Департамент профессионального образования Томской области

Областное государственное бюджетное профессиональное образовательное учреждение

«Томский индустриальный техникум»

X РЕГИОНАЛЬНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ СТУДЕНЧЕСКАЯ КОНФЕРЕНЦИЯ «БЕЗОПАСНОСТЬ ЧЕЛОВЕКА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ»

СБОРНИК МАТЕРИАЛОВ

24 ноября 2022 г.

г. Томск, 2022

В данном издании представлены работы участников десятой региональной научно-практической конференции «Безопасность человека в информационном пространстве», состоявшейся 24 ноября 2022 г. на базе Томского индустриального техникума.

Материалы сборника сгруппированы по тематике секций конференции:

- ✓ Информационно-психологическая безопасность личности;
- ✓ Современные средства защиты Internet of Things («IoT») объектов;
- ✓ Защита прав и интересов граждан в информационно-телекоммуникационных сетях;
- ✓ Информационная безопасность профессиональной деятельности в плакатах.

Сборник предназначен для студентов и преподавателей системы среднего профессионального образования, интересующихся проблемой формирования информационной культуры и безопасности пользователя в информационном пространстве.

Ответственность за содержательную часть статьи, грамматические и стилистические ошибки возлагается на авторов

СОДЕРЖАНИЕ

СЕКЦИЯ 1. «ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ»..... 4

СЕКЦИЯ 2. СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ IOT ОБЪЕКТОВ 36

СЕКЦИЯ 3. ЗАЩИТА ПРАВ И ИНТЕРЕСОВ ГРАЖДАН В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ 89

СЕКЦИЯ 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ПЛАКАТАХ..... 121

СЕКЦИЯ 1. «ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ»

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО РФ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Шилоносов Денис Николаевич,
Трифонов Иван Алексеевич
Областное государственное бюджетное профессиональное образовательное учреждение «Промышленно-коммерческий техникум»
Руководитель: Тырышкина Елена Анатольевна

Информация является важнейшим фактором во всех сферах жизни общества в России. Развитие информационного общества создает новые возможности для экономического роста, но и новые угрозы информационной безопасности.

Международное сотрудничество РФ в области обеспечения информационной безопасности – неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Россию.

Особенностью международного сотрудничества РФ в области обеспечения информационной безопасности является то, что оно осуществляется в условиях:

-обострения международной конкуренции за обладание информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики;

-противодействия укреплению роли России как одного из влиятельных центров формирующегося многополярного мира;

-усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания «информационного оружия».

Все это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной ин формационной инфраструктуры.

Основными направлениями международного сотрудничества РФ в области обеспечения информационной безопасности являются:

-запрещение разработки, распространения и применения «информационного оружия»;

-обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

-координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

-предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также с торговлей людьми.

Для осуществления международного сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

В настоящее время наблюдается колоссальный рост эффективности средств информационного воздействия на психику людей и общественное сознание. Современные и перспективные информационные технологии и средства позволяют практически неограниченно контролировать и управлять информационном воздействием на общественное сознание.

На сегодняшний день СМИ – действенный канал информирования общества о деятельности власти. С другой стороны, это индикатор, отражающий основные проблемные вопросы социума в целом и отдельных его страт. Массовость, периодичность, выполнение оперативность – все это делает СМИ важнейшим социальным институтом и объектом государственной информационной политики. Современные СМИ не только отражают мировые события, но занимаются и анализом информации, ее предварительной фильтрацией и целенаправленным отбором. Благодаря этому СМИ являются эффективным средством воздействия на сознание людей.

Существуют огромные возможности информационного воздействия на личность с помощью современных средств массовой информации. По существу, сегодня СМИ практически единственная структура, через которую население ежедневно, ежечасно получает информацию о процессах в стране, регионе, мире, через которую буквально навязывают различные идеологические воззрения. Поэтому нельзя не согласиться с тем, что сегодня СМИ в России могут выступить и в качестве силы, стабилизирующей обстановку в обществе, и в качестве детонатора социального взрыва.

В связи с коммерциализацией СМИ, что характерно и естественно для рыночной экономики, со стороны телевидения на личность и общество обрушились поток рекламы, фильмы и передачи, пропагандирующие насилие, садизм, порнографию. Все это можно классифицировать как несанкционированный к ней доступ к сознанию людей.

Телерадиовещание сегодня может не только воздействовать на человека посредством донесения недостоверной информации, но и влиять на психо-физиологическое здоровье личности.

Неподготовленному человеку очень сложно распознать негативное информационное воздействие, если оно применяется, поэтому очень актуальными становятся вопросы связанные с техниками противостояния негативному информационному влиянию и вопросам образования в области информационной безопасности.

Профессор психологии В. Левицкий в статье «Информационно-психологическая безопасность личности» предлагает четыре способа защиты от негативного информационного влияния:

Способ защиты 1-й: «Уход» - увеличение дистанции, прерывание контакта, выход за пределы досягаемости информационного воздействия. Действия в различных информационных ситуациях могут быть такими: отключение определенных каналов СМИ (раздражающего канала телевидения, выход из Интернета и пр.), отказ от просмотра (прослушивания) конкретных теле-радиопрограмм; отказ от чтения некоторых газет, статей, рубрик и пр.; уход, под различными предлогами, с массовых зрелищных мероприятий: театра, концертного зала, кинотеатра и пр., митингов, собраний и др.; смена неприятной темы беседы, стремление не обострять межличностные отношения во время беседы (обход «скользких тем», «острых углов» и пр).

Способ защиты 2-й: «Блокировка» - контроль информационного воздействия, выставление психологических барьеров, ограждение психики от внешнего негативного информационного воздействия. Действия, выполняемые при «блокировке»: критическое восприятие информации; эмоциональное отчуждение (восприятие негативной информации «без эмоций»); увеличение межличностного пространства – «зоны общения» во время беседы; использование «психологических барьеров» (несерьезное восприятие информации).

Способ защиты 3-й: «Управление» - контроль процесса информационного воздействия, влияние на его характеристики и источник. Выполняемые действия: использование обратной связи; выражение в

зрелищных мероприятиях своего отношения к происходящему (неодобрения, недовольства выступающими); использование при беседе принципа «своих не обижают», для чего продемонстрировать желание стать другом, членом одной общности; ослабить или дестабилизировать активность собеседника неожиданным отвлечением (например, сделать комплимент, высказать сочувствие) и др. Способ защиты 4-й: «Затаивание» – контроль своей реакции на внешнее информационное воздействие. Выполняемые действия: отсрочка своих реакций, поспешных выводов и оценок, задержка или отказ от действий и поступков, вызываемых информационным воздействием; маскировка, сокрытие чувств, проявлений эмоций и др.

С появлением Интернета мир превратился как бы в одну большую деревню, в которой люди разных континентов могут обмениваться информацией за считанные секунды. Но свобода информации, как и свобода слова, дает положительный эффект, если ее содержание не только полезно для жизни, но и благостно для человеческой души. К сожалению, как на ТВ, так и в Интернете содержится наряду с добром много мусора и даже зла. Наряду с вещественными атрибутами прогресса незримые информационные сети, как паутина, наброшены на человеческое сознание по всей планете.

Источников угроз информационно-психологической безопасности существует великое множество, и проявляться они могут через СМИ, разные направления массовой культуры, воспитание, личное общение, образовательные системы и культовые образования, а наиболее подвержены такому воздействию подростки и молодежь.

Выделяют несколько видов так называемой «вредоносной» информации, могущей нанести серьёзный вред психике человека. К ней можно отнести:

- информацию, возбуждающую социальную, расовую, национальную или религиозную ненависть и вражду;

- призывы к войне;

- пропаганду ненависти, вражды и превосходства;

- распространение порнографии;

- посягательство на честь, доброе имя и деловую репутацию людей;

- рекламу (недобросовестную, недостоверную, неэтичную, заведомо ложную);

- информацию, оказывающую неосознаваемое деструктивное воздействие на психику людей.

Какие же неблагоприятные информационные факторы привели к тому, что возникли угрозы для личности? Основной из них является так называемый "информационный взрыв" или лавинообразное увеличение всех видов традиционной, печатной информации (научной, научно-технической, экономической, научно-популярной, юридической, коммерческой, эстетической и так далее). Еще большими темпами развиваются электронные информационные ресурсы, масштабы которых трудно поддаются измерению. Количественный рост информации привел к тому, что личность не может воспринять, осмыслить, систематизировать даже те источники информации, которые необходимы ей в профессиональной деятельности.

Другим неблагоприятным информационным фактором, который влияет на психику человека и даже на его душевно-нравственные устои, является значительное "загрязнение" информационной среды, получившей название информационной экологии.

Зарубежные авторы, изучающие качественную сторону потоков информации, связанную с изучением информационной экологии, считают, что информации не может быть много, и информационный стресс вызывает не обилие информации, а большое количество низкокачественной информации и неумение личности критически отсеивать, отбирать и перерабатывать информацию в интеллектуальный продукт (знания). Представитель данной концепции Б. Мильтон пришел к выводу, что информация - это лишь сырье, которое дает возможность вырабатывать знания, и что решения принимаются не на основе информации, а на основе знаний, мудрости, интуиции, понимания.

Угрозы личности, связанные с использованием информации, исходят как от самой личности (внутренние угрозы), основными из которых является низкая культура умственного труда или информационной культуры (неспособность к самостоятельному отбору информации и ее критической оценке), недооценка личностью возможностей обучения методам защиты (нейтрализации) угроз от воздействия на нее недоброкачественной информацией. Гораздо большее количество угроз личности представляет информационная сфера (внешней угрозы), а именно:

* отсутствие необходимой личности информации, неполная информация, нарушение прав и свобод человека в области доступа к информации, неправомерное ограничение доступа к открытым информационным ресурсам;

* информация, возбуждающая социальную, расовую, национальную или религиозную ненависть или вражду, пропагандирующая культ насилия и жестокости, порнографическая информация;

* искаженная, недостоверная, ложная информация, дезинформация;

* хаотичность и противоречивость информации и др.

Таким образом сейчас существует огромное множество информационной угрозы личности, которые реализуются при помощи определённых средств и способов.

В рамках нашего техникума, мы провели соц.опрос среди учащихся в возрасте от 15 до 19 лет, на тему «Информационная безопасность». В участие приняло 340 учащихся (муж. и жен. пола). В анкете содержались такие вопросы, как: чувствуете ли вы в наше время информационное давление? Были ли у вас лично конфликты в соц.сетях (негативное высказывание в ваш адрес по любым темам)? Как вы считаете, на сегодняшний день наша информационная система безопасна?

В ходе опроса было выявлено, что 68% учащихся чувствуют информационное давление на себе в соц.сетях. У 70% учащихся были личные

конфликты в соц.сетях. А 51% учащихся считают, что на сегодняшний день наша информационная система не безопасна.

Таким образом мы видим, что в наше время очень большое влияние оказывает информационное пространство на наше молодое поколение. Мы видим, что они чувствуют не защищенность и давление, что нуждаются в защите, находясь в информационном пространстве.

Безопасность является важнейшим критерием оценки стабильности систем социальных, политических, экономических, информационных, психологических отношений современного общества.

