способов обеспечения безопасности в интернете – использовать надежный антивирус. Kaspersky Premium круглосуточно обеспечивает безопасность ваших устройств и данных: обнаруживает уязвимости устройств и угрозы, блокирует киберугрозы до начала их распространения, а также изолирует и устраняет непосредственные опасности.

Вопросы.

1. Что такое кража данных?
2. Кража данных считается серьезным нарушением безопасности только для частных лиц?

3. Какие цели преследуют преступники при краже данных?
4. В результате чего происходит утечка данных?
5. Перечислите наиболее распространённые способы цифровой кражи?
6. Что такое скимминг?
7. Какие данные крадут чаще всего?

❽ Атаки «man-in-the-middle»

Атака посредника, или атака «человек посередине» (англ. *man-in-the-middle attack*), наиболее известная как MITM-атака — вид атаки в криптографии и компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. Является методом компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.

Одним из примеров атак типа «человек посередине» является активное прослушивание, при котором злоумышленник устанавливает независимые связи с жертвами и передаёт сообщения между ними. Тем самым он заставляет жертв поверить, что они разговаривают непосредственно друг с другом через частную связь, фактически же весь разговор управляется злоумышленником. Злоумышленник должен уметь перехватывать все передаваемые между двумя жертвами сообщения, а также вводить новые. В большинстве случаев это довольно просто: например, злоумышленник может вести себя как «человек посередине» в пределах диапазона приёма беспроводной точки доступа (Wi-Fi).

Данная атака направлена на обход взаимной аутентификации или отсутствие таковой и может увенчаться успехом только тогда, когда злоумышленник имеет возможность выдать себя за каждую конечную точку

либо оставаться незамеченным в качестве промежуточного узла. Большинство криптографических протоколов включает в себя некоторую форму аутентификации конечной точки специально для предотвращения MITM-атак. Например, TLS может выполнять проверку подлинности одной или обеих сторон с помощью взаимно доверенного центра сертификации.

- *Как защититься от атаки «человек посередине»*

Представьте, что вы зашли в любимую кофейню, взяли чашку латте и подключили свой ноутбук к бесплатному Wi-Fi, чтобы побродить по интернету, пообщаться, а может быть, и поработать. И тут рядом с вами оказывается невидимка. Вы его не видите, но этот незваный привратник находится между вами и интернетом, делая небезопасным просмотр сайтов, общение в соцсетях, чтение электронной почты. Этот некто видит все, что вы делаете, и ждет удобного момента, чтобы нанести удар.

Звучит страшновато, правда? В ходе атаки man-in-the-middle хакер перехватывает электронную почту, историю поиска в интернете и информацию из социальных сетей, чтобы похитить персональные данные своей жертвы и использовать их для совершения преступных действий. В отличие от фишинга, когда жертва сама является активным, хотя и невольным участником атаки, ослабляя бдительность и убирая защитные барьеры, пассивная атака man-in-the-middle происходит вообще незаметно для жертвы.

Объектами такой атаки могут стать и частные лица, и организации любого размера, от нее никто не застрахован. В 2015 году в результате масштабной операции Европола были схвачены 49 членов группировки, ответственной за хакерские атаки по всей Европе. С помощью различных методов взлома и социальной инженерии они внедрялись в доверенные каналы связи между компаниями и их клиентами. Оказавшись внутри контура, злоумышленники мониторили все коммуникации и обманом вынуждали ничего не подозревающих жертв переводить деньги на свои банковские счета.

- *Методы атаки*

Стремительный рост числа бесплатных точек беспроводного доступа и увеличение скорости широкополосного интернета дает нам все больше возможностей для подключения к Сети, но одновременно является настоящим подарком для тех, кто хочет нас подслушивать и перехватывать наши действия.

Один из популярных методов атаки – создание хакером собственной точки доступа к Wi-Fi. Представьте, что вы сидите в любимой книжной лавке и открываете настройки Wi-Fi, чтобы подключиться к бесплатной сети. Как вы думаете, все ли доступные сети в открывшемся списке принадлежат законным владельцам бизнеса или часть из них может принадлежать хакеру?

Это крайне важный вопрос, поскольку как только вы подключитесь к фальшивой сети, хакер немедленно получит доступ к вашему устройству. Хакеры легко создают поддельные точки доступа к Wi-Fi, позволяющие им получать доступ к персональным данным каждого, кто пытается к ним подключиться.

Взломав электронную почту, хакеры получают контроль над почтовым аккаунтом и могут мониторить всю корреспонденцию. Проникнув в эту закрытую систему, они могут начать рассылку поддельных, но правдоподобно выглядящих писем с просьбой перевести деньги, прислать финансовую информацию, сообщить какие-либо пароли и т. д. Самые серьезные проблемы могут возникнуть, если хакеры отправляют руководящим сотрудникам компании фальшивые запросы на перевод денег, которые выглядят как подлинные.

Один из самых распространенных методов атаки – это перехват сеанса, когда хакер получает контроль над cookie-файлами в вашем браузере – небольшими фрагментами данных, содержащими информацию о взаимодействии с веб-сайтами, которые вы посещаете. Получив доступ к cookie-файлам, хакер может похитить целый ряд данных: от логина и пароля до персональных данных, которые автоматически подставляются в онлайн-формы.

- *Как защититься от атаки*

Самое главное – всегда следите за безопасностью своего поиска в интернете. Шифрование трафика между вашим устройством и сетью при помощи программ для шифрования данных поиска позволяет защититься от возможных атак man-in-the-middle.

Пользуйтесь только безопасными веб-сайтами. Если сайт безопасен, в большинстве браузеров рядом с его URL-адресом появляется значок замка. Если такого значка нет, убедитесь, что адрес сайта начинается с https. Буква «s» означает, что сайт безопасен и хакеры не смогут перехватить ваши данные.

Установка файервола – еще один надежный способ защитить свои данные при просмотре страниц в интернете. Хотя файервол не гарантирует стопроцентную защиту, он повышает безопасность при использовании общедоступных сетей Wi-Fi. Если без публичного Wi-Fi не обойтись, имеет смысл использовать VPN (виртуальная частная сеть). Этот тип сетей защищает трафик, и хакерам гораздо труднее бывает его перехватить.

Своевременно обновляйте свое защитное ПО. Злоумышленники непрерывно адаптируются к изменениям и оттачивают свои навыки, поэтому честному пользователю всегда надо быть во всеоружии. Своевременно обновляя защитное ПО, вы всегда будете иметь в своем распоряжении передовые инструменты, которые будут обеспечивать защиту ваших действий онлайн и позволят сделать просмотр страниц в интернете увлекательным и безопасным занятием.

Вопросы.

1. В чем заключается атака MITM-атака?
2. На что направлена атака «человек посередине»?
3. Как защитится от атаки «человек посередине»?
4. Назовите методы атак?
5. Как установка фейервола поможет при цифровых атаках?
6. Для чего необходимо своевременно обновлять ПО?

❾Организационные меры защиты информации

В современном мире, где данные становятся новым «золотом», защита информационных ресурсов стала особенно актуальной. Избавиться от угроз ИБ позволяют технические решения. Но! Пока компания не примет организационные меры защиты информации (ЗИ), она не сможет создать надежную систему безопасности.

