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 информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации

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:
21,22% авторского текста

Работа рекомендована к защите
«17» 12 2025 г.
Зав. кафедрой АТИТ и МОТД
_____ Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Пастухова Екатерина Игоревна

Научный руководитель:
к.п.н., доцент
Диденко Галина Александровна

Челябинск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В начале XXI века в условиях формирования единого мирового информационного пространства проблемы безопасности виртуальной реальности обрели глобальные масштабы и превратились в фактор, влияющий на выживание человечества. В таком случае появляются новые формы опасности информационного характера, традиционные методы безопасности не выполняют свои функции и под воздействием новых информационных технологий трансформируются. Именно поэтому Всемирная федерация ученых в августе 2000 г. первой в списке угроз человечеству поставила угрозу информационной безопасности.

Информационная безопасность характеризуется способностью государства, общества, социальной группы, личности обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные попытки для поддержания своей жизнедеятельности и жизнеспособности, противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации, осуществлять информационно-психологическое противоборство.

Уровень жизни общества во многом зависит от владения новыми информационными технологиями, умелой ориентации в пространстве виртуальной реальности, являющейся неотъемлемой частью жизни современного человека. Особое место в пространстве виртуальной реальности занимают социальные сети, которые могут быть использованы для общения, самовыражения, заработка и других целей. Благодаря социальным сетям можно мгновенно получить или распространить любую информацию.

Опасность состоит в том, что многие пользователи доверяют информации, которая публикуется в социальных сетях.

Любая социальная сеть представляет собой своеобразную базу данных, которая содержит самую различную информацию о миллионах людей во всем мире. Многие личные данные пользователей становятся доступными для всех (интересы, образование, место работы, связи, личные мысли и др.). Часть информации можно получить без регистрации, остальную при регистрации в сети.

Некоторые социальные сети предоставляют широкий выбор инструментов для работы. С помощью социальных сетей можно найти работу, подходящего сотрудника, продать товары или услуги, найти партнеров по бизнесу. Популярность работы в социальных сетях настолько высока, что появляются виртуальные рабочие места. Нововведениями можно считать геолокацию, а также электронную коммерцию в социальных сетях.

Вопрос информационной безопасности в социальных сетях особенно важен в последнее время. Личные данные пользователей, находящиеся во всеобщем доступе, могут быть использованы без разрешения, например, для показа рекламы, подбора возможных знакомых пользователя и др. Серьезные последствия может иметь перехват личных данных по вине сети, взлом аккаунта для получения доступа ко всей информации определенного пользователя, появление вируса, который автоматически рассылает спам.

Информация может быть получена злоумышленниками через социальную инженерию, а также с помощью программных средств. Социальные методы включают в себя убеждение пользователя сообщить пароль, конфиденциальную информацию добровольно, ввести свои данные на мошенническом сайте. Пользователи могут заходить в свои рабочие аккаунты с зараженных машин, использовать простые для взлома пароли, пренебрегать настройками конфиденциальности. Многие пользователи игнорируют

пользовательские соглашения, в которых указываются права на данные, передаваемые и публикуемые в сети.

Самая большая угроза, заключается в том, что доступ ко всей информации, публикуемой в социальных сетях, независимо от поставленных барьеров, имеется у достаточно большой группы лиц, в состав которой входят администрация социальной сети, правоохранительные органы, которые имеют доступ к любому аккаунту и личным сообщениям.

Количество пользователей пространство всемирной паутины постоянно увеличивается с каждым днём, при том, что самыми частыми пользователями среди них являются поколение молодых людей. Наиболее активными участниками интернет-общения являются подростки.

По официальной статистике, в России проживает почти 21 миллион детей в возрасте до 14 лет. Ежедневно, подвергаясь риску вредоносного информационного воздействия, сетью «Интернет» пользуется 89 процентов подростков 12-17 лет. Проблема информационной безопасности граждан, а особенно несовершеннолетних, по мнению Президента Российской Федерации, стала носить международный характер, в связи с чем он поручил начать разработку предложений по созданию международной системы информационной безопасности.

Все эти новые информационные факторы оказывают самое прямое воздействие на психическое и физическое развитие подрастающего поколения. Современная юридическая наука пытается найти пути решения данной проблемы, проводя исследования по направлению информационной безопасности личности в условиях информационного общества. Под информационной безопасностью детей понимается состояние и условие жизнедеятельности личности ребенка, при которых отсутствует или сведена к минимуму угроза нанесения вреда как личному пространству индивида (в том числе информационному), так и той информации, которой он обладает.

Обеспечение информационной безопасности детей в социальных сетях является одним из направлений государственной информационной политики. Ведь подрастающее поколение – это необходимая база, основа для дальнейшего развития общества, а от того, как именно будет воспитано данное поколение, какие мировоззренческие идеи будут заложены в его сознание (в т.ч. правовое), зависит уже возможность самого существования государства как суверенной единицы.

В настоящее время функцию правового регулирования данной проблемы выполняют федеральные законы «О защите детей от информации, причиняющей вред их здоровью и развитию» 29 декабря 2010 г. № 436-ФЗ (ред. от 14.10.2014) [51] , «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ (ред. от 24.11.2014) [52], определяющие перечень информации, распространение которой ограничивается или запрещается.

Мониторинг сайтов Роскомнадзором на предмет выявления информации, запрещенной к распространению, по причинам технического характера не эффективен в отношении социальных сетей. Выходом могла бы быть активизация привлечения общественности к выявлению запрещенной информации, воспитание правового сознания подрастающего поколения.

Обеспечение информационной безопасности несовершеннолетних в социальных сетях является сложной и многофакторной проблемой, ее решение должно быть комплексным, включая в себя не только правовые механизмы, но и максимальное участие всех заинтересованных сторон – государства, родителей, государственных и общественных организаций и др., что определяет **актуальность** темы исследования.

Проблемой исследования является формирование информационной безопасности личности в социальных сетях.

Была сформулирована **тема исследования**: «Формирование информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации».

Цель исследования: на основе теоретического анализа литературы разработать рекомендации по формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации.

Объект исследования: формирование информационной безопасности личности в социальных сетях.

Предмет исследования: рекомендации по формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации.

Гипотеза исследования основана на предположении о том, что процедура формирования информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации будет эффективнее, если внедрить в образовательный процесс разработанные рекомендации по формированию информационной безопасности личности в социальных сетях.

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

1. Изучить сущность информационной безопасности личности в социальных сетях;
2. Рассмотреть классификацию угроз информационной безопасности в социальных сетях;
3. Разработать рекомендации по формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации;

4. Проанализировать эффективность разработанных рекомендаций по формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации на базе ГПБОУ «ЮУрГТК» г. Челябинска.

Методологической основой исследования являются отечественные и зарубежные исследования, связанные с проблематикой информационной безопасности, широко раскрывают следующие вопросы:

– общие научные и методологические вопросы информационной безопасности поднимаются в трудах А.П. Коваленко, Е.Б. Белов [33]; Р. В. Мещерякова, А.А. Шелупанова [34]; В.П. Шерстюк и др.);

– аспекты нормативно-правового обеспечения информационной безопасности (С.Л. Зефиров, В. М. Алексеев [35]; Ю. М. Батурин; Т.А. Кондратьева, В. С. Горбатов; О. А. Городов, Р. И. Дремлюга, Ю. А. Журавлев, Г. О. Крылов, Т. А. Полякова [36] и др.);

– аспекты ИБ как педагогической проблемы (Р. В. Амелин [37], А. А. Журин [38], П. Н. Корнюшин [39], А. А. Марков [40], В. А. Семененко [41], В. Н. Ясенев [42] и др.);

– проблемы подготовки кадров и формирования компетентности в области ИБ (А.П. Коваленко, Е. Б. Белов [33]; Е. Н. Бояров [43] и др.);

– практические аспекты ИБ и защиты информации (В. А. Галатенко [44], В.Н. Максименко [45], А. П. Даньков, Б.И., Скородумов [46], А. А. Круглов [47], А. В. Крысин, В. П. Мельников [48], Ю. С. Уфимцев [49], В. Л. Цирлов [50] и др.).

Методы исследования: теоретический анализ, изучение материалов научных и периодических изданий по проблеме исследования.

Практическая значимость работы заключается в разработке рекомендаций по формированию информационной безопасности личности в

социальных сетях у студентов ГБПОУ «ЮУрГТК»; возможности применения разработанных рекомендаций в других учебных заведениях СПО.

База исследования: ГБПОУ «Южно-Уральский государственный технический колледж» г. Челябинска.

Апробация и внедрение результатов исследования осуществлялись при реализации процесса педагогической и экспериментальной деятельности в ГБПОУ «ЮУрГТК»

Структура магистерской диссертации: работа состоит из введения, двух глав, заключения, списка использованных источников.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

1.1. Сущность информационной безопасности личности в социальных сетях

Информационные и коммуникационные технологии сегодня стали одним из важнейших факторов, влияющих на развитие общества. Они не только прочно закреплены в государственных структурах, институтах гражданского общества, в экономической и социальной областях, науке и образовании, культуре, но и в повседневной жизни людей. Движение к информационному обществу - это путь вперед для человеческой цивилизации. За последние несколько лет изменились способы и формы общения в Интернете. Сегодня наиболее распространенным и доступным средством коммуникации и самой популярной услугой, привлекающей внимание большей части интернет-аудитории, являются социальные сети [1].

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. [32]

С появлением социальных сетей и различных мессенджеров их востребованность у пользователей только растет. Возможности применения постоянно множатся и уже присутствуют во всех сферах нашей жизни.

Социальные сети - достаточно недавнее, но популярное явление в Интернете. Социальная сеть (от англ. social networking service) - платформа, онлайн сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений. Поскольку социальная сеть состоит из людей и «сообществ», а люди и сообщества в социальной сети связаны отношениями, другими словами, социальная сеть - это интернет-сервис, целью которого является создание онлайн-сообщества пользователей, объединенных определенными признаками: хобби, интересы или профессиональная принадлежность.

Сам термин «социальная сеть» был введен в 1954 г. английским социологом Джеймсом Барнсом. Так, ученый определил совокупность узлов, которыми являются социальные объекты (общность, социальная группа, индивид). Более точная формулировка встречается у Д. М. Бойд и Н. Б. Элисон, которые называют виртуальной социальной сетью (social network site) базирующийся на интернет-технологиях сервис, который позволяет отдельным пользователям: — создавать открытые (публичные) или частично открытые профили пользователей; — создавать список пользователей, с которым они состоят в социальной связи; — иметь доступ к спискам коммуникаций «друзей», то есть к социальным сетям других пользователей внутри системы. Ученый Д. Гилпин определяет социальные сети как интерактивные онлайн-СМИ, которые выступают в качестве каналов для отношений и передачи информации. А. Хэндли и А. Чапмэн под социальными сетями понимают неуклонно растущую и развивающуюся коллекцию онлайновых инструментов, платформ и приложений, которые позволяют всем нам взаимодействовать и обмениваться информацией.

Под термином «социальная сеть» в области информационных технологий понимают интерактивный многопользовательский веб-сайт, контент которого наполняется самими участниками сети. Это определение отличается от используемого в социологии, где под термином «социальная сеть» принято понимать социальную структуру, состоящую из группы узлов, которыми являются социальные объекты, и связей между ними.

Основными принципами социальной сети являются:

− идентификация – возможность указать информацию о себе (школу, институт, дату рождения, любимые занятия, книги, кинофильмы, умения и т. п.);

− присутствие на сайте – возможность увидеть, кто в настоящее время находится на сайте, и вступить в диалог с другими участниками;

− отношения – возможность описать отношения между двумя пользователями (друзья, члены семьи, друзья друзей и т. п.);

− общение – возможность общаться с другими участниками сети (отправлять личные сообщения, комментировать материалы);

− группы – возможность сформировать внутри социальной сети сообщества по интересам;

− репутация – возможность узнать статус другого участника, проследить его поведение внутри социальной сети;

− обмен – возможность поделиться с другими участниками значимыми для них материалами (фотографиями, документами, ссылками, презентациями и т. д.).

Мессенджер — это программа или веб-сервис для быстрого обмена сообщениями. Обычно речь идет не только о текстовых сообщениях, но и о текстовых файлах, картинках, видео; некоторые мессенджеры позволяют проводить голосовые и видеоконференции. Таких программ сейчас очень много, и самые популярные из них — Viber, WhatsApp, Facebook Messenger, Skype, ICQ, Telegram.

Использование мессенджеров и социальных сетей в обучающих целях становится новой социальной практикой и привлекает внимание ученых [3].

Опыт использования социальной сети в обучении описан многими исследователями. Например, Н. В. Родионова и М. Н. Яранская внедряют социальные сети в учебный процесс в качестве средства для постоянного взаимодействия преподавателей и студентов. Ими отмечены широкие и разнообразные функциональные ресурсы сети Вконтакте, а именно — организация групп, отслеживание активности студентов, размещение информации различных форматов. Помимо этого, преподаватели имеют

возможность провести различные контрольные мероприятия, такие как тестирование, опрос, коллективное обсуждение темы [2, с. 66-69].

Появление информационных технологий кардинальным образом воздействовало на представление о коммуникационных способностях человека. С каждым годом появляется все более и более новых возможностей, которые в настоящее время еще не до конца изучены. Ход глобализации непосредственно объединён с информационным пространства, какое на сегодняшний день все глубже уходит в виртуальную сферу и тесно связано с современными информационными технологиями. Любой пользователь глобальной сети попадает в огромную и нескончаемую «реку» информации. Начинает погружаться все глубже, впитывая в себя информацию. Однако в любой реке есть камни, и камнями информационной реки являются системы массово контроля и цензура в глобальной сети. Именно появление глобальной информационной сети с открытым доступом определило новую проблему безопасности личности в целом – информационную безопасность. [4]

С точки зрения информационной безопасности пользователей социальных сетей, очень важно, в какой стране располагаются серверы, на которых хранятся данные о пользователях, и кто является непосредственным владельцем социальной сети. Например, серверы сетей Facebook, LinkedIn, MySpace, Instagram расположены в США; Одноклассники, Мой Круг, Вконтакте – В России. Существуют сети, которые принадлежат конкретным странам: Германии, Израилю и другим и в каждой располагаются сервера с конфиденциальной информацией пользователя, его личными переписками и т.д.