На уровне государственной политики Россия принимает меры, направленные на мирное развитие информационной сферы и обеспечение информационной безопасности от внутренних и внешних угроз. Но на уровне гражданина также важно уметь распознавать ложь от правды и не стать объектом враждебной информационной манипуляции.

Список используемой литературы:

1. Брусницин Н.А. Информационная безопасность. М.: Вита-Пресс, 2001

2. Екимовская, М. А. Информационно-психологическая безопасность, как глобальная проблема человечества.

3. Петров С. В. Учебное пособие: «Информационная безопасность человека и общества»

4. Электронное периодическое издание «Вестник Дальневосточного государственного технического университета» 2011

5. Ссылка https://studfile.net/preview/9141627/page:3/ Безопасность личности, общества и государства в условиях информационно-психологической войны.

«СЕТЕВОЙ ЭТИКЕТ» КАК ОДИН ИЗ ИСТОЧНИКОВ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ»

Чернов Александр Александрович
Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум водного транспорта и судоходства»
Руководитель: Киселева Елена Викторовна

Актуальность исследования:

В настоящее время интернет-коммуникация плотно вошла в нашу жизнь и исследуется учёными с разных сторон: изучается специфика языковых средств электронной коммуникации, изучается взаимосвязь и взаимовлияние языка и общества, языка и культуры.

Очень часто общение в сети выходит за рамки привычного оффлайн- общения. Появляется грубость, неприятие другой точки зрения, а также непонимание собеседника. А между тем этикет — основа безопасного речевого взаимодействия в сети.

В связи с тем, что интернет-пространство — это возможность общаться на расстоянии, особую важность приобретает умение правильно выстроить общение, учитывая этический аспект электронной коммуникации. Ведь это, в том числе, обеспечивает информационно-психологическую безопасность личности.

Гипотеза

Общение в интернете — нарушение традиционного этикета, а грубость отчасти вызвана непониманием пользователями сложившихся интернет-дефиниций.

Методы исследования

В ходе работы мы применили следующие методы исследования:

• Изучение разнообразных источников информации.

• Анализ полученных сведений.

• Опрос в виде анкетирования.

Творческий подход автора

Предположив, что интернет-общения выходит за рамки привычного этикета, основывается на непонимании особенностей интернет-

коммуникаций, мы изучили на различных интернет-форумах и в мессенджерах лексику общения пользователей.

Составив некий глоссарий наиболее употребимых слов и сокращений, предложили ответить студентам на вопросы анкеты. Опрос выявил, что более 35 % пользователей недостаточно чётко понимают суть сообщения.

Мы задались целью выяснить, какие факторы влияют на этикет в сети.

В каждом языке мира существует система сформированных формул, служащих для установления контакта между собеседниками и поддержания общения в конструктивной тональности. Эта система называется речевым этикетом, она помогает правильно построить коммуникацию с учётом социальных, возрастных и психологических факторов, а также сферы общения. Традиционные формулы речевого этикета известны каждому: это формулы приветствия, прощания, благодарности, знакомства, просьбы и так далее. Однако новое коммуникативное пространство интернета требует иных форм вежливости.

В сети общение можно назвать «электронным диалогом». Исследуемый речевой жанр родился путём трансформации и взаимопроникновения речевых жанров «разговор» и «письмо». Он представляет собой обычное, повседневное общение, только в письменной форме, отсюда такие особенности, как индивидуальность, моноадресность (один получатель сообщения), нехудожественность (разговорная речь, часто стилистически сниженная, используются единицы нелитературных разновидностей языка), неклишированность и производность (так называемый гипержанр, включающий другие речевые жанры, например, просьбу, приглашение, ответ, спор и прочее).

Отбор языковых средств обусловлен целью и темой общения, особенностями коммуникантов, дистантным характером разговора.

Среди факторов, влияющих на формирование интернет-этикета, или как его именуют пользователи, «сетикета» («нетикета»), можно выделить следующие. Во-первых, дистантный характер общения. Опосредованность

компьютером накладывает отпечаток на всю речеповеденческую деятельность индивида. В интернет-коммуникации происходит снятие целого ряда социокультурных и психологических ограничений, обычно налагаемых на речевое поведение в реальной коммуникации в целях создания гармоничного, неконфликтного общения [1, с. 443; 4, с. 99; 5, с. 4]. Во-вторых, возраст коммуникантов. Активными интернет-пользователями чаще всего являются молодые люди, и именно они устанавливают правила. В-третьих, установка на языковую игру. Все эти факторы определяют возникновение специфических норм речевого поведения в интернет- коммуникации, которые часто трактуют как нарушение традиционного этикета.

Мы проанализировали тексты разговоров в мессенджере с целью выявления формул речевого этикета, используемых виртуальными собеседниками. Было выявлено, что вне зависимости от отношений между коммуникантами, их степени близости, темы и содержания разговора формулы приветствия и прощания присутствуют практически во всех случаях. Это связано с желанием коммуникантов успешно начать и завершить контакт. Наряду с традиционными конструкциями приветствия типа «привет» и «здравствуй» («здравствуйте») широко распространены и специфические, представляющие собой усечённые или графически изменённые стандартные формулы вежливости: прив; прива; дарова; здарофф; приветик. Широко используется для вхождения в разговор междометие «ку-ку», которое в данном случае имеет значение «ты здесь?», «готов ли ты к общению?». Подробнее отметим такую необычную форму приветствия как «ку», не имеющую аналогов в реальной коммуникации и активно использующуюся в переписке онлайн-геймеров. Н. А. Карабань приводит следующие версии происхождения данной единицы: «1. Слово из вымышленного чатлано-пацакского языка, взято из фильма «Кин-дза-дза», так чаще приветствуют, а вообще и разговаривают на планете Альфа. 2. Две первые буквы на русской раскладке клавиатуры от анг. “respect”» [2, с. 168]. Чаще всего встречается в мессенджере онлайн-игр, таких как «LineAge II», «World of Warcraft» и тому

подобных. Однако приобрело широкое распространение за пределами игрового мира. Следует отметить активное речетворчество, использование языковой игры уже в самом начале общения. Нами зафиксировано приветствие «Дутро», образованное путём слияния слов «доброе» и «утро». В ответ на такое приветствие адресат, поддерживая заданный шутливый тон, пишет: — Дутро. — Дутро-дутро) [здесь и далее орфография и пунктуация источника сохранены]. Такое речевое поведение адресанта изначально задаёт своеобразный характер общения, провоцирует собеседника на использование приёмов языковой игры, устанавливает особую тональность общения. Кроме того, пишущие экспериментируют со сменой регистра, желая разнообразить арсенал языковых средств: шАЛом); пИриУэД!). Частотно использование формул приветствия из английского, немецкого и французского языков, что связано, во-первых, с тематическими особенностями общения, а во-вторых, с распространением европейского (в частности, англо-американского) образа жизни и культурных ценностей: — Хай. Как дела?; — guten Abend, ma chèr ami — Привет-привет

Графическое изменение претерпели и этикетные формулы благодарности. Желание сэкономить время написания сообщения приводит к оригинальным решениям — возникновению акронимов и слоговых сокращений, смешению букв и цифр: — спс! — нз4 (ср.: спс — спасибо, нз4 — не за что); — спокойночи; — СН — спс; — споки (ср.: СН, споки — спокойной ночи); — спс — пжл; — Ссылочку кинь) // Плиз (ср.: пжл, плиз — пожалуйста). Последний пример иллюстрирует не только стремление к быстроте набора, но и особую прагматику включения английских слов в русскую речь. Так, английское «please» придаёт высказыванию умоляюще-ироничный оттенок. Этикетные речевые формулы носят конкретно-исторический характер, то есть изменяются с течением времени в соответствии с коммуникативными потребностями общества. Ещё несколько лет назад привычные сегодняшнему интернет- пользователю конструкции воспринимались как отклонение от нормы, как невежливость. Так, в

сообщении от 3 ноября 2008 г. читается возмущение автора пренебрежением в написании этикетных слов: — Ё-моё! Куда мир катится?!?!?!? Сейчас гласные употреблять немодно что ли? Пжл, спс, пздрвл. Я еле написала такое...а уж про прочитать это, вообще молчу! =). А в настоящее время все эти редуцированные формы стали привычными и воспринимаются как должное. Напротив, если вы напишете вместо короткого пжл полную форму пожалуйста, то это может быть расценено в рамках разговора в мессенджере как анахронизм и даже привести к коммуникативной неудаче, ведь, как показывает проведённый интернет- опрос, «почти две трети пользователей социальных сайтов испытывают проблемы и непонимание в том, что касается неписаного сетевого этикета» [3].

Стандартными формулами выхода из общения являются следующие языковые единицы: — Понятно. // привет передавай // До связи. — Ок) =) // Пока-пока. Я побежала)); — А щас в магазин) // Суббота!!!! — Давай давай. // Ага. — Наконец-то) // Ну пока. // ; — Сладких снов); — приятных снов; — приятно было поговорить с тобой; — ухожу в реальность! и прочие. Однако участники интернет-разговоров нередко выходят из Сети не попрощавшись. Как правило, такое поведение не рассматривается говорящими как проявление неуважения, так как это может быть связано с технической стороной вопроса. Кроме того, утрата приветствия — прощания в беседе посредством мессенджера создаёт впечатление бесконечности и непрерывности разговора, делает возможным возврат к ранее обсуждаемой теме.

Обратим внимание на то, что коммуниканты обычно не называют друг друга по имени в мессенджере, исключение составляет лишь официально-деловая переписка. Причина, во-первых, заключена в законе экономии речевых усилий. Во-вторых, использование обращений является необязательным для представленных друг другу коммуникантов (разговор в мессенджере чаще всего предполагает наличие определённого знания о своём собеседнике, некий сложившийся образ). Но главную роль, на наш взгляд, здесь играет графическое оформление сообщений, заложенное компьютерной

программой: перед каждой репликой пишется имя отправителя, поэтому написание имени было бы избыточным. В качестве

представим фрагмент разговора в социальной сети «ВКонтакте»:

Иван Эгей! А у меня новай телефон *YAHOO*

Мария Привет) Поздравляю!!! Что, вернуть тот надежду потерял?

Иван Ну, ты б тово В часть бы заходила Пинала их-))

Мария Да ну) Я лучше поем)

Иван Ну а то хрен они пошавелятся. Приятного опетиту

Мария спс

Возможность постоянно видеть имя собеседника в электронном диалоге привела к переосмыслению использования обращения по имени: вокативная и номинативная функции утрачиваются, на смену им приходит эмоционально-оценочная.

Ещё одной особенностью сетевого этикета является преобладание общения на ты. Распространённость местоимения 2-го лица единственного числа обусловлена несколькими факторами:

1) возрастной категорией (большую часть интернет-пользователей составляют молодые люди, в среде которых бытует обращение на ты);

2) статусной равноправностью собеседника (близкими, неофициальными отношениями между коммуникантами);

3) статусной неопределённостью собеседника (отсутствием информации о социальных различиях);

4) стремлением преодолеть возрастные, социальные и статусно- ролевые различия для непринуждённости общения, в связи с чем наблюдается быстрый переход на ты.