- *Зачем защищать данные*

Защита данных является одной из важных задач, так как данные — это ценный актив. Неправомерный доступ и раскрытие важных сведений повлекут за собой нарушение конфиденциальности и целостности информации, а последствия могут быть критическими для компании, вплоть до остановки бизнес-процессов. Кроме того, утечка сведений о конкретных людях может привести к краже денег с их банковских счетов, использованию данных в мошеннических целях. В случае утечек данных, за которые предусмотрена ответственность, организации грозят штрафы и судебные иски.

- *Что понимается под информационной безопасностью*

Информационная безопасность (ИБ) — это защита информации и обслуживающей ее инфраструктуры от несанкционированного доступа (НСД), утечки, искажения и уничтожения данных. Сюда же входят и меры по предотвращению, выявлению и устранению последствий угроз. Главная цель ИБ — обеспечить конфиденциальность, целостность и доступность информации.

Конфиденциальность и доступность означает, что информация предоставляется только тем, кому разрешен доступ.

Целостность — защита данных от неправомерных изменений.

- *Основные угрозы безопасности данных*

Выделяют три основных группы угроз.

Угрозы конфиденциальности — несанкционированный доступ к данным: взлом информационных ресурсов, использование уязвимостей ПО, их кража или копирование, перехват информации (взлом электронной почты, мессенджеров, перехват СМС-сообщений). Такая ситуация возникает, если злоумышленник получит доступ к системе.

Угрозы целостности — неправомерное изменение информации (подмена реальной информации на фиктивную для получения выгоды) или ее уничтожение (например, в результате сбоев системы). К этому может привести как преднамеренное действие злоумышленника, так и ошибка в работе.

Угрозы доступности — действия злоумышленников, в результате которых добросовестные пользователи не могут получить доступ к данным. Например, атака типа «отказ в обслуживании» приводит к нарушению штатного режима функционирования информационной системы в результате подложных запросов.

Также угрозы ИБ бывают внешние и внутренние, умышленные и случайные, естественные и искусственные.

- *Принципы защиты информации*

Под принципами ЗИ понимают набор правил, которые указывают, как обрабатывают и защищают персональные данные. Перечислим их:

- *Легитимность, справедливость и прозрачность* — данныех получены законно и открыто.
- *Целевая ограниченность* — данные используют для конкретных целей, например, банки собирают личную информацию о клиентах для ведения финансовых операций, и эта информация не должна передаваться третьим лицам.
- *Минимизация данных* — собирают сведения, необходимые для достижения указанных целей.
- *Точность* — данные должны быть точными и актуальными, опечатка в данных может привести к проблемам с госорганами или банками.
- *Ограничение хранения* — информация хранится ограниченное время, необходимое для достижения конкретных целей. Дальнейшее хранение данных увеличивает риск утечки.

- *Целостность и конфиденциальность* — при обработке информации необходимо обеспечить ее безопасность, включая защиту от НСД, случайной потери, уничтожения или повреждения.
- *Ответственность* — сотрудник, ответственный за обработку данных, обязан соблюдать эти принципы. Для протоколирования процесса обработки данных устанавливается специальное ПО, ведутся журналы учета.

В каждой компании выбирают наиболее подходящие ей меры обеспечения ИБ.

- *Меры обеспечения информационной безопасности*
  Различают организационные и технические меры ИБ.

Организационные меры защиты информации (ЗИ) — обучение персонала, определение правил доступа, статусов и обязанностей пользователей, способов профилактики компьютерных преступлений, восстановления данных и проверки безопасности. Сюда входит разработка и поддержание системы управления ИБ, проведение регулярных аудитов безопасности и комплекса мер по предупреждению инцидентов безопасности.

Все эти меры нужны, чтобы обеспечить охрану объектов информатизации (помещений с оборудованием: серверами, компьютерами, предназначенными для работы с данными, коммуникационными узлами),; сохранность и конфиденциальность информации и предотвратить несанкционированное использование данных.

Для реализации организационных мер в компании создают необходимые условия: выделяют помещения, закупают необходимое оборудование, устанавливают пропускной режим к объектам информатизации. А также разрабатывают и вводят локальные документы, устанавливающие порядок работы с защищенной информацией.

Основу таких документов составляют федеральные, региональные и ведомственные нормативно-правовые акты. В них определены порядок разработки и внедрения политики ИБ, принципы, стандарты и требования к работе с информационными ресурсами, обучение персонала взаимодействию с

конфиденциальными данными, периодичность проведения плановых проверок оценки информационных систем и средств.

Однако на деле соблюдать все правила непросто. Необходимо знать много нормативно-правовых актов по ИБ и определить их для своей организации самостоятельно, ведь в законе не перечислены документы по обеспечению ИБ. Для этого нужно разбираться в юридической сфере и в информационной безопасности.

Приведем примерный перечень документов по ЗИ:

- *Положения:* о защите персональных данных и правилах использования внутренней ИТ-инфраструктурой.
- *Распоряжения:* о назначении ответственных лиц, правилах хранения и допуска к носителям данных.
- *Должностные инструкции* специалистов и ответственных за ПО.
- *Список лиц* с доступом к важной информации.
- *Правила:* отождествления пользователя, установки ПО, резервного копирования.
- *Журналы учета:* съемных носителей, технических средств обработки и передачи информации, проведения инструктажей, тестирования средств ЗИ, профилактических мероприятий.

Кроме того, сейчас ощущается острая нехватка специалистов в области ИБ: по данным «СерчИнформ», 66% организаций РФ считают, что ИБ-специалистов не хватает, а 12% организаций понимают, что кадровый голод только усиливается.

Технические меры ЗИ зависят от технических возможностей организации и уровня сотрудников. Для защиты информации компании могут использовать шифрование данных при передаче и хранении, системы аутентификации и авторизации для контроля доступа, антивирусное ПО.

Оптимальное решение — использовать комплексное программное обеспечение для контроля действий пользователей, информационных потоков и событий системы.

- *Распространенные уязвимости программного обеспечения*

Уязвимости — это ошибки программного обеспечения (ПО), которые позволяют злоумышленникам получить непосредственный доступ к коду программного продукта, настройкам, конфигурации и т. д. Ошибки могут присутствовать во всех типах ПО. Браузер, в котором вы читаете данную заметку, неважно Google Chrome это, Firefox или что-то другое, может содержать ошибки. Аналогично любая операционная система не лишена различных уязвимостей, о которых разработчик, возможно, и не догадывается.

К сожалению, даже тщательная разработка не гарантирует отсутствие ошибок в программном продукте. Уязвимости могут появиться вследствие задействования сторонних компонентов или свободно распространяемого кода (open source). Такие компоненты чаще всего используются «как есть», без углубленного тестирования на безопасность.

Многие компании предпочитают не откладывать обозначенную дату публикации продукта, выпускают первоначальную версию, собирают отзывы и на их основе вносят исправления, в том числе, касающиеся безопасности. Случается, что программисты просто не успевают внести исправления к определенному сроку.

Поддержка старых версий программных продуктов рано или поздно заканчивается, перестают выходить патчи, а далеко не каждый пользователь спешит приобрести новую разработку, пользуясь привычным функционалом. Это дает злоумышленникам шанс найти уязвимости в старом ПО, даже если более новые версии уже не имеют таких недостатков.