Социальные сети создаются физическими или юридическими лицами, и принадлежность к той или иной стране естественно условна. При регистрации в социальной сети от пользователя требуется лишь подписать пользовательское соглашение и ничего более. Нет необходимости верифицировать свою личность и вносить каки либо паспортные данные. Из

этого вытекают как положительные, так и отрицательные тенденции. С одной стороны человек получает полную свободу слова, почти полную безнаказанность за публикацию тех или иных высказывания и точек зрения, с другой же открывает свободу для публикации экстремистских сообщений, призывов к террористическим актам и т.д. Помимо этого владельцы социальных сетей нередко в пользовательском соглашении оставляют для себя лазейки, позволяющие им свободно собирать и передавать личную информацию пользователей и передавать её рекламодателям.

Таким образом в руках у владельцев данных ресурсов содержится колоссальный инструмент для анализа социальной структуры общества или отдельной личности. Не редко случается и то, что личные данные пользователя продаются третьим лицам, так как пользовательское соглашение не запрещает этого.

Угрозы, исходящие от сетевого коммуникативного пространства, принято называть информационными. Их обычно рассматривают в контексте проблемы обеспечения информационной безопасности, которая в российских нормативно-правовых актах определяется как состояние защищенности информационной среды и деятельность по предотвращению утечки защищаемой информации, по защите от несанкционированных и непреднамеренных воздействий на нее. [5,6]

Соответственно, информационная безопасность личности определяется как состояние сохранности информационных ресурсов личности и защищенности законных прав в информационной сфере.

В нормативно правовых актах преобладает понимание информационной безопасности в ее техническом и правовом аспектах. Как правило, она трактуется как защита конфиденциальности (обеспечение доступа к информации только авторизированным пользователям), целостности (обеспечение достоверности и полноты информации и методов ее обработки)

и доступности (обеспечение доступа к информации и связанным с ней активам авторизированных пользователей по мере необходимости) информации.[7]

Кривоухов А.А. в ходе своей научной работы установил, что социальные сети имеют низкий уровень безопасности информации и данных их пользователей. По этой причине, необходимо формирование компетенций в области информационной безопасности, как составляющей информационной культуры современного человека [8].

Тумбинская М.В. описывает, что ключевой причиной информационной небезопасности пользователей социальных сетей является таргетированная информация, вызывающая информационные атаки на мнение людей [9].

Муромцева А.В. рассматривая особенности построения, взаимодействия и характеристики социальных сетей в Интернете, выявила основные проблемы информационной безопасности участников социальных сетей [10].

При этом, ключевым объектом информационной безопасности в социальных сетях выступает защита личных и персональных данных, которые выступают набором организационных, технических и организационно - технических мероприятий, направленных на защиту информации, что относится к конкретной личности.

Современный период трансформации мировой и отечественной экономики способствует усилению интеграционных процессов между деятельностью и цифровыми технологиями. В рамках данной тенденции прослеживаются такие процессы, как развитие информационных технологий, разработка интеллектуальных технологий, практическое применение высокоинтеллектуальных инноваций в рамках совершенствования процессов образовательной организации и развитие мессенджеров и социальных сетей, которые используются как населением (как средство коммуникации и связи), так и субъектами образовательного процесса.

Одним из последних процессов выступает и развитие цифровых технологий в составе комплексной системы информационной безопасности образовательной организации, которые совершенствуют деятельность образовательных организаций по сбору, обработке, анализу и хранению информационных данных. Их задачей выступает формирование основы и фундамента информационной безопасности организации, что крайне актуально в виду развития цифровой экономики Российской Федерации.

Одним из самых эффективных способов воздействия на целевую аудиторию в социальных сетях является предоставление информации, восхваляющей или порочащей какой-либо товар, услугу или даже человека. Данный прецедент принято называть инфо-поводом. Иногда такие средства становятся откровенной информационной ложью, которая в свою очередь наносит сильный ущерб имиджу человеку, товара или услуги. Однако, такие действия попадают под нарушение 7 статьи 152 ФЗ «О персональных данных»: Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом [1].

Особенно подвержены влиянию социальных сетей дети и подростки. Они прикованы взглядами к своим кумирам и вторят их действиям и мышлению не задумываясь о том к чему может привести такого рода мышление, как пример мы можем увидеть влияние запрещенной на территории РФ организации «ФБК» на разум и сознание детей, они не пытаются и не хотят анализировать реальную ситуацию в стране, а просто по призыву, как марионетки выходят на улицы и скандируют опасные лозунги не задумываюсь что нарушают общественный порядок и спокойстве людей. Они не бояться ничего ни органов власти, ни своих родителей, они просто не понимают что то что они делают опасно и это лишь внедренная в их мысли идея, идея которую вложил в них интернет кумир.

На сегодняшний день в социальных сетях особенно активно проходят различные информационные кампании, которые нацелены на создание положительного образа на конкретные информационные события по актуальным экономическим, политическим, социальным и другим вопросам. Благодаря социальным сетям появились и продолжают появляются все новые инструменты воздействия на человеческое сознания и другие инструменты манипуляции над ним, коих в современном мире уже с избытком.

Значение социальных сетей для обучения и развития пока не определено, так методисты скептически относятся к возможности использования данного объекта информационных технологий, как педагогического средства обучения. В обществе сложилась четкая позиция: социальные сети – среда для развлечений и траты свободного времени от учебы и работы. Однако в педагогической деятельности устройство социальных сетей можно использовать для ряда организационных задач:

– эффективная организация групповой учебной работы; – долгосрочную проектную деятельность;

– международные обмены, в том числе научно-образовательные, мобильное непрерывное образование и самообразование;

– организация работы людей, находящихся в разных городах или даже странах.

Можно выделить следующие преимущества использования именно социальной сети в качестве учебной площадки [3].

1. Привычная среда для обучающихся;

2. В социальной сети человек выступает под своим именем-фамилией;

3. Технология Wiki позволяет всем участникам сети создавать сетевой учебный контент;

4. Возможность совместной работы;

5. Наличие форума, стены, чата;

6. Каждый обучающийся – участник может создать свой блог, как электронную тетрадь;

7. Активность участников прослеживается через ленту друзей;

8. Удобно использовать для проведения проекта;

9. Подойдет в качестве портфолио как для обучающегося, так и для педагога.

Существует ряд проблем, связанных с использованием мессенджеров и социальной сети в образовательном процессе. Например, отсутствие сетевого этикета участников, невысокий уровень мотивации и ИКТ-компетенций преподавателя, высокая степень трудозатрат по организации и поддержке учебного процесса для преподавателя, частое отсутствие открытого доступа к социальным сетям из учебных аудиторий.

Кроме того, преподаватель должен интуитивно чувствовать обучаемую аудиторию и целесообразно подбирать под нее учебную площадку и инструменты. Для решения названных проблем нужно создавать условия для повышения ИКТ-квалификации преподавателей, осуществлять материальное и моральное поощрение педагогов, активно использующих новые технологии, разрабатывать эффективные методики применения социальных сетей в образовательном пространстве.

Партнерское сотрудничество педагогического сообщества с разработчиками социальных медиа и законодательное регулирование этой сферы может обеспечить условия для принятия конструктивных решений проблемы информационной безопасности виртуальных сетей. Конечно, социальные сети не являются основным средством сетевого обучения, но их возможности в решении образовательных задач сегодня недооцениваются профессиональным сообществом.

Социальные сети предлагают отличные возможности для социализации, например, такие как возможность общаться с людьми, живущими по всему миру, развитие способности быть членом группы, что невозможно в реальной жизни из-за географических и физических ограничений, способствует самовыражению и способности не только получать информацию, но и делиться ею. Конечно, есть проблемы с конфиденциальностью информации и зависимостью от социальных сетей, однако правильное использование предоставляемых ими возможностей имеет огромное положительное значение. Сегодня можно говорить об интенсификации процесса использования интернет-технологий в непрерывном образовании. В связи с этим возникает ряд острых проблем, которые являются предметом обсуждения ученых, сочетающих развитие образования с активным использованием Интернет-технологий, создание единого неформального образовательного пространства.

Зарубежные авторы выделяют следующие преимущества использования социальных сетей в качестве дополнительного инструмента профессионального обучения:

− индивидуализировать обучение;

− дать слушателю возможность повторять содержание курса столько, сколько ему нужно;

− независимость от времени и места;

− повысить успешность, качество и эффективность образования за счет использования ИКТ в образовательном процессе;

− возможность учиться более систематично и за меньшее время благодаря достижениям компьютерных технологий;

− позволяет создавать визуальный и слуховой дизайн учебной среды;

− приложения для архивирования содержания курса и синхронизации занятий (виртуальный класс);

− возможность формирования добровольного поведения обучаемыми с целью улучшения исследовательских навыков и знаний по сравнению с традиционными программами;

− возможность повышения навыков обучающихся и педагогов для достижения, оценки и эффективного использования полученных знаний.

Важным преимуществом социальных сетей является то, что пользователь определяется одновременно как потребитель и как создатель информации. Он занимает активную позицию, то есть создает и потребляет контент.

Следует отметить, что социальные сети не предоставляют слушателю тех же возможностей для объяснения и уточнения, которые возникают при личном общении. Поэтому они сталкиваются с некоторыми трудностями при письменно выражении своих взглядов и идей в социальных сетях, поскольку многие участники курсов предпочитают выражать свои мысли устно. В то же время, чтобы успешно учиться через социальные сети, пользователям необходимо приобрести навыки письма, чтобы иметь возможность свободно выражать свои идеи и мнения.

Сети можно разделить на:

− социальные сети общего формата;

− профессиональные социальные сети;

− социальные сети по интересам.

В электронной сети каждый имеет возможность выразить свою точку зрения, встретить единомышленников, пообщаться на любую тему, поделиться опытом, научить других, позволить вам стать тем, кем хотел бы быть человек; можно заводить новые знакомства; можно найти знакомых и

друзей, контакты, которые давно утеряны, а люди навсегда остались в памяти. Но у социальных сетей есть не только преимущества, но и недостатки. Слово «сеть» невольно появляется в связи с рыболовной сетью или паутиной. И это, в общем, недалеко от истины. В социальных сетях пользователи надолго пропадают. Прежде всего, это психологическая зависимость от них, потому что многие пользователи проводят на сайте дни, заменяя виртуальное общение реальным.

Споры о том, вредны или полезны социальные сети, также не утихают среди педагогов и психологов, но однозначного мнения по этому поводу до сих пор нет. По мнению некоторых психологов, в социальных сетях нет необходимости, а некоторые считают, что социальные сети опасны, это просто онлайн-наркотик. Пришло время для новых социальных сетей, которые будут более эффективно выполнять образовательные функции за счет структурирования информации, за счет введения определенных правил, соблюдения внутрисетевой этики. Основная задача этих сетей - обеспечить вхождение мирового сообщества, в том числе России, в шестой технологический уклад. Функцией этих сетей будет не только информация и коммуникация, но и полноценное информальное образование взрослого населения. По определению О.В. Павловой, информальное образование представляет собой процесс формирования активной жизненной позиции, условие социальной адаптации.

Научные междисциплинарные исследования человека, при котором «отношения и социальные связи становятся более независимыми и основываются на индивидуальных характеристиках человека, его творческого поиска, возросших возможностях выбора своей социальной ниши, на основе усиления социальной мобильности, снижения зависимости человека от определенных обстоятельств» [3].

Основными проблемами использования социальных сетей в образовании можно считать:

1. Педагоги часто имеют низкий уровень мотивации и навыков использования ИКТ, что не позволяет им активно использовать социальные сети в своей профессиональной деятельности.

2. Высокий уровень трудозатрат на организацию и сопровождение учебного процесса в среде непрерывного обучения педагога;

3. Отсутствие открытого доступа к социальным сетям из аудиторий в образовательных организация.

Использование форумов и вики-технологий в виртуальных учебных группах позволяет всем участникам независимо или совместно создавать онлайн-образовательный контент, стимулирующий независимую познавательную деятельность. Возможность совмещения индивидуальных и коллективных форм работы способствует лучшему пониманию и усвоению материала, и построению индивидуальных образовательных траекторий. Коммуникативное пространство, общее для всех участников образовательного процесса, позволяет коллективно оценивать процессы и результаты работы, наблюдать за развитием каждого участника и оценивать его вклад в коллективное творчество. Высокий уровень взаимодействия гарантирует непрерывность учебного процесса, выходящего за рамки аудиторных занятий.

Не каждый преподаватель способен создать сайт или написать программу для компьютера (смартфона). Когда мы говорим о цифровизации образования, речь должна идти не только (и даже не столько) о создании новых цифровых продуктов, но и об использовании уже существующих, тех, к которым мы привыкли в повседневной жизни. Их применение не требует специальных навыков, продолжительного обучения, специализированных классов, разработки (покупки) и установки программного обеспечения, выделения дополнительных часов в программе. Полагаем, что именно такое решение — использовать уже существующие мессенджеры и социальные сети

— является методически правильным. Речь должна идти в первую очередь о новых принципах организации учебного процесса.

Таким образом, сегодня мессенджеры и социальные сети — это новая среда обучения, где студенты в основном читают или просматривают учебный контент, делятся комментариями или аудио- и видеоматериалами собственного производства, при создании которых применяются те знания, которые ранее были приобретены. Не следует игнорировать современную тенденцию, которая заключается в том, что процесс обучения в наши дни происходит не только в стенах образовательной организации, но и после аудиторных занятий, а возможно, и одновременно.

Социальные сети имеют и свои недостатки: переизбыток развлекательной информации, отсутствие жесткого контроля, игнорирование этических моментов, а также неточность содержания. В целом, использование социальных сетей в образовательном контексте имеет спорный характер и следует учитывать как преимущества, так и недостатки, для того чтобы сделать его более эффективным как для педагогов, так и для студентов. Однако социальные сети могут стать дополнительным средством обучения.

Обеспечение информационной безопасности в мессенджерах и социальных сетях - актуальная проблематика не только для корпоративных структур, коммерческая информация и интеллектуальный капитал которых находится в поле поиска злоумышленников, но и для образования.

Исходя из этого, важно определить то, какие инструменты и механизмы необходимо применять, чтобы формировать информационную безопасность виртуального пространства социальных сетей, сохраняя интересы всех его участников.