Вежливое, уважительное отношение к собеседнику, лежащее в основе этикета, может быть выражено невербальными средствами: жестами, мимикой, позой, интонацией. Для этого в интернет-общении активно используются так называемые эмотиконы (смайлы), позволяющие выразить

собственное отношение говорящего к сказанному. Чтобы выразить симпатию к собеседнику или показать, что общение с ним приятно.

Вывод

Итак, в интернет-коммуникации как относительно новой сфере виртуального общения, обладающей специфическими чертами, правила речевого поведения, в том числе и этикетного, находятся в процессе формирования. Мы можем говорить о трансформации традиционных этикетных средств и появлении нового интернет-этикета, который характеризуется свободой самовыражения, стремлением к речетворчеству, уменьшением количества коммуникативных барьеров. В заключение отметим, что, на наш взгляд, некорректно говорить об отсутствии этикетных норм в Интернете, скорее всего мы являемся свидетелями становления новых форм вежливости, обеспечивающих вежливое, конструктивное общение.

Литература

1. Жичкина, А. Е. Самопрезентация в виртуальной реальности и особенности идентичности подростка-пользователя Интернета / А. Е. Жичкина, Е. П. Белинская // Образование и информационная культура. — М., 2000. — С. 431–460.

2. Карабань, Н. А. Этический аспект интернет-коммуникации / Н. А. Карабань // Интернет-коммуникация как новая речевая формация: колл. монография / науч. ред. Т. Н. Колокольцева, О. В. Лутовинова. — М.: ФЛИНТА: Наука, 2018. — С. 158–177.

3. Правила сетевого этикета [Электронный ресурс]. — Режим доступа: http://news.a.ua/Internet/4997_pravila_setevogo_etiketa/

4. Усачева, О. Ю. Лингвокультура языковой личности в интернет-коммуникации / О. Ю. Усачева // Государственная служба. — 2015. — No 5. — С. 97–102.

5. Голошубина, О. К. Нормы речевого этикета в интернет-коммуникации (на примере речевого жанра «разговор в мессенджере») / О.

К. Голошубина. — Текст : непосредственный // Молодой ученый. — 2021. — No 8 (67). — С. 944-947.

БЕЗОПАСНОСТЬПОДРОСТКОВ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Серякова Маргарита Евгеньевна
Володькина Александра Андреевна
Областное государственное бюджетное профессиональное образовательное учреждение «Томский лесотехнический техникум»
Руководитель: Чудная Юлия Сергеевна

Информационные технологии и информация становятся глобальными и охватывают все сферы жизни человека, поэтому вопросы обеспечения информационной безопасности в интернет-пространстве становятся все более **актуальными**. В статье рассматриваются основные угрозы информационной безопасности в сети Интернет среди подростков.

Гипотеза исследования: предполагается, что распространение сети интернет увеличивает степень возникновения глобальных угроз информационной безопасности подростков.

Проблема исследования: в условиях активного развития информационных технологий важной проблемой становится повышение уровня безопасности детей и подростков в сети интернет.

Методы исследования: теоретические (анализ, систематизация, обобщение), эмпирические (опросные методы).

Компьютерные сети, как вид телекоммуникации – новый пласт общественной реальности. По данным совместного исследования Google и Ipsos, результаты которого были обнародованы в сентябре 2016 г., 98 % молодых людей в возрасте от 13 до 24 лет используют Интернет ежедневно. Ежедневное время, которое человек проводит в интернете, за последние 5 лет увеличилось на пол часа. Если в 2015 году это время составляло, примерно, 6 часов 20 минут, то на конец 2020 года цифра достигла 7 часов.

Стремительное развитие средств массовой информации, компьютерных технологий, а также популяризация сети Интернет не только влияет на саморазвитие и доступность общения, но и способствует возникновению глобальных угроз информационной безопасности, особенно для несовершеннолетних. Серьезной угрозой является угроза сетевого общения, т.е. агрессия и провокация со стороны виртуальных собеседников.

Безопасность подростков связана напрямую с коммуникативными рисками. Коммуникативные риски связаны с межличностными отношениями пользователей Интернета и включают в себя риск нападок и оскорблений от других людей. Примерами таких рисков могут быть: незаконные контакты (например, груминг), киберпреследования, кибербуллинг [3].

Кибербуллинг – это преследование пользователя сообщениями, содержащими оскорбления, агрессию, домогательства с помощью различных интернет-сервисов. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами, запугивание, подражание, хулиганство (интернет-троллинг); социальное бойкотирование. Лица, подвергающиеся кибербуллингу или жертвы, находятся в постоянном состоянии страха, депрессии, обиды, гнева не только в киберпространстве, но и в реальном мире, так как это может повлиять на их здоровье.

Тролинг – форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации [1].

Флейминг – это бесцельная дискуссия в чате, личной переписке или комментариях, сопровождающаяся негативными эмоциями. Как и любой конфликт, флейминг порой приводит стороны к использованию недопустимых техник словесной атаки, в первую очередь грубых: оскорбления и угрозы. К одной или обеим из сторон конфликта может спонтанно подключаться большое количество людей. Флейминг – это не травля, а просто «вспышка» эмоций, но он может положить травле начало [4].

Классификацию основных угроз, связанных с сетью интернет можно представить следующим образом:

1. Пропагандирование запрещенных понятий, таких как терроризм, фашизм, наркомания, жестокое отношение к людям и прочее.

2. Информация, вызывающая сексуальные девиации.

3. Виртуальные игры, целью которых является пропаганда насилия, самоубийств, развивающие игроманию, не способствующие развитию интеллекта.

4. Социальные сети, способствующие созданию компьютерной зависимости, риска доступа взрослых с криминальными намерениями, условий для приобретения запрещенных товаров (наркотические и психотропные вещества, краденые вещи, оружие) [2].

5. Мошенничество, воровство, склонение к приобретению дорогостоящих информационных продуктов.

К последствиям пребывания в сети Интернет для психологического здоровья относятся:

• Увеличение количества времени, проводимого за гаджетами;

• Пренебрежение семьей и друзьями;

• Ощущения пустоты, депрессии, раздражения при нахождении вне компьютера;

• Проблемы с учебой.

• общее истощение организма – хроническая усталость, вызванная дефицитом сна и отдыха.

Целью нашего исследования является определение следующих данных:

– как долго подростки проводят в сити интернет;

– чувствуют ли они себя в безопасности.

Используемые диагностики:

1. Шкала интернет-зависимости Чена (2003 г.) Тест включает в себя 5 оценочных шкал. Тест позволяет одновременно измерять специфические симптомы зависимости, среди которых: толерантность, симптом отмены,

компульсивности и в тоже время психологические аспекты такие как: способность управлять собственным временем и наличие внутриличностых проблем. Достоинством данного теста является его многогранность, способность измерять с нескольких точек единый процесс поведения, связанного с интернет ресурсами.

2. После изучения отношения подростков к компьютерной деятельности необходимо проанализировать их психоэмоциональное состояние, так как некоторые нарушения психологического здоровья (например, депрессивный компонент) могут образовывать коморбидную связь с киберзависимым поведением. Шкала реактивной тревожности Спилберга-Ханина была раработана в 1976 г. Данная шкала является информативным способом самооценки уровня тревожности в данный момент (реактивная тревожность, как состояние) и личностной тревожности (как устойчивая характеристика человека) [5]. Испытуемому предлагается внимательно прочитать по 20 суждений ситуативной и личной тревожности и не задумываясь зачеркнуть цифру в соответствующей графе справа в зависимости от того, как он себя чувствует в данный момент. Необходимо вычислить среднегрупповой показатель РТ и ЛТ и их сравнительный анализ в зависимости, например, от половой принадлежности испытуемых. Общий итоговый показатель может находиться в диапазоне от 20 до 80 баллов. При этом чем выше итоговый показатель, тем выше уровень тревожности. Интерпретация результатов: до 30 баллов – низкая, 31 – 44 - балла умеренная; 45 и более высокая.

Нами было проведено диагностическое исследование. За основу исследования были взяты такие методики как шкала интернет-зависимости Чена и шкала реактивной тревожности Спилберга-Ханина. По результатам исследования были выделены подростки, которые обладают признаками интернет-зависимости. Выборку исследования составили 50 подростков в возрасте 16–17 лет, учащиеся 1 курса. На основании первого теста были выделены подростки, которые имеют склонность к возникновению кибераддикции (n=24), что составляет 48 % от общего числа участников

исследования, а также подростки со сформированной кибераддикцией (n=6) – 12 %. И только 40 % опрошенных подростков (n=20) отнесены к группе с минимальным риском возникновения интернет зависимого поведения.

Результаты исследования подростков представлены на рис.1.

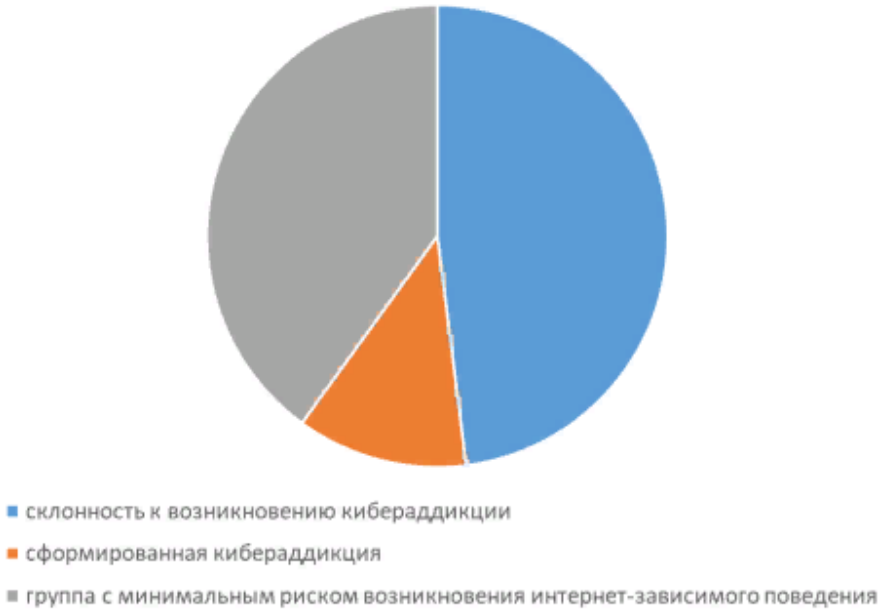


Рис. 1. Результаты исследования

На основании второго теста был выявлен среднегрупповой показатель РТ и ЛТ. Бланк шкал самооценки Спилбергера включает в себя 40 вопросов - рассуждений, 20 из которых предназначены для оценки уровня ситуативной тревожности и 20 - для оценки личностной тревожности.

Из 50 респондентов было выявлено, что 20 набрали в среднем от 17 до 30 баллов 40% (низкий уровень тревожности), от 31 до 44 набрали 25 человек 50% (средний уровень тревожности), и от 45 и более 5 человек, 10%(высокий уровень тревожности).

Известно, что тревога и тревожность тесно связаны со стрессом. Благодаря этому, тесты, оценивающие выраженность тревожности, могут быть успешно использованы также и для диагностики уровня стресса. При этом, ситуативная тревожность будет характеризовать уровень стресса в

данный момент, а личностная тревожность – уязвимость (или устойчивость) к воздействию различных стрессоров в целом [6].