Уязвимости в зависимости от стадии появления возникают при проектировании, в процессе реализации, в конфигурации аппаратной части и программной среды.

Сложнее всего обнаружить уязвимости, допущенные на этапе проектирования. Это могут быть ошибки алгоритмов, несогласованность протоколов взаимодействия функционала и аппаратной части, использование неоптимальных технологий. Даже при своевременном обнаружении устранение таких уязвимостей весьма трудоемко, так как может потребоваться значительная переработка продукта и соответственно это приведет к срыву сроков. Существует риск замалчивания проблем, откладывания их устранения, а тем временем «плохие парни» получают реальный шанс подзаработать.

Уязвимости реализации возникают при написании кода программы и внедрении в нее алгоритмов безопасности. Их обнаружение и исправление также занимает немало времени и влечет за собой риски, упомянутые выше.

Довольно часто встречаются ошибки конфигурации аппаратной части и программного обеспечения, что влечет за собой сбои в работе продукта, большую вероятность утери данных. К этой категории ошибок также можно отнести слишком простые пароли и использование первоначальных учетных записей (по умолчанию), оставленных без изменений.

Знакомо ли вам понятие уязвимости нулевого дня? Этот термин используется в отношении ошибок в программном коде, не найденных разработчиками на этапе тестирования. Сюда же можно отнести вредоносные программы, вирусы, сетевые черви, боты и трояны, против которых еще не разработана какая-либо защита.

Когда происходит атака с нулевым днем — это означает, что у разработчиков не было времени, чтобы справиться с этой проблемой, прежде чем ее начали использовать. Однако злоумышленники, обнаружившие «баг», успели придумать способ его применения, создали вирус и начали вредить. Программное обеспечение остается уязвимым для атаки до тех пор, пока не будет выпущено обновление. К тому же пользователям тоже необходимо время для обновления ПО, а это может занять дни и даже месяцы.

Свежий список наиболее распространенных уязвимостей традиционно публикуется на сайте Common Weakness Enumeration (CWE). Данный перечень

представляет собой официальный реестр или словарь общих дефектов безопасности, способных проявиться в архитектуре, проектировании, коде продукта, и теоретически могут быть использованы злоумышленниками. Рейтинг CWE Top 25, позволяет разработчикам сократить количество слабых мест в своем программном обеспечении.

- Пользователи могут минимизировать влияние уязвимостей и предупредить возможный ущерб, придерживаясь, как минимум, следующих правил:
- Своевременно устанавливать выпускаемые разработчиками исправления (патчи) для приложений или настроить автоматическое обновление (при наличии возможности);
- Не устанавливать программы, качество которых вызывает сомнения;
- Использовать антивирусное программное обеспечение с актуальными базами данных.

Вопросы

1. При каких условиях компания может создать надежную систему безопасности?
2. Зачем защищать данные?
3. Что такое информационная безопасность?
4. Основные угрозы безопасности данных.
5. Перечислите правила защиты информации.
6. Что такое уязвимости?
7. Какие уязвимости сложнее всего обнаружить?
8. Что такое уязвимость нулевого дня?

❿Личная информация и приватность

В эпоху цифровых технологий, когда большая часть нашей жизни переместилась в онлайн-пространство, вопросы защиты личной информации и приватности становятся критически важными, особенно для молодого поколения, вступающего в мир цифровых возможностей. Студенты, активно использующие интернет для учебы, общения и развлечений, подвергаются повышенному риску стать жертвами киберпреступлений. Понимание основ кибербезопасности и ответственное отношение к личным данным – это не просто желаемый навык, а жизненно необходимый навык.

Что такое личная информация в цифровом контексте? Это не только имя, адрес и номер телефона, но и история поисковых запросов, публикации в социальных сетях, геолокация, данные банковских карт и множество других цифровых следов, которые мы оставляем в сети. Все эти данные могут быть использованы злоумышленниками для кражи личных данных, шантажа, мошенничества и других незаконных действий.

Осознание ценности своей личной информации – первый шаг к ее защите. Студентам необходимо понимать, какие данные они предоставляют онлайн, с кем они ими делятся и как эти данные могут быть использованы. Критическое мышление, осознанность и скептическое отношение к сомнительным ссылкам и предложениям – ключевые элементы цифровой грамотности.

Помимо теоретических знаний, важную роль играет практическое применение основ кибербезопасности. Внедрение двухфакторной аутентификации, использование надежных паролей, регулярное обновление программного обеспечения и осознанное использование социальных сетей – это лишь некоторые из мер, которые могут значительно повысить уровень защиты личной информации.

Защита личной информации и приватности – это непрерывный процесс, требующий постоянного обучения и адаптации к новым угрозам. Формирование основ кибербезопасности у студентов – это инвестиция в их

будущее, обеспечивающая им безопасное и осознанное использование цифровых технологий.

Образовательные учреждения играют ключевую роль в формировании культуры кибербезопасности среди студентов. Интеграция курсов по кибербезопасности в учебные программы, проведение семинаров и тренингов, организация интерактивных занятий и игровых симуляций – все это способствует развитию критического мышления и практических навыков в области защиты личных данных. Важно не только рассказывать о рисках, но и показывать конкретные примеры киберпреступлений и их последствий, а также обучать эффективным методам защиты.

Не менее важным является создание поддерживающей среды, в которой студенты могут свободно обсуждать вопросы кибербезопасности и обращаться за помощью в случае возникновения проблем. Организация студенческих клубов и сообществ, посвященных кибербезопасности, позволяет обмениваться опытом, участвовать в тематических мероприятиях и получать поддержку от экспертов.

Защита личной информации и приватности – это не только индивидуальная ответственность, но и коллективная задача. Студенты, осознающие риски и умеющие принимать меры предосторожности, становятся агентами позитивных изменений, распространяя знания и навыки среди своих сверстников и способствуя формированию более безопасного цифрового пространства.

Формирование основ кибербезопасности у студентов – это необходимый и своевременный шаг для обеспечения их защиты в цифровом мире. Это требует комплексного подхода, включающего образовательные инициативы, развитие практических навыков, создание поддерживающей среды и осознание личной ответственности. Только так мы сможем подготовить поколение, способное безопасно и эффективно использовать цифровые технологии.

Приватность — многозначный термин, мы ограничимся ее пониманием как личной жизни человека, его частной сферы. В нее входят телесность,

эмоции, отношения с родственниками, друзьями и сексуальными партнерами, предпочитаемое времяпрепровождение, внешний вид и одежда, выбор жизненного пути, личная история, идентичность и многое другое. Растущее проникновение цифровых технологий вызывает следующие риски для автономии и приватности:

Личности сложнее скрыться от нежелательного внимания со стороны

Существуют риски утечки данных и их несанкционированного оборота.

Информация о человеке может быть использована в коммерческих целях, в дальнейшем заинтересованные лица могут целенаправленно нарушать автономию личности.

Люди предпочитают защищать свою частную сферу от вторжений. Речь идет не только о защите от прямого вмешательства, например в виде переселения в другое жилье или, скажем, принудительных медицинских процедур. Чаще всего люди хотят, чтобы частная сфера была закрыта от внимания посторонних, информация об их личности и частной жизни оставалась тайной или хотя бы не распространялась бесконтрольно. Контроль за распространением информации о себе и своей частной жизни — неотъемлемый элемент приватности.