1.2. Классификация угроз информационной безопасности в социальных сетях

Информационная безопасность стала новой проблемой после появления всемирной информационной сети Интернет. Люди столкнулись не только с

ограничениями восприятия информации, но и со снижением способности к генерации собственных мыслей и идей.[11]

Социальные сети и Интернет являются технологиями, которые значительно изменили жизнь многих людей, предоставляя им широкий спектр онлайн-услуг [12,13]. Не случайно уже в январе 2022 года в Российской Федерации насчитывалось 106,0 млн пользователей социальных сетей. Количество пользователей социальных сетей в России на начало 2022 года составляло 72,7% от общей численности населения [14].

Используя сеть "Интернет", современные дети сталкиваются с множеством угроз и рисков [15]. К сетевым угрозам безопасности детей киберпреступления, мошенничество (кража личных данных, вымогательства), распространение недостоверной информации и deepfake (реалистичная замена контента, созданной при использовании нейросети), общение в сети "Интернет", влекущее такие последствия, как кибербуллинг, целенаправленное запугивание, унижение детей.

Также насущной проблемой является злоупотребление общим доступом к файлам, выражающееся в несанкционированном обмене различными файлами (фото, видео, аудиозаписи и т.п.), что может повлечь за собой нарушение авторских прав владельцев данных файлов или же сопроводить за собой загрузку вредоносных программ. Неконтролируемый доступ к нежелательному контенту, пропагандирующему насилие, употребление запрещенных веществ, может оказать негативное влияние на психическое и эмоциональное состояние, развитие детей [16].

Имеется рад опасностей, которым дети собственноручно подвергают себя и других при использовании информационно-телекоммуникационной сети "Интернет", например, реализация фото- и видеосъемки для размещения в сети "Интернет", сопряжённая с угрозой жизни и здоровью (пропаганда руфинга, зацепинга).

В Российской Федерации механизмы защиты молодого поколения от негативной информации, размещенной в сети "Интернет", закреплены на законодательном уровне различными нормативными правовыми актами. В Федеральном законе от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" представлены меры защиты детей от травмирующего воздействия на их несформированную психику негативной и развивающей порочные наклонности информации [17].

В Концепции информационной безопасности детей в Российской Федерации, утвержденной распоряжением Правительства Российской Федерации от 28.04.2023 № 1105- р, представлены основные принципы обеспечения информационной безопасности детей, приоритетные задачи государственной политики в этой области [18].

Информационные угрозы в сетевой коммуникации возможно классифицировать разными способами. Классификация всегда будет зависеть от базового критерия классификации, который ложится в основу для определения групп и выделения одних информационных угроз в сетевой коммуникации. Первая классификация в рамках выпускной квалификационной работы проведена по двум базовым критериям: психологические и технические аспекты информационных угроз для личности в сетевой коммуникации [19].

Под техническими угрозами будут пониматься вредоносные атаки, нацеленные на хищение, блокировку, искажение личной информации пользователя при помощи технических средств. К таким угрозам можно отнести все виды вредоносных программ: компьютерные вирусы, сетевые черви, троянские программы, логические бомбы, программы шпионы, кейлоггеры, рекламное обеспечение. Распространению таких угроз способствует незащищенное соединение, отсутствие защитных программ на персональных компьютерах, неполадки в системе, доступность для взлома, отсутствие способов защиты от нежелательных собеседников и другое [20].

Следует отметить, что в настоящее время популярные социальные сети оснащены надежными защитными механизмами, позволяющими блокировать вредоносные программы и предотвращать заражение пользовательских компьютеров. По этой причине технические угрозы в социальных сетях ограничиваются недостаточным функционалом: отсутствием возможности скрыть персональные данные на страницах, заблокировать пользователя по 1Р-адресу. Также к техническим опасностям можно отнести распространение на публичных страницах зашифрованных ссылок с недостоверной информацией, а также файлов сомнительного содержания.

Психологические угрозы личности представляют собой более обширную группу, связанную с негативными воздействиями мошенников на психику пользователя, а также использованием персональной информации во вред ее владельцу. Психологические угрозы представляют наибольшую опасность, так как доказать вред нанесенного ущерба не всегда возможно. В большинстве случаев пользователь совершает указанные действия самостоятельно и несет полную ответственность за них. Еще одной проблемой является то, что предоставленной информации может оказаться недостаточно для комплексной оценки ситуации и осуществлении мер по поиску преступника [21].

Что касается данной группы информационных угроз, представляющих собой полноценные диалоги злоумышленника и жертвы, то она является наиболее трудной для анализа и идентификации исследователями. Это связано с отсутствием каких-либо четких критериев для оценки сообщений как противоправных и деструктивных, ведь в данном случае зачастую используются тонкие манипулятивные приемы, методы воздействия на сознание и подсознание.

Прежде чем перейти к описанию сущности и особенностей психологических угроз необходимо рассказать о таком важном феномене, как социальная инженерия. Автор книги «Социальная инженерия и социальные

хакеры» М.В. Кузнецов, описывает его как взлом компьютера посредством психологической атаки на пользователя. Социальные инженеры или социальные хакеры добывают конфиденциальную информацию не посредством технического взлома, а путем психологического воздействия на пользователя. В арсенале инженеров существует множество различных методов от шпионажа, сбора персональных данных в виртуальном пространстве и в реальной жизни, до шантажа, эмоционального воздействия манипуляций, подкупа, обмана и использования в своих целях неблагополучное состояние индивида [10].

Социальные инженеры или социальные хакеры добывают конфиденциальную информацию не посредством технического взлома, а путем психологического воздействия на пользователя. В арсенале инженеров существует множество различных методов от шпионажа, сбора персональных данных в виртуальном пространстве и в реальной жизни, до шантажа, эмоционального воздействия, манипуляций, подкупа, обмана и использования в своих целях неблагополучное состояние индивида [6].

Как правило, социальных инженеров не интересуют обычные пользователи, ведь наиболее крупную выгоду они получают от доступа к данным успешных компаний: банков, концернов, иных финансовых учреждений. Но вполне возможно, что известная и богатая персона или имитированный под нее профиль может стать их мишенью. В этом случае для достижения своих целей хакеры могут установить дружескую коммуникацию с ближайшим окружением пользователя, а после намеренно создавать ситуации, побуждая других из чувства ревности, мести делиться необходимыми данными. Также в ход могут пойти угрозы, предложение финансовой помощи, воздействие на эмоции коммуниканта. Похожую, но немного отличную от представленной схемы используют представители террористических и экстремистских организаций. Отслеживая потенциальных жертв на различных социальных площадках, они устанавливают близкий

контакт и доверительное общение, что в дальнейшем используется для вербовки сторонников. С целью привлечения новых членов, террористы используют различные манипулятивные техники, создавая впечатление внимательного, чуткого и доброго собеседника, а также обещая различные выгоды и блага за внесенный в деятельность организации вклад.

Похожую, но немного отличную от представленной схемы используют представители террористических и экстремистских организаций. Отслеживая потенциальных жертв на различных социальных площадках, они устанавливают близкий контакт и доверительное общение, что в дальнейшем используется для вербовки сторонников. С целью привлечения новых членов, террористы используют различные манипулятивные техники, создавая впечатление внимательного, чуткого и доброго собеседника, а также обещая различные выгоды и блага за внесенный в деятельность организации вклад.

Следует также иметь ввиду, что потенциальной жертвой террористов могут стать разочарованные, подавленные, угнетенные, недовольные своей жизнью люди, открыто выражающие негативные эмоции на социальных площадках, а также демонстрирующие потребность в поддержке и понимании.

Помимо представленных выше методов психологического воздействия, преследующих очевидную выгоду для ее субъектов, широкое распространение получили деструктивные коммуникативные акты, целью которых является унижение и подавление личности собеседника. Примерами таких явлений являются троллинг и кибербуллинг. Понятие кибербуллинга авторы Е.А. Еремина, Ю.В. Калинина, Е.А. Заплатина, Л.В. Лопатин определяют как нападения с целью нанесения психологического вреда, осуществляемые на различных информационно-коммуникационных площадках [22].

Существует несколько наиболее популярных методов кибербуллинга [23], к которым относятся: использование личной информации с целью

воздействия на пользователя, компрометация взломанных профилей, шантаж интимными фотографиями и секретными данными; киберпреследование, которое заключается в систематическом отправлении пользователю оскорбительных и неприятных сообщений; флейминг, а именно, оскорбление и унижение пользователей в публичных места; клевета; хеппислепинг, что означает создание и размещение видео с избиением и унижением пользователя без его согласия. Отдельно необходимо отметить навязчивое преследование с сексуальным подтекстом, характерное для отдельной группы психически неуравновешенных людей — эротоманов, которые используют любые способы, чтобы привлечь внимание жертвы и вступить в контакт [22].

Такие информационные угрозы, как психологические воздействия и манипуляции социальных хакеров, представителей террористических группировок, наркодилеров, мошенников, эротоманов, а также кибербуллинг представляют наибольшую опасность в условии сетевой коммуникации, так как могут стать причиной серьезных психологических проблем, физических травм, а также привести к суициду [24].

Последняя группа информационных угроз представляет собой совокупность технических и психологических приемов. Мошеннические атаки осуществляются путем отправки единичного сообщения или небольшого стандартного диалога. Такие операции представляют меньшую степень опасности по сравнению с психологическими угрозами в связи с наличием универсальных приемов и отчетливого алгоритма действий хакеров. Все виды информационных угроз, связанных с совокупностью информационно технических и информационно-технических способов атаки, можно обозначить таким понятием, как спам. По мнению О.В. Лутовиновой, спамом является анонимная рассылка сообщений пользователям, не дававшим на это согласие и не выражавшим желание ее получить.

Автор предлагает собственную классификацию спам-сообщений среди которых: коммерческий спам, целью которого является получение какой-либо

коммерческой выгоды; спам для раскрутки ресурса, посредством которого владельцы сайта накручивают трафик и увеличивают посещаемость; мошеннический спам, направленный на кражу личных данных или денег, в том числе спам с рассылкой вредоносных программ; спам для сбора необходимых данных, который маскируется под видом опросников и анкет; религиозный спам; «письма счастья» или сообщения, которые с помощью тех или иных методов убеждают пользователя продолжать участвовать в рассылке сообщений [25].

Исследователь также отмечает, что наряду с укреплением информационной безопасности пользователей и увеличением осведомленности о различных формах спама и негативных последствиях, содержания нежелательных писем становятся все более персонифицированными, креативными и интригующими. Для того чтобы обеспечить посещаемость субъекта рассылки, способствовать продвижению определенного товара или услуги, а также из иных соображений, авторы спам-сообщений могут придумывать захватывающие заголовки, вызывающие немедленный эмоциональный отклик, а также использовать вопросы, просьбы поделиться интересной информации и взамен посмотреть содержание письма и многое другое [25].

Однако большая часть перечисленных методов используется в коммуникации посредством электронной почты. Что касается информационных угроз в контексте сетевой коммуникации, а в частности, коммуникации в социальных сетях, необходимо обратить более пристальное внимание на следующие явления: фишинг — это особый вид интернет-мошенничества, который основан на отсутствии у пользователя представлений о способах и приемах информационной защиты. [26]

Субъекты негативного воздействия отправляют коммуникантам сообщение с просьбой перейти на определенный сайт, который является мошенническим (фишинговым), и зачастую может представлять точную

копию официальных ресурсов крупных компаний. Подобные сайты предназначены для сбора персональной информации: паролей, логинов, данных банковских карт и др. Также создатели фишингового сайта могут предлагать пользователям воспользоваться услугой за символическую сумму денег, которая после совершения операции перечисляется на счет мошенников.

Другой распространенной угрозой является фарминг. Технология фарминга заключается в том, что на компьютер пользователя устанавливаются программы, так называемые «трояны», которые перенаправляют запросы на ложные IP-адреса, тем самым инициируя кражу личных данных.

После того, как конфиденциальные данные пользователя стали доступны мошеннику, происходит массовая атака фишинговыми сообщениями дружеских профилей в социальных сетях. В содержании сообщения может быть указана любая информация, способная заинтересовать потенциальную жертву, как, например, просьба зайти и оценить видео или фотографии, адресованные лично пользователю, рекомендация полезного ресурса или эмоциональный отклик на содержимое страницы. Также со взломанного профиля возможна прямая рассылка с просьбой о помощи в трудной ситуации, просьба перечислить небольшую сумму денег на мобильный номер или банковский счет. В редких случаях после кражи персональных данных мошенник может полностью изменить содержание страницы, адаптируя ее для собственных коммерческих целей [27].

Обозначенные информационные угрозы редко наносят серьезный урон участнику сетевой коммуникации, так как после первого неудачного контакта с фишинговыми сайтами, пользователи становятся более бдительными и стараются игнорировать информацию о непроверенных ресурсах. Кроме того, технические специалисты сетевых площадок постоянно совершенствуют способы защиты от мошеннических рассылок, блокируя сомнительные профили и мгновенно реагируя на жалобы пользователей.

Однако, несмотря на наличие системы безопасности, объектами мошеннических операций с большой долей вероятности могут стать новые пользователи социальные сетей и виртуального пространства, а также дети и пожилые люди.

Специалисты информационной безопасности компаний, которые занимаются развитием онлайн-платформ и различных ресурсов, регулярно повышают уровень информационной безопасности, блокируют миллионы попыток вторжения. Однако, многие пользователи всё равно становятся жертвами хакеров.

Этому есть несколько причин:

– Злоумышленники действуют на шаг впереди, а сторона защиты в многих случаях должна реагировать на новые вызовы, которые предлагают им хакеры;

– Пользователи слабо информировано о том, какими возможностями обладают хакеры, также у них нет навыков, которые необходимы для надежной защиты своих собственных данных;

– Злоумышленникам проще действовать, видя те механизмы защиты, которые применены в системе. Хакеры подбирают нужные ключи и обладают преимуществом перед слабыми системами.

Однако не только технические ошибки и несовершенства виртуальных платформ открывают мошенникам доступ к информации. Зачастую сами пользователи проявляют невнимательность при вводе зашифрованных данных на сторонних ресурсах. Ради выгодного предложения, интригующих сведений, удовлетворения любопытства посетители социальных сетей игнорируют простые правила безопасности и становятся жертвами фишинговых атак.

Обобщая данные о фишинговых атаках пользователей, важно отметить, что несмотря на большое значение технической составляющей, успешность

операции зависит от психологических факторов, а именно, ответной реакции участников сетей. Жажда легкой наживы, любопытство и беспечность посетителей эксплуатируются хакерами с целью взлома аккаунтов и кражи секретных сведений. Для предотвращения подобных действий следует тщательно анализировать входящую информацию, игнорировать подозрительные ссылки и файлы, внимательно изучать URL страницы, не вводить свои данные на посторонних ресурсах и в скачанных приложениях. При поступлении сомнительных просьб от друзей, знакомых и представителей компаний, необходимо своевременно связываться с ними любыми другими доступными способами для уточнения деталей [14].

