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 ПОО

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:
78 % авторского текста

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

Выполнил:
Студент группы ЗФ-309-210-2-1
Рыжиков Михаил Сергеевич

Научный руководитель:
кан.пед.н., доцент кафедры АТ, ИТ и МОТД
Гафарова Елена Аркадьевна

Челябинск
2024

Оглавление

ВВЕДЕНИЕ

Появление и внедрение новейших технических устройств, работающих на основе сетевой логики, принудительно инициировало эволюцию многих форм социальной активности. Особенно весомое влияние данные процессы повлияли на сферу сетевой коммуникации, способствуя появлению более простых инструментов взаимодействия между пользователями и сетевыми факторами.

Однако наряду с огромным количеством выгодных и продуктивных решений, основанных на свободном доступе и обмене информацией с участниками любых возрастных, гендерных, социальных, национальных групп, своё развитие получили также различного рода деструктивные процессы, как информационные атаки, информационный терроризм, хищение данных, сокрытие и искажение информации. Эти феномены стали объектом активных дискуссий и исследований в научных кругах, задавая курс на актуальную проблематику, связанную с минимизацией и ликвидацией информационных угроз, защитой информационной безопасности личности и особенностями сетевой коммуникации.

Широкое обсуждение в научном дискурсе получили такие темы, как информационная безопасность общества, информационные войны, манипуляции и скрытое принуждение, психологическая безопасность личности в интернет-пространстве. Современные научные исследования, как правило, охватывают большую сферу вопросов, позволяя изучать особенности современных информационных угроз со всех сторон.

Информатизация общества навязала современному миру свои правила. С одной стороны люди получили доступ к нескончаемому потоку информации, который открывает двери на совершенно новые уровни познания и усваивания новейших данных, с другой же, человечество просто неспособнофильтровать полезную информацию от «токсичной» и «неправильной» в таком объёме, в котором она поступает. Таким образом можно сделать несложный вывод, что с наступлением цифровой эры, человечество получило как огромный прирост

в функциональном и информационном плане, так и огромный ворох проблем, связанных с непрерывным развитием информационной среды.

К положительным факторам можно отнести массовое отторжение унификации и стандартизации – каждый член общества стал волен проявлять себя в тех областях в каких он непосредственно был заинтересован, стерлись границы и появилась возможность легко найти единомышленников, где каждый индивидуум мог легко выражать свое субъективное мнение по любому вопросу.

Благодаря огромному информационному потоку, человечество получило инструментарий для быстрого принятия решений – если раньше требовалось как минимум быть подкованным в конкретной теме, сейчас же достаточно пары интернет- запросов, для принятия решения в важных вопросах.

К неоспоримым плюсам информатизации можно так же отнести и развитие, и рост всех видов интернет потребностей у населения, за счет доступности и многообразия видов интернет- досуга.

В информационном обществе неостановимо изменился приоритет ценностей, а с ними и обычный уклад жизни. Как пример если раньше люди с ограниченными возможностями могли только положиться на близких людей, теперь они могут зарабатывать деньги и обеспечивать себя сами. Благодаря тому насколько информационное пространство стало комфортным для конечных пользователей, оно несет собой прогрессивное развитие общества и в большей степени способствует его развитию, однако в некоторых ситуациях оно способно влиять негативным образом.

Как пример с развитием технологий остро встала проблема манипулирования сознанием людей, современные масс медиа способны влиять на взгляды людей, выставляя любые события под тем светом, каким им или тем, кто стоит за ними более выгодно. Так же не стоит забывать и о преступлениях, с ростом информционного пространства выросло и количество так называемых киберпреступлений, которые несут собой очень

негативный осадок как для обычный пользователей так и для государства, общества в целом. Помимо этого, с развитием информационных технологий стала актуальна проблема адаптации определенных категорий людей к новой среде. Так, в частности, огромное количество преподавателей и учителей, которые в силу своего возраста не были способны к такой радикальной перестройке существующего уклада и были вынуждены покинуть свои должности. Эта проблема так же не обошла стороной и пожилое поколение. Неспособные в полной мере освоить информационные технологии, данная категория людей стала наиболее подвержена негативному влиянию киберпреступлений, кибермошенничеству и шантажу со стороны преступников.

Объектом исследования является феномен информационной безопасности личности в сетевой коммуникации

Предметом исследования выступает алгоритм по обеспечению информационной безопасности личности в социальных сетях.

Цель исследования: разработать рекомендации по обеспечению информационной безопасности личности в социальных сетях

Для достижения цели исследования необходимо решить следующие задачи:

1. Изучить молодёжную аудиторию социальных сетей и дать им общую характеристику
2. Проанализировать угрозы и способы защиты от них контексте коммуникативных практик молодёжной аудитории социальных сетей
3. Выявить алгоритм и разработать рекомендации по обеспечению защиты личности от информационных угроз в условиях сетевой коммуникации для студентов СПО.

Выпускная квалификационная работа состоит из 60 страниц машинописного текста, содержит рисунков — 4, список использованных источников составляет 40 наименований.

Глава 1. Теоретические основы информационной безопасности личности в сетевой коммуникации

1.1 Информационная безопасность: сущность и особенности феномена

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 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. [19]

На сегодняшний день мы люди пытаемся получить доступ к большему объёму информации и экстраполировать её в своих интересах. На фоне этого вполне очевидно свою нишу заняли социальные сети, как нескончаемые источники информации и удобнейший ресурс для навязывания своего мнения. Конечному пользователю необходимо научится прокладывать себе путь через нескончаемые потоки информации, чтобы в конечном итоге получить интересующие его знания.

Глобальные информационные технологии заметным образом изменили привычные всем методы изучения и изменения информации. Человечество получило в свои руки инструменты и системы для межсетевого общения который облегчили коммуникацию и перевернули привычное общение как таковое. Раньше требовалось купить условную газету, чтобы получить сводку

последней информации о происходящем в мире, сейчас же достаточно просто зайти на главную любого браузера. Чтобы встретится и пообщаться с другим человеком раньше требовалось заранее договорится о встрече или позвонить по телефону, сейчас достаточно обычного сообщения в любой социальной сети, или видеозвонка. Исходя из этого один из самых популярных сервисов глобальной сети, который широко представлен в современных сетях являются популярные ныне социальные сети.

Впервые понятие социальных сетей в реальном мире ввел Дж. Барнс в 1954 г. Он определял их как социальное поле, в рамках которого люди являются друзьями или просто знакомы друг с другом. [5] Похожее определение было дано в 1987 г. психологами М.С. Денофф и П.А. Пилконис, которые определили социальную сеть как набор межличностных отношений, связывающих людей. [17]

В социальных сетях правдивость и реальность информации устанавливаются за счет реальных знакомств между людьми, которые входят в это самое сообщество и знакомы друг с другом за пределами социальных сетей. В таких сообществах все участники следуют правилам установленными админами и руководителями данной сети.

Социальные сети — это своего рода отголосок виртуального мира, он подчиняется тем же правилам и имеет ту же конструкцию. Если говорить проще, то социальные сети можно описать набором конкретных свойств, формирующих настроение и поведение всех участников сети, а именно неочевидность, безответственность и безнаказанность любых источников информации.

Как и любая популярная вещь социальные сети были обречены на огромный успех, что в конечном итоге закрепила их на пьедестале лидеров в интернет-среде. Однако они все так же имеют ворох проблем, которые используют определенные лица и владельцы сетей себе на благо.

Социальные сети по своей конструкции делятся на 3 категории, а именно:

-открытые;

-закрытые(корпоративные);

-условно открытые;

По направленности социальные сети могут быть: узкотематические, полемические, информационные и т.п. Одна из самых важных составляющих, непосредственно влияющих на жизнеспособность сети является её экономическая составляющая. То есть кто получает выгоду от её эксплуатации:

-владелец виртуального пространства;

-владелец сайта;

-участники сети (опосредственную, в случае открытой и условно открытой сети и непосредственно участники закрытой сети);

-группы людей, заинтересованных в реализации информационного воздействия:

Однако, кроме людей в социальных сетях можно найти и много различных сообществ, представляющих конкретные фирмы и организации из реального мира. Это продиктовано тем, что в современном обществе проще всего воздействовать на многомиллионную аудиторию через лидеров мнений, которые в большом достатке обитают в социальных сетях. Они помогают сформировать положительное мнение о продукте, навязывать молодой аудитории свою точку зрения, и просто вынудить приобрести продукцию рекламодателя.

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].

На сегодняшний день множество людей, не может даже представить своей жизни без социальных сетей. Утро такого человека будет начинаться нес какой-либо физической активности, а с просмотра новостных лент иобщения с друзьями. Люди становятся зависимы от общественного мнения исоциальных сетей, в частности. Социальные сети сопровождают человека напротяжении всего дня с момента пробуждения, до того момента как человекляжет в кровать. В такой ситуации человек почти полностью теряет контрольнад собственной жизнью. Им движет не желание к саморазвитию, а желание быть лучше остальных, показать, насколько он уникален и насколько его жизнь ярка и необычная, хотя зачастую это лишь грим и декорации. Человек теряет возможность трезво оценивать свою жизнь, ему необходимо что общество делало это за него посредством комментариев. В погоне за статусом человек теряет понимание о рамках приличия, дозволенности и безопасности.

С другой же стороны, социальные сети помогают человеку избавиться от одиночества. Здесь он может пообщаться с людьми, которых никогда не знал в жизни, он активно включается в коммуникацию между личностями. Однако, при это реально общение замещается виртуальным. Люди уходят в виртуальный мир, что приводит к трагическим последствиям, которые не решить без помощи специалиста, это превращается в реальное заболевание.

Социальные сети активно влияют на процесс коммуникации, в результате чего, отношение людей к окружающему миру изменяется, деформируется. Чувство нарциссизма противопоставляется семейным и национальными связям пользователя. Этот процесс, по мнению антрополога Ш. Теркл, включает в себя:

-исчезновение одиночества как части процесса социализации;

-зависимость от социальных сетей и гаджетов, обеспечивающих непрерывный процесс «виртуальной коммуникации» в ущерб «традиционны» социальным практикам общения;

-исчезновение причастности в региональной культуре;

-зависимость от гаджетов, часто западного производства;

-деформация процесса общения;

-отчуждения в семье;

-деформация языкового общения;

-формирование новой этики;

-потенциальное разрушение личного пространства;

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.

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. Наверняка каждый из вас сталкивался с таким феноменом : вы со своим другом обсуждали какой то продукт в котором вы заинтересованы и хотели бы приобрести, и вот во всех рекламных окнах начинает появляться именно этот продукт, знакомо, не правда ли?

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.

Можно понять точку зрения тех людей, что заходят в социальные сети чтобы найти группу единомышленников по интересующих их темам. Человек — это социальное существо, которому необходимо общественное общение в любых проявлениях. Социальные сети в свою очередь предоставляют

возможность высказываться на интересующие нас вещи анонимно, что открывают двери людям, с опаской оглядывающихся на большие скопления людей(интровертов) и прочих типов личностей к свободному самовыражению.

Из предоставленного выше, мы можем сделать вывод, что социальные сети имеют уйму негативных черт, которые могут легко подорвать психическое здоровье человеку и даже вынудить его на поступки, которые в отсутствие социальных сетей он вряд ли бы осуществил. 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.[9,10] 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.[1] Но в юридических документах в наибольшей степени находит отражение аспект, связанный с защитой программного обеспечения и обеспечением безопасности связи (коммуникации).

Однако существующая защищенность информационных ресурсов не гарантирует личности его информационной безопасности. Из-за

недозволенности существует огромная прослойка людей разово или нет попадавшие под влияние киберпреступников посредством шантажа и т. п. Они не обладают базовой информации о защите своего личного информационного пространства и попадаются на различные уловки, как пример каждый год в полицию обращаются огромное количество девушек и парней, которым злоумышленники отправили угрозу опубликовать их личные данные/фото/видео если они не переведут условную сумму на подставной кошелек. И с ростом пользователей социальных сетей количество киберпреступников не идет на спад, а наоборот только растёт. Таким образом можно сделать вывод что отражение возникающих информационных угроз напрямую зависит об осведомленности пользователей о способах их отражения.

1.2. Общая характеристика молодёжной аудитории социальных сетей

Для анализа молодёжной аудитории в социальных сетях, необходимо определить понятие молодёжи и разграничить хронологический интервал представителей, которые относятся к данной группе. В науке существует множество подходов и мнений о понятии «молодёжь». Так, например, такие учёные, как В. Т. Лисовский, И.С. Кон, Р.В. Сергеев, Л.Я. Аверьянов затрагивал данный термин. Однако, подходы у учёных разные, они отличаются олицетворением и не олицетворение молодёжи с социализацией, особенной восприимчивостью сознания и мировоззрением. Помимо этого, многие учёные ограничивают возраст молодёжи 30 годами [13].

До конца 2023 года в законодательном плане хронологический интервал молодёжи (16-30 лет) сохранялся и был таким же, как и в науке. Однако 30 декабря 2020 Президент Российской Федерации Владимир Путин подписал новый федеральный закон, который вступил в силу 10 января 2021 года, «О молодёжной политике в Российской Федерации» №489. Помимо того, что Федеральный закон был создан для того, чтобы регулировать все возникающие взаимоотношения между субъектами молодёжной политики, в статье 2 Федерального закона закреплены расширенные рамки хронологического интервала. Так, нижняя хронологическая грань молодёжи стала равняться 14 годам, а верхняя повысила на пять лет и стала равной 35 годам [2].

В рамках государство такая мера важна так, как расширяется перечень лиц, которые могут претендовать на различные меры поддержки для молодых людей и семей. Однако, в рамках настоящей выпускной квалификационной работы это также важно так, как позволяет определить, каких пользователей считать молодёжной аудиторией и учитывать при сравнении социальных сетей между друг другом, а каких пользователей считать возрастной аудиторией.

Далее мы рассмотрим лучшие и актуальные российские социальные сети, которыми можно пользоваться в 2023 году. Это небольшой рейтинг

платформ, которые станут альтернативой зарубежным — и некоторым заблокированным — соцсетям: например, «Инстаграму» или TikTok.

В подборку попали только рабочие и актуальные платформы. Так, например, здесь не будет LiveJournal («Живой Журнал» или просто «ЖЖ»), так как этот сервис давно потерял свою популярность.

ВК (ВКонтакте) — самая популярная российская социальная сеть. Основана в 2006 году Павлом Дуровым. Сегодня принадлежит компании VK (ex. Mail.ru Group).

Главная страница соцсети ВК. Официальный сайт: https://vk.com/. Это своеобразный аналог зарубежной социальной сети Facebook. Что можно делать в ВК:

1. Общаться с друзьями через встроенный мессенджер.
2. Слушать музыку.
3. Делиться фотографиями.
4. Смотреть видео и прямые трансляции.
5. Вести свое сообщество: например, личный блог или группу по интересам.
6. Запускать таргетированную рекламу для продвижения бизнеса.
7. Размещать объявления о продаже.
8. Коротки видеоролики, как в «ТикТоке».

Пользоваться ВК можно с компьютера (веб-версия) и телефона (приложение VK для Android и iOS).

Одноклассники (ОК) — одна из крупнейших социальных сетей в России и странах ближнего зарубежья, входит в холдинг VK (ранее Mail.Ru Group). Сайт создан в 2006 году и в настоящее время переведен на 16 языков, включая русский.

Так выглядит профиль в Одноклассниках. Официальный сайт: https://ok.ru/.

ОК — это технологичная контентная и сервисная платформа: в социальной сети можно смотреть трансляции в качестве 4К, слушать

актуальную музыку, покупать товары и услуги и осуществлять денежные переводы в 18 стран мира.

Лидер рынка онлайн-видео и первая социальная сеть в России по просмотрам видеоконтента: в пике в сутки видео в ОК набирают более 1 млрд просмотров.

Telegram — популярный российский мессенджер, созданный Павлом Дуровым. Несмотря на то, что это — мессенджер, «Телеграм» давно стал эдаким «заменителем соцсетей».

Главная страница «Телеграма». Официальный сайт: https://telegram.org/

Помимо базового функционала в виде переписок, здесь пользователи могут создавать свои каналы и группы (чаты). Поэтому платформа идеально подходит для авторов контента.

Пользоваться «Телеграмом» можно с компьютера (веб-версия) и телефона (приложение для Android и iOS).

TenChat — российская деловая социальная сеть. Платформа для авторов, профессионалов, бизнесменов.

Главная страница TenChat. Официальный сайт: https://tenchat.ru/

Сообщество активных людей со всей России, где каждый открыт к нетворкингу, знакомствам и партнерствам. Заводите полезные связи, читайте экспертов или делитесь опытом.

Читайте также: Как скачать видео с любого сайта [Без дополнительных программ]: ТОП-6 онлайн-сервисов

Алгоритм «Зевс» отвечает за факт попадания записи в рекомендации. Каждый пользователь с первой публикации может получить до 300 000 охватов и тысячи подписок.

TenChat является открытой и бесплатной платформой, где нет платных функций и навязчивой рекламы. Использование всех сервисов возможно без ограничений.

Дзен (раньше назывался Яндекс.Дзен) — российское приложение для просмотра и создания контента. Здесь сотни тысяч авторов делятся постами,

статьями, видео и короткими роликами.

Пример ленты в Дзене. Официальный сайт: https://dzen.ru/

Умные алгоритмы подстраивают ленту под ваши интересы. Год основания — 2015.

Это платформа для авторов и зрителей:

1. Блогеры и авторы могут писать статьи, публиковать видео и зарабатывать на этом деньги.
2. Зрители могут получать качественный и интересный контент от блогеров.
3. Пользоваться Дзеном можно с компьютера (веб-версия) и телефона (приложение для Android и iOS).

RUTUBE — российский видеохостинг, аналог популярной зарубежной платформы YouTube; видеопортал, предлагающий к просмотру кинофильмы, сериалы, мультфильмы, передачи от известных ТВ-каналов и пользовательское видео.

Главная страница «Рутуба». Официальный сайт: https://rutube.ru/

Платформа подходит для зрителей и авторов контента:

Авторы контента — видеоблогеры — могут публиковать свой контента на «Рутуб».

Зрители могут смотреть видеоролики на интересующие их темы. Платформа принадлежит Газпром-медиа Холдинг. Год основания 2006.

Yappy — приложение вертикальных видео. Российский аналог TikTok.Главная страница Yappy. Официальный сайт: https://yappy.media/

Здесь вы можете смотреть и создавать классные ролики самостоятельно или вместе с друзьями, звездами и популярными блогерами.