Цифровые технологии обострили вопрос о защите информации о частной жизни. Это в первую очередь вызвано тем, что в цифровой среде информация о частной жизни (как, впрочем, и любая другая) распространяется гораздо шире и гораздо быстрее, чем раньше. Кроме того, технологии позволяют фиксировать такой объем сведений о личности, который раньше невозможно было представить, а его обработка дает возможность сделать такие выводы о человеке и его жизни, которые он сам не в состоянии сделать. Контролировать распространение и использование информации о себе и таким образом защищать свою частную сферу от вторжений становится сложнее. Риски нарушения приватности растут. Почему эти риски так беспокоят? Причин несколько:

Данные о человеке и его частной жизни могут быть использованы злоумышленниками, например чтобы похитить его имущество, обманом выманить его деньги, или спланировать нападение на него. Именно поэтому утечки данных о людях — клиентах какого-то сервиса или просто лицах, учтенных в каком-то регистре — одна из ключевых угроз, связанных с цифровыми технологиями. Всякий раз, когда государственный орган, или учреждение, или негосударственная структура запрашивают у гражданина данные, ему необходимо задаваться вопросами: какие гарантии дают операторы данных, какие меры защиты они предпринимают, какие формы ответственности и перед кем предусмотрены за утечки, не избыточен ли набор собираемых данных.

Разглашение приватных сведений может повлиять на положение человека в обществе. Как социальному существу, человеку важны отношение и реакции других людей: одобрение или осуждение, восхищение или насмешки, репутация и пр. Для того чтобы получить поддержку от референтной группы, человек будет стараться вести себя таким образом, который этой группой одобряется. Если при этом человек предпочитает что-то неодобряемое референтной группой, он может следовать своим предпочтениям в частной сфере: на работе носить костюм с иголочки, а дома ходить неряхой. Кроме того, пользуясь покровом приватности, человек может реализовывать разные стороны своей личности в разных сообществах: в одном быть серьезным ученым, а в другом — писателем фанфиков. Однако такая стратегия перестает работать в ситуации, когда человек не может контролировать распространение информации о своей частной жизни, когда возможности агрегировать и анализировать информацию о человеке делают частную жизнь прозрачной.

Вопросы.

1. Что такое личная информация в цифровом контексте?
2. Назовите способы защиты личной информации и приватности?
3. Дайте определение приватности?

4. Назовите примеры прямого вмешательства.

Лабораторная работа №1 «Вредоносное программное обеспечение»

Цель работы: ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методы борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Проверка настроек антивирусов, сканирование файлов, папок и дисков, обновления антивирусной базы. Получить навыки работы с антивирусным пакетом Антивирус Касперского.

Теоретические сведения представлены (в виде видеоматериала и лекции) на сайте:

Задание 1.

Подготовить доклад на тему: «Общие сведения и особенности работы антивирусной программы [Название антивирусной программы]” (Название антивирусной программы выбрать согласно своему варианту из вариантов заданий к работе).

Задание 2.

Изучить антивирусный пакет Антивирус Касперского. Подготовить отчет по лабораторной работе.

Порядок выполнения

1). Сканирование папок на наличие вирусов:

- Двойным щелчком на значке антивируса на панели индикации открыть главное окно программы;
- Изучитьсодержимое окна: обратить внимание на дату последнего обновления антивирусной базы и дату последней полной проверки компьютера;

- В своей личной папке создать папку **Подозрительные файлы** и создать там 2 файла: **Текстовый файл** и Документ Microsoft Word. Имена файлов ввести согласно своему варианту по **Вариантам задания к работе**;
- Выбрав пункт в главном окне программы пункт **Проверка – Быстрая проверка** и добавить в окно заданий папку **Подозрительные файлы.**
- Выполнить проверку папки. По завершению сканирования, использую кнопку «Отчеты» - «Сохранить как…», сохранить отчет с результатами проверки в папке Подозрительные файлы. Имя файла-отчета – Scan_Log.

2). Обновление антивирусной базы:

- Нажмите на пункт **Обновление** и, используя кнопку **Обновить,** осуществите обновление базы известных вирусов.
- По завершению обновления, используя кнопку **«Отчеты» - «Сохранить как…»**, сохранить отчет об обновлении в папке **Подозрительние файлы. Имя файла**- отчета – **Upd_Long.**
- Закройте окно **Антивируса Касперского.**

Задания 3.

Изучить антивирусный пакет **Avast!**

Порядок выполнения;

1. Найдите иконку антивируса Avast! В системном трее, правой кнопкой мышки вызовите меню и выберите «Открыть интерфейс пользователя Avast!»
2. Перейдите на вкладку «Сканировать компьютер». Вам будет представлены 4 вида сканирования: Экспресс, Полное, Сканирование носителей и возможность выбрать папку для сканирования вручную.
3. Выберите «Сканирование съемных носителей» и нажмите кнопку «Пуск» в окне антивируса – будут автоматически проверены все подключенные к компьютеру съемные носители (диски, флэшки, дискеты).

4. По завершении сканирования выберите четвертый вид сканирования и вручную укажите любую папку на вашем съемном носителе и проверьте ее.
5. Во вкладке «Экраны в реальном времени», в подменю «Экран файловой системы» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:
   - Сканировать программы при выполнении (например, программа excel.exe будет сканироваться при каждом выполнении Microsoft Excel)
   - Сканировать сценарии при выполнении (например, файл JS (JavaScript) будет сканироваться при каждом его выполнении)
   - Сканировать библиотеки (DLL) при загрузке (при выполнении программы будут сканироваться её вспомогательные файлы – библиотеки DLL и т.д.)
6. Во вкладке «Экраны в реальном времени», в подменю «Веб-экран» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:
   - Включить веб-сканирование
   - Использовать интеллектуальное сканирование потока
7. Во вкладке «Обслуживание» в подменю «Обновить» есть возможность ручного запуска обновлений для «Модуля сканирования и определения вирусов» и непосредственно для программы. (По умолчанию модуль обновляется автоматически, а обновление программы запрашивает разрешения пользователя).
8. По завершению сканирования, используя кнопку «Отчеты» «Сохранить как…», сохранить отчет с результатами проверки

Задание 4.

Изучить антивирусный пакет **Dr. Web CureIt**

1. При запуске этого портативного антивируса вам будет предложено запустить его в режиме усиленной защиты – он необходим в случае, если

вредоносные программы блокируют работу операционной системы. Нажмите «Отмена».

2. Далее появится предупреждение, т.к. использование антивируса бесплатно доступно только для лечения домашних компьютеров. Нажмите «Нет».
3. Нажмите «Пуск» и будет автоматически запущены быстрая проверка компьютера. В этом режиме проверяются:
   - Оперативная память
   - Загрузочные секторы всех дисков
   - Объекты автозапуска
   - Корневой каталог загрузочного диска
   - Корневой каталог диска установки Windows
   - Системный каталог Windows
   - Папка Мои Документы
   - Временный каталог системы
   - Временный каталог пользователя
4. По окончании быстрой проверки выбрать в меню пункт «Выборочно» и указать путь к съемному носителю – выполнить его проверку.
5. По завершению сканирования, используя кнопку «Отчеты» - «Сохранить как…», сохранить отчет с результатами проверки

Содержание отчета

1). Название и цель лабораторной работы;

2). Доклад на выбранную по варианту тему;

3). Содержимое файла Scan_Log.txt по пункту 1 Порядка выполнения работы

4). Содержание файла Upd_Log.txt по П.2 Порядка выполнения работы.