1.3 Обеспечение информационной безопасности личности в социальных сетях

Система защиты информации - рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке. [31]

Полноценная информационная защита от пользовательских атак возможна только при соблюдении определенных правил поведения и рекомендаций, изучении способов технической, психологической и правовой защиты, формировании информационной культуры. Необходимо помнить, что сетевая коммуникация в силу своих особенностей является более свободной, демократичной, а значит менее доступной для единого контроля. Следовательно, особое внимание следует сосредоточить на способах защиты от информационных воздействий и манипуляций, развитию психологических навыков.

Для предотвращения негативных информационных воздействий на пользователя социальной сети необходимо осуществить последовательность следующих шагов: идентифицировать угрозу, описать и проанализировать особенности реальной или потенциальной опасности, выбрать подходящие

методы защиты, определить план осуществления защитных действий, реализовать способы противодействия по обозначенной инструкции.

Под идентификацией угрозы понимается распознавание негативного воздействия в соответствии с обозначенными критериями. Способы идентификации информационных угроз были подробно изложены в предыдущем разделе. Идентификация угрозы может осуществляться в рамках общего мониторинга технического устройства или целенаправленно при возникновении подозрительной активности установленных программ, аккаунта в социальных сетях, изменении адреса ресурса в поисковой строке, потери персональных данных или некорректной работы компьютера [28]

Обнаружить психологическую угрозу можно в результате анализа действий собеседника. Если пользователь настойчиво призывает совершать необходимые ему действия, будь то публикация или отправка персональных сведений, интимных фотографий, помощь в осуществлении определенных операций, и при этом скрывает данные о себе, то существует высокая вероятность информационной атаки для достижения собственных корыстных целей. Также психологические угрозы могут выражаться в публичных оскорблениях, унижениях, распространении ложной информации, порочащей честь и репутацию, дискриминации и возбуждении вражды и ненависти [29].

Описание и анализ реальной или потенциальной опасности заключается в соотнесении обнаруженной угрозы с определенной группой на основе классификации, обозначение основных характеристик, источников воздействия, цели атаки, используемые технические и/или психологические методы, установление количества нападающих злоумышленников и их личностные особенности. В первую очередь следует обозначить группу угрозы в зависимости от используемых методов: технические, психологические или их совокупность. Также важно обозначить источник угрозы: автоматизированная программа, реальный пользователь со своей настоящей или поддельной страницы, или группа пользователей и цели

воздействий: кража данных с целью дальнейшей продажи, шантажа или иных преступных действий; кража денег путем обещания крупного выигрыша, накрутки рейтинга, быстрого решения какой-либо проблемы; получение секретной информации о персоне или организации, или иное. После этого следует более подробно изучить способы воздействия злоумышленников: распространение вредоносных программ, поддельных сайтов, ложной информации, манипуляция данными и другие. Возможно, мошенник использует несколько перечисленных в предыдущих разделах способов. Идентификация и описание каждого из них поможет выбрать наиболее эффективных для защиты методы [28]

Выбор подходящих способов защиты осуществляется на основе полной характеристики угрозы и анализе существующих прецедентов. Прежде всего изучается эффективность применения правовых, психологических и технических способов защиты. После этого осуществляется выбор активной или пассивной стратегии поведения. Активная стратегия предполагает возбуждением судебного процесса против нарушителя, жалобы на подозрительную активность администрации сайта, а также психологическую оборону. Пассивная стратегия связана с игнорированием негативных воздействий или использованием метода решения конфликтных ситуаций. В рамках пассивной стратегии также возможны обращения к администрации ресурса, однако публичное дело против нарушителя не инициируется.

Перед использованием активной стратегии необходимо оценить возможный ущерб публичного обсуждения дела, вероятность массовой информационной атаки в будущем и наличие достаточного количества и качества доказательств для победы в ходе процесса обвинения. Пассивной стратегия поведения предпочтительнее при отсутствии полной информации о перспективе и характере будущих угроз, а также при недостатке документально оформленных доказательств своей правоты.

На основе анализа прецедентов можно утверждать, что пассивная стратегия защиты более эффективна в ситуации массового троллинга, когда любое публичное действие и ответная реакция жертвы возбуждают интерес злоумышленников. В результате настойчивого сопротивления конфликт разгорается сильнее, а число вовлеченных в него участников начинает увеличиваться в геометрической прогрессии. Если же посетитель стал мишенью информационной атаки со стороны одного зарегистрированного пользователя, то выбор активной стратегии позволит не только оградить себя от негативных воздействий в коммуникативных ситуациях, но и потребовать от обидчика возмещения морального ущерба [28]

В случае негативного воздействия при помощи совокупности информационно-технических и информационно-психологических методов, следует обозначить несколько методов противодействия, среди которых может быть как техническая блокировка аккаунта, изменение настроек на странице социальной сети, так и психологические способы защиты, в том числе использование стратегий решения конфликтных ситуаций, постепенное прерывание беседы и игнорирование собеседника, разъяснение своей позиции, реакция с помощью шутки или нейтральный ответ на реплики пользователя.

Разработка плана защиты включает последовательность совершения выбранных способов для достижения большей эффективности в борьбе со злоумышленниками. В большинстве случаев более предпочтительной является следующий порядок действий: использование психологических, технических и затем правовых методов. Такая очередность применима к информационно-психологическим и смешанным воздействиям и обусловлена рядом некоторых факторов, которые выявляются на этапе анализа.

С учетом возможных негативных последствий предпочтительнее в первую очередь реализовать выбранную психологическую стратегию: игнорирование или решение конфликтной ситуации. При невозможности блокировать угрозу психологическими методами, следует применить

технические средства для удаления нежелательного аккаунта, ограничения доступа к своей странице.

В последнюю очередь, при уверенности в отсутствии негативных последствий правовой защиты, следует собрать необходимые для судебного разбирательства документы и потребовать наказания злоумышленника. В случае предъявления обвинения по статье «Оскорбление» административного кодекса все документально заверенные доказательства угрозу пользователю необходимо собрать самостоятельно. Если же в деле фигурирует обвинение по Уголовному кодексу РФ, профессиональная экспертиза и разбор дела проводятся правоохранительными органами [28]

После совершения всех указанных выше действий, а именно идентификации угрозы, ее анализа и описания, выбора защитных методов и составления плана необходимо осуществить описанные в инструкции шаги и не забывать корректировать план в зависимости от реакции собеседника и других обстоятельств.

Несомненно, многообразие различных зловредных программ очень велико, и зачастую оно заставляет задуматься о правильной защите компьютера. [30]

Выводы по главе 1

Сегодня наиболее распространенным и доступным средством коммуникации и самой популярной услугой, привлекающей внимание большей части интернет-аудитории, являются социальные сети.

С появлением социальных сетей и различных мессенджеров их востребованность у пользователей только растет. Возможности применения постоянно множатся и уже присутствуют во всех сферах нашей жизни.

Использование мессенджеров и социальных сетей в обучающих целях становится новой социальной практикой и привлекает внимание ученых.

Используя сеть "Интернет", современные дети сталкиваются с множеством угроз и рисков. К сетевым угрозам безопасности детей киберпреступления, мошенничество (кража личных данных, вымогательства), распространение недостоверной информации и реалистичной замены контента, созданной при использовании нейросети, общение в сети "Интернет", влекущее такие последствия, как кибербуллинг, целенаправленное запугивание, унижение детей.

Также насущной проблемой является злоупотребление общим доступом к файлам, выражающееся в несанкционированном обмене различными файлами (фото, видео, аудиозаписи и т.п.), что может повлечь за собой нарушение авторских прав владельцев данных файлов или же сопроводить за собой загрузку вредоносных программ. Неконтролируемый доступ к нежелательному контенту, пропагандирующему насилие, употребление запрещенных веществ, может оказать негативное влияние на психическое и эмоциональное состояние, развитие детей.

Имеется рад опасностей, которым дети собственноручно подвергают себя и других при использовании информационно-телекоммуникационной сети Интернет, например, реализация фото- и видеосъемки для размещения в сети Интернет, сопряжённая с угрозой жизни и здоровью.

Такие информационные угрозы, как психологические воздействия и манипуляции социальных хакеров, представителей террористических группировок, наркодилеров, мошенников, эротоманов, а также кибербуллинг представляют наибольшую опасность в условии сетевой коммуникации, так как могут стать причиной серьезных психологических проблем, физических травм, а также привести к суициду.

Полноценная информационная защита от пользовательских атак возможна только при соблюдении определенных правил поведения и рекомендаций, изучении способов технической, психологической и правовой защиты, формировании информационной культуры. Необходимо помнить, что сетевая коммуникация в силу своих особенностей является более свободной, демократичной, а значит менее доступной для единого контроля. Следовательно, особое внимание следует сосредоточить на способах защиты от информационных воздействий и манипуляций, развитию психологических навыков.

ГЛАВА 2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ У СТУДЕНТОВ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ НА БАЗЕ ГПБОУ «ЮУрГТК» Г. ЧЕЛЯБИНСКА

2.1. Общие сведения об образовательной организации

ГБПОУ «ЮУрГТК» реализует основные профессиональные образовательные программы среднего профессионального образования — программы специалистов среднего звена.

Организационная структура управления ГБПОУ «Южно-Уральский государственный технический колледж» представлена на рисунке 1.

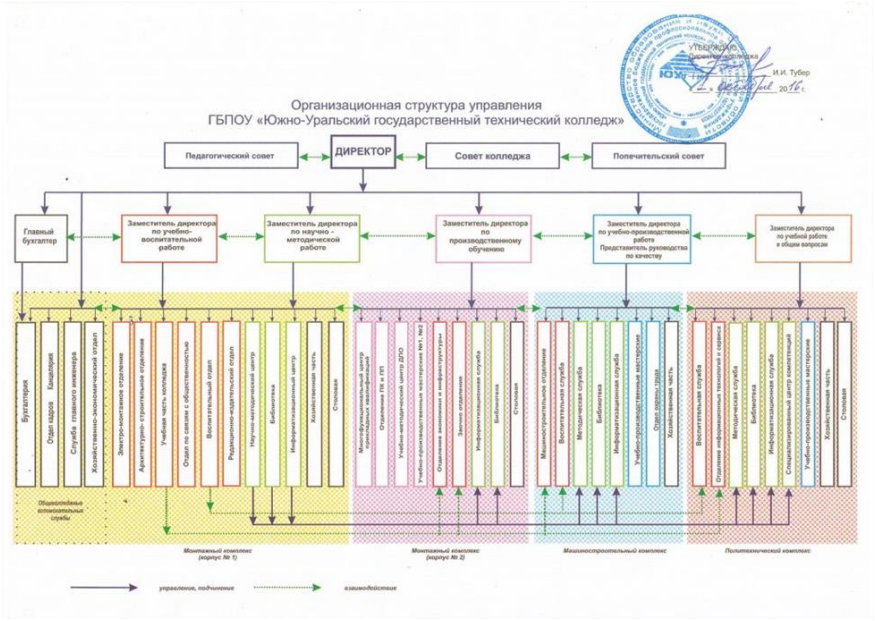

Рисунок 1 – Организационная структура управления ГБПОУ «ЮУрГТК»

Материально-техническое оснащение

Колледж обладает достаточной учебно-материальной базой для качественного осуществления образовательного процесса:

Общее количество объектов недвижимости — 56, общая площадь – 59596 кв.м.

Колледж сегодня – это:

- 4 учебных корпуса,
- 2 стадиона;
- 1 лыжная база;
- 2 спортивные площадки;
- 5 спортивных залов;
- 9 учебно-производственных мастерских;
- 3 учебных полигона;
- 4 библиотеки;
- 36 кабинетов по общеобразовательным дисциплинам и дисциплинам циклов ОГСЭ и ЕН;
- 80 кабинетов профессионального цикла;
- 55 учебных лабораторий;
- 30 компьютерных классов;
- 25 аудиторий, оснащенных интерактивными досками или мультимедийными установками.

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

Учебно-производственные мастерские и полигоны оснащены необходимым учебно-производственным оборудованием, вспомогательным оборудованием, инструментом и расходными материалами, необходимыми для организации и проведения учебных практик студентов, в том числе и для получения квалификации по рабочей профессии.

В машиностроительном комплексе ЮУрГТК, расположенном по адресу ул. Марченко, д. 33, имеется специализированная аудитория, оснащенная компьютерной техникой с установленным специализированным программным обеспечением, позволяющим проводить практические занятия, занятия на тренажерах-симуляторах, групповые и индивидуальные консультации, текущий контроль и промежуточные аттестации, организовывать самостоятельную работу студентов с учетом имеющихся нозологий.

Колледжем разработан значительный объем электронных образовательных ресурсов – электронных учебных курсов, собранных и систематизированных в системе дистанционного обучения ЮУрГТК.

Вход в систему дистанционного обучения осуществляется по логину и паролю, полученному при зачислении на обучение.

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

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

Для работы читателей с электронными изданиями, электронным каталогом, справочно-поисковыми системами и интернетом в библиотеке

МНК оборудована автоматизированная зона на 14 единиц компьютерной техники.

Проблему книгообеспеченности библиотека колледжа решает путём сочетания традиционных методов заказа учебной литературы и использования её в учебном процессе с применением электронных изданий, приобретаемых на стороне. Коллекции электронных документов составляют электронную (цифровую) библиотеку. Одной из составляющей частей электронной библиотеки являются электронные библиотечные системы (ЭБС). Сотрудники библиотеки проводят обучающие занятия для студентов 1-х курсов и преподавателей (в рамках школы молодых педагогов), где рассказывают и показывают приёмы работы с ЭБС. Выпускаются закладки с правилами работы с ЭБС.

Каждому студенту обеспечен доступ к электронным учебным курсам, собранным и систематизированным в системе дистанционного обучения ЮУрГТК.

В электронных учебных курсах учебная информация представлена в различных формах: в форме электронного документа с возможностью увеличения шрифта, в форме аудиофайла, видеофайла, мультимедийных материалов, иллюстраций.

Обучающиеся всех комплексов имеют доступ к компьютерному парку колледжа, включающему 800 персональных компьютеров с выходом в сеть Интернет.