Подводя итоги исследования, можно сделать вывод о том, что большинство опрошенных респондентов имеет склонность к кибераддикции. Так же установили, что уровень тревожности в исследуемой выборке подростков выражен низкий и средний уровень тревожности.

Результаты исследования подростков представлены на рис.2.

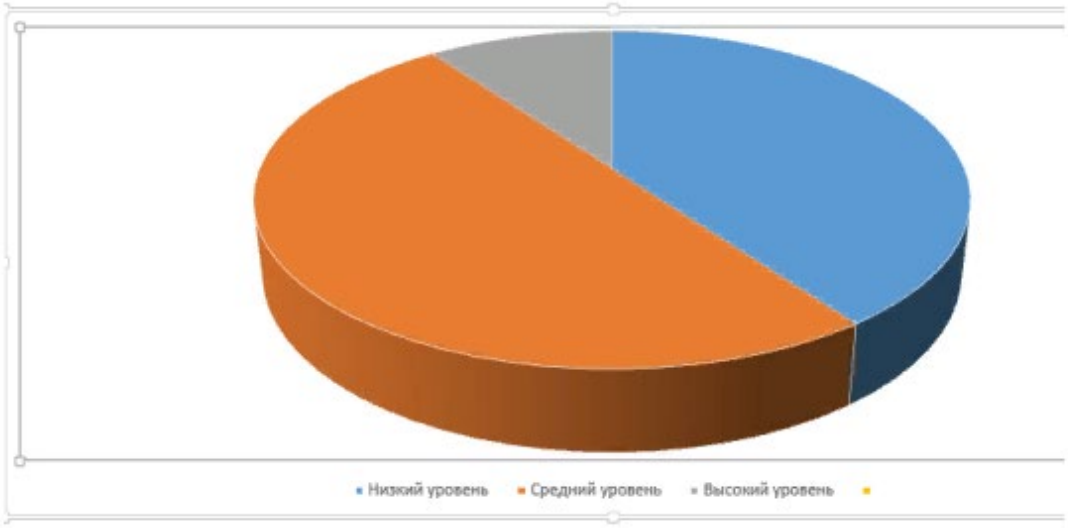


Рис.2. Результаты диагностики

Советы по безопасности в возрасте от 13 до 17 лет. (Для родителей)

1. Совместно с подростками необходимо обсудить с ребенком «черный список» запрещенных сайтов и часы провождения в Интернете, а также руководство по общению в Интернете (в особенности в чатах).

2. Не забывать беседовать с детьми об их виртуальных друзьях, а так же о том, чем они занимаются, будто разговор ведется о реальных друзьях.

3. Компьютер, подключенный к Интернету, должен находиться в общей комнате.

4. Средства блокирования вредоносных сайтов использовать как дополнение к стандартному родительскому контролю.

6. Научить подростка не устанавливать программы без разрешения. Обговорить, что он может случайно загрузить вирусы или иное нежелательное программное обеспечение.

7. Приучить подростка сообщать о любых тревогах или угрозах, связанных с Интернетом. Подсказать, что он в безопасности, если сам рассказал о своих переживаниях.

8. Научить не делиться своей личной информацией, используя средства электронной почты, систем мгновенного обмена сообщениями, чатов, регистрационных форм, личных профилей и при регистрации на online-конкурсы.

9. Самим не забывать знакомиться с сайтами, которые посещает подросток.

10. Поговорить о том, что нельзя использовать Интернет для распространения сплетен, хулиганства или угроз другим людям.

11. Следить за тем, чтобы ребенка подросток уважал других в Интернете. Проверить, что он знает правила хорошего поведения, которые действуют везде – даже в виртуальном мире.

Таким образом, подводя итоги выше изложенного, хотелось бы отметить, что информационная среда имеет отрицательные стороны (риски), особенно для подростков. Создавая что-то новое, не всегда можно найти противовес. Но можно уберечь себя, если прислушиваться к достоверной информации, знать меры по безопасному использованию информационных ресурсов, следить за использованием сети Интернет. Виртуальное пространство имеет безграничные возможности, поэтому оно всегда открыто для новшеств, открытий, исследований и анализа. А возникающие на пути проблемы всегда будут, но их можно преодолеть, если знать их причины и особенности возникновения.

Список литературы

1. Акулич М. М. Интернет-троллинг: понятие, содержание и формы // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. – 2012. – No8. – С. 47-54.

2. Савельев, А. И. Проблема информационной безопасности несовершеннолетних в сети Интернет // Юридическая наука и правоохранительная практика. 2016. No 2 (36). С. 59– 66.

3. Смирнова А. А., Захарова Т. Ю., Синогина Е. С. Киберугрозы безопасности подростков // Научно-педагогическое обозрение (PedagogicalReview). 2017. Вып. 3 (17). С. 99–107. DOI 10.23951/2307-6127-2017-3-99-107

4. Стексова Т.И. Речевая агрессия в интернет-комментариях как проявление социальной напряженности // Политическая лингвистика. – 2013. – No3. – С. 77-81.

5. Шкала интернет-зависимости Чена [Электронный ресурс]https://psytests.org/clinical/inet.html (дата обращения:14.11.2022).

6. Шкала реактивной тревожности Спилберга-Ханина [Электронный ресурс] https://www.nekrasovspb.ru/doc/18spilberg.pdf (дата обращения:14.11.2022).

НЕГАТИВНОЕ ВЛИЯНИЕ СОЦИАЛЬНЫХ СЕТЕЙ НА СОВРЕМЕННОГО ПОДРОСТКА

Макарова Анастасия Игоревна

Областное государственное бюджетное профессиональное образовательное учреждение «Колледж индустрии питания, торговли и сферы услуг»

Руководитель: Элис Татьяна Владимировна

Актуальность исследования. В современном мире практически каждый подросток использует интернет и социальные сети в своей жизни. Эти блага цивилизации помогают быстро найти нужную информацию и социализироваться, но вместе с этим они могут губительно сказываться на психологическом состоянии и адаптации к реальной жизни.

Цель исследования. Проанализировать и выявить негативное воздействие социальных сетей на психологическое состояние современного подростка.

Гипотеза. Социальные сети негативно влияют на психологическое здоровье подростков.

Исходя из цели и выдвинутой гипотезы были поставлены следующие **задачи:**

1. Изучить и собрать материал по данной теме.
2. Провести исследование среди подростков методом анкетирования.
3. Обработать полученные результаты.
4. Написать рекомендации по безопасному использованию социальных сетей.

Методы исследования. Изучение и анализ различных информационных источников по данной теме, обобщение полученного материала, создание и проведение опросов среди подростков.

Тема влияния социальных сетей имеет большое значение особенно сейчас, когда подрастающее поколение все чаще используют интернет в своей жизни. О его вреде и пользе до сих пор спорят ученые. Поэтому я и захотела выяснить как влияют социальные сети на подростков.

Я считаю, что подросток и социальная сеть – это одна из актуальных тем нашего времени. Социализация человека происходит в процессе воспитания и под значительным влиянием среды. Среда современного человека, в которой происходит воспитание, существенно изменилась. В наше время наиболее сильное влияние оказывает Интернет и, в частности социальные сети. Для подростков социальная сеть стала инструментом самовыражения, а общение не ограничивается определенным кругом людей.

Среди основных потребностей нахождения в социальных сетях подростков можно выделить следующие:

1. Общение. Основная потребность в социализации, поиска единомышленников, круга общения по интересам.
2. Развлечение. Просмотр видеороликов, игры, музыка.
3. Обучение. Возможность проходить треннинги, курсы, находить экспертов в своей области.

Чрезмерное увлечение социальными сетями может плохо сказаться на психическом состоянии подростка. Он может перестать общаться с окружающими и замкнуться в себе. При наличии у него проблем в общении, комплекс развивается с большей силой. И как следствие этого, возникают трудности в адаптации к реальной жизни.

Проанализировав социальные сети, можно выделить следующие опасности и негативное влияние на подростков:

1. Мошенничество. Самые популярные виды мошенничества в социальных сетях являются экстрасенсы, возможность быстрого обогащения, шантаж, фейковые онлайн-магазины.
2. Кибербуллинг. Унижение или травля в Интернете оказывает на подростков болезненное воздействие.
3. Зависимость. Постоянное и неконтролируемое время препровождение в соцсетях.
4. Содержание негативного характера. Порнография, насилие, убийства, аварии, теракты и их последствия.
5. Неблагоприятные группы. Суицидальные группы, группы по похудению, приводящие к анорексии, вербовка в запрещенные организации и т.п. [2]

Подростки слишком много времени тратят на бессмысленное времяпрепровождение в социальных сетях. Они заводят свою страничку на просторах Интернета в среднем в возрасте от 10 лет. В социальной сети любой подросток может выдавать себя за героя, уверенного в себе человека, а в действительности иметь много комплексов и психологических травм. Имея такой образ в соцсетях, ему будет сложно общаться и знакомиться с людьми в реальной жизни, переживать процесс социализации в обществе.

Таким образом, влияние социальных сетей на подростка сегодня становится все более явным и не всегда положительным.

В рамках своей работы я решила провести анкетирование среди подростков, чтобы выяснить пользуются ли они социальными сетями и оказывают ли соцсети влияние на их психологическое состояние.

Анкета содержала следующие вопросы:

1. Являетесь ли вы пользователем социальных сетей? (да, нет)
2. Какова причина регистрации в социальных сетях? (Общение, поиск информации, видео/кино/музыка, игры с друзьями)
3. Не имея возможность выйти в соцсеть что вы испытываете? (раздражение, скуку, агрессию, мне все равно)
4. Сколько времени вы проводите в социальных сетях? (до 5ч в день, 5-10ч в день, более 10ч в день)
5. Что приносит больше удовольствия: реальная жизнь или социальные сети? (первое, второе)
6. Считаете ли вы себя зависимым от социальных сетей? (да, нет)
7. С какими негативными воздействиями вы сталкивались в соцсетях? (травля, мошенничество, нет)
8. На какое время вы бы смогли отказаться от соцсетей? (на день, больше часа не выдержу, мне все равно)

В опросе участвовало 55 человек, результаты я представила в виде диаграмм.