5). Выводы.

Контрольные вопросы

1). Что называется компьютерным вирусом?

2). Какая программа называется "зараженной"?

3). Что происходит, когда зараженная программа начинает работу?

4). Как может маскироваться вирус?

5). Каковы признаки заражения вирусом?

6). Каковы последствия заражения компьютерным вирусом?

7). По каким признакам классифицируются компьютерные вирусы?

8). Как классифицируются вирусы по среде обитания?

9). Какие типы компьютерных вирусов выделяются по способу воздействия?

10). Что могут заразить вирусы?

11). Как маскируются "невидимые" вирусы?

12). Каковы особенности самомодифицирующихся вирусов?

13). Какие методы защиты от компьютерных вирусов можно использовать?

14). В каких случаях применяют специализированные программы защиты от компьютерных вирусов?

15). На какие виды можно подразделить программы защиты от компьютерных вирусов?

16). Как действуют программы-детекторы?

17). Что называется сигнатурой?

18). Всегда ли детектор распознает зараженную программу?

19). Каков принцип действия программ-ревизоров, программ-фильтров, программ- вакцин?

20). Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?

21). Перечислите меры защиты информации от компьютерных вирусов.

22). Каковы современные технологии антивирусной защиты?

23). Каковы возможности антивируса Касперского для защиты файловых серверов? почтовых серверов?

24). Какие модули входят в состав антивируса Касперского для защиты файловых систем?

25). Каково назначение этих модулей?

26). Какие элементы электронного письма подвергаются проверке на наличие

вирусов?

27). Как обезвреживаются антивирусом Касперского обнаруженные подозрительные или инфицированные объекты?

28). Как обновляется база вирусных сигнатур?

Варианты заданий к работе

Вариант	Название антивирусной программы	Название файла
1	Dr.Web	Test_01_01.txt Test_02_01.doc
2	McAfee VirusScan	Test_01_02.txt Test_02_02.doc
3	Антивирус Касперского	Test_01_03.txt Test_02_03.doc
4	Panda Anti-Virus	Test_01_04.txt Test_02_04.doc
5	Avast!	Test_01_05.txt Test_02_05.doc
6	AVS	Test_01_06.txt Test_02_06.doc
7	AVG	Test_01_07.txt Test_02_07.doc
8	Avira	Test_01_08.txt Test_02_08.doc
9	Clam AntiVirus	Test_01_09.txt Test_02_09.doc
10	ClamWin	Test_01_10.txt Test_02_10.doc
11	NOD32	Test_01_11.txt Test_02_11.doc
12	Trojan Hunter	Test_01_12.txt Test_02_12.doc
13	VirusBuster	Test_01_13.txt Test_02_13.doc
14	Norton AntiVirus	Test_01_14.txt Test_02_14.doc
15	Windows Live OneCare	Test_01_15.txt Test_02_15.doc
16	PC-cillin	Test_01_16.txt Test_02_16.doc
17	F-Prot	Test_01_17.txt Test_02_17.doc
18	F-Secure Anti-Virus	Test_01_18.txt Test_02_18.doc
19	Comodo AntiVirus	Test_01_19.txt Test_02_19.doc

Лабораторная работа №2 «Угрозы и обеспечение информационной безопасности компьютерных систем»

Цель работы: Изучить основные виды вирусных угроз и механизмы их поведения. Изучить и охарактеризовать дополнительные средства и технологии защиты компьютера от вредоносных программ. Рассмотрите, изученные средства и технологии на Вашем ПК (с учетом браузера и операционной системы).

Порядок выполнения работы:

1. Изучить основные виды вирусных угроз и механизмы их поведения.
2. Данные систематизируйте в таблице.

№	**Название группы вирусов**	**Разновидности**	**Механизм порчи информации**	**Рекомендуемые средства защиты**
11	Черви	1..... 2..... 3.....		
2	Трояны			
3	Баннеры			
4	Спам			
5	Фишинг			
6	Ложные антивирусы			
7	Потенциально нежелательные программы			

8	Spyware			

3. Изучить и охарактеризовать дополнительные средства и технологии защиты компьютера от вредоносных программ. Рассмотрите, изученные средства и технологии на Вашем ПК (с учетом браузера и операционной системы).
4. Данные систематизируйте в таблице.

№	**Технология**	**Общая характеристика**	**Как работает на Вашем ПК**
1	Веб-защита браузеров (Web and Browser protection)		
2	Контроль плагинов (Plugin Control)		
3	Фильтры URL-адресов, блокировка рекламы (Domain and URL Filters, Blocking Ads		
4	Виртуализация браузера (Browser Virtualization)		
5	Браузерный и поисковый помощник, анти-фишинг (Browser and Search Advisor, Anti-phishing)		
6	Родительский контроль (Parental Control)		
7	Анти-спам (Anti-spam)		
8	Обновления (Updates)		

Лабораторная работа №3 «Исследование методов защиты беспроводной связи Bluetooth»

Цель лабораторной работы: Ознакомление с методами защиты

терминала беспроводной связи Bluetooth в системе Android.

Перед выполнением лабораторного задания студенты должны ориентироваться в основных аспектах информатики и иметь основные понятия о функционировании системы беспроводной связи Bluetooth и используемых методах защиты информации.

В результате выполнения лабораторного задания студенты должны получить навыки обеспечения защиты терминала беспроводной связи Bluetooth в системе Android.

Теоретические сведения.

В данной работе рассматриваются средства безопасности, используемые при передаче информации посредством технологии Bluetooth.

Bluetooth − технология беспроводной передачи данных по радиоканалу между различными типами электронных устройств с целью обеспечения их взаимодействия.

При разработке Bluetooth-интерфейса выдвигались следующие требования: аппаратура должна быть компактной, недорогой и экономичной, т. е. должна быть способна работать при малых значениях потребляемого тока.

Система Bluetooth позволяет объединять в одну беспроводную пикосеть (piconet) от двух до восьми различных электронных устройств, таких как, например, сотовый телефон, беспроводная гарнитура, ноутбук, цифровой фотоаппарат, принтер, клавиатура и др., но общее количество объединяемых устройств (как результат объединения пикосетей) может достигать 71.

По сравнению с интерфейсом беспроводной связи IEEE 802.11, работающим в том же диапазоне частот − 2,4 ГГц, Bluetooth-система обеспечивает меньшую скорость передачи информации (721 Кбит/с против 11 Мбит/с в стандарте IEEE 802.11b), меньшую дальность и меньшее число объединяемых в сеть устройств (максимально до 71 устройства у Bluetooth, 128 на одну сеть у IEEE 802.11). Но система Bluetooth может по трем каналам

передавать голосовую информацию, а главное, более дешева (в десятки раз), малогабаритна и экономична.

Bluetooth способна осуществлять передачу данных даже при наличии препятствий и не только по принципу «точка−точка», но и по принципу «точка−много точек», что в положительную сторону отличает Bluetooth от технологии беспроводной инфракрасной связи IrDa, которая обеспечивает связь лишь в зоне прямой видимости и только по принципу «точка−точка».