Обучающиеся имеют доступ к трем электронным библиотечным системам (Академия, Знаниум, Лань).

Для студентов организован неограниченный доступ к электронным учебным курсам в системе дистанционного обучения ЮУрГТК.

Студенты, осваивающие общеобразовательные учебные дисциплины, имеют доступ к верифицированному образовательному контенту на платформе МЭО.

Обучающиеся имеют неограниченный доступ к следующим ресурсам:

– Министерство просвещения РФ;

– Федеральный портал “Российское образование”;

– Единая коллекция цифровых образовательных ресурсов.

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

В своей деятельности Информатизационный Центр руководствуется следующими документами:

– Конституцией РФ;

– Законом Российской Федерации от 29 декабря 2012 г. №273-1 «Об образовании в Российской Федерации»;

– Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»;

– Уставом колледжа;

– Документацией внутриколледжной системы менеджмента качества;

– Документацией внутриколледжной системы менеджмента охраны труда и техники безопасности;

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

– Положением об информатизационном центре колледжа.

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

– Лаборатория технического обеспечения;

– Лаборатория информационных технологий.

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

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

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

Структуру и штатную численность информатизационного центра утверждает директор колледжа.

Сотрудники информатизационного центра являются штатными сотрудниками колледжа.

Для достижения поставленной цели информатизационный центр решает следующие задачи:

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

– Выполнение работ по созданию и развитию единой информационной сети колледжа;

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

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

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

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

– Проектирование, создание и развитие автоматизированной системы управления колледжем;

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

– Предоставление платных дополнительных услуг для сотрудников и студентов согласно утвержденному положению.

Основные функции лаборатории технического обеспечения:

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

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

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

Основные функции лаборатории и информационных технологий:

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

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

3. Установка, настройка и сопровождение сетевых программных продуктов;

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

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

6. Организация централизованной антивирусной защиты информационных ресурсов;

7. Предоставление сетевых ресурсов для автоматизации управленческой деятельности подразделений;

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

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

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

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

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

Информатизированный центр имеет право:

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

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

– Запрашивать и получать от руководства информацию, необходимую для выполнения работ, реализующих функции информатизационного центра;

– Формировать заявки на приобретение необходимой нормативной, технической и справочной документации;

– Участвовать в разработке текущих и перспективных планов работы колледжа;

– Представлять перспективные планы развития единого информационного пространства колледжа, докладывать о текущем состоянии их реализации;

– Вносить предложения руководству колледжа по формированию внутренней структуры и штатного расписания информатизационного центра.

Информатизационный центр обязан:

– Осуществлять стратегическое планирование деятельности колледжа в области информационных технологий;

– Обеспечивать бесперебойную работу компьютерной техники, сетевых сервисов и офисного оборудования;

– Своевременно предоставлять отчетную документацию;

– Принимать участие в мероприятиях, предусмотренных планами работ;

– Осуществлять деятельность в соответствии с руководством по качеству и другой документации СМК и СУОТ колледжа.

2.2. Разработка рекомендаций по формированию информационной безопасности личности в социальных сетях

Информационная безопасность личности в сети Интернет означает состояние и условие нахождения личности в информационном пространстве сети Интернет, использование различных сайтов и мессенджеров, при которых реализуются ее права и свободы.

Социальные сети позволяют субъектам свободно общаться и обмениваться информацией. Существует множество примеров, когда информация в социальных сетях становится доступной третьим лицам в позитивных целях, таких как помощь спецслужбам, поиск пропавших лиц с помощью интернет-ресурсов для организации работы волонтеров и прочее.

К сожалению, ввиду того, что пользователи сами оставляют много персональной информации, например для заполнения аккаунтов социальных сетей и профилей в интернет-магазинах, применение данных, полученных в ходе анализа такой информации, может повлечь за собой негативные последствия.

Многие пользователи крайне легкомысленно относятся к социальным сетям, считая их обычным развлечением. Они уверены, что уж их профили точно никому не интересны, особенно если не указывать свои настоящие данные.

Цель деятельности большинства современных киберпреступников — получение выгоды. В связи с этим основная ценность социальных сетей для мошенников состоит в графе социальных связей — друзьях и подписчиках, которые в той или иной степени доверяют владельцу профиля. Чем больше у пользователя подписчиков, тем больший интерес его профиль в соцсети представляет для злоумышленника. Взломав такой профиль, он может, например, опубликовать трагическую историю и просьбу о сборе денег:

В процессе исследования темы были сформулированы рекомендации по формированию информационной безопасности личности в социальных сетях.

1. Использовать надёжные пароли для доступа к профилю социальной сети и ящику электронной почты, к которой привязан этот профиль. Обратить внимание — пароли для почты и для соцсети должны быть разными.

2. Надёжный пароль должен содержать не меньше 12 символов, в том числе заглавные и строчные буквы, цифры и специальные символы. Не рекомендуется использовать «секретные» пароли из русских слов, набранных на английской раскладке, все актуальные программы для перебора паролей очень быстро раскроют такую хитрость.

3. Необходимо обязательно включить двухфакторную аутентификацию. Эту функцию поддерживают все популярные соцсети. Тогда для входа в профиль с нового устройства нужно будет ввести дополнительный

код, направленный в СМС-сообщении на номер или полученный с помощью специальной программы-аутентификатора.

4. Проверить в настройках, где и с каких устройств входили в учётную запись. При необходимости подтвердить, что вход произведён пользователем, или отключить активные сеансы.

5. Проверить, какие приложения и сайты имеют доступ к учётной записи. Даже вполне безобидное приложение или сайт могут получить излишние права и доступ к аккаунту. Отключить доступ для всех приложений, которым в нём нет необходимости.

6. Не переходить по ссылкам, которые получили через социальные сети, даже если они получены от родственника, друга или знакомого. Необходимо позвонить отправителю по телефону или воспользоваться другим способом связи, чтобы выяснить, действительно ли он отправлял сообщение.

7. Не загружать файлы, которые присылают в соцсетях, если не обговорили это заранее с отправителем.

8. Не публиковать в соцсетях личные данные: номер телефона, адрес, место работы и даже настоящую фамилию. Используя эту информацию, злоумышленники могут составить убедительные фишинговые послания, на которые пользователь с большой вероятностью отреагирует.

9. Не вступать в споры, конфликты или агрессивные дискуссии в социальных сетях. В таком состоянии сложно действовать рационально, и, поддавшись эмоциям, можно совершить действия, которые приведут к утере контроля над профилем.

10. Не верить заманчивым предложениям заработать большие деньги без усилий.

Для входа в соцсети использовать только безопасные браузеры, загруженные из официальных источников. Установить и обновлять антивирусные программы, сканировать компьютер на наличие вредоносного ПО. Устаревшие версии не могут гарантировать защиту устройства от

ежедневно обновляющихся угроз информационной безопасности, а значит, и личной безопасности пользователя.

Перед регистрацией в социальной сети необходимо обязательно ознакомиться с текстами Согласия на обработку персональных данных, Пользовательским соглашением и Политикой конфиденциальности, а также иными документами, размещенными на сайте. Так можно понять, кому персональные данные могут быть переданы.

Использовать разные пароли для соцсети и для электронной почты, которая указывается в социальной сети. Пользоваться специализированными генераторами паролей или выбирать сложные пароли, регулярно их менять и не хранить в открытом виде.

Завести два адреса электронной почты: частный - для переписки (который не публикуется в общедоступных источниках), и публичный – для соцсетей, форумов, чатов и т. д. Если нужно сообщить свой приватный адрес в переписке, лучше сделать это способом, непригодным для автоматического прочтения сборщиком адресов, например, в виде картинки.

Настроить профиль в социальной сети таким образом, чтобы только друзья могли его просматривать. Такая настройка лишит злоумышленников возможности получить доступ к информации, которую пользователь скрыл от просмотра незнакомцев.

Внимательно относиться к информации, которая публикуется о себе в социальной сети. Использовать никнейм. Злоумышленник может использовать личную информацию и войти в учетную запись, а также создать правдоподобные истории для злоупотребления доверием и просьбами о переводе денежных средств.

Перед тем как выложить фотографию, оценить каждую деталь: свой внешний вид, окружающую местность, людей, находящихся рядом, и многое другое. Даже если пользователь сразу удалил публикацию, кто-то мог ее сохранить. Помнить о возможных репутационных рисках.

Не устанавливать приложения для соцсетей, которые позволяют отследить активность подписчиков на странице. Нередко при установке такие сервисы запрашивают логин и пароль от аккаунта – все это ухищрения хакеров, создающие риски последующего взлома страницы.

Не отправлять важные документы через социальные сети и не публиковать фотографии документов. Часто обнаруживается, что молодые люди, когда получают водительские права, публикуют их фотографии в открытом доступе.

Такими фотографиями могут воспользоваться злоумышленники, изменив их с помощью графических редакторов. Впоследствии от имени пользователя они могут совершать действия, которые будут иметь юридически значимые последствия.

Перепроверять сообщения от друзей с просьбой срочно выслать денег. Сначала перезвонить другу и удостовериться, что просьба действительно направлена от него.

Проявлять осторожность при переходе по ссылкам, полученным в сообщениях от других пользователей, если не знакомы с отправителем.

Воздерживаться от ответа на провокационные сообщения и комментарии других пользователей. Блокировать навязчивых провокаторов.

Продвинутые социальные сети ввели двухфакторную аутентификацию. Она состоит из двух этапов: первый – вход с помощью логина и пароля, второй – уникальный код по смс или уникальный список кодов, которые действуют лишь единожды, или специальный код, который можно сканировать с помощью мобильного телефона.

Для обеспечения защиты личных данных используются программные и криптографические средства.

Программные средства:

− DLP-системы - комплексные системы, предотвращающие утечку данных;

− SIEM-системы - комплексные системы управления событиями и информационной безопасностью, отслеживающие в режиме реального времени событий безопасности (тревог) (MaxPatrol SIEM от Positive Technologies, КОМРАД от «НПО «Эшелон», RUSIEM).

DLP (Data Loss Prevention) — специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. Эта аббревиатура на английском расшифровывается как Data Loss Prevention (предотвращение потери данных) или Data Leakage Prevention (предотвращение утечки данных).

Предотвращение потери данных является фундаментальным принципом безопасности в компании любого масштаба.

DLP-система включает в себя набор методов и инструментов для борьбы с утечками данных, исходящими от лиц, которые могут разглашать важную для бизнеса информацию по небрежности или злому умыслу с использованием своих или украденных учетных данных.

Программное обеспечение и инструменты защиты от потери данных осуществляют мониторинг и контроль действий пользователей на конечных точках; при помощи специальных алгоритмов фильтруют потоки информации и коммуникации в корпоративных сетях, контролируют перемещение данных. В случае выявления несанкционированной передачи данных DLP-система блокирует операцию либо оповещает об этом офицера информационной безопасности, а также может использовать определенные защитные действия (например, блокирование и изменение сообщений).

Решения класса Data Leak Prevention (DLP) можно сравнить с «водопроводной системой» для потоков конфиденциальных данных. Они обнаруживают и предотвращают несанкционированное использование

(Datain-use), передачу (Data-in-motion) и хранение (Data-at-rest) конфиденциальных данных.

Data-in-use – это данные, к которым пользователи активно обращаются, обрабатывают и обновляют их. DLP предотвращает утечку данных благодаря функции мониторинга действий на рабочих станциях (например, съемные USB-носители, буфер обмена, приложения) и анализа поведения пользователей.

Data-in-motion – это информация, которая перемещается из одной точки в другую. DLP предотвращает утечку данных через сетевые коммуникации (например, электронная почта, инструменты совместной работы, программы мгновенного обмена сообщениями и практически любой публичный канал связи). При этом типе мониторинга делается акцент на идентификации данных, их источнике и назначении, и последующем контроле потока информации в соответствии с политикой безопасности.

Data-at-rest – это данные, которые не перемещаются между устройствами или сетями. DLP обнаруживает конфиденциальный контент в данных, хранящихся на корпоративных ИТ-ресурсах (например, сетевые файловые ресурсы, файловые системы конечных устройств, базы данных, хранилища документов и облачные хранилища), и устраняет нарушения политики хранения данных.

После того как данные перехвачены, они отправляются на полнотекстовый поиск, контентный (анализ содержимого) и контекстный (основанный на контексте операции – например, отправитель, получатель, используемый канал) анализ для обеспечения соблюдения политик использования и обработки данных, принятых в организации. При обнаружении подозрительного действия система принимает решение о блокировке или оповещении сотрудников службы безопасности о нарушении политики безопасности. Полученные сведения могут быть использованы для

проведения расследований со стороны служб информационной, внутренней и экономической безопасности.

Технологии, которые могут быть использованы для обеспечения оперативного перехвата конфиденциальной информации, профилактики инцидентов безопасности и контроля конфиденциальных данных:

Контроль идентификаторов (IDID, ID identification) – технология позволяет распознавать в тексте сообщений специальные идентификаторы в виде последовательности цифр или букв, однозначно определяющей данные, интересные с точки зрения информационной безопасности, в частности контроля утечек информации и работы с персональными данными, и осуществляет:

1. Выявление финансовых данных: банковских реквизитов, ИНН налогоплательщика, номеров пластиковых карт и т. д.

2. Выявление персональных данных: паспортных данных, СНИЛС.

3. Выявление документов, создаваемых по шаблону: договоров, регламентов и т. д.

4. Выявление слов и фраз определенной тематики.

Цифровые отпечатки (DiFi, digital fingerprints) – технология позволяет сравнивать текстовые, графические и табличные данные с эталонными документами, что дает возможность находить как полностью, так и частично скопированные документы, и выявляет:

1. Текстовые документы (планы, уставы, приказы, типовые договоры, тендерные документы и т. д.).

2. Табличные данные (базы клиентов, персональные данные и т. д.).

3. Графические документы (сканы, фотографии, чертежи и т. д.).

4. Шаблонные элементы ГОСТ и документов внутреннего стандарта.

5. Печать-гриф («конфиденциально», «копия», «ДСП», и т. д.).

Графические шаблоны – технология позволяет распознавать конфиденциальные сведения в графических форматах с учетом их деформации (растяжение, поворот, наложение на другие объекты), а также при полном отсутствии текста и выявляет:

− печати организации;

− изображения паспортов с персональными данными;

− платежные карты.