Приложение доступно для Android и iOS.

Как пользовать заблокированными социальными сетями в России?

Как вы знаете, многие зарубежные социальные сети заблокированы на территории России: например, Instagram*, Facebook*, Twitter. Также

пользователям из РФ нельзя публиковать видео в TikTok.

Если вы хотите пользовать этими соцсетями, то можно обойти ограничения. Для этого воспользуйтесь VPN.

Мы рекомендуем VPN Hidemy.name. Что делает VPN-сервис:

Скрывает действия в сети.

Защищает пароли и переписку.

Создает закрытый канал между пользователями.

Открывает интернет без цензуры.

Hidemy.name позволяет подключит 5 устройств одновременно: например, компьютер, смартфон и планшет. Доступно 45 стран для выхода в сеть на ваш выбор.

Hidemy.name доступен для Windows, Android, iOS, macOS, Linux.

Конечно, количество авторов и постов в социальных сетях разное – это связано с общем интересом к социальной сети и с распределенностью аудитории. Молодёжь, более активно воспринимает технологические изменения и, соответственно, в сети она более активна.

Однако, стоит также заметить и оценить корреляцию между количество авторов и публикуемым контентом. В 2023 года контента было опубликовано примерно столько же, сколько и годом раннее, а общее количество пользователей возросло более, чем на 25% — с 49 млн публичных авторов в 2019 года до 64 млн публичных авторов в 2023 году. Подробная история о количестве ежемесячных сообщений на всех площадках и количество ежемесячных авторов представлена на рисунке 2.1, который отражает краткую выжимку результатов за 2023 год.

Рисунок 2.1. Исследование Brand Analytics по количество пользователей-авторов социальных сетей и количеству опубликованного контента.

Из анализа рисунка 2.1 можно сделать вывод о том, что ВКонтакте является самой популярной социальной сетью для авторов контента. Одноклассникам по количеству создаваемого пользователями контента и предпоследнее место по количеству пользователей, опережая только Twitter. Направленность социальных сетей на молодёжь является ключевой причиной того, почему одни социальные сети популярнее других. Так, например, социальная сеть ВКонтакте, является исторически «молодой», в которой основное количество пользователи представители до 35 лет. Перейдём к более детальному анализу трёх социальных сетей от самой крупной по количеству пользователей-авторов, которые находятся на территории Российской Федерации, до более мелких.

Всего лишь 33% аудитории являются молодёжью, то есть из трёх человек всего один. Здесь свою роль играет позиционирование социальной сети, как место «для профессионалов», что является непривлекательным для молодой аудитории. По соотношению мужчин и женщин, здесь также выигрывают женщин, опережая мужчин почти на 20%.

1.3 Сетевая форма коммуникации как фактор развития информационных угроз

Как уже говорилось ранее, наиболее опасными источниками угроз можно считать манипулирование сознанием человека посредством формирования вокруг него среды с измененным «более правильным» мнением, что приводит его к неизбежному следованию за новыми идеалами. Так же к отрицательным остаткам можно отнести информационную перегрузку личности. Если вкратце это происходит из-за возникновения у человека интернет-зависимости, вследствие чего человек начинает ощущать дефицит новой информации, межличностного общения и прочих видов потребностей, которые он никак не может утолить. В свою очередь это приводит к обесцениванию устоявшихся норм и правил привычной жизни.

Одним из наиболее опасных источников угроз для людей является использование его же персональных данных против него. Инструментарий социальных сетей позволяет с легкостью надавить на нужные рычаги и выставить любое лицо в необходимом свете.

К таким угрозам можно отнести публичную клевету, процедуру «удаления» очень популярную в США и странах западной Европы, когда какую-либо медийную личность, знаменитость, актера или любого мало-мальски знаменитого человека начинают массово травить в социальных сетях за какие-либо высказывания, которые он мог опубликовать несколько лет назад, ещё до становления той медиа личностью, которой он является сейчас. Помимо этого, к угрозам можно так же отнести прямые угрозы или распространение ложной информации о личности.

Сетевые коммуникации и сейчас обладают огромным инструментарием и предоставляют большие возможности для СМИ. В современном обществе большинство СМИ начало работать «на два фронта». Они комбинируют традиционные и современные медиа с целью привлечения большей аудитории. Посему в интернет-среде появляется такое огромное количество «Веб порталов» и Интернет-магазинов. Современное сетевое информационное

пространство характеризуется медиа глобализацией. Их называют «новыми электронными медиа», для того чтобы отрезать их от привычных всем традиционным медиа: печати, радио, телевидения. [10]

Новые электронные медиа обладают почти безграничными возможностями передачи любой информации любым ее отправителем в различных направлениях, но медийные информационные потоки формируются в интересах владельцев транснациональных информационных агентств. Процесс монополизации на медиарынке приводит к угрозам манипулирования общественным мнением по отношению к тем или другим значимым событиям и, что еще более серьезно, к деформации моральных устоев общества, его национальной культуры путем навязывания ему чужих ценностей. Разумеется, сетевые коммуникации сами по себе являются просто эффективной технологией для успешного развития бизнеса владельцев транснациональных информационных агентств. Западный бизнес не ставит своей целью разрушение нормативно-ценностной системы общества, но стремится распространить свои «правила игры», свою логику экономического, социального действия с тем, чтобы реализовывать коммерческие проекты в адаптивной для себя среде. Попутно глобальный медиарынок выполняет заказы, продиктованные ведущими геополитическими игроками. Ярким тому примером является мощная подача в информационных международных агентствах заведомо ложной информации о нападении России на Грузию в августе 2008 г.

Одной из самых распространенных групп угроз в современном обществе, можно без зазрения совести назвать киберпреступления. Они нацелены в основе своей на мошеннические махинации с использованием современных сетевых систем. Так же они служат для отмывания денег, полученных преступным путем, неправомерного использования финансовой, банковской информации и т.п.

Нет никаких сомнений, что социальные сети — это единственное место, хозяева которого если не напрямую нарушают установленные законом

предписания, то занимают нейтральную позицию в правовом секторе. Это наглядно можно увидеть если обратить свое внимание на проблему авторских прав. На сегодняшний день в социальных сетях находится огромное количество пиратского и не нелицензионного контента, из-за которого обладатели прав интеллектуальной собственности находятся в не уделе. Однако только на этом противоречия между правом и сетевыми коммуникациями никак не останавливаются.

По данным аналитиков, число опасных Интернет-ресурсов за последнее время увеличилось в три раза. Эксперты по Интернет-безопасности утверждают, что сегодня атаки на ресурсы Всемирной паутины происходят каждые четыре с половиной минуты. Во многих странах отмечается увеличение объемов утечки данных, при этом только около 20% происходит из-за хакерских атак. По данным МВД, в 1 квартале 2020 года Количество IT-преступлений выросло на 83,9%, а удельный вес таких деяний достиг 19,9% от общего числа. В основном из-за этого фактора уровень преступности в стране в целом вырос на 4%. [8]

Во Всемирной паутине сегодня существуют различного рода закрытые сети. Сетевые структуры эффективно используются организациями в условиях конспирации. Их главным козырем становится молниеносность распространения информации и новые возможности дистанционного управления террористическими актами. Террористические группы и мафиозные структуры используют нелегальные, полулегальные и криминальные методы политической борьбы, игнорируя правовые нормы и традиции, нарушая законы, расшатывая политический строй обществ.

Бесспорно опасный источник угроз в условиях сетевой коммуникации — это непрерывно разрастающееся влияние информационных войн и распространение информации, напрямую влияющее на сознание и мировоззрение людей. Информационные войны идут на всех уровнях и механизмы их работы практически всегда идентичны. У тех людей кто её ведут, остаются одни и те же рычаги давления на общественное мнение. Кто-

то недосказывает часть информации и намеренно вызывает её дефицит, чем и подогревает внимание общественности. Кто-то в свою очередь наоборот давит на неудовлетворённость людей конкретной ситуацией или продуктом и заставляет активно противостоять и оппонировать ей. Существуют также методы ведения информационной войны на территории информационной среды противника с целью полной дезинформации и создания хаоса и паники посредством методов и технологий дающих воздействовать на информационную среду. И. Л. Морозов различает три вида информационно-психологического оружия относительно стратегии нападения:

1. Системы дистанционного искажения или уничтожения информации: компьютерные вирусы общего и специализированного назначения (программы, проникающие извне и разрушающие систему); логические бомбы, тайно внедряемые в компьютер на этапе заводской сборки, которые при активизации парализуют работу компьютера;

2. Системы хищения информации: электронные шпионы (программы, проникающие извне и производящие незаметный для пользователя сбор служебной и непосредственно личной информации);

3. Системы комплексного воздействия на психику пользователя: мультимедийные сайты в виде информационно развлекательных или аналитических страниц с «горячей», «сенсационной» информацией.

Существует мнение, что повышение уровня «прозрачности» и доступности информации для всех участников политического процесса (например, в случае проведения президентских и парламентских выборов) облегчает общественный контроль за ним со стороны общественности. Однако И. Л. Морозов выделяет два блока угроз, ведущих к подрыву политических режимов: системные и периферийные угрозы.

Первый тип угроз направлен на дестабилизацию конкретных политических систем или их сегментов со стороны враждующего государства и затрагивает в основе своей атаки на информационное поле оппонента с

использованием информационно-психологических атак властных и околовластных структур

Не менее серьезную опасность представляют угрозы второго типа, которые связаны с деятельностью широкого спектра внесистемных сил — от международных террористических организаций до всевозможных хакерских групп. Неструктурируемость и непрогнозируемое возникновение периферийных информационных угроз крайне затрудняют выработку действенной защиты от них .

И. А. Василенко, анализируя состав политических факторов, различает их на носителей власти и внесистемную оппозицию . Сетевые пользователи, составляющие внесистемную оппозицию, делятся им на две группы — легальное «самобытное сопротивление», которое находит себе опору в традиционных и нетрадиционных ценностях сообщества, и на нелегальные криминально-мафиозные сети. Основной силой легального и нелегального сопротивления является исключительно сетевая, децентрализованная форма организации и политических действий. Характерным примером такого сопротивления становится стремительно нарастающее движение антиглобалистов, которое строится на основе национальных и международных сетей, активно используется Интернет, и при этом сети не только обеспечивают организацию их деятельности, но и совместное использование информации.

Децентрализованный, неуловимый характер сетевых структур сопротивления антиглобалистов и других самобытных движений (экологисты, «зеленые», женские движения, различные молодежные субкультуры, представленные, в частности, в блогосфере) во многом затрудняет их восприятие и идентификацию со стороны государственного управления. «Новые гибкие сетевые структуры внесистемной оппозиции становятся сегодня главным козырем в борьбе с неповоротливыми институтами политической власти, которая в большинстве случаев имеет старую

иерархическую организацию и только отдельные силовые подразделения в ней перестроены по сетевому принципу».

В конечном итоге я могу выделить основные категории информационных угроз, оказывающих свое влияние на общество, государство личность посредством сетевых коммуникаций.

— Угрозы безопасности личности, связанные с манипуляцией над сознанием и информационной перегрузкой человека, с непосредственным увеличением в информационную зависимость. Сюда же можно отнести и использования личных данных во вред личности, как пример сбор личных данных с целью внедрения таргетированной рекламы конкретному человеку.

-Угрозы, связанные с управлением и манипуляцией над общественным мнением, появлением особых механизмом управления массы людей с целью организации процессов направленных на разрушение привычных ценностей общества.

-Угрозы безопасности всех структур, на которые пытаются повлиять посредством международной преступности и терроризма.

-Угрозы стабильности существующих режимов власти, обусловленные неконтролируемыми всплесками высказывания и активизации опасной оппозиции в социальной и сетевой коммуникации.

1.4 Классификация информационных угроз в сетевой коммуникации

Для создания классификации информационных угроз в сетевой коммуникации необходимо определиться в терминологии. Понятие «информационная угроза» встречается в трудах многих авторов-теоретиков. Ученые используют различные подходы, которые описывают сложность термина и те деструктивные характеристики, которые в нём содержаться. По мнению А.А. Акмасова, информационная угроза – это некая возможность информационного воздействия, которая прерывает адекватное постепенное развитие личности с помощью того, что вносит изменения в собственных интересы и потребности личность для того, чтобы получить некоторую выгоду субъекту, который оказывает воздействие на личность [5].

В трудах учёного С.В. Вихорева также встречается определение информационной угрозы. К ней автор относится любую потенциальную или реально возможную опасность того, что произойдёт некоторое действие, которое способно причинить вред пользователю, который будет выражен для него в том, что информация, с которой он взаимодействует и к которой обращается, будет искажена, вовсе удалена или станет достоянием иных пользователей, которые изначально не имеют право на обращение к такой информации. С.В. Вихорев олицетворяет два понятия и связывает их: «информационная угроза» и «ущерб». По мнению ученого, любая информационная угроза несёт ущерб и доказать это можно через правовой аспект. Деятельность злоумышленника, который реализует информационную угрозу трактуется как преступление и доказываться через законы и уголовный кодекс [7].

Можно сделать локальный вывод о том, что информационная угроза неразрывна с некоторым ущербом и негативным воздействием на определенный субъект. Поскольку в рамках выпускной квалификационной работы рассматриваются сетевые коммуникации и информационные угрозы в сетевой коммуникации, то под субъектом негативного влияния понимается

некоторая группа лица или отдельное лицо, которое действует злонамерено и заинтересовано в том, чтобы нанести вред объекту негативного влияния для того, чтобы стать обладателем некоторой материальной или нематериальной выгоды. В свою очередь под объектом понимается участник сетевой коммуникации, который оказывается жертвой действия субъекта.

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 [16].

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 [13].

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 [12].

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].

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. 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 [17].

Существует несколько наиболее популярных методов кибербуллинга[35], к которым относятся: использование личной информациис 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 иунижением 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 [17].

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[34].

Последняя группа информационных угроз представляет собой совокупность технических и психологических приемов. Мошеннические а таки 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 дававшимна 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 [19].

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 [19].

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. [37]

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 ГР-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 [6].

Обозначенные информационные угрозы редко наносят серьезный урон участнику сетевой коммуникации, так как после первого неудачного контактас 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.

Так, например, несколько лет назад, в сеть утекла информация о продажи данных 100 миллионов аккаунтов, которые относятся к популярной в России социальной сети ВКонтакте.[36] СМИ подтвердили, что база данныхпродавалась на специализированных электронных ресурсах. В базе данных хранились данных для входа, которые необходимы для авторизации, а также номера телефоны, которые привязаны к аккаунту, и электронная адреса почты пользователей. Платформа слив данных не опровергла, но заявила, что слитая информация старая и не представляет ценности в текущем времени. Однако, сам факт слива информации подтвердился. Электронный ресурс также заявил, что основная проблема в отсутствии цифровой грамотности у пользователей, которые пренебрегают классическими и фундаментальными правилами

информационной безопасности, в частности создания паролей [24].

Другие случаи информационно-технических атак на пользователей были зафиксированы в социальной сети Instagram. Во-первых, оказалось, что

Instagram-аккаунты пользователей можно было взломать с помощью картинки. Данный баг возникал из-за особенностей работы старой версии приложения и обработке картинок. Во-вторых, многие посетители социальной сети жаловались на подозрительную активность: добавление новых подписок, рассылку спама, искажение личных данных. В результате поиска возможных источников угроз опытные программисты обнаружили недочеты в настройках персонального аккаунта и приложений, позволяющих собирать личные сведения и управлять пользовательской страницей. Для решения данной проблемы, по их мнению, достаточно внимательно читать инструкции ресурсаи требования установленных программ [31].

Еще один способ незаконного захвата страницы, которые актуален для таких социальных сетей, как Телеграмм и ВКонтакте, связан с особенностями авторизации. Для взлома аккаунта хакеру достаточно знать логин пользователя и ответ на секретный вопрос. В некоторых случаях указанную информацию посетители самостоятельно размещают в новостной ленте. Для защиты от подобных атак следует более внимательно относится к размещаемому контенту и не разрешать доступ к личным данным другим пользователям.

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 жертвамифишинговых атак.

Одной из таких мошеннических операций является кража данных с помощью приложения «Музыка ВКонтакте» (приложение не является официальным приложением платформы), свободно распространявшееся в онлайн магазине Google P1ay. Механизм работы программы достаточно прост:

для доступа к архивам социальной сети Вконтакте пользователь добровольно

вводит логин и пароль. Все собранные данные отправляются напрямую к злоумышленникам, которые используют их для собственных целей. Во избежание подобных ситуаций администрация ресурса настоятельно рекомендует не устанавливать сторонние приложения для социальных сетей и проявлять бдительность при вводе личных данных в незнакомых формах [14]. Фишинговые атаки участились и в популярной сети Одноклассники [38].

Хакеры под видом сотрудников компании EA Games предлагают пользователям приобрести новых игроков для компьютерной игры абсолютно бесплатно. Для совершения операции необходимо лишь перейти по указанной под фотографией ссылке и ввести персональные сведения. После того, как секретная информация попадает в руки нарушителей, пользователь теряет доступ к своему аккаунту и его настройкам. Подобный ход является универсальным для большинства хакерских атак. В связи с чем следует крайне осторожно реагировать на обещание бесплатных вознаграждений и преимуществ, особенно если в обмен на них нужно отправить какие-либо сведения.

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].

Действие обозначенных угроз основано на сложных программных

алгоритмах и психологических уловках. Чаще всего мошенники используют простые и универсальные механизмы воздействия — интригующие заголовки, директивные послания, просьбы перевести деньги, обещания бесплатных подарков и другие. Для противодействия атакам достаточно быть осведомленным о возможной угрозе и внимательно фильтровать информацию.

В отличие от спама и фишинговых атак, информационно-психологические операции представляют собой комплекс более серьезных и деструктивных воздействий на психику пользователя с целью унижения достоинства личности, кражи секретной информации, провокации. Для совершения противоправных действий злоумышленники предпочитают виртуальные платформы с возможностью легкой и быстрой обратной связи, именно поэтому участники популярных сетей часто становятся мишенью негативных воздействий [8].

Одним из наиболее известных примеров информационно-психологической атаки является история Николы Брукс, одинокой англичанки, оставившей свой комментарий в поддержку выбывшего участника программы Х-фактор. Вслед за размещением нейтрального сообщения в социальной сети Телеграмм посетительница неожиданно стала мишенью для яростного троллинга. Больше, чем полгода британку оскорблялии унижали на просторах Сети. Помимо этого, обидчики создали страницу от ее имени и распространяя непристойные сообщения. По данным СМИ, тролли также атаковали близких Николы, отправляя им грязную информацию якобы под ее авторством. Также они обнародовали данные о месте жительства Николь и начали преследовать женщину за пределами виртуального пространства [29].