В результате анализа анкетирования я получила следующие данные:

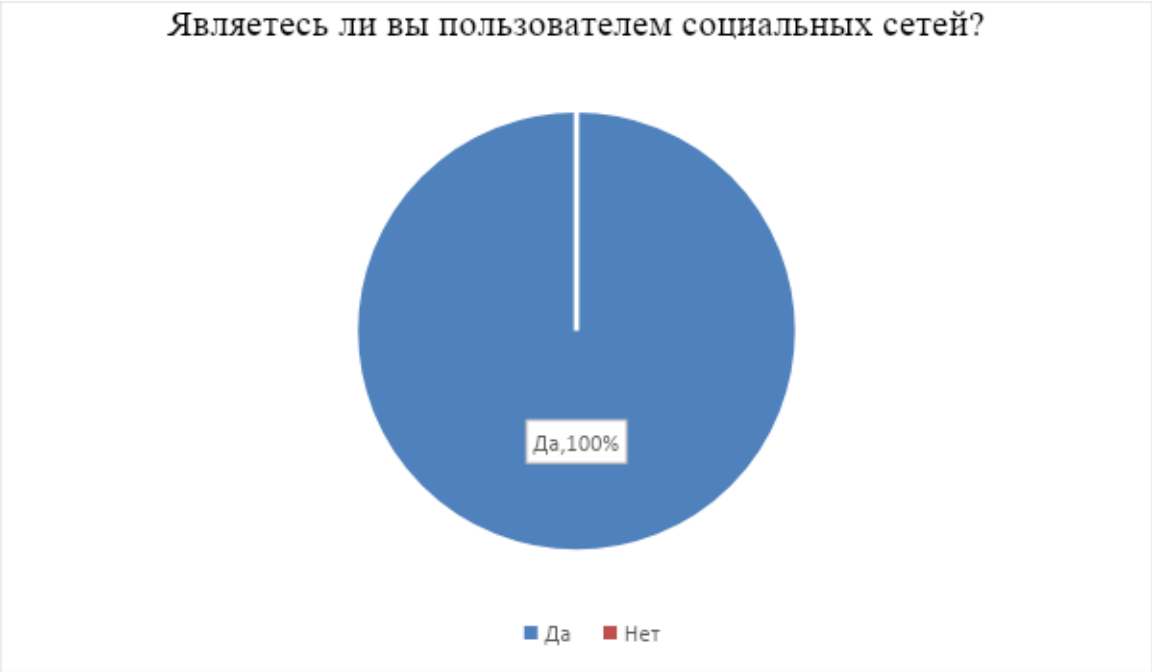


Рисунок 1 – Вопрос 1

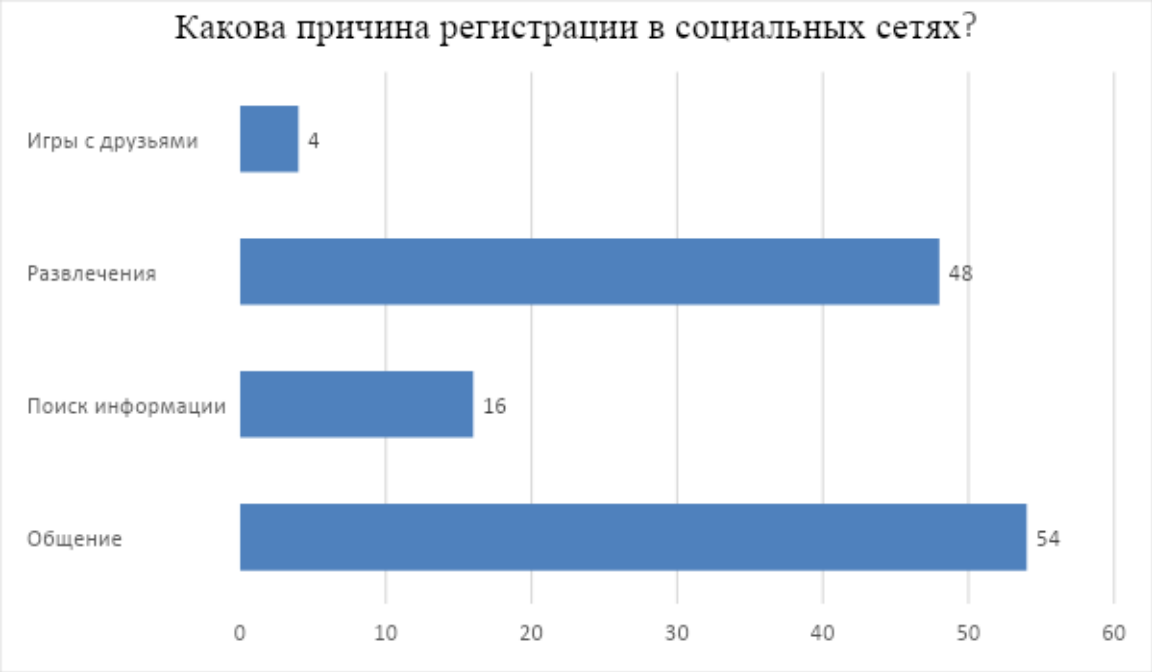


Рисунок 2 – Вопрос 2

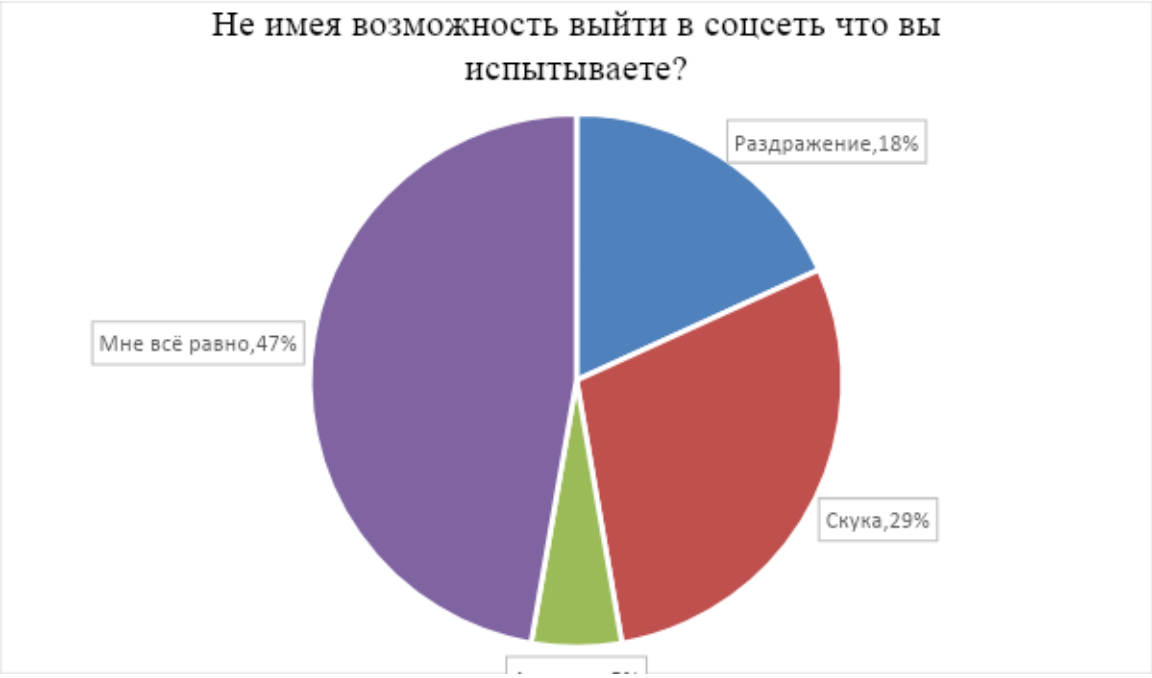


Рисунок 3 – Вопрос 3

Рисунок 4 – Вопрос 4

Рисунок 5 – Вопрос 5

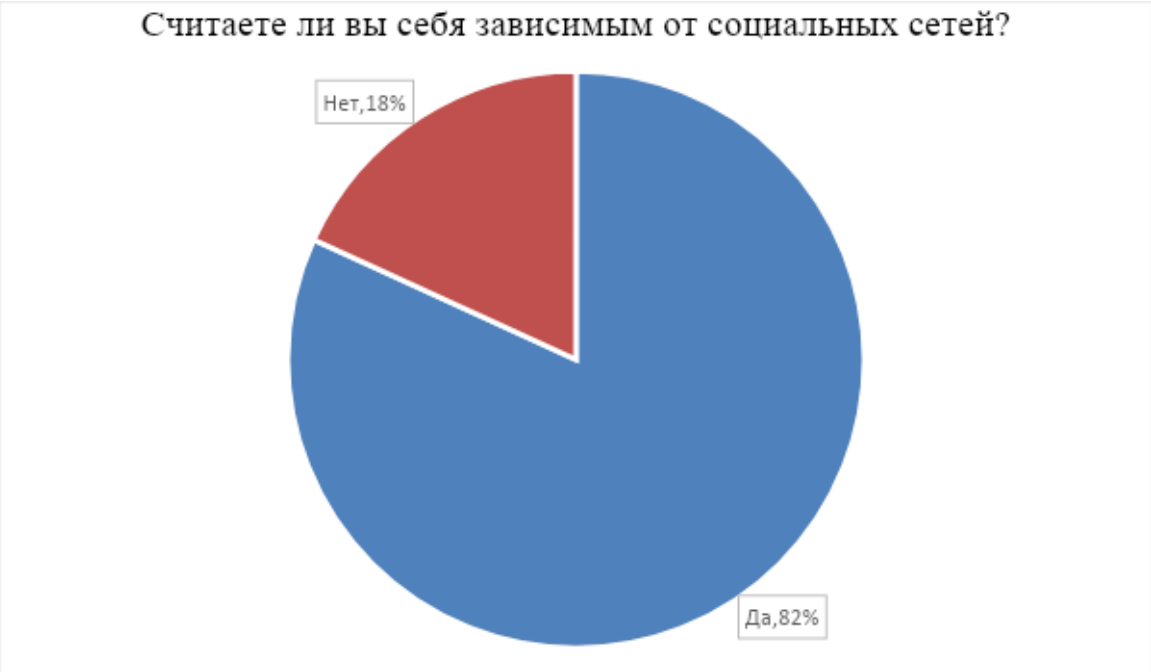


Рисунок 6 – Вопрос 6

Рисунок 7 – Вопрос 7

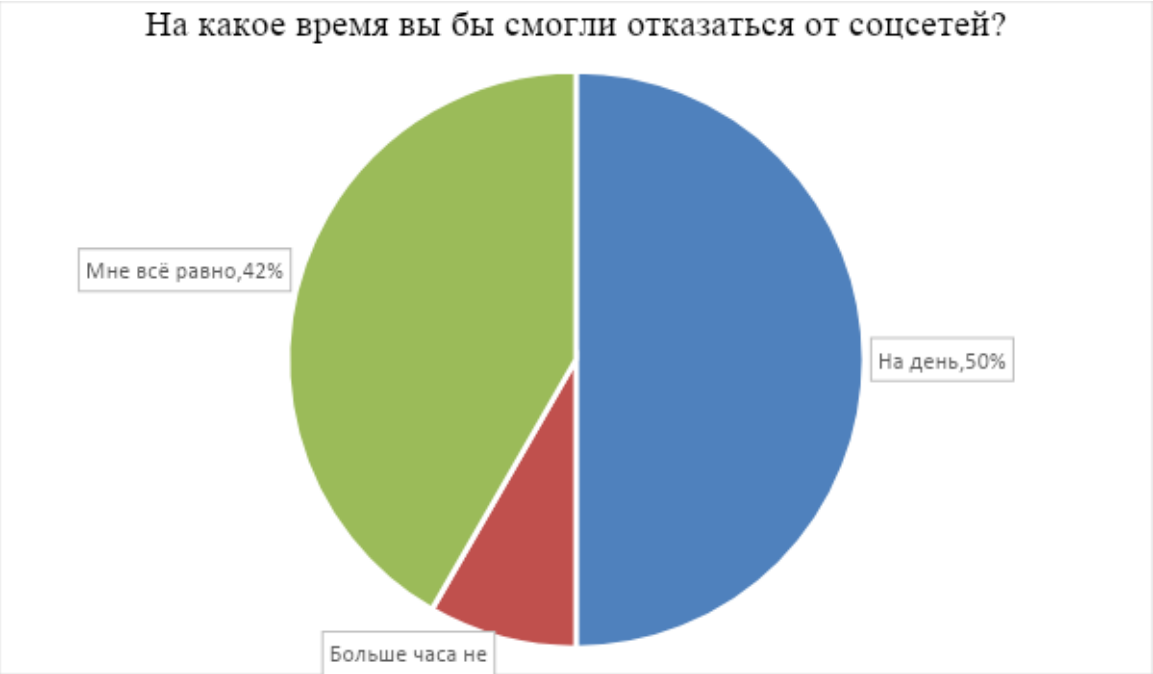


Рисунок 8 – Вопрос 8

Как мы можем увидеть, все опрошенные пользуется социальными сетями. Большинство идут туда за общением и развлечениями. Больше половины опрошенных испытывают дискомфорт при отсутствии возможности выхода в соцсети. Около 36 % проводят половину дня в социальных сетях, но в тоже время большинство опрошенных не считают себя зависимыми от соцсетей и предпочитают реальную жизнь виртуальной. Около 40%

сталкивались с негативным воздействием в социальных сетях таких как мошенничество и травля.