Поведенческий анализ – передовая технология, основанная на машинном обучении, благодаря чему стало возможно получать сведения о зарождающихся угрозах через анализ собранной информации о поведенческой динамике пользователей, их связях и выявленных аномалиях. Детальный анализ показателей поведения может выявить негативные тенденции, что позволяет офицеру безопасности работать с рисками утечек конфиденциальных данных превентивно, вовремя принимая соответствующие меры.

Файловый краулер – технология, благодаря которой становится возможно проводить проверку узлов корпоративной сети и составлять ее наглядную карту, после чего контролировать ресурсы сети. Это позволяет находить конфиденциальную информацию в корпоративных и облачных хранилищах, электронной почте и других ресурсах.

Задачи информационной безопасности, которые решает DLP-система, включают защиту конфиденциальных данных организации от утечек, контроль использования, передачи и хранения информации. Кроме того, DLP-система позволяет проводить расследования инцидентов, связанных с утечками конфиденциальной информации, путем мониторинга и анализа активности пользователей. Система позволяет определить какие действия

выполнялись с данными. Это помогает выявить причины нарушения и принять меры по предотвращению подобных инцидентов в будущем.

DLP-система также способствует обеспечению экономической безопасности, предотвращая финансовое мошенничество, утечки коммерческой и бухгалтерской информации. DLP-система может использоваться для мониторинга коммуникаций и обнаружения любых подозрительных действий, таких как попытки передачи конфиденциальной информации третьим лицам или изменение условий сделок без соответствующего разрешения.

В борьбе с коррупцией DLP-система помогает обнаруживать и предотвращать несанкционированные действия с конфиденциальными данными, связанные с получением взяток, конфликтом интересов, вымогательством, неправомерным использованием ресурсов организации и другими видами коррупции.

Внутренний контроль также является важной задачей DLP-системы. Она позволяет контролировать исполнение управленческих решений, определять сокрытие нарушений и факты саботажа, а также проводить анализ реакций на различные распоряжения.

Наконец, DLP-система способствует обеспечению внутренней безопасности организации, выявляя компрометирующие связи, признаки шпионажа и разведки, предотвращая мошенничество и нарушения законодательства.

Криптографические методы защиты. Пересылаемую информацию между пользователями в социальных сетях зачастую шифруют программой PGP. Он шифрует сообщения с помощью открытого (публичного, public) ключа и расшифровывает их с помощью закрытого (секретного, private) ключа.

Шифрование PGP включает в себя такие этапы:

1. Хеширование;

2. Сжатие данных;

3. Шифрование с симметричным ключом;

4. Шифрование с открытым ключом.

Сеансовый ключ получается с помощью криптографически стойкого генератора псевдослучайных чисел, затем он шифруется открытым ключом получателя. Открытые ключи соответствуют адресу электронной почты или имени пользователя. При генерации ключей задаются их владелец, тип ключа, длина ключа и срок его действия.

PGP также позволяет использовать цифровые подписи. Подписанное закрытым ключом зашифрованное сообщение получатель может проверить открытым ключом. Если сообщение до расшифровки было изменено, то подпись будет признана недействительной.

Протокол Signal – криптографический протокол, обеспечивающий сквозное шифрование голосовых вызовов, видеозвонков и мгновенных сообщений. Этот протокол реализовывали такие популярные мессенджеры, как WhatsApp, Viber. Signal позволяет создавать сквозные зашифрованные групповые чаты, обеспечивает конфиденциальность, целостность, аутентификацию, прямую секретность, проверку назначения, согласованность участников, отказ от сообщений, отказ от участия, асинхронность. Он не обеспечивает сохранение анонимности и требует наличие серверов для ретрансляции сообщений и хранения информации об открытом ключе.

Пользователи самостоятельно оставляют много персональных данных в социальных сетях. Это объясняется самой сутью социальных сетей – обмениваться информацией с другими пользователями. Эта информация в руках злоумышленников может повлечь негативные последствия.

2.3. Реализация и анализ эффективности разработанных рекомендаций по формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации на базе ГПБОУ «ЮУрГТК» г. Челябинска

Для проведения анализа эффективности разработанных рекомендаций был использован метод анкетирования. Оценка результатов производилась в 2 этапа, первый из которых проводился для сбора информации об уровне формирования информационной безопасности личности у студентов до апробации разработанных рекомендаций и после. Для оценки студентам группы ИС-31 в количестве 30 человек была предоставлена ссылка на анкетирование, разработанное на платформе Online Test Pad. Анкетирование расположено по адресу https://onlinetestpad.com/xjr33vzd32tse.

Online Test Pad – бесплатный многофункциональный сервис для проведения анкетирования и обучения.

Возможности сайта:

1. Гибкая настройка опроса параметрами: В конструкторе опросов предусмотрено большое количество различных настроек. Можно быстро и удобно создать опрос для любых целей;

2. Одиннадцать типов вопросов: Одиночный выбор, множественный выбор, матрица одиночных выборов, матрица множественных выборов, ввод текста, ответ в свободной форме, выбор из списка, матрица выборов из списка, ранжирование, загрузка файла, служебный текст;

3. Удобный инструмент статистики: Пользователю доступен просмотр каждого результата, статистики ответов по каждому вопросу. В табличном виде представлены ответы на все вопросы, которые пользователь может сохранить в Excel;

4. Стилизация и брендирование: Широкие возможности для управления внешним видом опроса (цвет, шрифт, размер, отступы, рамки и многое другое) с возможностью добавить собственный логотип бренда;

5. Удобно на всех девайсах: Интерфейс заполнения опросов адаптирован под любые размеры экранов. Опросы удобно заполнять как на персональных компьютерах, так и на планшетных и мобильных устройствах.

Способы доступа к опросу:

1. Основная ссылка: По основной ссылке опрос всегда доступен. Эту ссылку подобрать практически невозможно, поэтому опрос заполнят только те, кому пользователь отправит эту ссылку;

2. Виджет для сайта: Специальный html-код, который позволит пользователю встроить опрос на собственный сайт, блог, форум;

3. Публикация в общий доступ: Возможность опубликовать опрос в общий доступ на сайте в соответствующую категорию. Опрос сможет заполнить любой пользователь сайта;

4. Приглашения: с помощью приглашений есть возможность сформировать группы пользователей и разослать им приглашение по email с персонализированной ссылкой на заполнение опроса.

Анкетирование предназначено для выявления сформированных знаний об информационной безопасности личности в социальных сетях студентов в профессиональной образовательной организации. Сайт, на котором опубликовано анкетирование, является бесплатным и общедоступным, а также поддерживается не только на ПК, но и на мобильных устройствах.

Для ответа на вопрос было предложено использование 3-балльной системы оценки, где: 0 – отсутствие влияния угроз (проблем) ИБ; 1 – низкий уровень влияния угроз (проблем) ИБ; 2 – высокий уровень влияния угроз (проблем). Система оценки анкетирования представлена в таблице 1. В

таблице 2 представлены результаты анкетирования до интеграции разработанных рекомендаций.

Таблица 1 - Система оценки анкетирования

	часто	редко	никогда
Как часто Вы меняете пароли от аккаунтов?	2	1	0
Включаете ли Вы функцию двухфакторной аутентификации?	2	1	0
Проверяете ли Вы в настройках, где и когда входили в Вашу учетную запись?	2	1	0
Переходите ли Вы по ссылкам, полученным от знакомых в соц. сетях, не удостоверившись, действительно ли они делали рассылку?	0	1	2
Публикуете ли Вы в социальных сетях личную информацию: адрес проживания, номер телефона, место работы/учебы и т.д.?	0	1	2
Отвечаете ли Вы на сообщения, отправленные с незнакомых аккаунтов, с предложением заработать больше деньги без усилий?	0	1	2
Читаете ли Вы тексты с согласием на обработку персональных данных перед регистрацией?	2	1	0
Реагируете ли Вы на провокационные сообщения и комментарии в Ваш адрес?	0	1	2

Таблица 2 – Результаты анкетирования до интеграции разработанных рекомендаций

Вопрос	Суммарное количество баллов
Как часто Вы меняете пароли от аккаунтов?	37
Включаете ли Вы функцию двухфакторной аутентификации?	16
Проверяете ли Вы в настройках, где и когда входили в Вашу учетную запись?	21
Переходите ли Вы по ссылкам, полученным от знакомых в соц. сетях, не удостоверившись, действительно ли они делали рассылку?	49
Публикуете ли Вы в социальных сетях личную информацию: адрес проживания, номер телефона, место работы/учебы и т.д.?	29
Отвечаете ли Вы на сообщения, отправленные с незнакомых аккаунтов, с предложением заработать больше деньги без усилий?	22
Читаете ли Вы тексты с согласием на обработку персональных данных перед регистрацией?	12
Реагируете ли Вы на провокационные сообщения и комментарии в Ваш адрес?	31

Вопросы анкетирования «Информационная безопасность в социальных сетях», предложенные студентам на платформе Online Test Pad, представлены на рисунке 2 и рисунке 3.

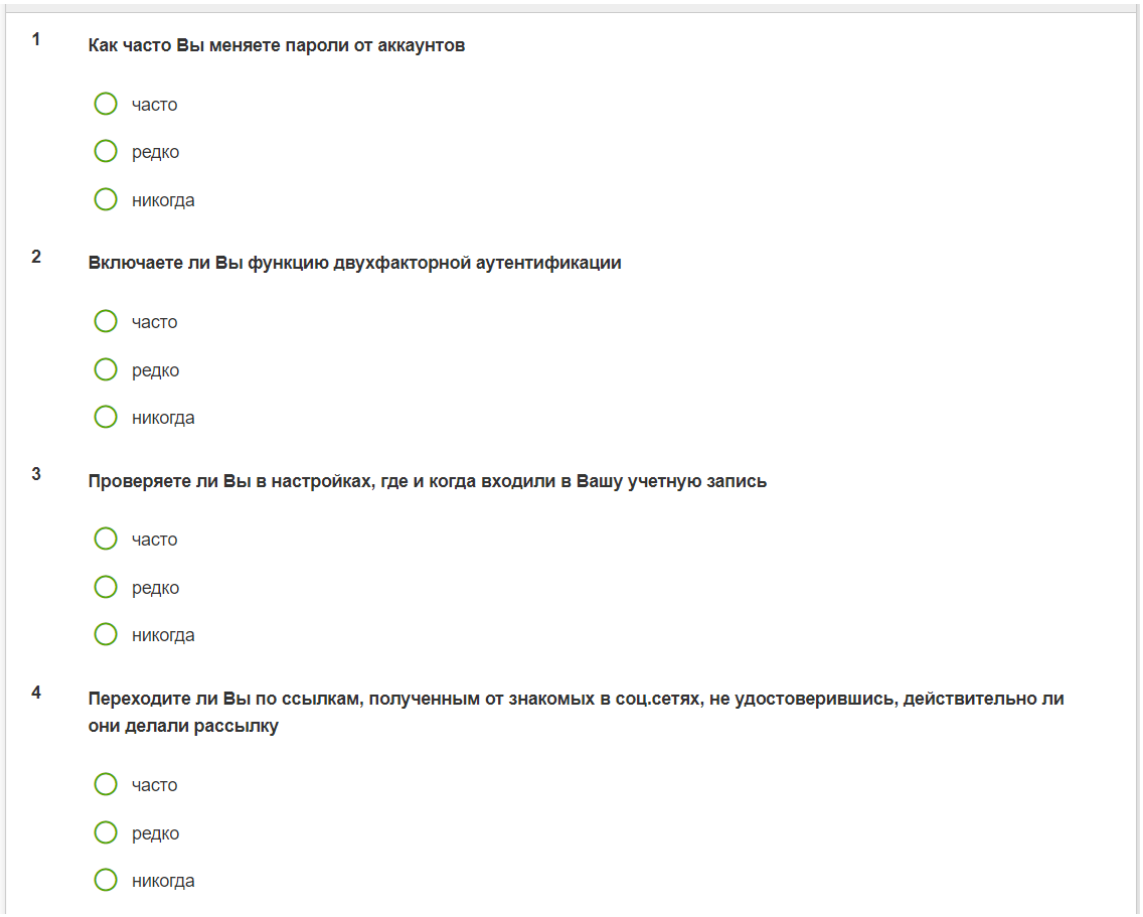

Рисунок 2 – скриншот вопросов 1-4 анкетирования «Информационная безопасность в социальных сетях»

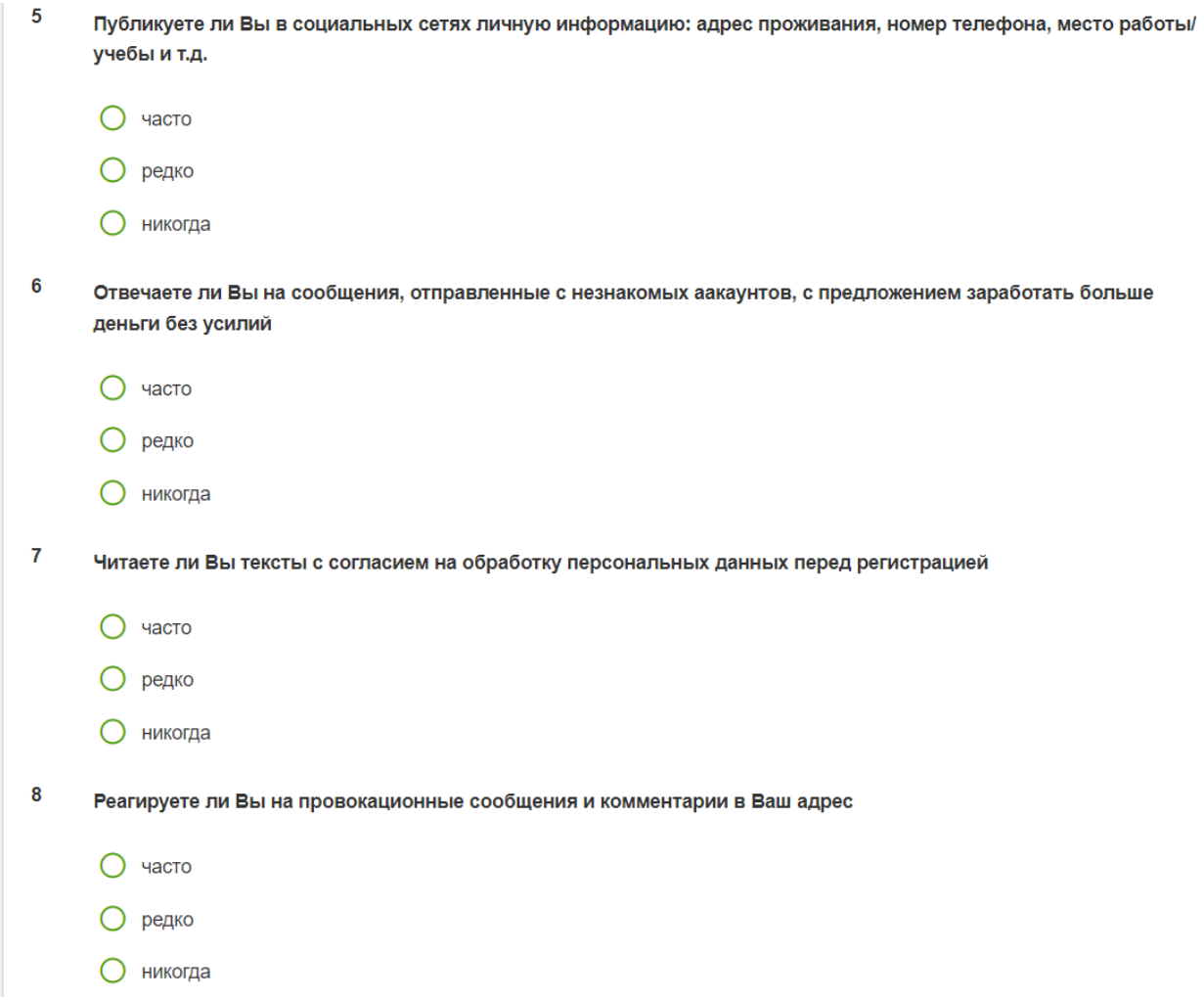

Рисунок 3 - скриншот вопросов 5-8 анкетирования «Информационная безопасность в социальных сетях»

Следующим этапом проведения исследования стала интеграция разработанных рекомендаций на базе ГБПОУ «ЮУрГТК» г. Челябинска.