Информационная безопасность системы беспроводной передачи данных Bluetooth

Конкретные средства обеспечения безопасности мобильного терминала зависят от конкретного терминала, наличия или отсутствия в нем предустановленной операционной системы и типа операционной системы, используемой в данном терминале.

Информационная безопасность системы беспроводной передачи данных Bluetooth базируется на использовании частотных шаблонов и необходимости синхронизации процессов приема и передачи данных, возможности реализации односторонней или двусторонней аутентификации, а также на шифровании передаваемых данных. Длина ключа шифрования может варьироваться от 8 до 128 бит, что дает возможность регулировать криптостойкость используемого алгоритма шифрования.

Хотя в Bluetooth предусмотрена криптографическая защита конфиденциальности передаваемых данных, а также процедура аутентификации, предназначенная для защиты от несанкционированного доступа к системе, возможны нарушения информационной безопасности устройств, снабженных Bluetooth.

Через Bluetooth-интерфейс возможна реализация следующих трех основных угроз информационной безопасности связи:

- проникновение в абонентский аппарат мобильных вирусов и связанные с этим угрозы потери конфиденциальности передаваемой информации,

а также целостности, доступности и конфиденциальности информации, хранящейся в абонентском аппарате;

- перехват информации, передаваемой по радиоканалу системы Bluetooth;
- дистанционный перехват управления абонентским аппаратом, позволяющий злоумышленнику осуществлять звонки и/или отсылку SMS и MMS сообщений за счет законного владельца аппарата, изменять настройки аппарата, считывать информацию, хранящуюся в памяти аппарата.

Защита от атак на систему беспроводной передачи данных Bluetooth.

Технология Bluetooth предполагает выполнение 6-ти основных рекомендаций по ее безопасному использованию:

1) не следует оставлять систему Bluetooth включенной постоянно, включать Bluetooth рекомендуется только при необходимости (особенно опасно держать Bluetooth включенным в общественных местах: метро, торговых центрах, на вокзалах, в аэропортах и т. п.);
2) обязательным требованием является использование парольной защиты; рекомендуется использовать при соединении более длинные PIN-коды, чем четырехзначный код, желательно не менее, чем из восьми символов;
3) необходимо внимательно отслеживать сообщения системы о запросе устройств на подключение по каналу Bluetooth и разрешать подключение только, если есть уверенность в его безопасности;
4) осуществлять контроль за использованием устройств с Bluetooth-системой для подключения к локальным Wi-Fi сетям, так как их использование может быть эквивалентом созданию непредусмотренных дополнительных беспроводных точек входа в защищенную сеть;
5) соблюдать осторожность при соединении устройств, особенно в общественных местах, где выполнение «паринга» вообще нежелательно;

6) использовать защищенные от обнаруженных уязвимостей обновления программного обеспечения для устройств, использующих Bluetooth.

Рекомендация использовать достаточно длинные (не менее восьми символов) персональные идентификационные коды (PIN-коды) связана с тем, что PIN-коды используются при установлении шифрованной связи между Bluetooth-устройствами. Это является существенной уязвимостью в спецификации Bluetooth. Если атакующий имеет возможность контролировать канал связи во время работы соединенных Bluetooth-устройств, а значит, перехватывать и записывать процесс соединения устройств, то он достаточно легко может определить короткие PIN-коды.

Наиболее вероятна реализация угрозы прослушивания радиоканала Bluetooth в общественных многолюдных местах, поэтому, по возможности, в таких местах следует избегать соединения Bluetooth-устройств.

Особого внимания требует ситуация, когда ранее соединенные устройства неожиданно требуют нового соединения − это может быть атака с попыткой инициировать соединение с целью наблюдения за информационным обменом. Для этого атакующий посылает подложное сообщение, выдавая себя за известное устройство и утверждая, что PIN-код забыт. В результате Bluetooth- устройство, получившее запрос на соединение, пытается повторить соединение, но теперь уже под контролем атакующего.

Если имеется возможность контролировать процесс установления соединения, то атакующий может вклиниться в обмен PIN-кодами и определить PIN-код с целью его последующего использования.

Лабораторное задание.

При подготовке к лабораторному занятию следует предварительно изучить: методы передачи информации посредством технологии Bluetooth, основные угрозы безопасности Bluetooth и методы защиты.

1. Включить Bluetooth на двух или более смартфонах, используя их меню.
2. Включить режим обнаружения расположенных вблизи устройств Bluetooth.

3. Выбрать файл данных для его передачи с использованием технологии Bluetooth.
4. Выбрать получателя для передачи данных.
5. Произвести процедуру «спаривания» передающего и принимающего терминалов.
6. Передать файл.
7. Удостовериться в получении файла противоположной стороной.

Порядок выполнения задания.

При выполнении задания рекомендуется соблюдать следующую последовательность:

1. Изучить методические указания к данному лабораторному занятию.
2. Выполнить лабораторную часть.
3. Ответить на контрольные вопросы.

Содержание отчета.

1. Краткие теоретические сведения по методам кодовой защиты мобильного терминала.
2. Выполненное задание.

Контрольные вопросы.

1. Что такое технология Bluetooth?
2. Какие технические особенности технологии Bluetooth можно выделить?
3. Какие средства безопасности предусмотрены в технологии Bluetooth?
4. Сколько основных угроз и какие возможны при Bluetooth-связи?
5. Сколько основных рекомендаций и какие следует выполнять при Bluetooth-связи?

Лабораторная работа №4«Количественная оценка стойкости парольной защиты»

Цель работы: реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Теоретические сведения.

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации являются одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя, как правило, передний край обороны СЗИ. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель последнего в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя наиболее просты и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю:

1) минимальная длина пароля должна быть не менее 6 символов;
2) пароль должен состоять из различных групп символов (малые и

большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.);

3) в качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации:

1) администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, пароль следует сменить;
2) в подсистеме парольной аутентификации необходимо установить ограничение числа попыток ввода пароля (как правило, не более трёх);
3) в подсистеме парольной аутентификации требуется установить временную задержку в случае ввода неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля: если пароль состоит только из малых английских букв, то $A = 26$), L – длина пароля, $S = A^L$–число всевозможных паролей длины L, которые можно со- ставить из символов алфавита A, V – скорость перебора паролей злоумышленником, T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течение срока его действия V

определяется по следующей формуле:

$$P = (V \cdot T) / S = (V \cdot T) / A^L.$$

Эту формулу можно использовать в обратную сторону для решения следующей задачи.

Задача. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных V, T, P однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

$$S^* = [V \cdot P / T], \qquad (1)$$

,где [] – целая часть числа, взятая с округлением вверх.

После определения нижней границы S^* необходимо выбрать такие A и L для формирования $S = A^L$, чтобы выполнялось следующее неравенство:

$$S^* \leq S = A^L. \qquad (2)$$

При выборе S, удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P.

Следует отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример. Исходные данные: $P = 10^{-6}$, T = 7 дней = 1 неделя, V = 10 (паролей / минуту) = $10 \cdot 60 \cdot 24 \cdot 7 = 100800$ паролей в неделю. Тогда, $S^* = [(10800 \cdot 1) / 10^{-6}] = = 108 \cdot 10^8$.