Исходя из анализа можно сказать, что социальные сети всё больше проникают в повседневную жизнь подростков и вместе с этим возникают риски негативного влияния на психологическое состояние.

Изучив весь материал, я решила написать рекомендации по безопасному использованию социальных сетей:

1. При регистрации в социальных сетях необходимо использовать длинные и сложны пароли, нежелательно использовать один пароль для разных сервисов, также рекомендуется использовать двухфакторную аутентификацию при возможности.
2. Не следует публиковать свои личные данные: пароли, телефоны, адреса, дату рождения и другую личную информацию.
3. Не сообщайте данные аккаунта друзьям и знакомым. Если заходите в социальную сеть с чужого компьютера, не забудьте выйти.
4. Необходимо ограничить список друзей: в друзьях не должно быть случайных и незнакомых людей.
5. Устанавливайте антивирусные программы.
6. Никогда не открывайте подозрительные сообщения, в которых находятся ссылки на неизвестные ресурсы, и никогда не переходите по этим ссылкам, не устанавливайте неизвестные файлы.
7. Не устанавливайте приложения для социальных сетей, которые якобы позволяют скачать музыку, видео и другое, если вы не уверены в безопасности этих приложений.
8. Не пересылайте конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через мессенджеры социальных сетей.
9. Если Вы действительно хотите встретиться с человеком, с которым познакомились в интернете, то договоритесь о встрече в общественном месте и желательно взять с собой кого-то еще, например, друга.

Если твой сетевой друг считает, что присутствие кого-то еще плохая идея, то стоит отказаться от встречи.

10. Во время общения в онлайн-среде с другими пользователями игнорируйте плохое поведение других пользователей, воздержитесь от ответа на провокационные сообщения. [3]

Вывод. В результате проведенной мною исследовательской работы, можно сделать вывод о том, что социальные сети – это основной способ коммуникации подростков, где необходимо соблюдать меры предосторожности, которые помогут не стать жертвой мошенничества и других негативных воздействий.

Список литературы

1. Донцов Д.А. Детский образ как фактор рекламного воздействия. – М. 2001.

2. Цхай Е.В. Психологическое воздействие рекламы и социальных сетей на человека. – Красноярск. 2004.

3. Правила безопасного общения в социальных сетях. [Электронный ресурс]. URL:https://internetpolicy.kg/literacymodule/course_1/module3/glava3_1.html

4. Интернет-безопасность для детей - Безопасное использование социальных сетей. [Электронный ресурс]. URL:https://edu.gcfglobal.org/en/tr_ru-internet-safety-for-kids/-social-networks/1/

СЕКЦИЯ 2. СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ IOT ОБЪЕКТОВ

ВИДЫ КОМПЬЮТЕРНЫХ ВИРУСОВ И МЕТОДЫ БОРЬБЫ С НИМИ

Штаненко Егор Максимович

Областное государственное бюджетное профессиональное образовательное учреждение «Томский экономико-промышленный колледж»

Руководитель: Федорова Анна Николаевна

Ключевые слова: вирусы, методы, безопасность, заражение, ПО.

Любая вредоносная программа считается компьютерным вирусом. Название получило популярность в фантастических рассказах 70–90 гг. В голливудских фильмах часто встречается компьютерный гений, который взламывает Пентагон. Хотя хакеру куда проще усыпить бдительность жертвы. Достаточно подсунуть что-то в красивой оболочке, чтобы человек установил программу, перешел по ссылке или скачал файл. Установка не лицензированного софта может привести к утрате ценной информации, выводу девайса из строя, незаконному использованию ресурсов системы или IP. Рассмотрим основные виды компьютерных вирусов и методы защиты от них.

Они строго делятся на те, которые ищут уязвимости в системе, и те, что запускаются пользователем за счет социальной инженерии (хакерская атака с применением психологических уловок).

Если разделять типы хакерского ПО не по задачам (вымогательство, вандализм, шпионство), а по способу проникновения, то их всего три: троян; червь; вирус.

Троянский конь всегда используется в нелицензионном ПО. Но он не всегда бывает опасен. Программа устанавливается вместе с софтом и запускается в фоновом режиме. Безобидные трояны идут вместе с “кряками” на популярные игры или Windows ОС (англ. operating system – “OS”). Они позволяют обходить активацию лицензионного ключа, что решает вопрос

бесплатного использования лицензионного софта. Вторая сторона медали – не безобидные трояны, которые способны выводить из строя систему безопасности, скачивать другие виды компьютерных вирусов и др.

Червь делает свою работу тоже очень тихо. Иногда его очень сложно удалить. Червь проникает через “дыры” в программном обеспечении. Он записывается на все устройства, которые контактируют с компьютером и сетью. Сюда относится все, где есть память (смартфон, принтер).

Даже после переустановки ОС червь снова появляется, как только к нему подключат зараженный гаджет или другой ПК. Подобные вирусы создают свои копии повсюду, используя сетевые протоколы и устройства.

Обычный вирус распространяется только с помощью социальной инженерии. Он размножается в пределах одного ПК, постепенно загружая его различными задачами. Часто вирусы сами шифруются под антивирус, который легко купить. Чтобы избежать проблем нужно использовать только лицензионное ПО.

КАК СЕБЯ ОБЕЗАПАСИТЬ? Выявить вредоносные программы можно при помощи антивируса. Он всесторонне проверяет компьютер на заражение и отражает различные атаки. Более подробно об это можно узнать в интернете.

Существует множество видов программ вирусов и их подвидов. Они делятся между собой по способу вредительства. Наиболее распространенные виды вирусов:

1. Логическая бомба или бомба замедленного действия.
2. Руткит (права суперпользователя).
3. Адвар (рекламные баннеры).
4. Шпион (мониторинг).
5. Эксплойт (захват системы).
6. Винлокер (смс-вирус).
7. Кейлогер (мониторинг действий пользователя).
8. Буткит (сектор на жестком диске).

9. Бэкдор (незаметное проникновение).

10. Ботнет (зомбинет).

Нежелательное ПО не всегда является опасным. Многие программы содержат полезные функции, однако, их действия расцениваются антивирусом как угроза. Иногда довольно сложно найти грань между пользой и вредом для компьютера. Однако есть одно качество, которое их кардинально отличает друг от друга. Вирусное ПО всегда действует без ведома владельца.

Нанесение пользователю ущерба связано с тем, что данные и ресурсы компьютера используют третьи лица без его согласия.

ВИДЫ ЗАРАЖАЕМЫХ ОБЪЕКТОВ

Файлы —Заражают ваши программы, системные и обычные файлы.

Загрузочные секторы —резидентные вирусы. Заражают как понятно из названия загрузочные сектора компьютера, приписывают свой код в автозагрузку компьютера и запускаются при запуске операционной системе. Порою хорошо маскируются что трудно убрать из автозагрузки.

Макрокоманды — Документы word, excel и подобные. Использую макросы и уязвимости средств Microsoft office вносит свой вредоносный код в вашу операционную систему.

ПРИЗНАКИ ЗАРАЖЕНИЯ

Не факт, что при появлении некоторых из этих признаков означает наличие вируса в системе. Но если они имеются рекомендуется проверить свой компьютер антивирусом или обратиться к специалисту.

Один из распространенных признаков — **это сильная перегрузка компьютера**. Когда у вас медленно работает компьютер, хотя у вас ничего вроде бы не включено, программ, которые могут сильно нагружать компьютер. Но если у вас антивирус заметьте антивирусы сами по себе нагружают компьютер очень хорошо. А в случае отсутствия такого софта, который может грузить то скорее тут вирусы. Вообще советую по уменьшить для начала количество запускаемых программ в автозапуске.

Медленная загрузка программ, так же может быть одним из признаков заражения. Но не все вирусы могут сильно нагружать систему, некоторые практически трудно заметить изменения.

Системные ошибки. Перестают работать драйвера, некоторые программы начинают работать неправильно или часто вылетают с ошибкой, но раньше допустим такого не замечалось. Или начинают часто перезагружаться программы. Конечно, такое бывает из-за антивирусов, например антивирус удалил по ошибке посчитав системный файл вредоносным, либо удалил действительно зараженный файл, но он был связан с системными файлами программы и удаление повлекло за собой такие ошибки. **Появление рекламы в браузерах** или даже на рабочем столе начинают появляться баннеры.

Появление не стандартных звуков при работе компьютера (писк, щелчки ни с того ни с сего и подобное).

Открывается сам по себе CD/DVD привод, или просто начинает словно читать диск хотя диска там нет.

Длительное включение или выключение компьютера. **Угон ваших паролей**. Если вы заметили, что от вашего имени рассылается различный спам, с вашего почтового ящика или странички социальной сети, как вероятность что вирус проник в ваш компьютер и передал пароли хозяину, если вы заметили такое рекомендую провериться антивирусом в обязательном порядке (хотя не факт, что именно так злоумышленник получил ваш пароль).

Частое обращение к жесткому диску. У каждого компьютера есть индикатор, который мигает, когда используют различные программы или когда копируете, скачиваете, перемещаете файлы. Например, у вас просто включен компьютер, но не используется никаких программ, но индикатор начинает часто мигать якобы используются программы. Это уже вирусы на уровне жесткого диска.

ЗАКЛЮЧЕНИЕ. Наличие заражения можно определить по разным признакам. Сюда относятся частые ошибки в работе интерфейса,

всплывающие окна, постоянная загрузка интернет-трафика, проблемы с мощностью процессора, блокировка доступа на официальные сайты, неожиданный запрет на права администратора. Цель злоумышленника – получить удаленный доступ к компьютеру. Решить проблему можно путем использования антивируса.

Вот, собственно, и рассмотрели компьютерные вирусы, которые могут вам встретиться в интернете. Но на самом деле их в разы больше, и полностью защититься невозможно, разве что не пользоваться интернетом, не покупать диски и вообще не включать компьютер.

Советую по возможности не пренебрегать использованием виртуальных машин или песочницы.