Ответной реакцией британки стало обращение в полицию за просьбой возбудить уголовное дело против нарушителей. К сожалению, доступных способов поиска и привлечения к ответственности троллей слуги закона не обнаружили. Однако инициативная британка не сдалась и подала обращение в высокий суд Лондона, обязавший социальную сеть Телеграмм раскрыть IP-

адреса обидчиков, с помощью которых можно установить личность нарушителя и привлечь его к ответственности.

Одним из положительных результатов дела Николы Брукс стало введение меры наказания британских пользователей, публикующих оскорбительную информацию и угрозы, сроком до шести месяцев заключения. Также подобный прецедент стал поводом для обсуждения способов защиты граждан страны от информационных атак, осуществляемых в Интернет-пространстве.

Что касается негативных последствий, то сама Никола Брукс призналась, что наряду с популяризацией данной темы количество негативных комментариев в ее адрес только увеличилось, тогда как поймать всех обидчиков не представлялось возможным и целесообразным. По данным полицейских, британка провоцировала троллей негативными репликами и яростными ответами на оскорбления в свой адрес, чем только усугубила свое положение [29].

Анализируя особенности данного случая, необходимо в первую очередь отметить важность способов самозащиты, включающих в себя как защиту психологическую, так и техническую. Отсутствие знаний о психологических угрозах, правилах поведения в сетевой коммуникации, способах реагирования на провокативные действия, методах технической защиты стало причиной разжигания конфликта до национального масштаба. С большой вероятностью можно предположить, что своевременные действия по защите личного аккаунта, ограничению нежелательных собеседников и спокойной адекватной реакции могли бы спасти женщину от трагичных последствий информационных атак.

Приведенные примеры являются уникальными прецедентами борьбы с информационными угрозами. Несмотря на то, что все обозначенные иски были удовлетворены, а пострадавшие лица получили моральную компенсацию и возможность наказания злоумышленников, результаты такого судебного вмешательства можно оценить неоднозначно.

Во-первых, необходимо отметить, что использование правовых механизмов целесообразно и оправдано только в случае единичных атак на пользователя. Это связано с возможностью установления личности и привлечения его к ответственности. Что касается массового троллинга, то, как показала история Николы Брукс, поиск виновных не только не помогает устранить всех субъектов психологического воздействия, но и становится катализирующим фактором информационной агрессии.

Во-вторых, 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. Информационные угрозы и способы защиты от них в контексте коммуникативных практик молодёжной аудитории социальных сетей.

2.1. Алгоритм действий по обеспечению информационной безопасности личности в социальных сетях

Алгоритм представляет собой последовательность действий, необходимых для осуществления самозащиты в рамках коммуникативных практик. Разработка данного алгоритма базировалась на теоретических моделях представителей психологического направления. Также в основу легли данные аналитического исследования теоретического материала даннойработы.

В соответствии с результатами научного поиска, 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 [31]

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[38].

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 [31]

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 [31]

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 [31]

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.

2.2. Разработка рекомендаций по обеспечению информационной безопасности личности в социальных сетях для студентов ПОО на базе Миасского машиностроительного колледжа

В связи с бурным развитием информационных технологий, характерным для последних десятилетий, и обострения информационной войны против России, во время проведения Специальной Военной Операции на Украине, их проникновением во всевозможные сферы человеческой жизни, особую актуальность приобрело такое направление науки и техники, как кибербезопасность.

Кибербезопасность никогда не была так важна, как сейчас. Поскольку мы проводим больше времени в Интернете, мы часто создаем и передаем больше наших личных данных. И если эти данные попадут в чужие руки, личная и финансовая информация может оказаться под угрозой. Таким образом, как для предприятий, так и для частных лиц защита конфиденциальных данных имеет решающее значение.

10 ЗАКОНОВ КИБЕР БЕЗОПАСНОСТИ !!!!!

Закон №1. Если вы запустили на своем компьютере приложение злоумышленника, это больше не ваш компьютер.

Закон №2. Если злоумышленник внес изменения в операционную систему вашего компьютера, это больше не ваш компьютер.

Закон №3. Если у злоумышленника есть неограниченный физический доступ к вашему компьютеру, это больше не ваш компьютер.

Закон №4. Если злоумышленник смог загрузить приложения на ваш сайт, это больше не ваш сайт.

Закон №5. Ненадежные пароли делают бесполезной любую систему безопасности.

Закон №6. Безопасность компьютера напрямую зависит от надежности администратора.

Закон №7. Безопасность зашифрованных данных напрямую зависит от того, насколько защищен ключ расшифровки.

Закон №8. Устаревшее антивирусное приложение лишь немногим лучше, чем его отсутствие.

Закон №9. Абсолютная анонимность недостижима ни в жизни, ни в Интернете.

Закон №10. Технология не является панацеей

Вы главная цель для киберпреступников!!!! ОТ ВАС ХОТЯТ:

1. Деньги (опустошить счет, платные подписки, обман при покупке/продаже, в переписке, благотворительность и т.д.).

2. Информация (для подмены личности, атаки на вас, близких, для рекламы, слежки).

3. Эксплуатация устройства (майнинг, DDoS-атаки, скрытая накрутка рекламы, голосов, рассылка спама, заражение других устройств через ваше и т. д.)

ГЛАВНАЯ ОПАСНОСТЬ ДЛЯ ВАС !

1. Иметь слабые пароли.

2. Заразить устройство вредоносной программой.

3. Ввод пароля в поддельном окне.

4. Отсутствие резервных копий.

5. Доверие (без проверки).

1. ПАРОЛИ

- 81% вторжений хакеров связаны со слабыми или украденными паролями пользователей

(Verizon Data Breach).

- Критичные сервисы должны быть самыми защищенными (почта, банковские приложения, гос. услуги, соцсети)

• Взлом почты — позволяет восстановить все пароли к привязанным аккаунтам.

• Взлом банковских приложений — лишает вас средств на счетах.

• Взлом гос. услуг — делает возможным установить электронную подпись и открывает доступ к полному перечню государственных услуг, например,

переоформление недвижимости. (Проверяйте периодически её отсутствие в личном кабинете).

• Взлом соцсетей — позволяет манипулировать близкими, заражать вирусами через посты и сообщения, похитить все файлы из переписок и т.д.

Базы данных воруются, их методично расшифровывают и массово перебирают все аккаунты на популярных сайтах. Нужен сложный пароль!

Ненадежные пароли делают бесполезной любую систему безопасности.

В современном мире не нужно запоминать все пароли — только один!

Для критических сервисов пользуйтесь спец. программой "Менеджер паролей". Нужно запомнить всего один пароль от входа (остальные генерируются автоматически и сохраняются в программе), но этот пароль должен быть максимально надёжным. Если забудете его, то просто восстановите все пароли уже на самих сервисах.

Хранение паролей

• Слабая защита — Мастер-пароль в настройках браузера (пароли шифруются).

Подходит для неважных паролей и регистраций. Браузер очень ненадёжное место для хранения важных паролей.

• Средняя защита — Менеджер паролей (онлайн, LastPass). Пароли зашифрованы и хранятся в Облаке (синхронизация между устройствами). Есть автоматическое заполнение форм, генерация паролей и журналирование входа на сайты.

• Высокая защита — Менеджер паролей (KeePassXC). Это лучший выбор!

Все пароли хранятся только у вас на устройстве в зашифрованном виде.

Минимум 25 знаков на все пароли (сочетайте цифры, знаки и буквы разного Регистра).

Пароль не должен включать в себя реально существующие слова или известные фразы.

Не применяйте пароль повторно нигде (нет похожести!).

Двух факторная аутентификация всегда и везде (лучше многофакторная).

При потере смартфона лицо можно подделать, используя 3D фото, и добраться так до всех приложений.

Меняйте пароли обязательно — раз в 3 месяца (ведь их последовательно и автоматически расшифровывают).

На "секретный вопрос" — давайте ложные ответы (но помните их!).

2. ПОЧТА

Почта — ключ ко всему!!!

Завладев вашей почтой, можно сбросить пароли вашего банка, гос. услуг или соцсетей и захватить аккаунты.

Пароль от почты вводить только на самой почте — больше нигде!

По умолчанию любое письмо может быть опасным!!! Не считать безопасным любое пришедшее вам послание. Обычно начало всех историй одинаковое: «Жертва открыла фишинговое письмо, и тут началось!».

Опасные действия (к которым вас призывают письма мошенников):

• отправка данных

• отправка денег

• открытия вложения

• установка приложения

• переход по ссылки на сайт (сразу можно загрузить вредоносный код).

Не нажимайте кнопку "Отписаться" (она может вести на вредоносный сайт).

Удаляйте отправленные документы из папки "Отправленные" (ваши переданные файлы могут украсть при проникновении).

Проверяйте подлинность адреса Отправителя.

• Опечатки в доменном имени (vasiliy.petrov@sberdank.ru; dmitriy.poklovsky@abbyyy.ru)

• Удвоение букв в доменном имени (...@ozzon.ru)

• Перестановка букв (...@sbfr.ru)

• Написание с ошибкой (...@yandeks.ru)• Подмена букв (...@migrosoft.ru)

Подлинность любой ссылки в самом письме (проверяйте даже от друзей).

Полный анализ!

• Маскировка доменов 2-ого уровня (facebook.com.af.com). Mail.ru — .ru, это первый уровень, mail — это второй уровень. Читаются всегда справа на лево, стоят первыми.

Домен 1,2-ого уровня являются настоящим адресом сайта, остальное неважно.

• Выявляйте поддельные буквы другого алфавита (скопируйте ссылку и вставьте в новую вкладку, но не запускайте). В адресной строке сам адрес сайта (он же домен) всегда отображается в формате Punycode и подмена сразу обнаружится.

• Адресная строка внутри почтового сервиса (Gmail, Mail, Yandex) показывает домен имени в истинном виде (...@rbk.ru), а вот домен ссылки внутри письма НЕТ. То есть @домен имени Отправителя/Получателя подделать нельзя, а домен ссылки можно.

• Короткие ссылки опасны, раскрывайте их до перехода (используйте декодер, например, longurl.info).

Файлы, прикреплённые к электронным письмам.

• Внимательно проверяйте все файлы.

• ИмяФайла.exe (любые файлы с таким окончанием) — не открывайте их здесь вообще!

• Бойтесь исполняемых файлов, которые запускают программу — .exe, .js, .src, .bat, .vbs, .com, .dll (если расширение незнакомо — погуглите).

• Не исполняемые — .jpg, .png, .pdf, .txt, .docx и т.д.

• Всегда выделяйте исполняемые файлы, из массы прочих.

Отключите макросы в Word и Excel (перед открытием скаченного и даже проверенного файла). Это программный алгоритм действия, записанный пользователем.

Проверяйте подлинность информации (по сторонним каналам), прежде чем предпринимать какие-то действия.

Создайте 4 шт. для себя (домашняя почта, рабочая, для сайтов, для

мусора). Не будет спама и риск взлома снизится. Для удобства можно настроить пересылку всех писем на один из аккаунтов. В идеале хорошо бы иметь и отдельный «мусорный» номер телефона.

Не указывайте в адресной строке ФИО@, телефон@ или год рождения@. Меньше внимания и данных к привязки вашей личности.

Проверяйте свой адрес почты в украденных базах haveibeenpwned.com.

Открывайте почту в песочнице, «Sanboxie» (https://sandboxie.ru/) и проводите проверку почтовых вложений и ссылок на сайте https://www.virustotal.com/gui/home/upload.

3. БАНКОВСКАЯ КАРТА

Никому и никогда нельзя пересылать фотографию или скан карты (видны другие данные помимо номера).

Номер карты + ФИО + мм.ГГ = возможна оплата в некоторых интернет-магазинах.

Номер карты + ФИО + мм.ГГ + CVV = бронь отеля/авто, привязка этой карты к Google Play, оплата на Литресе.

Номер карты + ФИО + мм.ГГ + CVV + код (SMS) = любой платеж и перевод (без исключений).

Зная номер карты, можно узнать Имя и Фамилию из соцсетей и подобрать механическим образом дату окончания действия карты. Теперь Интернет-магазины открыты для покупок, например Amazon.

Заведите спец. карту(дубликат карты или виртуальную карту) с нулевым балансом только для получения переводов (в своём же банке).

Установите суточный лимит по выводу и переводу средств (так вы обезопасите большую часть денег на счёте).

Подключите SMS-оповещение о фактах списания (мошенники пользуются тем, что интернет-магазины позволяют делать покупки на небольшие суммы без кодового подтверждения по SMS, даже если подключена двухфакторная аутентификация).

При списании средств без вашего ведома — успейте подать заявление в

первые сутки!

Там, где возможно, не оставляйте реквизиты карты (интернет-магазины, электронные кошельки). Данные часто утекают в Сеть.

4. ПЛАТЕЖИ

Опасным может быть абсолютно любой сайт.

В России нашли более 1,5 тыс. фейковых банков за первые три месяца 2021 г.

Изучите сайт, прежде чем оставлять на нём данные своей банковской карты, используй только дубликат или виртуальную карту!!! Проверь, когда сайт был создан (если недавно, значит подозрительный!) проверь сайт на reg.ru/whois/

Признаки подлинного платежного сайта:

1. Указаны системы защиты вашего платежа (Visa, VasterCard, SafeKey). После ввода реквизитов вас перенаправит на страницу банка-эмитента, где нужно ввести одноразовый пароль (SMS).

Но не у всех такая технология.

2. Есть возможность оплаты разными способами (злоумышленники не предлагают альтернатив).

3. Проверьте поставщика платёжных услуг (скопируйте адрес/название и введите в поисковике).

Внимание на "подписку по умолчанию" (мелкий шрифт и галочки-согласия на "автопродление"). Если сервис подразумевает обязательную подписку — заплатите с виртуальной(дубликата) карты с небольшим балансом (отказаться от подписок крайне трудно!).

Если покупаете физический товар — выбирайте "оплата курьеру". Платите при доставке картой или наличными (избежите интернет-мошенничества).

При оплате на заправках, в аптеках и прочее, не упускайте свою карту из поля видимости, используйте дубликат карты, (карту могут "прокатать" карту через устройство, спрятанное под одеждой официанта или продавца магазина и

снять её копию/дубликат). Лучше вообще не передавайте свою карту в чужие руки.

При снятии наличных, при физической оплате картой — пользуйтесь встроенным микрочипом, а не магнитной лентой (прикладывайте карту к аппарату, а не вставляйте).

Лучше всего использовать другие способы перевода и оплаты средств (где данные карты не передаются!):

• по номеру телефона

• платежные сервисы (PayPal, WebMoney, Qiwi). Только не привязывайте к ним свою основную карту.

• виртуальная карта или дубликат карты (в личном кабинете своего банка делается быстро). Можно привязать к отдельному счету и хранить там ограниченную сумму денег для покупки.

• бесконтактная оплата с телефона (NFC)

• оплата по QR

• отпечаток пальца или скан лица

Тёмные паттерны (их используют 11% интернет-магазинов)

• Информация мелким шрифтом.

• Использование одних элементов дизайна, чтобы отвлечь от других.

• Лёгкое оформление платной подписки и сложная её отмена.

• Списание денег без уведомления после окончания бесплатного периода.

• Заранее добавленные товары в корзине в интернет-магазине.

• Изменение стоимости покупки на последнем этапе оформления товара. Chargeback (чарджбэк) — это универсальная процедура отмены транзакции (по карте Visa, MasterCard, МИР). Если вы получили некачественный товар, услугу или вообще не получили ничего, или даже были обмануты мошенниками, вы в праве написать заявление в ваш банк на принудительный возврат денежных средств.

• Карту использовали без ведома владельца.

• Доступ к реквизитам карты получили мошенники.

• Продавец списал с карты затребованную сумму несколько раз.

• Сумма транзакции была произвольно изменена продавцом.

• После оплаты товара/услуги продавец перестал отвечать на запросы.

• Продавец не соглашается на возврат товара.

• Товар поставили со значительным опозданием.

• Заказанная вещь оказалась не соответствующей заявленному описанию.

• Товар оказался с дефектом или поврежденным, или низкокачественным и т.д

5. ИНТЕРНЕТ (WEB)

Самые распространенные ошибки пользователей — лень и спешка. Эти две вещи, несомненно, ставят под удар нашу безопасность.

• Опасным может быть абсолютно любой сайт. Покиньте сайт при появлении первых подозрений в подделки.

• На сайте много "визуального шума", чтобы сбить вас с толку, меньше думать и быстрее кликнуть на ссылку (всплывающая реклама, предложение обновить браузер, выигрыш в лотерею, звуки)

• Если вас призывают отправить SMS, введя свой номер на сайте — это подписка на платные услуги, либо ваш номер внесут в базу рекламы (с перепродажей всем-всем)

• Переадресация на другой сайт.

• Внешние дефекты сайта (ошибки, старые новости, не работают кнопки, ссылки, пустой подвал без технической информации).

• Перед вводом своих данных на любом сайте — обязательно проверяйте его на подлинность (reg.ru/whois/ , внешний вид, сам адрес, пробив на фишинг).

• Окно авторизации — проверяйте на подлинность даже во время работы на надёжных сайтах (оно может быть всплывающим от мошенников, например, через взломанный ими Wi-Fi).

• Не стоит бездумно ходить по разным сайтам (веб-сёрфинг) открывайте браузер в песочнице «Sanboxie» (https://sandboxie.ru/)

Ссылки

• Каждая ссылка несёт потенциальную опасность.

• Проверяйте ссылку на https://www.virustotal.com/gui/home/upload.

• Нужно доверять только официальным сайтам (обращайте пристальное внимание на доменное имя (адрес сайта), если оно отличается — вас пытаются обмануть).

• Просто зайдя на страницу с зараженным баннером, можно занести вирус на свой компьютер — это называется «скрытая загрузка». Установите расширение для блокировки такой рекламы (uBlock Origin или GHOSTERY) и запускайте браузер в песочнице «Sanboxie» (https://sandboxie.ru/).

• Всегда проводите базовую проверку — замаскированная кириллица (скопируйте в адресную строку), опечатка, сокращенный URL, только цифры, домен-зеркало (поддельный, как будто другой страны - ebay.la).