Условию $S^* \leq A^L$ удовлетворяют, например, такие комбинации A и L, как A = 26, L = 8 (па- роль состоит из восьми малых символов английского алфавита), A = 36, L = 6 (пароль состоит из шести символов, среди которых могут быть малые латинские буквы и произвольные цифры).

Задание на лабораторную работу

1. В табл. 3 найти для указанного варианта значения характеристик *P, V, T*.
2. Вычислить по формуле (1) нижнюю границу *S** для заданных *P, V, T*.
3. Выбрать некоторый алфавит с мощностью *A* и получить минимальную длину пароля *L*, при котором выполняется условие (2).
4. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины *L*, при этом должен использоваться алфавит из *A* символов.
5. Оформить отчет по лабораторной работе .

Коды символов:

1. Коды английских символов : «A» = 65, …, «Z» = 90, «a» = 97,…, «z» = 122.
2. Коды цифр : «0» = 48, «9» = 57.
3. «!» = 33, «“» = 34, «#» = 35, «$» = 36, «%» = 37, «&» = 38, «‘» = 39.
4. Коды русских символов : «А» – 128, … «Я» – 159, «а» – 160,…, «п» – 175, «р» – 224,…, «я» – 239.

Таблица 8. Варианты заданий

Вариант	P	V	T
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	110^{-6}	20 паролей/мин	3 недели
8	110^{-7}	15 паролей/мин	20 дней
Вариант	P	V	T

9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/день	5 дней
14	10^{-5}	20 паролей/мин	6 дней
15	10^{-6}	15 паролей/мин	12 дней
16	10^{-7}	3 паролей/мин	1 месяц
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней
23	10^{-6}	3 паролей/мин	5 дней
24	10^{-7}	10 паролей/мин	6 дней
25	10^{-4}	11 паролей/мин	12 дней
26	10^{-5}	100 паролей/день	1 месяц
27	10^{-6}	10 паролей/день	3 недели
28	10^{-7}	20 паролей/мин	20 дней
Вариант	P	V	T
29	10^{-4}	15 паролей/мин	15 дней
30	10^{-5}	3 паролей/мин	1 неделя

Контрольные вопросы

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Перечислить минимальные требования к выбору пароля.
3. Перечислить минимальные требования к подсистеме парольной аутентификации.
4. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?
5. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Лабораторная работа №5 «Успешность реализации политики безопасности»

Цель лабораторной работы: Выработка навыков выполнения мероприятий по защите информации

Теоретические сведения

Хорошо известно, что безопасность настолько сильна, насколько защищено ее самое слабое звено. Практика защиты информации показывет, что сотрудников отечественных компаний часто оказывается легче обмануть или ввести в заблуждение, чем системы или технологии безопасности. Поэтому правильно организованное обучение и учет человеческого фактора является необходимой составляющей процесса разработки политики безопасности. Давайте на примере компании Cisco Systems рассмотрим следующие семь пунктов успешной программы реализации политики безопасности, которые объединяют большинство возможных подходов по информированию, вовлечению и задействованию сотрудников компании к решению данной проблемы.

- Понимание необходимости защиты информации

Сотрудники, партнеры и клиенты, обладающие правами доступа к информационным активам и сервисам компании, должны быть

надлежащим образом проинформированы о необходимости обеспечения информационной безопасности. При этом каждый сотрудник компании должен знать, что он должен делать для создания и поддержания требуемого режима информационной безопасности.

- Обучение и информирование сотрудников компании

Новые сотрудники компании должны быть проинформированы о правилах политики безопасности и должны понимать ту важную роль, которую они играют в поддержании режима информационной безопасности. Каждый сотрудник должен быть ознакомлен с тем, что он должен и может делать для усиления и эффективности режима информационной безопасности. В связи с тем, что правила политики безопасности время от времени изменяются сотрудники должны быть своевременно проинформированы о всех текущих изменениях. Также, хорошей идеей является выпуск периодических напоминаний о правилах безопасности для поддержания осведомленности сотрудников компании на должном уровне.

- Персональная ответственность каждого сотрудника

Рекомендуется разделить правила политики безопасности на небольшие документы, каждый из которых должен содержать не больше одной страницы. Таким образом элементы политики безопасности будут затрагивать сотрудников индивидуально, т.е. сотрудники компании будут изучать только те правила политики безопасности, которые применимы к ним. Например, это могут быть правила создания и использования паролей, токенов, других средств систем контроля доступа, правила использования электронной почты и т.д.

- Юридическая ответственность сотрудников компании

После публикации новой или изменения существующей политики безопасности компании, все сотрудники компании должны подписаться под следующим предложением: "Ознакомлен и обязуюсь выполнять требования этого документа". Эти соглашения позволят сотрудникам

компании стать ответственными за выполнение требуемого режима информационной безопасности. При приеме на работу новые сотрудники компании также должны подписывать соглашения об обязательности выполнении требований политики безопасности. При изменении служебных обязанностей сотрудников документы должны быть пересмотрены и подписаны заново. Здесь основная идея заключается в том, чтобы сделать сотрудников компании юридически ответственными за надлежащее выполнение режима информационной безопасности.

- Закрепление ответственности сотрудников компании

В политиках безопасности компании должны быть четко прописано, что произойдет, если сотрудник намеренно или непреднамеренно нарушит требования политики безопасности. Последствия должны быть четко оговорены и должны доводить до сознания сотрудника, что они серьезны и "настоящие".

- Согласованность во взглядах

Иногда строгие правила политики безопасности и ограничивающие средства защиты хуже, чем слабые политики и слабо ограничивающие средства защиты, потому, что они, скорее всего, будут игнорироваться сотрудниками компании. При формулировании политики безопасности компании важно уметь слышать мнение сотрудников и руководства для поиска надлежащего баланса между производительностью, доступностью, удобством работы и безопасностью. Открытость к диалогу, желание найти баланс - ключевые факторы успеха в создании и внедрении реально выполняемой политики безопасности компании.

- Создание корпоративной культуры безопасности

Рядовые сотрудники компании часто являются первыми, кто замечает странные или экстраординарные события и начальные признаки атак в корпоративной информационной системе. Если удается вовремя донести до сознания сотрудников мысль о том, что обеспечение безопасности информационных активов компании является необходимой

составляющей повседневной деятельности, то сотрудники будут сами информировать службу безопасности о потенциальных угрозах и нарушениях политики безопасности до того, как атаки достигнут своей цели. Активно привлекая сотрудников компании в процесс обеспечения безопасности можно заметно улучшить общее состояние защищенности информационных активов компании и повысить культуру безопасности в компании.

Примеры политик безопасности:

Прежде, чем мы начнем рассматривать примеры политик безопасности компании - немного о проблеме доверия.

- Кому и что доверять

От правильного выбора уровня доверия к сотрудникам компании зависит успех или неудача реализации политики безопасности компании. При этом слишком большой уровень доверия может привести к возникновению проблем в области безопасности, а слишком малое доверие может заметно затруднить работу сотрудника компании, вызвать у него недоверие, и даже увольнение. Насколько можно доверять сотрудникам компании? Обычно используют следующие модели доверия.

- Доверять всем и всегда - самая простая модель доверия, но к сожалению не практичная.