Было проведено воспитательное мероприятие (классный час), направленное на формирование информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации.

После этого проведено повторное анкетирование группы по ранее заданным вопросам. В таблице 3 представлены результаты повторного анкетирования.

Таблица 3 – Результаты анкетирования после интеграции разработанных рекомендаций

Вопрос	Суммарное количество баллов
Как часто Вы меняете пароли от аккаунтов?	53
Включаете ли Вы функцию двухфакторной аутентификации?	33
Проверяете ли Вы в настройках, где и когда входили в Вашу учетную запись?	46
Переходите ли Вы по ссылкам, полученным от знакомых в соц. сетях, не удостоверившись, действительно ли они делали рассылку?	25
Публикуете ли Вы в социальных сетях личную информацию: адрес проживания, номер телефона, место работы/учебы и т.д.?	9
Отвечаете ли Вы на сообщения, отправленные с незнакомых аккаунтов, с предложением заработать больше деньги без усилий?	11
Читаете ли Вы тексты с согласием на обработку персональных данных перед регистрацией?	41
Реагируете ли Вы на провокационные сообщения и комментарии в Ваш адрес?	13

На рисунке 4 представлена схема, визуально отражающая динамику изменений уровня цифровой безопасности личности студентов до и после интеграции разработанных рекомендаций.

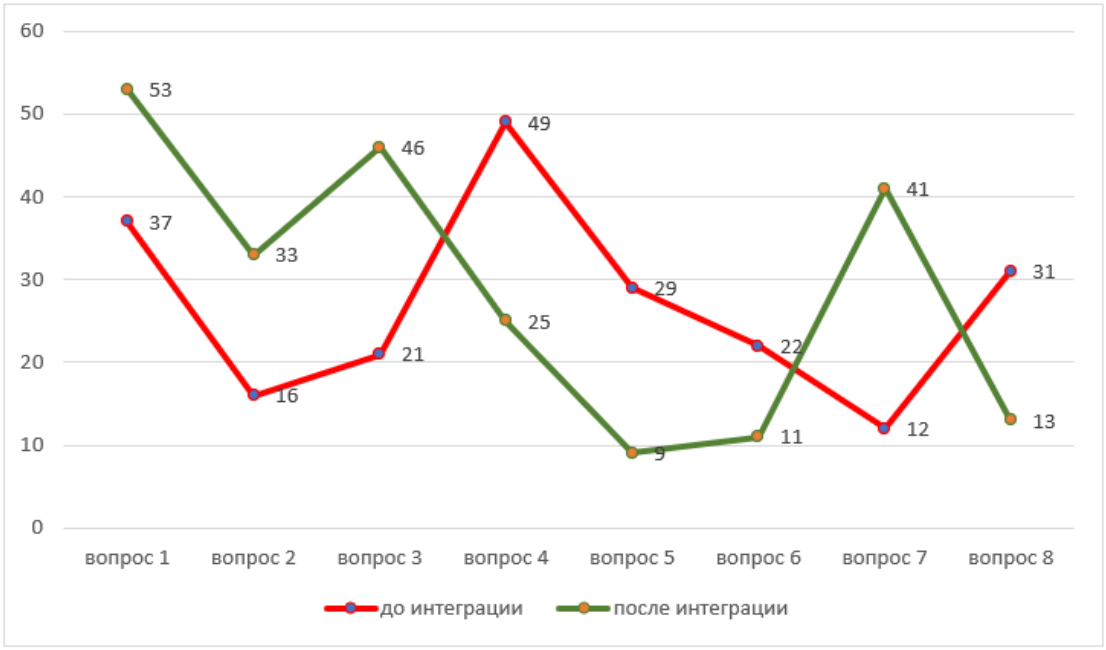

Рисунок 4 - Динамика изменений уровня цифровой безопасности личности студентов до и после интеграции разработанных рекомендаций

Как видно из приведенных таблиц и графика, наблюдается снижение уровня влияния угроз и проблем информационной безопасности личности в социальных сетях на студентов ГБПОУ «ЮУрГТК».

Приведенные результаты свидетельствуют о значительном сокращении влияния угроз и проблем ИБ и, как следствие, повышении информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации ГПБОУ «ЮУрГТК» г. Челябинска.

Выводы по Главе 2

В ходе исследования были разработаны рекомендации по формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации.

В течение семестра проводились профилактические мероприятия по формированию информационной безопасности личности в социальных сетях, на которых были использованы разработанные в рамках исследования рекомендации.

Также описаны результаты интеграции разработанных рекомендаций в колледже и приведены итоговые данные по оценке уровня формирования информационной безопасности личности у студентов. Полученные данные подтверждают целесообразность использования разработанных рекомендаций, а также указывают на необходимость дальнейшего использования данной системы в деятельности данного образовательного учреждения.

ЗАКЛЮЧЕНИЕ

Обеспечение информационной безопасности в мессенджерах и социальных сетях - актуальная проблематика не только для корпоративных структур, коммерческая информация и интеллектуальный капитал которых находится в поле поиска злоумышленников, но и для образования.

Информационная безопасность является важным аспектом в использовании популярных социальных сетей. В связи с ростом цифровой коммуникации и обменом информацией, защита данных и личной информации становится все более актуальной задачей.

Исходя из этого, важно определить то, какие инструменты и механизмы необходимо применять, чтобы формировать информационную безопасность виртуального пространства социальных сетей, сохраняя интересы всех его участников.

В процессе исследования темы была изучена сущность информационной безопасности личности в социальных сетях, рассмотрена классификация угроз информационной безопасности в социальных сетях, разработаны рекомендации по формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации, проанализирована эффективность разработанных рекомендаций по формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации на базе ГПБОУ «ЮУрГТК» г. Челябинска.

Исследовательская работа осуществлялась в условиях ГБПОУ «Южно-Уральский государственный технический колледж» и показала, что полученные результаты до и после интеграции разработанных рекомендаций по формированию информационной безопасности личности в социальных сетях свидетельствуют о значительном снижении негативного влияния угроз и проблем информационной безопасности на студентов.

Соответственно можно сделать вывод, что разработанные рекомендации, направленные на формирование информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации, являются эффективными.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций среднего профессионального образования с целью повышения эффективности формирования информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации.

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

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Амелин Р. В. Информационная безопасность. Конспект лекций // Амелин Р.В. Лаборатория преподавателя [Электронный ресурс]. URL: rv-lab.ru (2017).

2. Андреев К. Метод оценки экономической эффективности подразделения по защите информации / К. Андреев. – URL: https://lib.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnostipodrazdeleniya-po-zashite-informacii (дата обращения: 24.10.2024).

3. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/33430.html (дата обращения: 25.10.2024). — Режим доступа: для авторизир. Пользователей

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

5. Богатырева Юлия Игоревна. Подготовка будущих педагогов к обеспечению информационной безопасности школьников: диссертация ... доктора педагогических наук: 13.00.08 / Богатырева Юлия Игоревна; [Место защиты: Тульский государственный университет]. - Тула, 2014.- 416 с.

6. Бондаренко Е. Социальные сети как инструмент развития: виды и возможности / Е. Бондаренко. – URL: http://www.trainings.ru/library/articles/?id=10067 (дата обращения 20.10.2024).

7. Бояров Е.Н. Теоретические основы построение безопасной информационной образовательной среды подготовки педагогов в области безопасности жизнедеятельности. Социосфера (2012. № 4 С. 101–106)

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

9. Владимирова Т.В. Сетевые коммуникации как источник информационных угроз [Электронный ресурс] // URL: http://ecsocman.hse.ru/data/2011/09/20/1267451215/Vladimirova.pdf (дата обращения 05.10.2024)

10. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 2-е изд. — Москва : ИНТУИТ, 2016. — 266 с. — ISBN 978-5-94774-821-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100295 (дата обращения: 13.12.2024). — Режим доступа: для авториз. пользователей.

11. Гель А.В. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ / А.В. Гель, А. О. Путилов // Скиф. – 2020. – №5-1 (45). – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-vsotsialnyh-setyah (дата обращения: 10.10.2024).

12. Годик Ю.О. Угрозы и риски безопасности детской и подростковой интернет-аудитории // Вестник Московского университета. 2011. Сер. 10. № 6. 115-129 с.

13. Горбатюк Я.С., Кибербуллинг как педагогическая проблема — Актуальные проблемы физической культуры и безопасности жизнедеятельности, Сборник научных трудов факультета физической культуры и безопасности жизнедеятельности. Под редакцией Л.В. Кашицыной. Саратов, 2022, с. 53-57

14. Ефимова Е.С. Кибербуллинг как проблема психопедагогики виртуальных сред // Успехи в химии и химической технологии. 2019. Т. 28. №7(156). С.65-66

15. Журин А. А. Информационная безопасность как педагогическая проблема // Педагогика. - 2001. - № 4. - С. 48-55.

16. И. Астайкин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко: Информационная безопасность и защита информации: сборник статей в 2 т. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2015. – 498 с.: ил. ISBN 978-5-9515-0295-7 ISBN 978-5-9515-0296-4 (т. 1)

17. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебное пособие. Авторы: Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2021. – 198 с 92

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

19. Корнюшин П.Н., Костерин А.С. Информационная безопасность: Учебное пособие. - Владивосток: ТИДОТ ДВГУ, 2003. - 154 с.

20. Кривоухов А.А. Оценка информационной безопасности интернет-среды пользователями социальных сетей / А. А. Кривоухов // Коммуникология. – 2018. – №1.

21. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2021. — 368 с.

22. Максименко В. Н., Ясюк Е. В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. 2017. №2 (4). URL: https://cyberleninka.ru/article/n/osnovnye-podhody-k-analizu-i-otsenke-riskov-informatsionnoy-bezopasnosti (дата обращения: 13.12.2024).

23. Марков А.А. Актуальные вопросы информационной безопасности в постиндустриальном обществе. Монография / Изд-во СПбГИЭУ, 2010. 287 с

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

25. Муромцева А.В. Проблемы информационной безопасности в социальных сообществах в сети Интернет / А. В. Муромцева, В. В. Муромцев // Вестник РГГУ. Серия «Экономика. Управление. Право». – 2016. №3 (5).

26. Нестеров С. А. Основы информационной безопасности: учеб. пособие. — 5-е изд., стер. — Санкт-Петербург: Лань, 2019. — 324 с. [Электронный ресурс] // URL: https://e.lanbook.com/book/114688 (дата обращения 07.10.2024)

27. Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2023. — 287 с. — ISBN 978-5-238-02857-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/141624.html (дата обращения: 25.10.2024). — Режим доступа: для авторизир. Пользователей

28. Основы информационной безопасности : учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия-Телеком, 2011. — 558 с. — ISBN 5-93517-292-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111016 (дата обращения: 13.12.2024). — Режим доступа: для авториз. пользователей.

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

30. Распоряжение Правительства РФ от 28 апреля 2023 г. № 1105-р "Об утверждении Концепции информационной безопасности детей в РФ и признании утратившим силу распоряжения Правительства Российской Федерации от 2 декабря 2015 г. N 2471-р" // Справочная правовая система «Консультант Плюс». URL:

https://www.consultant.ru/document/cons_doc_LAW_446568/?ysclid=lmuyhtuq9c856989848.

31. Рыбакова О.С. Законодательное регулирование обеспечения безопасности ребенка в интернет-пространстве // Правовая информатика. 2017. №4. 49-54 с

32. Семененко В.А. Информационная безопасность. М.: МГИУ, 2010. 277 с. 10. Сычев Ю.Н. Основы информационной безопасности. М.: ЕАОИ, 2007. 300 с.

33. Скородумов, БЮ.И.. О ПОНЯТИЙНО-ТЕРМИНОЛОГИЧЕСКОМ АППАРАТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 15, n. 4, p. 43-45, dec. 2008. ISSN 2074-7136. https://bit.mephi.ru/index.php/bit/article/view/955. (Дата обращения: 13.12.2024)

34. Таржанов Т.В., Кудряшов В.Е., Макарова Д.Г., Вредоносное программное обеспечение и методы борьбы с ним — Интерэкспо Гео-Сибирь, том 9, 2022, с. 15-18

35. Тумбинская М.В. Обеспечение защиты от нежелательной информации в социальных сетях / М. В. Тубинская // Вестник МГУ. – 2017. – №2.

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

37. Усенко, Р. С. Информационная безопасность в социальных сетях / Р. С. Усенко // Проблемы информационной безопасности социально-экономических систем : Труды X Международной Юбилейной научно-практической конференции, Симферополь ¾ Гурзуф, 15–17 февраля 2024 года. – Симферополь: ИП Зуева Т.В., 2024. – С. 116-117.