• Всегда смотрите только на домены 1-ого и 2-ого уровней. Остальное неважно. (ebay.moneybook.com, это уже не eBay).

• При наведении курсором на ссылку — всегда отображается подлинный адрес сайта (в левом нижним углу браузера). Если нет, смотрите в коде (по мере возможности).

• Проверяйте подозрительные ссылки (или адреса) здесь https://www.virustotal.com/gui/home/upload.

• Никогда не переходите по рекламным ссылкам Яндекс, Google (они первые в выдачи).

Часто рекламируются неофициальные, ненадежные и даже фишинговые сайты.

Программное Обеспечение

• ПО — это программное обеспечение, то есть любая программа на компьютере.

• Устанавливайте ПО только с официального сайта (адрес см. в Википедии) или у официального дистрибьютора (ссылка на загрузку сразу ведёт на скачивание файла, а не на файл- обменник или торрент).

• Не нужно искать платное ПО на бесплатных сайтах или на торрентах — бесплатный сыр бывает только в мышеловке.

• Скачивайте любой файл в песочнице и проверьте антивирусом, дополнительно на https://www.virustotal.com/gui/home/upload.

• При запуске программы (.exe) проверяйте издателя в окне разрешения на запуск. Если издатель "Неизвестен" — не устанавливайте.

• При установки смотрите на "галочки" (реклама, поисковик, браузер). Не устанавливайте навязанные дополнения. файлы

• При загрузке из Интернета музыки, видео, книг, документов — обязательно обращайте внимание на расширение (формат файла). Их открытие может привести к установке вредоносного ПО.

• Проверяйте соответствие (фото - .jpg, .png, электронные книги - .epub, .fb2, .mobi и т.

д.) Расширение незнакомо — по Гуглите.

• Бойтесь исполняемых файлов — .exe, .js, .src, .bat, .vbs, .com и т.д.

• Внимание на двойное расширение "Документ.docx.bat" (так обманывают!).

• Включите на компьютере «расширение» файлов (чтобы видеть не только название файла, но и само расширение). Так легко обнаружить исполняемые файлы. (Папка indows -> сверху вкладка Вид -> Расширения имени файлов -> галочка).

• Архивы (.rar, .7z, .zip). Скачивать можно только незапароленные архивы, а после качивания проверять антивирусом и на https://www.virustotal.com/gui/home/upload.. Запароленные архивы антивирусы не могут проверить. Придется распаковывать в песочнице «Sanboxie» (https://sandboxie.ru/) , подвергая свой компьютер опасности.

Браузер

• Расширения для браузера (они же плагины, приложения, утилиты) в магазине браузера — это программы, такие же, как и любые исполняемые файлы. Среди них часто выявляются вредоносные.

• Не устанавливайте браузерные расширения без крайней необходимости и тщательно следите за тем, что вы им разрешаете.

• Выбирайте похожие расширения для браузера с наименьшими разрешениями (к которым вы их допускаете). И внимание к автору.

• Минимизируйте кол-во используемых расширений (удаляйте те, которыми не пользуетесь). Они не только снижают производительность компьютера, но и могут открыть лазейку для атак. Ещё расширения выкупают, а также взламывают самих разработчиков — устанавливая при этом зловредное обновление.

• Безопасное расширение — это большое кол-во скачиваний, много отзывов (не боты), высокая оценка, есть ссылка на сайт, контакты, частота обновлений, много скриншотов и нет орфографических ошибок.

• Лучший выбор браузера — это браузер Tor и JonDoBrowser(шифрует трафик, скрывает IP-адрес, изолирует cookie, удаляет историю) запускаемый через VPN. Там есть расширенная рамка экрана, которую можно убрать. Она предотвращает отслеживание пользователя через JavaScript или CSS, подгоняя размер окна браузера одинаковый для всех.

• Три полезных расширения для защиты HTTPS Everywhere, Privacy Badger и NoScript.

• Проверьте безопасность своего браузера здесь coveryourtracks.eff.org

Облако

• Необходим надёжный пароль и особое внимание к ссылкам, которые вы раздаёте (настройка прав доступа к файлам). Проверяйте ссылки лично.

• Внимание! Обычный "Доступ по ссылке" делает её сразу открытой для всех в Сети, т. к. саму ссылку можно подобрать простым перебором.

Торрент

• При любой возможности найдите какую-либо информацию без использования торрент-форумов и сайтов.• Под видом файла .torrent вы можете скачать вредоносное ПО.

• С помощью файла .torrent вы можете скачать вредоносное ПО уже

непосредственно через торрент-трекер.

• Если решились, то используйте торрент-программу только этих брендов и только на их официальном сайте (лучший это Transmission https://transmissionbt.com/).

• Выбирайте раздачу с наибольшим кол-вом сидов (пользователей, которые скачали весь файл до конца), читайте отзывы и комментарии под раздачей. Используйте сайты только с регистрацией (закрытые сообщества), там есть хоть какая-то административная проверка файлов.

• По вашему IP-адресу можно узнать, что вы скачивали через торрент (это видят все!) knowwhatyoudownload.com

Интернет на работе

• Всё, что проходит через корпоративную сеть, принадлежит компании (сканируются все входящие и исходящие информационные потоки). Отслеживается всё, что вы делаете в Интернете!

Интернет дома

• Любой российский провайдер (поставщик Интернета домой или на телефон) в автоматическом режиме прослушивает всех клиентов и может анализировать их трафик. То есть весь трафик клиента жестко контролируется для СОРМ (системы оперативно-розыскных мероприятий). Поэтому лучшим решением будет использование VPN по протоколу OpenVPN или WireGuard!!!

Потеря аккаунта

• Открывает доступ ко всем ресурсам (где вы регистрировались с помощью соцсети).

• Создаются зеркала (удаленная привязка и наблюдение). Регулярная смена пароля — хорошее средство от незаметного присутствия незнакомца.

• От вашего имени выпрашивают деньги у ваших друзей, а потом стирают эти сообщения в переписки (вы даже не узнаете об этом).

• Скачиваются моментально все документы из переписок (используют фильтр или спец. программу).

• Логинятся от вашего имени на сомнительных сайта, не оставляя следов (DarkNet).

Меньше личной информации о себе

• Сложнее причинить вам ущерб.

• Меньше возможности обращаться прикидываясь вами (к друзьям, родственникам, коллегам).

• Дополнительная информация в профиле о вашей работе, личной жизни и интересах помогает мошенникам сочинить более правдоподобную легенду.

• Измените настройки конфиденциальности (откажитесь от настроек по умолчанию).

Воспользуйтесь отличным пошаговым решением: privacy.kaspersky.com

• Яндекс, Google — обязательно измените настройки по умолчанию. Удалите всю историю, веб-поиск и геолокацию. Если не отключите геолокацию, все сведения будут доступны в Интернете и с их помощью можно восстановить ваши перемещения поминутно.

Используйте поиск DuckDuckGo вместо Яндекса и Google/

• Всегда выходите из аккаунтов, чтобы не вёлся сбор данных через принадлежащие им многочисленные сервисы (Microsoft, Facebook, Google, Яндекс).

• В целом применяйте к соцсетям простое правило: если вы передаете им какие-то данные, считайте их публичными, даже если применены какие-то настройки приватности.

Не стоит публиковать

• Интимную и компрометирующую информацию о себе (фото в непристойном/нетрезвом виде, признание в нарушении закона, измене).

• Негативные высказывания о знакомых или начальстве — клевета и оскорбление, это подсудное дело!

• Номера документов, любую финансовую информацию (фото с деньгами,

номер счета, номер банковской карты).

• Номер своего телефона. Преступники могут отправлять SMS-спам или звонить с мошенническими целями. Используя технологию подмены номера, могут звонить от вашего имени (принимающая сторона будет видеть, что звоните вы!). Возможна атака на родственников и ваших знакомых.

• Домашний адрес и когда вас нет дома.

• Запрещенный контент (обнажёнка, призыв к насилию, оскорбления)

• Билеты на самолет. По ним можно узнать: Имя, Фамилия, данные о рейсе, терминале, посадочных местах, о маршруте и последующих пересадках (по коду бронирования), данные о номере бонусной карты и логина личного кабинета на сайте авиакомпании, подробности о способе оплаты билета (клиентом какого банка вы являетесь), код постоянного пассажира. Прикрывать пальцами данные билета бессмысленно (вся информация "зашита" в штрих-коде).

• Перед публикацией остановитесь и подумайте — действительно ли это нужно выносить на всеобщее обозрение? Не может ли это мне сработать во вред? Лишь убедившись в безопасности поста можно его публиковать.

• Помните, что любую информацию из ваших публикаций могут использовать против вас.

Клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении или СМИ наказывается ещё более жёстко, чем клевета в частном разговоре. А социальная сеть — это как раз средство публичной демонстрации. Поэтому, если вы хотите написать что-то недоказуемое и недостоверное о другом человеке, подумайте дважды. Этот человек сделает скриншот вашей записи, распечатает его, заверит у отариуса — и у него будет 100%-ное доказательство вашей вины. Возможна судимость.

Документы

• Не используйте мессенджер соцсети для пересылки документов. Мошенники получат доступ ко всем документам, которые вы отправляли или получали от других людей.

• Никогда не публикуйте отсканированные документы на своей странице!

• Вот последствия использования только одной копии вашего паспорта: оформление микрозаймов, электронные кошельки для вывода нелегальных доходов, регистрация самих сайтов с запрещенными материалами (порно, терроризм, пиратский контент), оформление SIM-карты, фирмы-однодневки, регистрация на платном сервисе (каршеринг), восстановление логин/пароль от значимых сервисов (например, финансовых), фиктивное оформление на работу, оформление сделок, регистрация на сайтах-знакомств, онлайн-букмекеры.

• Иногда для получения копий документов используются фиктивные вакансии в интернете.

• С копией вашего свидетельства о собственности кто угодно может прописать в вашу квартиру незнакомца.• Вас могут просто шантажировать, угрожая отправить ваши конфиденциальные данные (скажем, медицинские) тем, кто не должен о них знать.

• Старайтесь не хранить копии документов в Облаке, в электронной почте или в соцсетях в незашифрованном виде. Если вам всё же пришлось отправить их в переписке, после получения удалите сообщение у себя и собеседника.

• Любой документ (или данные из документа) могут быть использованы против вас.

Фото

• Фото содержат метаданные (время и дата съемки, марка и модель фотокамеры) и, если на устройстве включена геолокация, то ещё указывается широта и долгота того места, где была снята фотография (отключите геолокацию).

• Не создавайте геотеги на фото (зная, что вы далеко, вас могут ограбить, а те, кто дома могут подвергнуться опасности). "Ага, теперь дома один ребенок или пожилой человек — можно грабить".

• Публикуйте фото уже после отпуска.

• Хотите скрыть часть фото или документа? Следует иметь в виду, что из замазанной — и даже обрезанной! — картинки довольно часто можно извлечь

те данные, которые вы пытались спрятать. Так можно добровольно и самостоятельно слить конфиденциальную информацию, не подозревая об этом.

Загрузка

• При загрузке из социальной сети музыки, видео, книг, документов — обязательно обращайте внимание на расширение.

• При загрузке любого файла обязательно открывайте его в песочнице«Sanboxie» (https://sandboxie.ru/) и проверяйте его антивирусом на сайте https://www.virustotal.com/gui/home/upload (даже от друзей и знакомых).

• Именно исполняемые файлы приводят к непосредственной установке вредоносных программ. Но не исполняемые тоже могут быть опасными (макросы, за пароленные архивы, PDF).

• Файлы, присланные без контекста предыдущего общения, следует игнорировать.

7. МОШЕЙНИЧЕСТВО В WEB:

Существует две методики мошенничества:

1. Угнать или сымитировать аккаунт реального человека (друга, коллеги, знакомого), обращаясь от его имени.

Клон (ваш или друга)

• Если знакомый обращается к вам непривычно или странно, убедитесь, что это не мошенник, клонировавший его страницу.

• Если вам второй раз приходит заявка в добавление от тех, кого уже "Friendly". Это клон!

• 80% добавляют в друзья своего знакомого, не пытаясь вспомнить, если ли он уже в списки "Friendly" или нет. Иногда лишь спрашивают — У тебя что, новый аккаунт? — Да, прежний угнали? Заморожен за нарушения а общаться хочется, вот и завёл новый. (Иногда текст объяснения присылают сразу при запросе дружбы).

• Если вам сообщают о сетевой активности от вашего имени (друзья говорят или пишут о том, что вы не делали) — убедитесь, что нет клона в соцсети.

• Проверяйте периодически нет ли у вас клонов (если есть, заявите в поддержку и сообщите друзьям, что от вашего имени им мог писать злоумышленник).

2. Втереться в доверие под видом незнакомого персонажа (организатора лотереи, матери больного ребенка и так далее).

Незнакомец

• С подозрением относитесь к любому общению с незнакомыми или малознакомыми людьми в социальных сетях.

• Никогда не сообщайте никакой ценной информации, не высылайте денег, не открывайте человеку душу — пока не познакомитесь с ним лично.

• Если ваш потенциальный партнер под любым предлогом избегает очной встречи или срывает её в последний момент — это повод задуматься о его подлинности.

• Кэтфишинг (любовный или сексуальный подтекст мошенничества с вымоганием денег).

Общие правила:

• Цели преступников: выпросить деньги, выманить информацию или вынудить установить вредоносное ПО.

1) По умолчанию считается, что любая просьба о деньгах или данных, присланная через социальную сеть, — является мошеннической.

2) Вам могут присылать фишинговые письма, фальшивые ссылки и вредоносные документы.

• Критически относитесь к любым неожиданным письмам и сообщениям — как от знакомых, так и от незнакомых людей.

• Если призыв к действиям выглядит правдоподобно — свяжитесь с источником по другому каналу. Если просьба настоящая, уточняющий звонок никого не обидеть.

• Вводите пароль от соцсети только на сайте и в приложении.

• На любых сайтах — всплывающее окно регистрации через соцсети может быть поддельным (особенно если вы уже авторизованы в данный момент.

Проверяйте адрес окна соцсети на подлинность).

• Никогда не переходите на нужный сайт по сторонней ссылке (она может быть поддельной). Используйте поисковик или сохраненные закладки.

• Если ссылка из поста в надежном сообществе или из поста хорошего друга — всё равно проанализируйте эту ссылку (могли взломать и группу и друга).

• Не получается проверить ссылку — никуда не переходите. Минутное любопытство не стоит последствий.

• *Всегда проверяйте ссылки, найденные в социальных сетях или присланные в сообщениях.*

Ваши данные:

Всем нужна ваша цифровая личность (чем точнее она будет, тем дороже перепродать).

Многие организации заинтересованы в детальной информации о вас:

• Рекламщики

• Банки

• Страховые компании

• Государственные органы (налоговая, судебные приставы, аналитические центры и т. д.)

• Работодатель

• Конкуренты

• Мошенники

"Гороскопы", "Тесты" и прочие подобные призывы в соцсетях — активно собирают как можно больше информации о вас и вашем устройстве (deviceinfo.me), а результаты, например, *тестирования* становятся недостающими частями пазла в вашем цифровом портрете (если вы импульсивный, то кредит на выгодных условиях в банке могут не предложить).

И чем больше данных о себе вы бездумно отдаёте третьим лицам, тем больше шансов, что эти данные могут «утечь» в руки мошенников. А они на их основе разработают схему того, как вас лучше завлечь, на какие точки давить и

с какой стороны к вам подходить. Вы просто дарите непонятно кому и зачем бесценные данные о себе.

Всё, что попадает в Сеть — остаётся там навсегда! (kribrum.ru)

БЕЗОПАСНОСТЬ КОМПЬЮТЕРА (ПК)

1. Физический доступ

• Установите сложный пароль на компьютере. Никто не сможет получить доступ к документам, фотографиям, проектам, паролям из браузера, установить следящее ПО, отформатировать жесткий диск или ваш ребенок случайно не сможет удалить папку и т.д. А ещё ноутбук можно потерять или его украдут.

• Меняйте рабочий пароль раз в 3 месяца (от возможного взлома путем подбора).

• Взломать перебором пароль, состоящий из 12 символов и включающий цифры и буквы разных регистров — почти невозможно!

• Оптимальное время автоматической блокировки экрана — через 2-3 минуты.

• Никогда не позволяйте другим людям использовать вашу учетную запись (для каждого пользователя отдельная учетная запись — дети, гости, муж/жена, коллеги).

• Всегда помните о шпионском ПО, установка занимает пол минуты (не давайте доступ к своим гаджетам никому).

• Не пользуйтесь публичными компьютерами, если там нужно авторизоваться на сайте (клавиатурный шпион). Либо позднее смените пароль, если необходимо зайти.

• Выходите из учетной записи Майкрософт (личный кабинет в Windows), чтобы не вёлся сбор данных.

2. Антивирус

• Выбирайте из топ-10 рейтинга PC Mag (самый авторитетный компьютерный портал в мире pcmag.com).

• Установите автоматическое обновление антивируса (для пополнения новыми базами).

Ведь каждое обновление — это ещё 100, 1000 или 10000 новых вирусов, которые появились в Сети.

• Сканируйте компьютер не реже раза в месяц!

• Сканируйте все внешние носители всегда (включите запрет на автоматическое их открытие в ПК).• *Важно! Антивирус всегда должен быть включен, его антивирусные базы должны быть актуальны, а лицензия — действительна.*

3. Обновления

• Регулярно обновляйте операционную систему (ОС) и браузер (то есть перезапускайте компьютер хотя бы раз в неделю).

• Редкое обновление ОС — накапливает много разных обновлений и начинает принудительный перезапуск (может занять более часа). Оставляет дыры для атак.

• Везде используйте автоматическое обновление (программы, приложения, расширения, антивирус, браузер).

• Регулярно обновляйте пользовательские программы — те, что сами установили на компьютер (в них тоже могут быть лазейки для преступников, а обновления закрывают эти кротовые норы). Обновляйте только из интерфейса уже установленной программы.

Кнопка "Обновить" в настройках программы — единственно правильный способ.

• При обновлении программ могут произойти две вещи:

1. Обновление загрузиться и установится.

2. Вас перенаправит на официальный сайт программы, где будет предложено скачать и установить вручную новую версию. (Это равноценные и безопасные способы).

• Любое предложение обновить ПО (программы), исходящее из Интернета, — является мошенничеством и содержит вредоносные программы (излюбленный трюк).

• Никогда не верьте предложениям обновить ПО, исходящим из

Интернета.