Список литературы

1. Компьютерные вирусы. Типы, виды, пути заражения: [Электронный ресурс.] – Режим доступа: https://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html (Дата обращения 1.11.2022)

Компьютерные вирусы. Типы, виды, пути заражения: [Электронный ресурс.] – Режим доступа: https://obrazovanie.guru/informatika/vidy-virusov.html (Дата обращения 1.11.2022)

МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ

Жилинкова Ангелина Геннадьевна

Областное государственное бюджетное профессиональное образовательное учреждение «Томский экономико-промышленный колледж»

Руководитель: Федорова Анна Николаевна

Ключевые слова: общество, Интернет, схема, мошенничество, совет.

Цель данной работы рассмотреть самые распространённые виды мошенничества в сети Интернет, особенно наиболее распространенные из них такие как фишинг, SMS-рассылки, а также мошенничество с приобретением

заказов и товаров в сети Интернет. В ходе исследования каждой схемы мошенничества будут рассмотрены и простейшие способы защиты от них.

В эпоху цифрового общества сеть Интернет считается ведущим фактором в сфере телекоммуникаций. С помощью компьютерных программ и мобильных приложений мы получаем доступ к возможностям дистанционного управления различными финансовыми операциями, возможности поиска и приобретения различных товаров и услуг. Благодаря Интернет-ресурсам мы можем дистанционно обучаться в учебных заведениях, посещать вебинары и видеоконференции, общаться и т.д. При всем удобстве и привлекательности сети Интернет, не стоит забывать и про опасности, которые притаились в виртуальном пространстве. Одной из таких опасностей является интернет-мошенничество.

Активность интернет-мошенников от года к году только растет, а сами методы и схемы, по которым проводится хищение становятся все сложней и запутанней. Не стоит говорить, что последствия их деятельности доставляют огромные неприятности не только частным лицам, но и компаниям. Для того чтобы не стать жертвой мошенников в сети Интернет мы рассмотрим самые распространённые способы мошенничества, методы защиты от них и правила безопасного поведения.

Среди всех известных видов мошенничества, совершенных с использованием информационно-телекоммуникационных технологий, большую часть составляют классические виды. К классическим видам интернет-мошенничества можно отнести фишинг, SMS-рассылки, а также мошенничество с приобретением заказов и товаров в сети Интернет. В ходе приступного замысла злоумышленники используют давно известные предлоги мошеннических действий, совершаемых по средством компьютерных технологий и средств мобильной связи: фейковая продажа и покупка товаров посредствам различных интернет ресурсов, включая такие проверенные платформы как Instagram, Авито, Юла и т.п. Если дело касается

фишинга, то сюда могут входить сообщения о ложных сведениях о выигрыше приза, ложная информация о близких людях и т.п.

Рассмотрим такую распространенную схему мошенничества как фейковые SMS-рассылки или электронные письма о выигрыше различных призов. Главная идея такого мошенничества заключается в том, чтобы убедить пользователя что якобы он и только он стал счастливым обладателем ценного приза и для получения *Выигрыша* осталось выполнить всего несколько простейших шагов. Потом мошенники просят перевести на поддельный электронный счет определенную сумму денег, мотивируя это необходимостью уплаты налогов, таможенных пошлин или транспортных расходов. После получения денежных средств злоумышленники либо перестают выходить на связь, либо, если дело касается особо наглых мошенников, просят перевести дополнительные суммы на оформление выигрыша. В результате «счастливый победитель» естественно остается без «приза» и без собственных денежных средств, переведенных мошенникам.

Совет в таких случаях прост: будьте благоразумны, задумайтесь над тем, а принимали ли Вы участие в каком-либо розыгрыше в последнее время? Если нет, то откуда организаторам акции известны ваши контактные данные. Так же необходимо почитать отзывы о организаторе акции и желательно не на одном сайте. Если хоть где-то появится сомнение, то рекомендуется проигнорировать поступившее сообщение и в дальнейшем помечать такие сообщения как спам.

Еще один вид мошенничества, участившийся в последнее время, это фейковые SMS от банка. Злоумышленники присылают на номер жертвы SMS с текстом о том, что карта заблокирована в конце указывается номер телефона, по которому нужно связаться с якобы сотрудником банка. Доверчивый пользователь звонит по номеру и попадает в руки опытного мошенника, который просит выполнить определенный набор шагов для якобы разблокировки карты и, пользователь, сам того не понимая, передает свои конфиденциальные данные в чужие руки, в следствии чего теряет и деньги.

Совет: никогда и никому не сообщайте свои данные, а также любую банковскую информацию по телефону, даже если номер телефона похож на официальный банковский. В век IP-телефонии для злоумышленника подделать номер не составит и труда. Запомните, сотрудники банка никогда не спрашивают номер карты, срок ее действия, а также CVV-код по телефону.

Следующая схема мошенничества Фишинг. Основное мошенничество с помощью фишинга в интернете связано с предоставлением различных финансовых услуг. Выманивание финансов с банковских карт осуществляется посредством кражи электронных данных – CVV-кодов, паролей, номеров, PIN-кодов. Эта схема мошенничества отличаются от других схем подходом к взаимодействию с жертвой. Данная схема заключается в том, что мошеннику нужно создать такую поддельную страничку, которая на первый взгляд будет визуально неотличима от реально существующей страницы нужного интернет-ресурса. Различием может быть точка, другая буква, тире или еще какой-нибудь незаметный на первый взгляд символ. Попадая на такую поддельную страничку пользователю, будет предложено ввести данные банковской карты, если дело касается интернет-покупок, либо данные своей учетной записи, если дело касается авторизации на каком-либо интернет-ресурсе. В это время происходит так называемый перехват данных, введённых пользователем, которые напрямую попадают в руки злоумышленников. В дальнейшем эти данные могут быть использованы на усмотрение мошенников, а именно: использованы мошенниками по назначению, например взлом страницы социальных сетей, покупки в интернете, перевод денежных средств или проданы другим злоумышленникам.

Рассмотрим один из гипотетических сценариев, который могут использовать Фишеры. После того, как фишинговая страница для входа готова, нужно заманить туда жертву. Поэтому сначала обрабатывают жертву со стороны его интересов:

1. На почту жертвы посылается предложение, зайти в Instagram и там поучаствовать в конкурсе или опросе, который может его заинтересовать. В

ссылке естественно указана поддельная страница, жертве останется только ввести свой логин и пароль.

2. Идет долгая обработка жертвы с самой странички. Иногда, на это уходит до полугода. Вы знакомитесь, начинаете общаться, узнаете интересы, потом предлагаете лайкать Ваши фото, взамен лайкая его. Потом уже, когда доверие жертвы к Вам зашкаливает, невзначай предлагаете поучаствовать в конкурсе или выполнить заказ и кидаете заготовленную ссылку взлома аккаунта.

3. Письмо на почту жертвы: «Кто-то пытался взломать Ваш аккаунт. Войдите через эту ссылку. Введите действующий пароль, чтобы подтвердить, что он Ваш. С уважением, служба безопасности. Ни для кого не секрет, что ссылка приведет жертву к нужной фишинг-странице.

Совет: прежде всего пользователям сервисов необходимо научиться распознавать фишинг самостоятельно. В ответ на письмо с просьбой *подтверждения* учетной записи или любой другой схожей просьбой следует пользователям связаться с организацией, от имени которой отправлено сообщение, чтобы проверить ее подлинность. Кроме того, рекомендуется самостоятельно вводить URL-адрес организации в адресную строку вместо использования любых гиперссылок.

Важно помнить также, что фишинговые сайты скрываются также за всплывающими окнами, где расположена таргетированная реклама. Бывают случаи, когда в поле *Логин* пользователь видит заполненный адрес электронной почты и все что ему остается только ввести *Пароль*. Есть вероятность увидеть ссылку на фишинговый сайт в комментариях на форумах и в социальных сетях. Ссылку может прислать вам также друг или знакомый, чей аккаунт был взломан. Если письмо или ссылка вызвали у вас подозрение, лучше не переходить по ней, стоит убедиться, что на другом конце Ваш контакт. Так же необходимо поддерживать актуальные сигнатуры угроз для установленного антивирусного ПО на компьютере, в состав которого входит антифишинговая защита.

Следующая схема мошенничества дешевые товары на интернет-досках и онлайн-магазинах. Жертвой часто движет желание сэкономить, что на руку мошенникам. Схема работы такого вида мошенничества, следующая: злоумышленники размещают товары на сайте объявлений по очень «*Выгодной цене».* Покупая товар через Интернет, вносится вся или частичная сумма оплаты на карту, после чего исчезает объявление с сайта и сам продавец.

Совет: здесь нужно быть очень внимательным, заказывая товары в новом магазине, проверяйте юридический адрес магазина, лицензию и ищите отзывы реальных покупателей, если Вы уверены в честности продавца, то придерживайтесь покупок исключительно наложенным платежом.

В заключение рассмотрим еще одну из распространённых схем обмана на фриланс-услугах. Сюда можно отнести удаленную работу, для многих такая работа стала главным источником дохода. Довольно часто можно встретить объявления и целые сайты, посвященные простому и быстрому заработку. Вам предлагается гибкий график, приличное вознаграждение и полный социальный пакет. Основная схема такого мошенничества заключается в том, что для того, чтобы приступить к работе Вас просят внести небольшую плату за обучающие материалы или доступ к заказам. Когда мошенник получит деньги, то скорее всего вы не увидите ни работы, ни обучающих материалов.

Совет: остерегайтесь таких предложений, ведь на большинстве фриланс-бирж начать работу можно абсолютно бесплатно.

Заключение. В настоящее время существует очень много различных видов мошенничества. В данной работе разобраны самые распространенные и наиболее популярные среди мошенников. Стоит отметить, что мошенники совершенствуются, придумывают новые креативные схемы мошенничества. Запомните мошенники вокруг нас, поэтому будьте бдительны и внимательны в повседневной жизни: не раскрывайте данные своих карт; не скачивайте неизвестные ссылки с неизвестных непроверенных источников; не выполняйте действия, которые отправляют Вас на неизвестный Вам сайт; не

отвечайте на подозрительные письма; не вводите в подозрительные сайты свой логин и пароль и тогда Ваши данные будут защищены.

Если Вы распознаете одну из перечисленных выше схем мошенничества советуем подать *Заявление в МВД РФ.* Ссылка на сайт МВД РФ https://mvd.ru/request_main. Ответственность за мошенничество предусмотрена ст. 159 УК РФ.

Литература

1. Интернет-мошенничество- уголовная ответственность: [Электронный ресурс.] – Режим доступа: https://07.xn--b1aew.xn--p1ai/news/item/11911464 (Дата обращения 10.11.2021)

2. Интернет-мошенничество – памятка для граждан: [Электронный ресурс.] – Режим доступа: https://xn--b1aew.xn--p1ai/document/1910260 (Дата обращения 10.11.2021)

3. Как распознать фишинг и как ему противостоять: [Электронный ресурс.] – Режим доступа: https://root-nation.com/ru/posts/internet-posts/ru-phishing-kak-emu-protivostoyat/ (Дата обращения 05.11.2021)

4. Про фишинг: [Электронный ресурс.] – Режим доступа: http://www.admbal.ru/news/sposoby-moshennichestva-v-internete (Дата обращения 12.11.2021)

АНАЛИЗ ВОЗМОЖНЫХ УЯЗВИМОСТЕЙ СИСТЕМ «УМНОГО ДОМА»

Кошкарев Никита Андреевич

Областное государственное бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»

Руководитель: Федорова Татьяна Викторовна

ВВЕДЕНИЕ

На данный момент системы управления и функционирования объектов находят всё больше и большее распространение в нашей жизни. Существуют

не только дома с такой системой, но и государственные предприятия: АЭС, аэропорты, медицинские учреждения, предприятия государственной важности. Такие системы развиты и будут дальше развиваться с течением времени. «Умный дом» – система автоматизации устройств, выполняющих свои действия без участия человека. Возможность управлять всем своим домом с помощью одного пульта дистанционного управления (например, смартфона), несомненно, очень удобна.