38. Усенко, Р. С. О последних изменениях в российском сегменте социальных сетей / Р. С. Усенко // Теория и практика экономики и предпринимательства: труды XIX Международной научно-практической

конференции, Симферополь - Гурзуф, 14-16 апреля 2022 года. - Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. - С. 267-268.

39. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 с. — ISBN 978-5-4497-2418-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133957.html (дата обращения: 25.10.2024). — Режим доступа: для авторизир. Пользователей

40. Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" от 29.12.2010 N 436-ФЗ

41. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

42. Федеральный закон от 27.07.2006 N 152-ФЗ // Статья 7. Конфиденциальность персональных данных (ред. от 24.04.2020) «О персональных данных»

43. Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 01.07.2021) "О защите детей от информации, причиняющей вред их здоровью и развитию" // Справочная правовая система «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_108808/?ysclid=lmuy9xvpi9579529526.

44. Фенина Виктория Владимировна Особенности речевого манипулирования в электронных спам-письмах // Язык и культура. 2017. №37. [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/osobennostirechevogo-manipulirovaniya-v-elektronnyh-spam-pismah (дата обращения: 07.10.2024).

45. Фенина Виктория Владимировна Особенности речевого манипулирования в электронных спам-письмах // Язык и культура. 2017. №37. [Электронный ресурс] // URL:

https://cyberleninka.ru/article/n/osobennostirechevogo-manipulirovaniya-v-elektronnyh-spam-pismah (дата обращения: 07.10.2024).

46. Фомина Н. А. Использование методов социальной инженерии при мошенничестве в социальных сетях. // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодёжи. 2022. С 443-453

47. Цирлов, В.Л. Основы информационной безопасности [Текст] : краткий курс / В. Л. Цирлов. - Ростов-на-Дону : Феникс, 2008. - 254 с. : ил. - (Профессиональное образование). - Библиогр.: с. 167-170 (44 назв.). - На пер. авт. не указан. - ISBN 978-5-222-13164-0 : Б. ц.

48. Черкасенко О.С. Травля в социальных сетях // Наука и Мир. 2020. Т. 2. № 8 (24). С. 107-108

49. Что такое фишинг? , CISCO , [Электронный ресурс] // URL : https://www.cisco.com/c/ru_ru/products/security/email-security/what-isphishing.html

50. Ю. С. Уфимцев [и др.] ; Методика информационной безопасности Московская академия экономики и права. - Москва : Экзамен, 2004. - 542 с. - Библиогр. в подстроч. примеч. - Авт. указ. на обороте тит.л. - ISBN 5-94692-517-2 (в пер.)

51. Ясенев В.Н. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ: Учебное пособие – Н. Новгород: Изд-во ННГУ, 2006 г.

ПРИЛОЖЕНИЕ

Классный час

Для обучающихся ПОО

«Информационная безопасность личности в социальных сетях»

Цель занятия: формирование культуры безопасного и эффективного использования цифровых ресурсов и устройств, знакомство с основами безопасности в сети и повышение уровня цифровой грамотности.

Задачи:

1. Познакомить видами Интернет-угроз и противоправных посягательствах в сети Интернет.

2. Познакомить студентов с правилами медиа-безопасности, с сайтами помощи в случае Интернет-угроз.

3. Сформировать чувство ответственности за свое пребывание в Интернет, за воспитание будущих поколений.

Оборудование: анкеты для студентов, памятки для студентов, презентация, видеофрагменты («Безопасность в Интернете», «Развлечения и безопасность в Интернете», социальный ролик «Безопасный Интернет-детям!»), проектор, ПК.

Ход занятия

1. Организационный момент.

- Добрый день, ребята! Нашу встречу с вами я хочу начать со следующего стихотворения: Ты есть, я есть, он есть,
А жизнь у каждого своя.
И ей цена – достоинство и
честь,
Есть возраст переходных
лет, Какой бы сложной не
была она. Для многих
начинается рассвет,
А кто-то погружается во
тьму.

Ты есть, я есть, он есть,
Лишь вместе мы сумеем зло
пресечь
И сохранить достоинство, чтоб
жить.

2. Сообщение темы, цели, задач занятия.

- Сегодня наш классный час называется «Информационная безопасность личности в социальных сетях». Как вы полагаете, о чем мы на этом уроке поговорим? (ответы студентов) А кто может сказать, что такое медиа-безопасность? (ответы студентов) Слово «медиа-безопасность» сочетает в себе два термина – медиа-грамотность и информационная безопасность. В международном праве «Медиа-грамотность - грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг». В российском законодательстве «Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию». Такие понятия появились благодаря инициативе Уполномоченного при Президенте РФ по правам ребенка Павла Астахова, который сказал: «Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиа-грамотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие

опасности подстерегают их в сети и как их избежать».

Я думаю, что каждый хочет жить в мире и безопасности, а это значит, что на душе будет радостно и спокойно. Мы не зря поднимаем сегодня этот вопрос. Как было бы здорово, если бы каждый человек соблюдал все правила приличия, был бы всегда доброжелателен. Но, к сожалению, так не бывает. И очень часто по чьей-то вине, нарушается мир другого человека.

С 1 сентября 2012 г. вступил в силу закон «О защите детей от информации, причиняющий вред их здоровью и развитию». В связи с этим, каждый пользователь должен знать о правилах ответственного и безопасного поведения в современной информационной среде, способной нанести вред физическому и психическому здоровью человека. Не многие знают, что более 80% вербовочного процесса детей, подростков и молодых людей проходит через Интернет! Сегодня мы рассмотрим наиболее распространённые виды Интернет-угроз, через которые злоумышленники воздействуют на человека, а также узнаем о способах защиты от противоправных посягательств в сети Интернет и мобильной сотовой связи. Ведь недаром поговорка гласит: «Предупреждён – значит вооружён».

3. Работа по теоретической части занятия. Интернет – это не только пространство для поиска информации, ведения личной переписки, знакомства с новыми людьми и общения, это еще и источник опасности, которую можно предотвратить. Для это нужно быть осведомленным о видах угроз, исходящих из Сети. Какие угрозы встречаются наиболее часто? Прежде всего:

• Угроза заражения вредоносным ПО.

• Доступ к нежелательному содержимому. Это насилие, наркотики порнография, страницы, подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще

всего порнографического характера;

• Контакты с незнакомыми людьми с помощью чатов, электронной почты или социальных сетей. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить молодежь выдать личную информацию.

• Неконтролируемые покупки в Интернет-магазинах. Подростки и молодые люди в возрасте 18-20 лет являются наиболее уязвимой группой и подвергаются наибольшей опасности. Они стремятся исследовать свою сексуальность, уйти из-под контроля родителей и завязать новые отношения вне семьи. Несмотря на то, что общение в Интернете может быть полностью анонимным, они больше подвержены опасности, даже если до конца не осознают возможные последствия.

Наиболее уязвимыми для злоумышленников являются следующие категории молодых людей:

• новички в Интернете, не знакомые с сетевым этикетом;

• недружелюбные пользователи;

• те, кто стремится попробовать все новое, связанное с острыми ощущениями;

• активно ищущие внимания и привязанности; • бунтари; • одинокие или брошенные;

• любопытные;

• испытывающие проблемы с сексуальной ориентацией;

• те, кого взрослые могут легко обмануть;

• те, кого привлекает субкультура, выходящая за рамки понимания их родителей.

Современный Интернет называют большой душеловкой? Как она работает? Мошенничество в Интернете существует столько же, сколько и сама Всемирная Сеть. На просторах Интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. Из года в год злоумышленники придумывают всё новые и новые уловки, направленные на

то, чтобы обмануть своих потенциальных жертв. В отличие от таких интернет-угроз, как вирусы, троянские программы, программы-шпионы, СМС-блокеры, спам и др…, мошенничество примечательно тем, что мишень злоумышленника – не компьютер, а человек, у которого, как известно, свои слабости (н-р, страх, любопытство, легковерность…). Человек в наше время стал товаром. Рынок живого товара сейчас догоняет обороты наркотиков. Поэтому, только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной.

По статистике, число детей и подростков – пользователей Интернета в России составляет около 14 млн. человек, из которых две трети выходят в Интернет ежедневно. Возраст начала самостоятельной работы в Сети для российских детей сейчас составляет 10 лет. Примерно 30% детей, пользующихся Интернетом, проводят в Сети ежедневно более трех часов в день.

- Как Вы думаете, каким образом можно избежать негативных последствий при использовании сети Интернет и социальных сетей? (ответы студентов). Верно. Сейчас расскажу Вам об основных правилах для безопасного использования сети Интернет и социальных сетей.

11. Использовать надёжные пароли для доступа к профилю социальной сети и ящику электронной почты, к которой привязан этот профиль. Обратить внимание — пароли для почты и для соцсети должны быть разными.

12. Надёжный пароль должен содержать не меньше 12 символов, в том числе заглавные и строчные буквы, цифры и специальные символы. Не рекомендуется использовать «секретные» пароли из русских слов, набранных на английской раскладке, все актуальные программы для перебора паролей очень быстро раскроют такую хитрость.

13. Необходимо обязательно включить двухфакторную аутентификацию. Эту функцию поддерживают все популярные соцсети. Тогда для входа в профиль с нового устройства нужно будет ввести дополнительный

код, направленный в СМС-сообщении на номер или полученный с помощью специальной программы-аутентификатора.

14. Проверить в настройках, где и с каких устройств входили в учётную запись. При необходимости подтвердить, что вход произведён пользователем, или отключить активные сеансы.

15. Проверить, какие приложения и сайты имеют доступ к учётной записи. Даже вполне безобидное приложение или сайт могут получить излишние права и доступ к аккаунту. Отключить доступ для всех приложений, которым в нём нет необходимости.

16. Не переходить по ссылкам, которые получили через социальные сети, даже если они получены от родственника, друга или знакомого. Необходимо позвонить отправителю по телефону или воспользоваться другим способом связи, чтобы выяснить, действительно ли он отправлял сообщение.

17. Не загружать файлы, которые присылают в соцсетях, если не обговорили это заранее с отправителем.

18. Не публиковать в соцсетях личные данные: номер телефона, адрес, место работы и даже настоящую фамилию. Используя эту информацию, злоумышленники могут составить убедительные фишинговые послания, на которые пользователь с большой вероятностью отреагирует.

19. Не вступать в споры, конфликты или агрессивные дискуссии в социальных сетях. В таком состоянии сложно действовать рационально, и, поддавшись эмоциям, можно совершить действия, которые приведут к утере контроля над профилем.

20. Не верить заманчивым предложениям заработать большие деньги без усилий.

Для входа в соцсети использовать только безопасные браузеры, загруженные из официальных источников. Установить и обновлять антивирусные программы, сканировать компьютер на наличие вредоносного ПО. Устаревшие версии не могут гарантировать защиту устройства от

ежедневно обновляющихся угроз информационной безопасности, а значит, и личной безопасности пользователя.

Перед регистрацией в социальной сети необходимо обязательно ознакомиться с текстами Согласия на обработку персональных данных, Пользовательским соглашением и Политикой конфиденциальности, а также иными документами, размещенными на сайте. Так можно понять, кому персональные данные могут быть переданы.

Использовать разные пароли для соцсети и для электронной почты, которая указывается в социальной сети. Пользоваться специализированными генераторами паролей или выбирать сложные пароли, регулярно их менять и не хранить в открытом виде.

Завести два адреса электронной почты: частный - для переписки (который не публикуется в общедоступных источниках), и публичный – для соцсетей, форумов, чатов и т. д. Если нужно сообщить свой приватный адрес в переписке, лучше сделать это способом, непригодным для автоматического прочтения сборщиком адресов, например, в виде картинки.

Настроить профиль в социальной сети таким образом, чтобы только друзья могли его просматривать. Такая настройка лишит злоумышленников возможности получить доступ к информации, которую пользователь скрыл от просмотра незнакомцев.

Внимательно относиться к информации, которая публикуется о себе в социальной сети. Использовать никнейм. Злоумышленник может использовать личную информацию и войти в учетную запись, а также создать правдоподобные истории для злоупотребления доверием и просьбами о переводе денежных средств.

Перед тем как выложить фотографию, оценить каждую деталь: свой внешний вид, окружающую местность, людей, находящихся рядом, и многое другое. Даже если пользователь сразу удалил публикацию, кто-то мог ее сохранить. Помнить о возможных репутационных рисках.

Не устанавливать приложения для соцсетей, которые позволяют отследить активность подписчиков на странице. Нередко при установке такие сервисы запрашивают логин и пароль от аккаунта – все это ухищрения хакеров, создающие риски последующего взлома страницы.

Не отправлять важные документы через социальные сети и не публиковать фотографии документов. Часто обнаруживается, что молодые люди, когда получают водительские права, публикуют их фотографии в открытом доступе.

Такими фотографиями могут воспользоваться злоумышленники, изменив их с помощью графических редакторов. Впоследствии от имени пользователя они могут совершать действия, которые будут иметь юридически значимые последствия.

Перепроверять сообщения от друзей с просьбой срочно выслать денег. Сначала перезвонить другу и удостовериться, что просьба действительно направлена от него.

Проявлять осторожность при переходе по ссылкам, полученным в сообщениях от других пользователей, если не знакомы с отправителем.

Воздерживаться от ответа на провокационные сообщения и комментарии других пользователей. Блокировать навязчивых провокаторов.

Продвинутые социальные сети ввели двухфакторную аутентификацию. Она состоит из двух этапов: первый – вход с помощью логина и пароля, второй – уникальный код по смс или уникальный список кодов, которые действуют лишь единожды, или специальный код, который можно сканировать с помощью мобильного телефона.

4. Итог. Современный мир, который вас окружает, сложен и труден. Нужно быть очень умным, осторожным, сообразительным, чтобы жить в нем. Безопасность в этом мире зависит от каждого из нас, прежде всего, от

отношения к самому себе. Природа создала всё для того, чтобы человек был счастлив. Деревья, яркое солнце, чистую воду, плодородную почву. И нас людей – сильных, красивых, здоровых, разумных. Человек рождается для счастья.

5. Рефлексия. И в заключении я попрошу тех, кому этот урок стал интересным, полезным и кто считает, что Интернет должен стать для нас другом, хором сказать: «Я за безопасный Интернет!». Всем спасибо.