• Никаких всплывающих окон или навязчивых обновлений официальные сайты предлагать не должны. (Только реклама новой версии продукта).

• Мошеннические окна в браузере нередко маскируются под напоминания, появляющиеся на панели операционной системы (выезжают в виде подсказки или иконки внизу окна) — они точно так же всплывают в правом нижнем углу. Закройте браузер — если окно закрылось вмести с ним, это были мошенники

4. Вредоносное ПО

• Вредоносное ПО — главный враг вашего компьютера.

• Любое отклонение от работы вашего компьютера — может быть признаком вредоносного ПО.

• Абсолютное большинство вредоносных программ не может появиться на вашем компьютере без вашего участия. (Ваша задача вовремя распознать обман и остановиться)

5. Установка ПО (программы)

• Устанавливайте на компьютер только лицензионное программное обеспечение (и только на официальном сайте или на сайте его официального дистрибьютера, другие программы там тоже можно покупать, статус официального делает его проверенным).

• Как найти официальный сайт:

1) Если уже установлено ПО, то ссылка есть в разделе "О программе".

2) Википедия.

3) Поисковик (вводите максимально полное или близкое к правильному написание искомой программы).

• Не нажимайте рекламную выдачу в поисковиках. В рекламной выдаче — чистой воды мошенники! Они врут, что их сайт официальный, и предлагают платное ПО бесплатно.

• Программы на рабочий компьютер можно устанавливать только с помощью IT- специалистов компании (возможно, у них уже есть лицензии и к тому же вы передаете ещё ответственность)

6. Wi-Fi настройки (в ПК)

• Отключайте Wi-Fi, если не пользуетесь (чтобы по MAC-адресу не собирались данные ваших передвижений). Во время поиска Wi-Fi ваше устройство передает сигнал с уникальным аппаратным адресом (MAC). С его помощью можно отслеживать ваши перемещения.

• Используйте случайные MAC-адреса, чтобы ваше устройство нельзя было выследить, когда вы ищете Wi-Fi. Например, провайдер общественной сети Wi-Fi может собирать данные о том, какие магазины вы чаще всего посещаете, и продавать эти сведения рекламодателям. Чтобы ваш компьютер нельзя было идентифицировать, включите использование случайных аппаратных адресов (в Wi-Fi настройках в ПК).

• Удалите или "забудьте" ранее использовавшиеся Wi-Fi-соединения.

• Отключите "автоматическое подключение" к другим станциям Wi-Fi (можно попасть в "капкан", подключившись к бесплатной раздаче злоумышленника)

• Используйте соединение через VPN (Virtual Private Network — виртуальная частная сеть) по протоколам OpenVPN или WireGuard.
7. USB-устройства

• Отключите опцию «авто запуска» для всех носителей и устройств. Некоторые вирусы, особенно черви, распространяются автоматически.

• Всегда проверяйте любые подключаемые USB-устройства антивирусом (настройте автоматическое сканирование).

• Есть вирусы, которые воруют данные с компьютера на USB-устройства.

• Не подключайте к своему компьютеру незнакомые внешние устройства — найденные в офисе или где-либо ещё. Если вы нашли флэш накопитель USB на улице, в поликлинике, в магазине, в общем, - не на работе, - не поднимайте. Если подняли с пола в кафе - передайте официанту. Если подняли на улице - выбросьте. Даже если это хороший дорогой внешний жесткий диск. Не надо рисковать!

• Блокируйте USB-порты на работе (чтобы нельзя было разблокировать

компьютер при помощи USB-устройства).

• DeviceLock DLP позволяет подключать только заранее подготовленные и авторизованные устройства — то есть вы не сможете подключить "чужую" флэшку, незнакомый жесткий диск и т.д.

• Любой контакт компьютера с внешним миром — будь то физический носитель (USB) или Wi-Fi-сеть — может стать угрозой для безопасности.

8. Потеря ПК

• При потере личного ноутбука следует, не откладывая, предпринять ряд действий для обеспечения безопасности хранящейся на ней информации. (Включите геолокацию, удалите все данные, смените все пароли на сайтах). Ключевой фактор — время.

• Заранее измените настройки для удаленной блокировки ноутбука, а также его поиска и администрирования (MacOS - "Локатор", Windows 10 - "Найти моё устройство").

• Имеется доп. защита от незаконного проникновения — установить пароль на BIOS (синий экран при запуске) и включить Secure boot (безопасная загрузка).

Злоумышленник не сможет, загрузив операционную систему с внешнего носителя, получить доступ к вашим файлам в обход пароля на вход в компьютер.

• Шифруйте свои данные — Bitlocker (Windows Pro), FileVault (MacOS), LUKS (Linux). Либо сторонняя программа GPG(GnuPG) и VeraCrypt. Используйте полно-дисковое шифрование.

9. Веб-камера и микрофон

• Выключайте, прикрывайте или заклеивайте веб-камеру, когда не используете её.

• Отключайте физически внешне подключаемую камеру, когда не используете (там встроенный микрофон).

• Если вы заметили, что диод камеры мигнул хотя бы на несколько секунд — сразу же отключите Интернет, запустите антивирус (возможно следящее ПО). При выключенной камере он не должен ни гореть, ни мигать ни при каких

обстоятельствах.

• Отключите микрофон в меню настроек ОС (Диспетчер устройств - Звуковые, игровые и видеоустройства - Микрофон - Драйвер или правой кнопкой мыши "Отключить").

• Отключите микрофон — вставьте любой обрезанный штекер в гнездо микрофона.

10. Резервное копирование

• *Регулярно* делайте резервные копии важной информации (ПК можно залить водой, забыть, его могут зашифровать, украсть).

• Резервное копирование — лучшее средство борьбы с программами-вымогателями. Даже если заплатите, шанс корректно разблокировать 30-50%.

• Жесткие диски имеют срок годности. После какого-то количества циклов перезаписи они могут выйти из строя сами собой, без внешнего вмешательства.

• Насколько регулярно? Если важные для вас данные обновляются ежедневно — создавайте резервную копию раз в 2-3 дня. Если ежемесячно — то раз в месяц. В среднем целесообразно *раз в неделю.*

• По возможности настройте автоматическое копирование важной информации в Облако — так вы не будете забывать обновлять резервную копию.

• Используйте правило 3-2-1.

а) Ценная информация должна иметь 3 резервные копии.

б) Они должны быть сохранены в двух различных физических форматах хранения. в) Одна из копий должна быть вынесена на вне офисное хранение.

1. Три копии первого уровня должны храниться *в трёх разных физических местах.*

2. Две копии второго уровня должны быть сделаны *в двух разных физических форматах* (электромагнитный импульс может вывести из строя электронное устройство, но не повредит DVD-диску, а если дом ограбят, то облачное хранилище останется в неприкосновенности).

3. Одна копия должна находится вне офиса (географическое распределение). Облачный сервис — идеальный способ.

• *Регулярно копировать* имеет смысл только те файлы, которые вы обновляете.

• Документы, с которыми вы работаете каждый день требуют регулярного бэкапа.

• *Имеет смысл дублировать рабочие документы и личные фотографии.* Дублировать системные файлы нет смысла — в случае чего ОС нетрудно переустановить, а резервное копирование системных файлов бесполезно.

• Регулярно создавайте *точки восстановления* (особенно перед каждым небезопасным действием, например, перед установкой новой программы или приложения).

11. Ремонт ПК

• Компьютер в ремонт отдавайте "стерильным".

• Снимите перед ремонтом сам жесткий диск (если проблема не в нём). • Зашифруйте, или удалите всю конфиденциальную информацию.

• Перенесите все данные на внешний жесткий диск.

• Не всегда сотрудники мастерской благонадежны. Они подменяют детали, копируют информацию, навязывают дополнительные услуги. Требуйте чек и упаковку от детали, которая установлена, а лучше, чтобы деталь извлекли из упаковки прямо при вас. Часто устанавливают пиратскую ОС (установите сами).

• Покупайте запчасти лучше в магазинах, а не в сервисах.

• Используйте шифрование диска — штатная BitLocker (Windows Pro), FileVault (MacOS) или VeraCrypte, CyberSafe.

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ

1. Физический доступ

• Всегда используйте пароль, даже если есть биометрия (отпечаток пальца, лица).

• Максимально сложный пароль, хотя бы *шесть знаков с не очевидной комбинацией* (защита от детей, любопытных коллег, близких,

злоумышленников).

• Не оставляйте смартфон без присмотра, даже если рядом только ваши друзья или родственники (шпионское ПО устанавливается за пол минуты).

Никогда не оставляйте телефон без присмотра *разблокированным и не давайте свой телефон другим людям.*

• Автоматическая блокировка экрана (1 минута).

• *Отключите вывод содержания сообщений на экране блокировки* (или настройте показ от кого пришло сообщение, а не само содержание).

• Подключите спец. приложение для двух факторной аутентификации, например Google Authenticator (надежнее SMS-кодов).

• *Настройте голосовой помощник* — в режиме блокировки он работать не должен (так можно разблокировать телефон похожим голосом или сделать перевод).

• Используйте *биометрию* (несколько пальцев с обеих рук, несколько выражений лица).

• Используйте *графический ключ* (хотя бы 5-6 движений, сложная фигура).

• При использовании *отпечатка пальца* выбирайте для авторизации мизинец и безымянный палец левой руки для правшей и правой руки — для левшей. Обычно пользователи выбирают указательный и большой палец. Это удобно, но неправильно, так как в работе со смартфоном мы в первую очередь пользуемся именно ими.

Получив «залапанный» смартфон, преступник сможет изготовить фальшивый отпечаток за пару часов — инструкций в интернете для этого достаточно.

• Напишите заявление (или отправьте команду*) о запрете перевыпуска SIM-карты по доверенности* (SIM-свопинг атака). Для Теле2, МТС команда (*156*2#), для Мегафон (*105*508#).

• *Установите ПИН-код на SIM-карту.* При потере телефона избежите переноса SIM-карты на другое устройство.

2. Антивирус

• Обязательно используйте антивирус (TOP-10, techradar.com). Не игнорируйте обновления и окончание лицензии.

• *Регулярно сканируйте.* Лучше всего это делать после установки каждого нового приложения. Ну или после того, как они обновятся (если боитесь забыть, настройте автоматическое сканирование по заданному вами расписанию).

• В настройках антивируса установите — "все подозрительные файлы приложения удалять по умолчанию".

3. Вредоносное ПО

• В App Store и Google Play — не все приложения безопасны.

• *Любое отклонение в работе смартфона - признак вредоносного ПО* (нагрев, "торможение", деньги быстро заканчиваются, много рекламы, даже там, где не должно быть; появляются запросы на установку неизвестных приложений (дропер), знакомое приложение отказывается запускаться или закрываться; форма в приложении выглядит необычно или непривычно; не принимаются пароли, хотя вы их не меняли.

• *Заметили признаки* — про сканируйте, откажитесь от любых действий в телефоне (ввод логинов, переписка). Измените все пароли в сетевых сервисах (с другого устройства).

Не пытайтесь удалить ПО самостоятельно — де инсталяция может привести к блокировке смартфона или активации других вредоносов.

• *Распространение вредоносного ПО:*

1) приложения

2) "фишинговый" путь — убеждение перейти по вредоносной ссылке, скачать зараженный файл, зайти на подозрительный сайт.

• *Никогда не устанавливайте на свое устройство пиратское и не лицензионное ПО.*

• Соблюдайте *правила безопасного сёрфинга*: не переходите по подозрительным ссылкам, не посещайте пиратские сайты, не загружайте пиратские файлы из Интернета.

• Никогда не переходите по ссылкам из SMS (которые вы не запрашивали и не ожидали, не открывайте даже от близких, их могли взломать!).

• *Проверяйте ссылку на скрытую подмену* (нажать и долго удерживать нажатую ссылку - скопировать URL - вставить *для просмотра* в записную книжку, а в адресную строку нельзя, есть риск случайно перейти по ней).

• Не контекстное несовпадение ссылки опасно (kfd2Wjn.to или bestcomputers.com).

• Проверяйте ссылки здесь (https://opentip.kaspersky.com или https://www.virustotal.com/gui/home/upload). Для мобильных и сёрфинга это наиболее удобный способ.

• SMS-настройки — *запретите установку программ из сторонних источников* в настройках устройства. Так вы сведете к минимуму вероятность заражения.

• Также с осторожностью относитесь к приложениям, которые требуют доступ к SMS.

• Некоторые вредоносные приложения обещают бесплатный пробный период. Обычно пользователь удаляет такое приложение, *но платная подписка остаётся!*

• *Проверяйте свои банковские выписки и мобильные платежи* на наличие подозрительных покупок и платных подписок. Убедитесь, что вы держите под контролем ваши транзакции.

4. Файлы

• Никогда *не открывайте файлы*, приложенные к сообщениям (которых вы не ждёте).

• Нужно помнить, что *расширение исполняемых программ* для Android - .apk, а для iOS - .ipa.

• *Никогда не загружайте исполняемые файлы ни из каких сообщений*

5. Приложения

• Загружайте только из официальных магазинов приложений.

• Если приложение в официальном магазине платное — никаких

бесплатных версий где- либо ещё быть не может (мошенничество).

• *В App Store и Google Play проникает вредоносное ПО.*

• При загрузке приложения — всегда обращайте внимание на рейтинг (2.5 из 5 баллов точно опасное), кол-во загрузок, кол-во отзывов с разными датами (качественные разные отзывы от людей, а не от ботов). *Выбор редакции,* это хорошо (разработчики проверили на себе). Сторонний рейтинг в СМИ.

• *Внимательно смотрите за разрешениями, которые даете приложениям!!!* Вы должны понимать, зачем нужно каждое из разрешений. Оставьте лишь самый минимум разрешений, необходимых для работы приложений (остальные — отозвать).

• Не выдавайте каким попало приложениям права на доступ к *«Специальным возможностям»* (программ, которым они действительно нужны, крайне мало).

• Странные разрешения — ещё один признак подозрительного приложения (Контакты для фонарика)!

• Никогда и ни за что нельзя давать права разрешения: *суперпользователя (root-права)*, на отображение поверх других окон (будет блокировка с выкупом или подмена формы логин/пароль), на доступ к SMS (платные SMS от вас, передача сообщений и кодов, отслеживание звонков).

• *Не давайте номер своего телефона автоматически ни одному приложению*, которое может запросить данные. Чем больше приложений запоминают ваш номер, тем более устройство уязвимо к мошенничествам с SMS (и даже к вторжениям в защищенные учетные записи 2FA).

• Устанавливать приложение *по пришедшим откуда-то ссылкам* — нельзя ни при каких обстоятельствах.

• Подлинное приложение — это переход в магазин *по ссылки с официального сайта!*

• Будьте внимательны и с умом относитесь к любому приложению, которое собираетесь загрузить в свой смартфон.

• *Избавьтесь от ненужных приложений.* Чем больше программ, тем выше

шанс, что какие-то из них будут заниматься недобросовестной деятельностью.

• Чем меньше приложений — тем быстрее работает смартфон.

6. Обновление

• *Обновляйте систему и браузер как можно скорее* (закрываются лазейки). Чем современнее ПО и браузер, тем выше уровень вашей защиты. Не игнорируйте уведомления или делайте все вручную, просто перезагружая телефон.

• Настройте *автоматическое обновление приложений*.

• В Google Play обновления находятся в разделе "Мои приложения и игры", а в App Store — за иконкой обновлений в правом нижнем углу экрана.

7. Bluetooth

• Когда Bluetooth включен, преступник может установить на устройство любую программу (используя уязвимость), удаленно управлять устройством, прослушивать и считывать вводимую информацию.

• Отключайте Bluetooth, когда не используете его.

• *Никогда не подключайтесь по Bluetooth к незнакомым устройствам* (возможен запуск вредоноса).

• *Никогда не принимайте запросы на подключение Bluetooth*, если не знаете их цели.

Возможно, это попытка атаки.

• Принимайте запросы на подключение через *Bluetooth только от знакомых* (до того, как одобрять connect).

• Устанавливайте сопряжение с сервисами только в случае, если вы им доверяете, и они нужны вам именно сейчас.

• Если есть постоянное сопряжение с другим устройством (фитнес-браслет, часы), — отключите *режим постоянной видимости Bluetooth.*

• По возможности настраивайте доступ для каждого подключения индивидуально.

• Если подключился неизвестный — отключите Bluetooth и удалите из списка незнакомые подключения. Запустите проверку антивируса.

• Сделайте проверку *на известные уязвимости через Bluetooth.* Найти приложения по запросу "сканер уязвимостей/vulnerability scanner" (например, приложение Armis BlueBorn Scanner App).

• Внимательно относитесь к Bluetooth - подключениям. Старайтесь не включать Bluetooth без причины и следить за тем, с чем сопрягается ваше устройство.

8. USB - устройства

• *Не используйте смартфон в качестве USB - носителя* (можно заразить вредоносным ПО или самим стать носителем).

• *Не заряжайте смартфон от компьютеров и общественных точек зарядки* (используйте внешний аккумулятор). Электроэнергия может передаваться с вредоносной информацией ("атака соковыжималка").

• В продаже имеются спец. устройства — безопасные переходники, зарядные провода без передачи данных и т. д.

• *Лучше заряжать смартфон исключительно от розетки или Powerbank.*

• Зарядка от розетки совершенно безопасна.

• Даже в режиме "только зарядка" телефон может обмениваться данными с компьютером.

• Трояны и вирусы, спроектированные для распространения через USB-порт, копируются на подключенное устройство *автоматически.*

• *Пользуйтесь облачным сервисом для переноса и передачи информации (*через Облако безопаснее, чем через смартфон или любой USB-носитель).

• *Всегда сканируйте* любое подключаемое устройство к компьютеру.

9. Резервное копирование

• *Регулярно создавайте резервные копии данных на смартфоне* (особенно если используете устройство для работы или храните на нём важные документы или файлы). Могут зашифровать, украсть или просто разбить.

• Настройте автоматическое копирование важной информации в "облако".

• Очень важно копировать рабочую информацию.

10. Дополнительные настройки

• Услышали об очередной утечки в новостях — смените пароль на этом ресурсе.

• Периодически удаляйте *геолокационные данные* в настройках.

• *Отключайте Wi-Fi, если не пользуетесь*, а также *"автоматическое подключение к Wi Fi"*.

• *Меры против прослушки* — не подключайте 2G (отказ от авто выбора), отключите роуминг (Оператор сети -> Отключить автоматический выбор сети).