- Не доверять никому и никогда - самая ограниченная модель доверия и также не практичная.
- Доверять избранным на время - модель доверия подразумевает

определение разного уровня доверия на определенное время. При этом доступ к информационным ресурсам компании предоставляется по необходимости для выполнения служебных обязанностей, а средства контроля доступа используются для проверки уровня доверия к сотрудникам компании.

- Вряд ли существует компания, в которой следуют модели

доверия "доверять всем и всегда". В сегодняшнем мире это мало возможно. То же самое относится и ко второй модели доверия" не доверять никому и никогда" (этой модели доверия часто стараются следовать в правительственных и военных организациях). Поэтому самая реалистичная модель доверия должна доверять некоторым из сотрудников компании на некоторое время.

Задание

Создать план мероприятий по обеспечению комплексной безопасности обучающихся в колледже.

ПРИЛОЖЕНИЕ Б

Блок 1. Парольная политика и доступ (1-8 вопросы)

1. Какая длина пароля считается минимально безопасной в 2026 году? (12 символов)
2. Что такое «Passkeys»? (Беспарольная технология аутентификации на основе биометрии/ключей устройства)
3. Безопасно ли использовать один пароль для почты и игрового сервиса? (Нет, из-за риска «атаки перебором»)
4. Зачем нужна двухфакторная аутентификация (2FA)? (Второй барьер, если основной пароль украден)
5. Где безопаснее всего хранить пароли? (В специализированных менеджерах паролей)
6. Как часто нужно менять пароли при отсутствии утечек? (По мере необходимости, если пароль стал слабым или скомпрометирован)
7. Является ли дата рождения в сочетании с именем надежным паролем? (Нет)
8. Какую опасность несет функция «Запомнить пароль» на общественном компьютере? (Доступ любого следующего пользователя к аккаунту)

Блок 2. Социальная инженерия и Фишинг (9-18 вопросы)

9. Что такое фишинг? (Вид мошенничества с целью выманивания данных через поддельные сайты/сообщения)
10. Признак фишингового URL-адреса? (Ошибки в написании домена, например, `g00gle.com` вместо `google.com`)
11. Что делать, если «друг» в мессенджере просит срочно проголосовать в конкурсе по ссылке? (Связаться с ним другим способом, это может быть взлом)

12. Как распознать телефонного мошенника, использующего подмену номера? (Задать личный вопрос, ответ на который знает только настоящий человек)
13. Что такое «квишинг» (Quishing)? (Фишинг через вредоносные QR-коды)
14. Безопасно ли перезванивать на незнакомые пропущенные номера? (Нет, возможна платная тарификация или социальная инженерия)
15. Может ли сотрудник банка запрашивать код из СМС? (Категорически нет)
16. Что делать при получении письма о «выигрыше», в котором нужно оплатить комиссию за перевод? (Удалить письмо, это мошенничество)
17. Что такое «вишинг»? (Голосовой фишинг по телефону)
18. Как проверить подлинность письма от госорганов? (Проверить наличие уведомления в личном кабинете «Госуслуг»)

Блок 3. Безопасность в сетях и Wi-Fi (19-25 вопросы)

19. Главная опасность публичного Wi-Fi без пароля? (Перехват трафика злоумышленником)
20. Можно ли проводить банковские операции через Wi-Fi в кафе? (Не рекомендуется без использования VPN)
21. Что означает протокол HTTPS в адресной строке? (Данные между браузером и сайтом зашифрованы)
22. Для чего нужен VPN в образовательных целях? (Для создания защищенного канала связи)
23. Безопасно ли подключать к компьютеру найденную на улице флешку? (Нет, на ней может быть вредоносное ПО)
24. Что такое «атака посредника» (MitM)? (Когда хакер встает между пользователем и сервером)

25. Нужно ли отключать Bluetooth, если вы им не пользуетесь? (Да, для исключения несанкционированного подключения)

Блок 4. Мобильная безопасность и Приложения (26-32 вопросы)

26. Откуда безопаснее всего скачивать приложения на Android в РФ в 2026 году? (Официальные сторы: Rustore, AppGallery и др.)

27. Зачем приложению «Фонарик» доступ к контактам и СМС? (Это признак шпионского ПО)

28. Что такое Jailbreak/Root-права и как они влияют на безопасность? (Снимают ограничения системы, делая её уязвимой для вирусов)

29. Нужно ли устанавливать антивирус на смартфон? (Да, особенно на ОС Android)

30. Что делать при утере смартфона, к которому привязаны карты? (Дистанционно заблокировать устройство и сим-карту)

31. Как защитить данные на телефоне при физической краже? (Установить сложный пароль на экран и шифрование данных)

32. Опасно ли устанавливать приложения через APK-файлы из мессенджеров? (Высокий риск заражения трояном)

Блок 5. Социальные сети и Цифровой след (33-39 вопросы)

33. Что такое «цифровой след»? (Вся информация, которую пользователь оставляет о себе в интернете)

34. Может ли работодатель в 2026 году проверять соцсети абитуриента/соискателя? (Да, это стандартная практика)

35. Безопасно ли выкладывать фото авиабилетов или ключей от квартиры? (Нет, по ним можно скопировать данные или изготовить дубликат)

36. Что такое кибербуллинг? (Травля и оскорбления в цифровом пространстве)

37. Как ограничить доступ к своим постам для незнакомцев? (Сделать профиль «закрытым» в настройках приватности)

38. Стоит ли указывать геолокацию своего дома в публикациях? (Нет, это угроза физической безопасности)

39. Что делать, если ваши интимные фото попали к шантажисту? (Не платить, заскринить угрозы, обратиться в полицию)

Блок 6. Искусственный интеллект и Deepfakes (40-45 вопросы)

40. Как отличить дипфейк-видео при звонке в мессенджере? (Попросить собеседника покрутить головой или провести рукой перед лицом — артефакты ИИ могут «поплыть»)

41. Безопасно ли загружать свои фото в сомнительные ИИ-редакторы «старения»? (Нет, вы передаете биометрические данные неизвестным лицам)

42. Может ли ИИ написать вредоносный код? (Да, киберпреступники используют нейросети для создания вирусов)

43. Стоит ли доверять юридическим советам от чат-бота без проверки? (Нет, ИИ может галлюцинировать/ошибаться)

44. Что такое «голосовой клон»? (Имитация голоса человека нейросетью для обмана родственников)

45. Как защитить свой голос от копирования ИИ? (Избегать долгих разговоров с незнакомцами по телефону, которые могут записывать образцы речи)

Блок 7. Правовые аспекты и Защита данных (46-51 вопросы)

46. Какой закон в РФ регулирует защиту персональных данных? (ФЗ-152)

47. Относится ли адрес электронной почты к персональным данным? (Да, если он позволяет идентифицировать человека)

48. Что грозит за взлом чужой страницы в соцсетях по УК РФ? (Уголовная ответственность по ст. 272)
49. Имеет ли право колледж собирать биометрические данные студентов без согласия? (Нет, требуется письменное согласие)
50. Куда жаловаться на утечку своих данных? (В Роскомнадзор)
51. Что такое «право на забвение»? (Право требовать удаления недостоверной или неактуальной информации о себе из поисковиков)

Инструкция для преподавателя:

- **Критерии оценки:** 45-51 правильный ответ — «5», 38-44 — «4», 26-37 — «3».