• *Apple — сбросьте сертификаты сопряжения на своих устройствах*

Если вы подключаете свой iPhone к компьютеру другого человека и доверяете ему, то между этим компьютером и устройством iOS будет установлена связь, позволяющая компьютеру получать доступ к фотографиям, видео, SMS - сообщениям, журналам вызовов, сообщениям WhatsApp и большинству других данных без введения кода доступа.

Ещё большее беспокойство вызывает то, что этот человек с помощью программы iTunes может сделать *резервную копию всей памяти вашего смартфона*, если только вы не установили пароль для создания зашифрованных резервных копий iTunes (установите пароль!)

11. Потеря или кража

• Настройте удаленный доступ к устройству на случай его потери или кражи, включите геолокацию (можно отследить местоположение, заблокировать устройство, стереть все данные или вывести на экран контактную информацию; можно включить автодозвон — устройство будет звонить регулярно и максимально громко, даже на беззвучном режиме).

• Перепишите себе IMEI (*#06#) и серийный номер устройства. На случай кражи это позволит полиции идентифицировать телефон среди других найденных или поможет заблокировать его через оператора и на сайте Гос. услуг (с июня 2021 года)!!!!!

• Имеются так же сторонние приложения для удаленного

администрирования (блокировка, очистка, геолокация).

• Некоторые приложения позволяют *стереть всю информацию даже без подключенного интернета* (по SMS, при извлечении SIM-карты, при неоднократном вводе неверного пароля). Если данные очень ценные для злоумышленников, установите такое приложение (Eradoo).

12. Остерегайтесь фишинга по телефону

• *Никогда не сообщайте никаких ДАННЫХ* незнакомым людям, позвонившим вам по телефону, помните, что «Социальную Инженерию» никто не отменял!!!!

• *Никогда не переводите никаких СРЕДСТВ* по рекомендации или просьбе незнакомых людей, позвонивших вам по телефону.

• Внимание! Часто используется служба *подмены номера* — при звонке от мошенников вы видите номер ваших родных, близких или банка.

• Не знаете как отвечать, *положите трубку и возьмите паузу, время Ваш помощник!!!!*

13. Заводской бэкдор (лазейка для удаленного управления)

• Изначальная цель — дополнительно заработать.

• Зачем производители устанавливают бэкдоры в смартфоны:

1. Чтобы обойти запрет на установку какого-нибудь ПО.

2. Чтобы зарабатывать на показываемой пользователям рекламе.

3. Чтобы собирать данные о пользователях в маркетинговых целях.

• На многих смартфонах (особенно недорогих китайских) *предустановлены невидимые «вредоносы»* (для слежки, рекламы, сбора статистики, "заглушка" для другого вредоносного ПО).

• Иные бэкдоры вообще не спрашивают разрешения, а сразу что-то устанавливают (веселую игру и т.д.).

• Подобный «бэкдор» — это лазейка для злоумышленников с доступом к любым данным. Ни антивирус, ни ОС её не замечают, поскольку она *предустановлена и считается фитчей.*

• Любой подобный «бэкдор» — это дверь, через которую может войти кто

угодно.

• *Не покупайте дешевые смартфоны малоизвестных производителей,* особенно производства Китая и Индии. Вы можете потерять гораздо больше, чем сэкономить.

• Если смартфон неизвестной компании с фантастическими характеристиками стоит 100 евро, то стоит задуматься: на чём ещё зарабатывает производитель?• При выборе смартфона поищите в Интернете о его потенциальных бэкдорах и возможности их ликвидации.

• Например, поищите статью по запросу "xiaomi backdoor" или "oneplus backdoor", плюс конкретная модель, которую вы рассматриваете. И если обнаружится, что есть подобная уязвимость, *стоит исключить её из рассмотрения.*

• Если вы всё-таки приобрели недорогой китайский смартфон, который можно подозревать в наличии бэкдора, никогда не используйте его для рабочих целей (не пересылайте конфиденциальную информацию, не сохраняйте рабочие пароли, не фотографируйте рабочие объекты и т.д.).

• Пользоваться смартфоном можно, но *не стоит делать с его помощью ничего, связанного с работой или учёбой* — от рабочей переписки до работы в Google-документах.

14. eSIM — встроенная SIM-карта

• Это физический чип, встроенный и распаянный на плате мобильного гаджета (вынуть его, перенести на другой телефон и отдельно купить не удастся).

• Есть возможность установки сразу 5 номеров.

• Экономия средств. Можно выбрать одного оператора, у которого самые выгодные тарифы на звонки, второго – интернета, третьего – для отправки SMS.

• Защита. Если злоумышленник украдет смартфон, он не сумеет извлечь eSIM.

• Невозможно повредить карту или потерять.

• Если вы часто путешествуете, не надо покупать в чужой стране

физическую SIM-карту. В другой стране достаточно посетить сайт местного оператора, оформить виртуальную карту, *оплатить услугу и отсканировать QR-код.*

• *Можно подключить все «умные» гаджеты к одному устройству*

2.3. Апробация разработанных рекомендации на базе Миасского машиностроительного колледжа

Апробация разработанных рекомендаций проводилась путем проведения опытно-практической работы по формированию информационной безопасности личности в социальных сетях у студентов ПОО на базе Миасского машиностроительного колледжа.

Проникновение современных технологий во все сферы жизнедеятельности общества и во все его возрастные группы неизбежно привело к вовлечению в информационное пространство подрастающего поколения. На сегодняшний день киберпространство стало неотъемлемой частью реальной жизни современной молодежи, позволяющей ей удовлетворить не только информационную потребность, но потребность в общении посредством киберкоммуникации.

Подрастающее поколение использует возможности киберпространства для поиска информации, подготовки домашних заданий, прослушивания музыки, просмотра кинофильмов, онлайн-игр, общения в социальных сетях, попыток заработать первые деньги, заявить о себе, творчески самореализоваться и многого другого. Подобного рода взаимодействие молодого человека с киберпространством сопряжено с подстерегающими его на каждом шагу киберопасностями – фишингом, травлей в сети, нежелательным контентом, мошенниками различного уровня, манипуляциями сознанием и др.

В силу возрастных особенностей студенческой молодежи, обучающейся в учреждениях среднего профессионального образования, ее социально-психологической незрелости, податливости к информационным воздействиям в сочетании с ее активностью в киберпространстве решение задачи формирование информационной безопасности обучающихся колледжа приобретает особую значимость. Решение этой задачи осуществляется в специально организованной образовательной среде, обладающей потенциалом для эффективного формирования у обучающихся колледжа системы практико-ориентированных знаний основ кибербезопасного поведения, а также умений и навыков их

реализации в киберпространстве. В связи с этим формирование информационной безопасности должно стать важной составляющей профессиональной подготовки и неотъемлемой профессиональной компетенцией обучающихся колледжа.

В системе деятельности образовательной организации СПО по обеспечению информационной безопасности обучающихся колледжа и формированию у них информационно безопасностного поведения можно выделить несколько взаимосвязанных направлений.

Первое направление включает в себя непосредственное взаимодействие педагогов с обучающимися посредством реализации разнообразных форм, методов и технологий, нацеленных на формирование информационной безопасности. К ним можно отнести:

− проведение кураторских часов, затрагивающих проблемы кибербезопасного поведения (например, «Интернет – друг или враг?», «Золотые правила безопасного поведения в сети», «Основы финансовой безопасности в киберпространстве», «Осторожно, кибермошенники!» и др.);

− размещение в электронной информационно-образовательной среде колледжа «Памятки по безопасному поведению в сети Интернет»;

− проведение в колледже «Недели кибербезопасности» (комплекс мероприятий, включая классные часы, конкурсы, круглые столы с приглашенными специалистами, квесты по кибербезопасности и др.);

− привлечение обучающихся колледжа к участию в онлайн-конкурсах и олимпиадах по кибербезопасности (например, на сайте Сетевичок.рф);

− организацию образовательных курсов по кибербезопасности, в том числе дистанционных;

− модернизацию программ учебных дисциплин под задачи формирования культуры кибербезопасности обучающихся;

− киберобучение в формате симуляции типичных жизненных ситуаций – встречи с киберопасностями (поиск и скачивание информации, проверка

электронной почты, покупка в интернет-магазине, поиск работы через интернет-сайты, интернет-знакомства и предложения о личной встрече и др.);

− решение кейсов по проблемам угроз кибербезопасности с учетом специфики будущей профессиональной деятельности и др.

Независимо от формы работы очень важно, чтобы обсуждаемые со студентами вопросы не носили абстрактный характер, а соответствовали встречающимся в реальной жизни обучающихся ситуациям, органически вписывались в процесс профессиональной подготовки будущих специалистов.

Второе направление деятельности включает в себя организацию и осуществление взаимодействия между педагогом и родителями студентов. Важность данного направления определяется тем, что значительную часть обучающихся в образовательных организациях СПО составляют несовершеннолетние. Здесь важно показать, что дома студент тоже может быть подвержен угрозам информационного характера, поэтому необходимо проводить с родителями работу для моделирования «цифровой гигиены». Главной формой психолого-педагогического и нормативно-правового просвещения по проблемам кибербезопасности является родительское собрание. В содержание родительских собраний можно включить следующие вопросы:

− нормативно-правовые основы защиты несовершеннолетних от киберопасностей;

− возрастные особенности обучающихся колледжа и их влияние на поведение в киберпространстве;

− причины, признаки и пути коррекции интернет-зависимости;

− модные в молодежной среде онлайн-игры, интернет-группы и сообщества, представляющие потенциальную опасность для психического и (или) физического здоровья, жизни и безопасности обучающихся;

− признаки, помощь и поддержка обучающихся, ставших жертвой кибербуллинга;

− поведенческие особенности студентов, попавших в сети под влияние религиозных сект, экстремистских организаций, и др.

Полученные родителями знания в области кибербезопасности позволят им защитить своих детей от киберугроз и научить их противостоять этим явлениям.

Третье направление деятельности образовательной организации СПО по обеспечению информационной безопасности студентов – построение взаимодействия со сторонними организациями. Так, например, различные компании, деятельность которых направлена на защиту от информационных угроз, могут оказывать свои услуги образовательным организациям либо предоставлять им программные продукты, осуществляющие защиту. Также это взаимодействие можно применить и в образовательном процессе, например путем приглашения экспертов по цифровой безопасности для работы со студентами, проведения различных тренингов и др.

Четвертое направление по обеспечению информационной безопасности обучающихся колледжа связано с взаимодействием между законодательными и исполнительными органами (разного уровня) и образовательными организациями. Рекомендуется на уровне образовательных стандартов ввести дисциплины, связанные с цифровой грамотностью и кибербезопасностью, а также регулярно проводить повышение квалификации и курсы профессиональной переподготовки для педагогических кадров системы СПО, направленные на совершенствование навыков безопасной работы с обучающимися в киберпространстве и формирование у них информационно - безопасного поведения.

Все перечисленные действия, направленные на обеспечение информационной защиты студентов в образовательном процессе колледжа, должны применяться в комплексе. Также необходимо назначать одного или нескольких лиц, ответственных за реализацию мер, определяющих информационную безопасност обучающихся.

Вывод по второй главе

Будьте осторожны со ссылками.

Ссылки в электронных письмах – это распространенный инструмент, используемый хакерами, чтобы обманом заставить людей отказаться от своей защищенной информации. Это часто бывает в форме банковских выписок, бронирования авиабилетов, электронных писем для восстановления пароля и т. д.

Если пользователь нажимает на одну из этих ссылок, он попадает на поддельный сайт, который очень похож на своего реального аналога. Сайт попросит их войти в систему или ввести личную информацию. Как только хакер получит эту информацию, он получит доступ к учетной записи пользователя.

Так что помните о ссылках в своих письмах. Если что-то выглядит подозрительно, не нажимайте на это. Фактически, самый безопасный вариант — посетить сайт провайдера напрямую, а не использовать ссылку по электронной почте.

Меняйте пароли.

Хотя проще запомнить один пароль для всех ваших учетных записей, он не самый безопасный. Лучше всего менять пароль для каждого используемого сайта и учетной записи. Таким образом, если компания, которую вы используете, будет взломана, украденные учетные данные не будут работать на других сайтах. Если вам интересно, как вы могли бы запомнить все эти пароли, вы не одиноки. Но это подводит нас к третьему совету.

Используйте диспетчер паролей.

Менеджер паролей — это программа или программа, которая хранит все ваши пароли в одном месте. У вас есть один пароль «мастер-ключ» для разблокировки доступа к этим паролям. С менеджером паролей вам не придется беспокоиться о запоминании каждого из ваших паролей. Это также избавит вас от необходимости записывать пароли (чего никогда не следует делать!)

LastPass, KeePass, Dashlane, 1Password и Roboform – хорошие программы. Многие предлагают бесплатные версии, а некоторые совершенно

бесплатны. И, если вы используете Dropbox, OneDrive, Google Drive или тому подобное, вы можете сохранить базу паролей на своем облачном диске, и она будет доступна где угодно.

Настройте многофакторную аутентификацию.

Без настройки многофакторной аутентификации(MFA) пользователь может получить доступ к своей учетной записи, используя только имя пользователя и пароль. Но MFA добавляет еще один уровень защиты. Для проверки личности пользователя при входе в систему требуется более одного метода аутентификации.

Один из примеров MFA – это когда пользователь входит на веб-сайт и должен ввести дополнительный одноразовый пароль. Этот одноразовый пароль обычно отправляется на адрес электронной почты или на телефон пользователя. Настройка MFA создает многоуровневую защиту, затрудняя несанкционированный доступ к вашей информации.

Не используйте дебетовые карты в Интернете.

Еще один важный совет по кибербезопасности касается онлайн-платежей. При совершении онлайн-платежей избегайте использования дебетовых карт. Или что-нибудь, что напрямую связано с вашим банковским счетом.

Вместо этого используйте параметры, которые обеспечивают дополнительный уровень защиты между хакерами и вашими банковскими счетами. Это может быть кредитная карта со страховкой или какой-либо способ оплаты онлайн, например PayPal.

Не сохраняйте информацию о платеже.

Многие веб-сайты позволяют сохранять информацию о кредитной карте, чтобы сделать будущие покупки быстрее и проще. Не делай этого. Нарушения случаются постоянно. Красть нечего, если ваша кредитная карта не сохранена на сайте. Это может показаться проблемой, но мы обещаем, что это не так плохо, как кража вашей информации.

Держите свои системы в актуальном состоянии.

Ваше программное обеспечение, операционная система и браузер всегда

должны быть в актуальном состоянии. Если в вашей компании используется брандмауэр, программное обеспечение и прошивка брандмауэра также должны быть обновлены. Чем старше система, тем больше времени у хакеров для поиска уязвимостей. Обновляя свои системы, вы предотвратите использование вредоносными программами или хакерами этих слабых мест в системе безопасности.

Итак, в следующий раз, когда вы увидите всплывающее окно с обновлением системы, не игнорируйте его!

Избегайте неизвестных сайтов.

В наш век социальных сетей легко поделиться ссылкой в Интернете. Но будьте осторожны при посещении новых сайтов. Возможно, на этих сайтах проводятся «атаки на скачивание», которые могут угрожать вашим данным.

При атаке с использованием закачки через диск пользователю даже не нужно нажимать на что-либо, чтобы компьютер мог заразиться. Достаточно просто посетить сайт, чтобы передать вредоносный код. Итак, лучше всего придерживаться хорошо зарекомендовавших себя сайтов, которым вы доверяете. Хотя эти сайты тоже можно взломать, это маловероятно.

Будьте осторожны в социальных сетях.

Социальные сети — отличный способ поддерживать связь с друзьями и семьей. Но помните, чем вы делитесь в Интернете. Преступники и хакеры могут узнать много информации о вас, наблюдая за вашим общедоступным профилем. И точно так же, как вы не стали бы делиться всей своей личной информацией с незнакомцем, вы не должны делиться ею в Интернете.

Установите антивирусное программное обеспечение.

Вирусы, шпионское ПО, вредоносное ПО, фишинговые атаки и многое другое. Есть так много способов, которыми ваши данные могут быть скомпрометированы. Установка антивирусного программного обеспечения на ваше устройство поможет бороться с этими атаками. Убедитесь, что программное обеспечение активно и в актуальном состоянии, и что оно должно предотвращать угрозы цифровой безопасности еще до того, как они возникнут.

Избегайте ненужных загрузок.

Загрузки — это основная тактика, которую используют хакеры для получения доступа к вашей сети. Чтобы защитить ваш компьютер и ваши данные, ограничьте количество скачиваний. Следует избегать любого ненужного программного обеспечения или расширений браузера. А в организации сотрудникам требуется авторизация перед загрузкой чего-либо из Интернета.

Если вы считаете, что загрузка безопасна, всегда выбирайте индивидуальную установку и внимательно смотрите. Если какие-либо надстройки или расширения появляются во время автоматической установки, отклоните их.

Будьте чрезмерно подозрительны.

Хотя многие вещи в Интернете безопасны, лучше перестраховаться. Будьте в курсе любых ссылок, которые вы нажимаете, программного обеспечения, которое вы загружаете, и сайтов, которые вы посещаете. Немного здоровой паранойи по отношению к электронной почте, социальным сетям и Интернету может помочь вам уловить вещи, которые в противном случае ускользнули бы от вас.

ЗАКЛЮЧЕНИЕ

Появление и популяризация инновационных технических устройств, функционирующих на основе сетевой логики, инициировали трансформацию многих форм социальной активности личности. Особенно сильное влияние обозначенные процессы оказали на коммуникативную сферу, способствуя формированию простого, доступного, моментального опосредованного взаимодействия с сетевыми факторами.

Однако наряду с поиском выгодных и продуктивных решений, основанных на свободном доступе и обмене информацией с представителем любой возрастной, гендерной, социальной группы, получили развитие такие разрушительные процессы, как информационные атаки, информационный терроризм, хищение данных, сокрытие и искажение информации. В этой связи изучение сущности и особенностей информационной безопасности в сетевых коммуникациях, описание реальных и потенциальных угроз в социальных сетях и способов защиты от них стало особенно актуальным.

Под информационной безопасностью в данном исследовании понимается состояние защищенности личности от деструктивных воздействий в информационной среде.

Объектами защиты являются: конституционные права, психика, физическая, духовная и интеллектуальная сферы.

Субъектами защиты могут выступать как государство, технические специалисты, так и сама личность. Система информационной безопасности обозначена как совокупность нескольких элементов: информационно-технической, информационно-правовой, информационно-психологической безопасности

Феномен сетевой коммуникации определяется в работе как коммуникационный процесс, организованный по принципу сетевой структурыи обладающий такими характеристиками, как динамичность, глобальность, опосредованность, анонимность, гибкость, децентрализованность, интерактивность и хаотичность.

Принцип сетевой коммуникации наиболее наглядно представлен в интеракциях пользователей социальных сетей. Под социальной сетью понимается онлайн сервис, посредством которого люди могут группироваться по различным принципам, а также общаться и самовыражаться при помощи специальных инструментов. Основным отличием социальных сетей является возможность быстрого поиска единомышленников, установления контактов с пользователями, передачи различной информации, создания и наполнения собственных персональных страниц и другое.

На основе анализа сущности и особенностей сетевой коммуникации и социальной сети показано, что несмотря на преимущества новой формы взаимодействия, которая позволяет устанавливать контакт независимо от географического положения, национальности, культуры, часового пояса, способствует формированию коммуникационных сетей, играющих ключевую роль в решении экономических, политических и иных проблем, а также помогает найти знакомых, друзей, родственников, деловых партнеров, единомышленников, существуют негативные последствия данных новаций.

Наряду с активным распространением сетевых средств коммуникации увеличивается сложность социальной системы в целом и системы коммуникации в частности, что является фактором ослабления стабильности. Распространение горизонтальной коммуникации, ее открытость и демократичность инициируют развитие новых способов деструктивной деятельности в виртуальном пространстве.

В контексте обозначенных тенденций изучены особенности наиболее активной аудитории виртуальных платформ — молодежи. Сделан вывод о том, что представители молодежной аудитории, обладающие неустойчивой психикой, восприимчивым сознанием, отсутствием сформированной системой ценностей, противоречивыми чертами личности и потребностью в идентификации и самопрезентации, являются уязвимой для информационных воздействий группой.

Помимо этого, в рамках исследования описаны и классифицированы

способы информационных атак в условиях сетевой коммуникации. Негативные воздействия в виртуальной коммуникации сгруппированы в три совокупности: технические, психологические и смешанные информационные угрозы.

Под техническими угрозами личности автор работы обозначил опасные воздействия, связанные с несовершенством технических устройств, программ, способов обработки, передачи информации, такие как компьютерные вирусы, вредоносное программное обеспечение, кейлогеры, неполадки в системе безопасности виртуальной площадки, незащищенное соединение ресурса, некорректно указанные настройки и пр.

Психологические угрозы личности определены как негативные воздействия мошенников на психику пользователя путем обмана, манипулирования данными, шантажа, угроз, распространения оскорбительной информации и пр. Было выяснено, что психологические угрозы представляют наибольшую опасность, так как доказать ущерб и причастность к делу конкретного лица не всегда возможно. В большинстве случаев преступник регистрирует аккаунты на компьютерах общего пользования или отрицает свою вину, что препятствует расследованию преступлений. К психологическим угрозам отнесены такие феномены, как кибербуллинг, троллинг, хеппислепинг, методы социальной инженерии и другие.

Отдельную группу составляют виртуальные опасности, основанные на применении информационно-технических и информационно- психологических методов в совокупности. Особенностью атак данного типа является использование одиночных сообщений или примитивных диалогов, содержащих подозрительные ссылки или вложения. Примерами таких информационных угроз являются спам, фишинг, фарминг.

В рамках исследования изучены реальные ситуации хакерских нападений на пользователей и связанные с ними судебные прецеденты. В

результате анализа представленных кейсов сделаны значимые выводы о необходимости комплексной защиты личности, базирующейся на совокупности технических, психологических, правовых методов и определенном алгоритме действий. В ходе работы доказано, что разрозненные способы защиты могут не только не привести к необходимому результату, нои повлечь за собой более серьезные негативные последствия для пользователя. На основании теоретических и практических данных описаны основные элементы комплексной модели защиты, обозначена последовательность действий для обеспечения личной безопасности: идентификация угрозы, описание и анализ особенностей реальной или потенциальной опасности,выбор подходящих методов защиты, разработка плана действий и его реализация.

Под идентификацией в рамках данной модели понимается распознавание негативного воздействия техническими и/или психологическими способами. Описание и анализ реальной или потенциальной опасности определены как совокупность процессов соотнесения обнаруженной угрозы с определенной группой на основе классификации, обозначения основных характеристик, источников воздействия, цели атаки, используемых методов, установления количества нападающих злоумышленников и их личностные особенности.

В работе также указаны критерии выбора подходящих методов защиты, основанных на анализе сущности и особенностей негативных воздействий, изучения существующих прецедентов и реальных кейсов. Автором обозначены основные стратегии поведения при угрозе негативного информационного воздействия в виртуальном пространстве, подробно описаны способы обеспечения личной безопасности.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

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

2. Федеральный закон от 30 декабря 2020 г. N 489-ФЗ «О молодежной политике в Российской Федерации»

3. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021)

4. ГОСТ Р 50922-96: «Защита информации. Основные термины и определения» (дата обращения 20.11.2020)

5. Акмасова А.А., Информационно-психологическая безопасность личности [Электронный ресурс] // URL: http://www.bla.by/public/conf_2/1_2003.pdf (дата обращения 05.03.2023)

6. 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: 05.03.2023).

7. Вихорев С.В., Классификация угроз информационной безопасности [Электронный ресурс] // URL: https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (дата обращения 07.10.2023)

8. Информационно-психологическая и когнитивная безопасность. Коллективная монография / Под ред. И.Ф.Кефели, Р.М.Юсупова. ИД «Петрополис», Санкт-Петербург, 2021. —300 с. 32 рис., 8 табл.

9. 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

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

11. Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2022. – 372 с.: ил. [Электронный ресурс] // URL: https://sccs.intelgr.com/editors/Makarenko/Makarenko- ib.pdf (дата обращения: 07.10.2023).

12. 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 07.10.2023)

13. 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

14. Эрик Кулман, Безопасная сеть. Правила сохранения репутации в эпоху социальных медиа и тотальной публичности, Альпина Паблишер, Москва, 2021 – 214 с.

15. Бритвин Н.И. Социальные сети как прообраз общественного устройства Власть. 2008. №1. Стр. 45-49 [электронный ресурс] // URL: https://cyberleninka.ru/article/n/sotsialnye-seti-kak-proobraz-obschestvennogo-ustroystva/viewer (дата обращения 10.11.2023)

16. 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 05.03.2023)

17. 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

18. Елишев С.О. Молодёжная проблематика и подходы к определению понятия «Молодёжь» в социологии – Вестник Московского университета, серия 18, Социология и политология. 2022. №3 с. 200-223

19. Фенина Виктория Владимировна Особенности речевого манипулирования в электронных спам-письмах // Язык и культура. 2017. №37. [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/osobennosti-rechevogo-manipulirovaniya-v-elektronnyh-spam-pismah (дата обращения: 07.10.2023).

20. Черных А. И. Социология массовых коммуникаций: учебное пособие. М.: Изд. дом ГУ-ВШЭ, 2008 [электронный ресурс] // URL: https://publications.hse.ru/mirror/pubs/share/folder/ox5oymyz2c/direct/549271 00.pdf (дата обращения 15.11.2023)

21. Bourdieu P. The forms of capital // Handbook of theory and research for the sociology of education / Ed. By J.G. Richardson. N.Y. : Greenwood, 1986

22. Muromtsev V.V., Muromtseva A.V. Human-Information Space in the Context of Contemporary Virtual Communications // Components of Scientific and Technological Progress, 2022. № 3(21). Стр. 38-46

23. Википедия [Электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Информационная_безопасность (дата обращения 23.11.2023)

24. «ВКонтакте» прокомментировала сообщения о краже данных 100 млн аккаунтов, Технологии и медиа, РБК, 2016 [Электронный ресурс] // URL: https://www.rbc.ru/technology_and_media/06/06/2016/575507249a7947351 eb7bc0f (дата обращения: 05.03.2023).

25. Социальные сети в России: цифры и тренды, осень 2020. Brand Analytics [Электронный ресурс] // URL: https://br-analytics.ru/blog/social-media-russia-2020/ (дата обращения 07.10.2023)

26. Соцсети и общедоступные данные пользователей [Электронный ресурс] // URL: https://vc.ru/legal/64191-socseti-i-obshchedostupnye-dannye-polzovateley (дата обращения: 07.10.2023).

27. «Касперский» заявил о краже данных сотен тысяч пользователей «ВКонтакте», Технологии и медиа, РБК, 2015, [Электронный ресурс] // URL: https://www.rbc.ru/technology_and_media/09/10/2015/5617a9d19a79477d5a3458f1 (дата обращения: 07.10.2023).

28. МВДМедиа [интернет ресурс] // URL: https://mvdmedia.ru/news/official/o—sostoyanii—prestupnosti—v—rossiyskoy—federatsii—v-1-m—kvartale-2020-goda/ (дата обращения 25.11.2023)

29. Личности интернет-троллей можно будет установить, BBC [Электронный ресурс] // URL: https://www.bbc.com/russian/uk/2012/06/120612_identify_trolls (дата обращения: 05.03.2023).

30. Угрозы информационной безопасности [Электронный ресурс] // URL: https://www.anti-malware.ru/threats/information-security-threats (дата обращения: 07.10.2023).

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

32. Фишинг [Электронный ресурс] // URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3_(phishing) (дата обращения: 07.10.2023).

33. Instagram-аккаунты пользователей можно было взломать с помощью картинки, Екатерина Быстрова, Anti-Malware, 2020, [Электронный ресурс] // URL: https://www.anti-malware.ru/news/2020-09-24-111332/33763 (дата обращения: 07.10.2023).

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

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

36. Хакер объявил о продаже базы со 100 млн аккаунтов «ВКонтакте» за 1 биткоин, VC.ru, 2016, [Электронный ресурс] // URL : https://vc.ru/social/16009-vk-hack-base (Дата обращения 07.10.2023)

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

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

39. Instagram фишинг использует 2FA в качестве приманки. [Электронный ресурс] // URL : https://bezmaly.wordpress.com/2019/08/24/instagram—phishing-2fa/ (дата обращения 07.10.2023)

40. Советы по созданию уникальных надёжных паролей. [Электронный ресурс] // URL : https://www.kaspersky.ru/resource—center/threats/how—to—create—a—strong—password (07.10.2023)

Приложение А

ЗАНЯТИЕ
для обучающихся СПО по теме
«КИБЕРБЕЗОПАСНОСТЬ»

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

Формирующиеся ценности: жизнь, права и свободы человека.

Продолжительность занятия: 30 минут.

Рекомендуемая форма занятия: эвристическая беседа. Занятие предполагает использование видеороликов, учебную игру и включает в себя анализ информации, групповую работу.

Комплект материалов:

сценарий;

методические рекомендации;

иллюстративные материалы и инструкции к игре;

видеоролики.

Структура занятия Часть 1. Мотивационная.

Анонс темы и просмотр мотивационного ролика.

Часть 2. Основная. ДВА ВАРИАНТА.

Вариант первый (для педагогов и обучающихся, обладающих повышенным уровнем компетенций в области ИТ).

Игра на тему кибербезопасности в группах. Разбор и обсуждение предлагаемых ситуаций и вывод правил безопасного и эффективного использования цифровых ресурсов. Обсуждение вопросов, связанных с правилами информационной безопасности.

Вариант второй.

Игра в группах на тему безопасного поведения в Интернете. Разбор и обсуждение предлагаемых ситуаций и вывод правил безопасного и эффективного использования цифровых ресурсов. Обсуждение вопросов, связанных с правилами поведения в интернете.

Часть 3. Заключение.

Подведение итогов занятия: фиксация правил, которые узнали обучающиеся, просмотр закрепляющего видеоролика от эксперта информационной безопасности.

Сценарий занятия. ВАРИАНТ №1. Часть 1. Мотивационная (до 5 минут).

Педагог.

Сегодня наше занятие посвящено кибербезопасности. Жизнь современного человека трудно представить без цифровых сервисов и приложений. Мы используем их для решения самых разных повседневных задач. При этом онлайн-среда связана не только с массой полезных возможностей, но и с рисками для безопасности пользователя. Именно поэтому так важно развивать собственную цифровую грамотность, знать о возможных рисках и владеть разными методами защиты, в том числе и технологическими. Также сфера кибербезопасности активно развивается, поэтому это ещё и перспективное направление для профессионального развития. О том, почему важно быть внимательными в цифровом мире, вам расскажет Наталья Ивановна Касперская — глава компании InfoWatch [Инфо-вОтч].

Демонстрация видео с Н. И. Касперской.

Педагог.

В продолжение занятия предлагаю вам погрузиться в настоящее состязание кибермошенников и специалистов по информационной безопасности. Мы проведем командную игру и научимся противостоять киберугрозам, разберём типичные сценарии атак и узнаем, как пользователи могут себя защищать.

Часть 2. Основная (до 20 минут).

Описание игры «Кибербезопасность».

Аудитория делится на две команды – «Кибермошенники» и

«Специалисты по информационной безопасности» (как вариант, можно предложить разделить аудиторию на несколько команд - специалистов по информационной безопасности; в этом варианте педагог сам озвучивает все карточки с киберугрозами).

Каждая команда получает набор карточек с возможными действиями (*см. дополнительные материалы*).

Механика игры:

Педагог выбирает одну из карточек-угроз (в любой последовательности) и озвучивает её.

Задача команды «Кибермошенники» — подобрать из набора карточек с действиями те, что злоумышленники типично используют в такой ситуации.

Задача команды «Специалисты по информационной безопасности» – оставить план защиты из своего набора карточек-действий и описать модель поведения пользователя.

На обсуждение отводится 3–5 минут.

«Кибермошенники» презентуют свой вариант плана «нападения», а «специалисты по информационной безопасности» – план защиты.

Педагог оценивает, отражена ли атака (при необходимости используя ключи к ситуациям, в которых представлены примерные планы атаки и защиты), если да, то присваивает балл команде «специалистов по ИБ».

Возможен вариант выбора команды экспертов из числа обучающихся, которые будут качественно оценивать планы действий команд и при необходимости дополнять их.

Тематики заданий из сферы кибербезопасности, которые встречаются в игре:

фишинговые ссылки;

социальная инженерия;

защита личной информации;

защита профиля.

Карточки-угрозы,карточки-действия для команды «Кибермошенники» и «Специалисты по информационной безопасности», ключи к ситуациям представлены в Приложении к сценарию и дополнительных материалах.

Пример проведения одного тура игры «Кибербезопасность». Педагог.

Итак, герой нашей истории молодой ученый Алексей, который давно ведёт свой профиль, у него много подписчиков, интересные и полезные научно-популярные публикации — потерять аккаунт для него будет обидно.

Первая угроза: кибермошенники пытаются совершить кражу профиля Алексея через взлом логина/пароля.

Педагог.

Команда «Кибермошенников» из своих карточек–действий составляет план атаки. Вам нужно отобрать те действия, которые злоумышленники типично используют в такой ситуации (можете добавить свои варианты действий).

Команда «Специалистов по информационной безопасности» составляет из своих карточек план защиты. Ваша задача – собрать эффективную при такой угрозе модель поведения для пользователя (можете добавить свои варианты действий).

Работа в группе 3–5 минут.

Педагог.

Время для обсуждения закончилось, давайте дадим слово каждой группе и узнаем, какие планы получились у команд. Слово команде «кибермошенников».

(Ответ представителей команды «кибермошенников».)

Педагог.

Теперь время ответить на атаку, вторая команда, вам слово.

(Ответ представителей команды «специалистов по информационной безопасности».)

Педагог.

С учетом планов команд я могу объявить победителей этого тура *(Педагог комментирует ответы команд, при необходимости используя ключ с примерными планами атак и защиты, и называет команду-победителя первого тура.).*

Следующие туры проходят по такой же схеме. Количество туров педагог определяет самостоятельно.

Методический комментарий.

Игра может проходить и в формате, когда все обучающиеся играют роль специалистов по информационной безопасности.

В таком варианте педагог озвучивает угрозу и выводит на экран примерный план атаки кибермошенников (из ключа к ситуациям, представленным в приложении).

Задача – всем вместе найти вариант отражения атаки и обезопасить профиль молодого ученого Алексея.

Педагог.

Теперь вы знаете чуть больше о том, как действуют мошенники онлайн и как можно предусмотреть риски. Это была отличная тренировка для вас.

Предлагаю вам из тех полезных правил для пользователя, что мы сегодня услышали и из тех, что вы можете назвать самостоятельно, составить

список – топ-5 полезных привычек кибербезопасности, которые каждый из нас может начать придерживаться с сегодняшнего дня.

Обучающиеся предлагаютполезные привычки кибербезопасности, педагог модерирует составление списка.

Педагог.

Спасибо вам за ваши идеи и комментарии, предлагаю подвести итоги занятия.

Часть 3. Заключение (до 5 минут).

Педагог.

Сегодня мы рассмотрели ситуации, когда пользователи не задумываются о последствиях своих действий и сами ставят себя под угрозу. Наша ответственность как пользователей цифровых сервисов — быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь мы можем соблюдать простые правила и внедрять в свою жизнь полезные привычки кибербезопасности. Чтобы узнать больше о том, как с технической стороны обеспечивается наша с вами информационная безопасность, послушаем рекомендации от эксперта компании VK [вэ-кА] и популярного российского певца Егора Крида.

Демонстрация видео с Р. Газизовым. Демонстрация видео с Е. Кридом.

Сценарий занятия. ВАРИАНТ №2. Часть 1. Мотивационная (до 5 минут).

Педагог. Сегодня мы с вами поговорим о том, с чем постоянно сталкивается современный человек — это использование Интернета для решения повседневных задач: для учебы, общения, творчества, профессиональной деятельности. Возможности, доступные нам благодаря подключению к сети, могут принести много пользы, но там же можно столкнуться и с разными угрозами. Важно использовать доступ в Интернет с умом, эффективно и безопасно. Как и в реальной жизни, в Интернете стоит придерживаться некоторых правил, именно их мы сегодня с вами обсудим. О том, почему важно быть внимательными в цифровом мире, вам расскажет Наталья Ивановна Касперская — глава компании InfoWatch [Инфо-вОтч].

Демонстрация видео с Н. И. Касперской.

Педагог.

В продолжение занятия предлагаю вам разобрать несколько ситуаций, которые иногда случаются в сети. Вы выступите в роли сторонних наблюдателей и предложите свои решения.

Часть 2. Основная (до 20 минут).

Методический комментарий. В основной части представлено два вида

заданий.

Интерактивное задание в форме анимационных фрагментов. Рекомендуется групповой вариант работы, но возможен и фронтальный.

Порядок работы с каждой ситуацией-кейсом строится по следующему алгоритму:

просмотр первой части видеофрагмента;

обсуждениеситуации в группе и формулировка правил-выводов безопасного поведения;

обсуждение правил-выводов безопасного поведения;

проверка правила-вывода на основе просмотра второй части ролика.

Работа с заданиями-карточками, описывающими конкретные ситуации, с которыми обучающиеся могут столкнуться в реальной жизни.

Предложена следующая тематика ситуаций-кейсов:

фишинговые ссылки;

социальная инженерия;

защита личной информации;

защита профиля.

Количество заданий педагог определяет самостоятельно.

Работа с интерактивным заданием.

Педагог.

Мы посмотрим небольшой ролик с ситуацией, которая знакома каждому из вас, ведь все мы общаемся с друзьями и заводим новые знакомства.

Смотрим первую часть ролика, думаем, что случилось и как можно было бы предотвратить эту ситуацию.

Видео-кейс № 1. Фишинговые ссылки.

Педагог.

Предлагаю вам разделиться на группы и попробовать сформулировать правила, при соблюдении которых можно было бы избежать подобной ситуации.

(Обучающиеся делятся на мини-группы по 4 человека и обсуждают возможные правила. На эту работу отводится 1–2 минуты.)

А теперь давайте обсудим получившиеся у вас правила. Что вы можете посоветовать делать в подобных ситуациях?

(От каждой группы один обучающийся предлагает одно правило. Педагог фиксирует на доске.)

Педагог.

Мы с вами обсудили, что пошло не так в ситуации Вани, теперь давайте досмотрим ролик и узнаем, какие цифровые привычки и правила нам предлагают создатели ролика, чтобы не попасться на удочку мошенников.

Продолжение демонстрации видео-кейса № 1. Фишинговые ссылки.

Методический комментарий.

Дополнительно в этом кейсе можно обсудить значение слова «фишинговая» ссылка. Действия мошенников называют «фишингом» из-за английского слова «фиш», что означает «рыба» или «рыбачить», то есть буквально мошенники стараются «выудить» информацию у пользователя.

Педагог.

Есть ещё одна ситуация, которую описывает в своем блоге герой мультфильма. Давайте посмотрим его, следите за сюжетом и поведением персонажей.

Видео-кейс № 2. Социальная инженерия.

Педагог.

Как вы считаете, какую ошибку допустил герой мультфильма? Каких правил надо придерживаться, чтобы не попадать в ловушки, в которые попала Кира? Давайте, как и в предыдущем случае, сначала обсудим это в группах, а потом все вместе.

(Работа в группах, обсуждение и последующие ответы обучающихся.)

Педагог.

Вы отлично справились, давайте досмотрим видео и узнаем, какие правила поведения в интернете мы с вами должны запомнить.

Продолжение демонстрации видео-кейса № 2. Социальная инженерия.

Методический комментарий.

Социальная инженерия — разные виды манипуляций и обмана, цель которых заставить человека раскрыть личные данные, получить доступ к его личной и финансовой информации.

Педагог.

Я предлагаю вам посмотреть другую ситуацию, которая произошла с любительницей классического искусства Ариной. Как и в прошлый раз, будьте внимательны и отмечайте поведение персонажей, чтобы ответить на мой вопрос. Смотрим.

Видео-кейс № 3. Защита личной информации.

Педагог.

Как думаете, что произойдет дальше? Что в этой ситуации в поведении Арины вы считаете опасным? Есть ли здесь ошибка? На что мы должны обращать внимание, чтобы не попасть в такие же ситуации, как Арина? Поработайте, пожалуйста, в тех же группах, а потом мы обменяемся с вами мыслями.

(Работа в группах, обсуждение, ответы обучающихся.)

Педагог.

Вы молодцы, сейчас мы посмотрим развязку, узнаем не только, что случилось с Ариной, но и то, как обезопасить свою личную информацию и какие правила в этом помогут.

Продолжение демонстрации видео-кейса № 3. Защита личной информации.

Педагог.

Сейчас мы посмотрим ещё один ролик, где рассказывается история Жанны. Предлагаю узнать, что с ней приключилось и как друзья смогли прийти на помощь. Следите за сюжетом, у меня будет вопрос для вас.

Видео-кейс № 4. Защита профиля.

Педагог.

Как вы считаете, почему в аккаунте появилась такая информация? Как друзья Жанны поступят дальше? Что важно помнить и соблюдать, чтобы сохранить свой профиль в безопасности? Попробуйте составить правила, которые помогут вам обезопасить ваш профиль в социальной сети.

(Работа в группах, обсуждение, ответы обучающихся.)

Педагог.

Вы хорошо справились с заданием. Теперь время узнать, как правильно защищать свой профиль, какие правила для этого нужно знать.

Продолжение демонстрации видео-кейса № 4. Защита профиля.

Педагог.

Давайте ещё раз назовем правила, которые мы узнали на нашем занятии сегодня? Почему важно их соблюдать, как вы думаете?

(Ответы обучающихся, обсуждение.)

Работа с заданиями-карточками Педагог.

Предлагаю вам посмотреть на знакомые действия и ситуации со стороны. Сыграем в игру и проверим, как хорошо вы умеете пользоваться цифровыми сервисами и приложениями.

Методический комментарий.

Педагог делит обучающихся на команды (*3–4 команды*). Каждая команда получает карточку с описанием ситуации, дополнительно карточка выводится на экран (*при наличии технических условий*). Также возможен и фронтальный формат работы.

Командам необходимо ответить на два вопроса:

Какую ошибку герой или герои ситуации допустили?

Какие правила для пользователя можно вывести из этой ситуации?

На обсуждение каждой ситуации дается 3 минуты. Дальше каждая группа представляет результаты обсуждения.

Педагог сверяет полученные результаты с ключом к заданию.

Карточка-задание №1

Ваша однокурсница Катя ведет видеоблог про образ жизни, увлечения, учебу. Она делится всем тем, чем живет современный обучающийся. Катя

выкладывает на свой канал рассказы о своей жизни, увлечениях, занятиях. В очередном выпуске своего блога Катя решает попробовать один из популярных форматов — прямой эфир с обзором комнаты.

В начале эфира Катя сообщает, что сегодняшнюю встречу она ведет из дома, называя свой адрес.

В одном из кадров она показывает, что есть у неё в комнате, как она всё украсила к Новому году, где делает уроки, какие у неё хобби, заходит в комнату к брату, который с друзьями разучивает на гитаре новую песню.

Во время эфира в кадр попадает фамильная реликвия — шкатулка с уникальными украшениями.

Педагог.

Подумайте, в чем могли быть ошибки Кати? Что она сделала не так, и о чем нужно помнить, когда что-то выкладываешь в сеть?

Работа обучающихся в группах.

Педагог.

Время для обсуждения закончилось, давайте обсудим, какие ошибки совершила Катя и что можно ей посоветовать?

Ответы обучающихся (по одному пункту поочерёдно от каждой группы), комментарии и дополнения педагога в соответствии с ключом к заданию.

Ключ к заданию.

не оставляйте информацию о себе и родственниках в открытом доступе: домашний адрес, телефоны, номер образовательного учреждения, свой возраст, геолокации;

в прямом эфире, где у вас нет заранее подготовленного текста и сценария вы говорите все, что придет в голову и ненамеренно можете сообщить информацию потенциально опасную;

не размещайте фото или видео, на которых видно обстановку вашей квартиры, все то, что может притягивать мошенников;

не выкладывайте фото или видео с участием ваших родственников, друзей без их разрешения;

используйте настройку «для близких друзей», чтобы контролировать

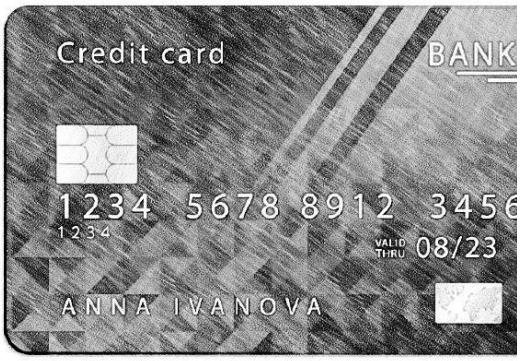
доступ к своему профилю и информации о себе.

Педагог.

Отлично, спасибо за ваши ответы! На данном примере стало понятно, что даже в таких знакомых ситуациях могут быть подводные камни.

Дополнительно к этому заданию обучающимся можно предложить набор фотографий и обсудить, стоит ли размещать их в социальных сетях, и объяснить почему.

Примеры фотографий (полный набор и ключ к заданию представлены в дополнительных материалах).



Карточка-задание №2.1 *(команды получают разные варианты карточек).*

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

persik1234

ANNa11

A!-2na1234

Аня останавливается на первом варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру

телефона.

Карточка-задание №2.2

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

Jack4321

ANNa11

A!-7n9aj234

Аня останавливается на втором варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Карточка-задание №2.3

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была захвачена злоумышленниками. Она решает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. 123456789

ANNA_JACK

A!-2na1234

Аня останавливается на первом варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Карточка-задание №2.4

Аня, ученица 6 класса, недавно ей исполнилось 11 лет. У Ани есть любимый пес Джек и кот Персик.

Аня регистрирует новую страничку в социальной сети, т. к. старая была

захвачена злоумышленниками. Она выбирает, какой пароль поставить для своего нового аккаунта в этой социальной сети. Вот варианты, из которых она выбирает:

1. 123456789

ANNAPERSIK

A!-7n9aj234

Аня останавливается на втором варианте пароля и отказывается от опции установить дополнительное подтверждение входа по почте или номеру телефона.

Педагог.

Обсудите, какие из вариантов паролей надежные, какие нет, и почему? Надёжный ли пароль выбрала Аня? Сформулируйте правила, о которых нужно помнить при создании паролей.

Работа обучающихся в группах.

Педагог.

Время для обсуждения закончилось, давайте обсудим надежность паролей, представленных на карточках, и выбор Ани.

Ответы обучающихся, комментарии и дополнения педагога в соответствии с ключом к заданию.

Ключ к заданию.

на всех карточках последний пароль подходит под критерии надежного пароля: содержит специальные знаки, заглавные буквы, цифры, при этом комбинация не связана с пользователем;

не следует использовать общеизвестные факты для создания паролей (ваши имя, возраст, дату рождения, клички животных, имена близких родственников и т. п.);

легко взломать пароли, состоящие только из цифр или букв;

не следует использовать элементарные пароли типа 123456…, абвгд…;

подключайте дополнительное подтверждение входа — двухфакторную аутентификацию.

Педагог. Проверить надежность пароля можно на сайте 2ip.ru/passcheck.

Предлагаю проверить, за какой период можно взломать пароли, которые были представлены у вас на карточках.

Обучающиеся проверяют надежность паролей persik1234 – ненадежный, возможно взломать за 254 часа ANNa11 – ненадежный, возможно взломать за 14 секунд Jack4321 – ненадежный, возможно взломать за 910 минут 123456789 – ненадежный, возможно взломать за 0 секунд

ANNA_JACK – ненадежный, возможно взломать за 1889 часов ANNAPERSIK – ненадежный, возможно взломать за 588 минут A!-2na1234 – надежный, может быть взломан за 6810 лет

A!-7n9aj234 – надежный, может быть взломан за 544770 лет

Дополнительно к этому заданию педагог может предложить обучающимся проверить на надежность свои пароли от социальных сетей.

Часть 3. Заключение (до 5 минут).

Педагог. Сегодня мы рассмотрели ситуации, когда пользователи не задумываются о последствиях своих действий и сами ставят себя под угрозу. Наша ответственность как пользователей цифровых сервисов — быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь мы можем соблюдать простые правила и внедрять в свою жизнь полезные привычки кибербезопасности. Чтобы узнать больше о том, как с технической стороны обеспечивается наша с вами информационная безопасность, послушаем рекомендации от эксперта компании VK [вэ-кА] и популярного российского певца Егора Крида.

Демонстрация видео с Р. Газизовым. Демонстрация видео с Е. Кридом.

Карточки-угрозы
кража профиля пользователя через взлом логина/пароля
манипуляция, чтобы пользователь самостоятельно передал свои данные
получение доступа к сохраненным личным данным/данным банковской карты
продуманное мошенничество на основе доступной информации о

человеке
мошенничество через подменные/анонимные профили
мошенничество на основе утечки данных пользователя на сторонних ресурсах

Набор карточек для группы «Специалисты по информационной безопасности»

Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.

Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.

Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.

Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?

Не переходите по ссылкам от малознакомых людей.

Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.

Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.

Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.

Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.

Не поддавайтесь агрессии и не ведитесь на провокации.

Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.

Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.

Защищайте всю информацию, даже если думаете, что она не важна.

Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.

Набор карточек для группы «Кибермошенники»

Проследить за открытой информацией в профиле, изучить подробности жизни человека.

Спровоцировать на эмоции, вызвать интерес у пользователя, использовать приём ограниченного времени.

Начать торопить пользователя, чтобы не дать разобраться в происходящем.

Разослать спам-сообщение друзьям пользователя.

Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.

Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.

Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.

Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.

Представиться сотрудником технической поддержки и выманить

конфиденциальные данные или склонить к выполнению сомнительных действий.

Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие — например, в кино.

Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.

Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Ключи к ситуациям угрозы (примерные планы атаки и защиты) Угроза: кража профиля пользователя через взлом логина/пароля.

Пример атаки:

Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.

Начать торопить пользователя, чтобы не дать разобраться в происходящем.

Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.

Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.

Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.

Используйте разные пароли на различных сервисах. Выбирайте сложные

пароли, не используйте ваши имя и дату рождения при создании пароля.

Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.

Угроза: манипуляция, чтобы пользователь самостоятельно передал свои данные.

Пример атаки:

Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.

Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.

Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.

Пример защиты:

Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.

Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.

Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

Угроза: получение доступа к сохраненным личным данным/данным банковской карты.

Пример атаки:

Предложить продолжить знакомство офлайн и отправить ссылку для

покупки билетов на мероприятие — например, в кино.

Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.

Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?

Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.

Не переходите по ссылкам от малознакомых людей.

Защищайте всю информацию, даже если думаете, что она не важна.

Угроза: продуманное мошенничество на основе доступной информации о человеке.

Пример атаки:

Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.

Проследить за открытой информацией в профиле, изучить подробности жизни человека.

Разослать спам-сообщение друзьям пользователя.

Пример защиты:

Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.

Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и

других документов, билетов, посадочных талонов и др.

Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.

Не поддавайтесь агрессии и не ведитесь на провокации.

Угроза: мошенничество через подменные/анонимные профили.

Пример атаки:

Проследить за открытой информацией в профиле, изучить подробности жизни человека. Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.

Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.

Начать торопить пользователя, чтобы не дать разобраться в происходящем.

Пример защиты:

Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.

Не поддавайтесь агрессии и не ведитесь на провокации.

Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.

Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.

Воспользуйтесь функцией «Пожаловаться» на комментарий, человека,

пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.

Угроза: мошенничество на основе утечки данных пользователя на сторонних ресурсах.

Пример атаки:

Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Разослать спам-сообщение по друзьям пользователя.

Пример защиты:

Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

Не переходите по ссылкам от малознакомых людей.

Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.

Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.

Приложение Б

Викторина "Информационная безопасность"

Автор: Л.Ю. Черновалова

Онлайн викторина по теме "Информационная безопасность" проводилась на сервисе MyQuiz в рамках проведения конкурса профессионального мастерства по профессии "Мастер по обработке цифровой информации" для студентов 3 курса «Турнир мастеров». Состоит из 10 вопросов с одиночным выбором. Викторина состоит из 10 вопросов с одиночным выбором. Правильный ответ оценивается в 2 балла. Максимальное количество баллов - 20 баллов.

Ссылка на он-лайн викторину: https://myquiz.ru/q/d9029c19-993f-4160-99ca-bc146a55e75b

1. Вам пришло письмо: «Новые снимки на сервере Яндекс.Фотки.Открой и увидишь! www.fotoyandex11234.ru ». Как вы поступите?

a) Обязательно посмотрю фотографии

b) Поделюсь ссылкой с друзьями

c) Удалю письмо

2. Что из нижеперечисленного не относится к антивирусным программам?

a) Dr. Web

b) AVP

c) Norton Disk Doktor

d) Kaspersky Free

3. Вы поехали в командировку в другой город и зашли в кафе чтобы отправить письма своим коллегам относительно текущих проектов. Для обеспечения безопасности при использовании этих общедоступных сетей нужно всегда:

a) Найти поблизости самый сильный сигнал WiFi

b) Отключить сервис обмена файлами

c) Использовать виртуальную частную сеть Virtual Private Network (VPN)

4. Какие типы атак приводят к нарушению нормальной работы web-сайта или другого сетевого ресурса?

a) Атака DoS

b) Атака POS

c) Фишинг

5. При установке приложения по обработке фотографий на смартфон просят доступ к СМС-сообщениям и вашей телефонной книге. Согласитесь ли вы?

a) Да, поскольку это безопасно

b) Нет, это небезопасно

6. Что из перечисленного является примером фишинга?

a) К вам пришло письмо по электронной почте от человека, с которым вы редко контактируете, и оно содержит только ссылку на адрес в web.

b) К вам пришло письмо по электронной почте из вашего банка с просьбой ввести номер вашего счета в этом банке и пароль, но адрес отправителя не похож на адрес вашего банка.

c) Вы получили сообщение о том, что вы выиграли в конкурсе, и для получения приза нужно щелкнуть по ссылке.

d) Все ответы верны

7. ВКонтакте просит ввести ваш мобильный номер для подтверждения аккаунта. Как вы поступите?

a) Откажусь. Вдруг мне будут присылать смс-спам

b) Откажусь:мне удобнее вводить логин, чем номер телефона.

c) Введу свой номер, чтобы в случае кражи аккаунта его можно было восстановить с помощью мобильного номера.

8.Хакер заблокировал пользователей и зашифровал хранящиеся на их персональных компьютерах файлы и данные, и предлагает восстановить доступ к ним если ему заплатят выкуп. Как называет такой тип кибератаки?

a) Browser hijacker

b) Ransomware (программа-вымогатель)

c) Brute-force

9. Какой из предложенных паролей лучше выбрать?

a) NH5te1A*

b) Ivan2003

c) Дата рождения родственника

10. Как называется провоцирование человека на агрессию с помощью нападок и неуважительных высказываний?

a) Мерчендайзинг

b) Троллинг

c) Джампинг