Благодаря интеллектуальным решениям можно, например, опустить жалюзи, включить освещение, выключать духовку, повысить температуру в помещении, заниматься многими другими делами, не вставая с кресла, и даже находясь вне дома.

Это становится возможным благодаря гибкости и структурированности автоматизированных сетей. В результате этого здание становится все более функциональным. Однако в такой интеграции существуют и свои недостатки.

Это объясняется тем, что сочетание разных технологий при построении одной автоматизированной системы увеличивает количество возможных недостатков решения с точки зрения безопасности функционирования объекта (здания).

Поэтому очевидна актуальность данного исследования, связанная с исследованием вопросов в области защиты информации устройств «умного дома».

Методы исследования: анализ литературы, конкретизация, обобщение.

Цель работы: проанализировать возможные уязвимости систем «умного дома».

1. Исследование основных характеристик «умного дома» как объекта защиты.

Что на самом деле можно назвать «умным домом»? Это понятие фактически означает систему повседневных устройств, которые могут

подключаться к Интернету (эти устройства часто также входят в категорию IoT).

Стоит помнить, что умные дома очень часто подключаются к той же сети, которую используют члены семьи, которые поддерживают свою электронную почту, учетные записи в социальных сетях, онлайн-банкинг и многое другое. По этой причине взлом одного устройства, принадлежащего сети, представляет серьезный риск для конфиденциальности его пользователей.

Что не так с «умным домом» и зачем его защищать?

Без проблем взломать умный дом можно и находясь прямо на месте. Как правило, при создании таких систем — особенно для жилых помещений — к существующей инфраструктуре просто «пристраивается» дополнительный уровень новых устройств. Новые гаджеты взаимодействуют между собой с помощью протоколов для беспроводного взаимодействия. И часто разработчики систем выбирают протоколы, которые не предполагают шифрования, так что перехватить данные может любой человек, подключившийся к сети помещения.

Киберпреступники часто атакуют устройства Интернета вещей, нападая не только на отдельные домохозяйства, но и на целые города, использующие интеллектуальные решения.

Почему «умные» инструменты пользуются все большим спросом у хакеров? Прежде всего, потому что они хранят бесчисленные объемы данных. Даже такие неприметные гаджеты, как «умные» холодильники или духовки хранят информацию о своих пользователях, которые иногда делятся ею, независимо от потенциальных угроз.

2. Анализ угроз безопасности системы «умный дом»

1.Кража паролей.

Многие пользователи систем «умного дома» совершают одну кардинальную ошибку - они используют один и тот же пароль для защиты всех

гаджетов, а иногда даже используют его в Интернете. Для хакеров это прямое приглашение взломать другие устройства в сети, а также профили в социальных сетях и многое другое.

Если вы используете простой пароль во всей системе «умного дома» и за ее пределами, вы можете быть уверены, что, если злоумышленникам удастся угадать его и взломать одно устройство, они также попробуют использовать его для других инструментов, а также с самим хабом (например, маршрутизатор), что может привести к получению доступа к сети.

Если хакер это сделает, он сможет не только манипулировать чужими устройствами, но и подслушивать всю сеть, получая доступ к конфиденциальным данным. Шутки о включении и выключении света - наименьшая из проблем на данном этапе.

Вот что должен содержать хороший пароль: минимум 8 символов как прописные, так и строчные буквы, числа, специальные символы (точки, подчеркивания и т. д.).

Кроме того, пароль не должен быть легко угадываемым. Поэтому имена родственников или даты рождения не допускаются.

2.Физическое проникновение в дом

Многие пользователи решений «умный дом» устанавливают в своих домах «умные» дверные замки, ставни или противовзломные ставни, управляемые смартфоном.

Это делается из соображений безопасности - эти типы гаджетов могут уведомлять пользователя о необычной активности. Так что, если вы окажетесь вне дома, и кто-то попытается манипулировать вашим дверным замком - вы узнаете об этом благодаря сообщению на своем смартфоне, которое позволит вам быстро отреагировать.

Проблема возникает, когда сами интеллектуальные домашние противовзломные устройства не защищены должным образом.

Уязвимости в их программном обеспечении и невнимательность пользователей могут привести к взлому. Если, например, преступник получит

контроль над интеллектуальной оконной системой, у него не будет проблем с отключением сигнализации.

3.Уничтожение оборудования

Получение контроля даже над одним интеллектуальным устройством может повредить оборудование. Даже если злонамеренный хакер не сможет взломать ценную информацию о ваших банковских счетах, это может привести к финансовым потерям.

Например, преступник, попавший в плохо защищенную систему отопления, сможет изменить ее настройки, повредив все оборудование, которое не является дешевым в ремонте или замене.

4.Подслушивание и подглядывание за домом

Интеллектуальные системы мониторинга - это решения, призванные обеспечить пользователю чувство безопасности. Благодаря им можно наблюдать за тем, что происходит перед домом, даже если хозяин находится далеко от него, и в наличии есть только смартфон.

Что, если сам хозяин станет жертвой шпионажа и подслушивания собственных камер? Это возможно, если они не защищены должным образом. Многие пользователи интеллектуальных веб-камер даже не меняют свои настройки по умолчанию, что позволяет легко взломать их с соответствующими знаниями.

Также стоит помнить о набирающих популярность голосовых помощниках. Хотя по умолчанию они должны только слушать команды, после взлома безопасности они могут превратиться в шпионов.

5.Установка вредоносного ПО

Хотя для большинства пользователей взлом холодильника не кажется серьезной угрозой, следует помнить, что даже такое незаметное оборудование может быть шлюзом к другим устройствам в доме. Если упомянутый «умный» холодильник использует ту же сеть, что и домашние телефоны, маршрутизаторы и компьютеры, то следует беспокоиться в случае взлома.

Киберпреступник, получивший доступ ко всей домашней сети, также будет иметь более легкий доступ к компьютерам и мобильным устройствам. Это позволит ему установить вредоносное ПО, которое может зашифровать важные пользовательские данные, чтобы потребовать выкуп за их восстановление или просто украсть.

Обеспечение безопасности «умного дома»

Некоторые города, ожидающие потенциальную обратную сторону цифрового преобразования, уже внедрили меры предосторожности. Во многих городах используются сертифицированные биометрические системы, криптография и политика в области цифровой конфиденциальности, что создает культуру кибербезопасности.

Признание необходимости начинать с кибербезопасности, а затем составлять бюджет на нее в рамках общей инициативы «умного города» может помочь избежать дополнительных расходов, когда система уже установлена. Как и в случае с IoT в потребительских продуктах, для подключенных к городу систем также требуются протоколы безопасности.

Чтобы обезопасить систему, необходимо в первую очередь повысить защищенность всех слабых звеньев. Например, выбрать безопасный способ передачи данных. Команда проекта провела анализ применяемых в подобных системах протоколов связи, по результатам этой работы выяснилось, что с точки зрения основных характеристик наилучшим выбором для таких систем является технология Zig-Bee. Этот протокол позволяет максимально повысить конфиденциальность, целостность и доступность данных.

ОСНОВНЫЕ КАНАЛЫ РАСПРОСТРАНЕНИЯ ВИРУСОВ

Рассмотрим основные возможные каналы распространения вирусов.

1. Сеть Bluetooth. Она является крайне ненадежной и легко может принять файл с вирусом от злоумышленника, не запросив авторизацию.

2. Сеть Wi-Fi. Такая сеть может быть легко взломана злоумышленником, который может, обойдя систему авторизации, передать вирус на сервер.

3. HTTP-канал для удаленного доступа. HTTP-обмен с сетью Интернет может быть одним из каналов попадания вируса в систему автоматизированного управления зданием. Множественные уязвимости программных продуктов, построенных на HTTP-протоколе, хорошо известны, но не закрыты.

4. GSM канал. Через канал GSM также возможно осуществить несанкционированное управление системой. Например, это можно сделать с помощью передачи SMS-сообщения с поддельным номером отправителя.

5. Сопряженные каналы. Если сервер системы «умный дом» подключен также и к локальной сети здания, то вирусная программа вполне может попасть из локальной сети.

6. Предустанавливаемое программное обеспечение и логические бомбы. Данный канал внедрения вирусов в серверное обеспечение системы «умный дом» подразумевает, что при установке такой системы злоумышленник, например, войдя в доверие к заказчику, устанавливает на сервере вирус самостоятельно. Доказать, что вирус установлен злонамеренно, практически невозможно. Обнаружить такой вирус также крайне сложно.

Следует отметить, что полноценных антивирусных систем, обеспечивающих комплексную защиту от вредоносного программного обеспечения, разработанных специально для систем «умный дом», не существует. Более того, программный код, свойственный вирусам для таких систем, не опознается большинством сканеров сигнатур. К основным уязвимостям в программном обеспечении систем «умный дом», которыми пользуются злоумышленники для внедрения вредоносных программ, относятся:

- отсутствие возможности блокировки подключений неавторизованных устройств;
- отсутствие контроля над широковещательной рассылкой датаграмм в сети системы «умный дом»;

- отсутствие проверки подлинности управляющей программы, передающей пакеты в сеть системы «умный дом».

На сегодняшний день вирусы для систем «умный дом» не могут быть опознаны по сигнатурам ни одним из существующих на данный момент антивирусов. Более того, в построении этих систем управления существует такая значительная уязвимость, как полное отсутствие контроля несанкционированных подключений к линиям передачи данных.

Выводы и рекомендации

Как можно видеть, при создании системы «умного» дома стоит быть предельно внимательным к компонентам и их уязвимостям. Все устройства, подключенные к системе, так или иначе подвержены риску взлома. Инсталляторам и администраторам, а также продвинутым пользователям таких систем можно посоветовать следующее:

внимательно изучите все возможности устройства: что оно делает, какие разрешения имеет, какую информацию получает и отправляет — отключите всё ненужное;

- регулярно обновляйте прошивку и встроенное ПО;

- используйте сложные пароли; везде, где можно, включайте двухфакторную аутентификацию;

- для управления «умными» гаджетами и системами используйте только те решения, что предлагают сами вендоры — это не гарантирует отсутствия брешей, но хотя бы снижает вероятность их появления;

- закрывайте все неиспользуемые сетевые порты, а открытые защищайте стандартными методами авторизации через стандартные настройки операционной системы; вход через пользовательский интерфейс, в том числе с веб-доступом, должен быть защищён с помощью SSL;

- «умное» устройство должно быть защищено от физического доступа посторонних.

Рекомендации менее опытным пользователям:

- не доверяйте чужим людям устройства, с помощью которых вы управляете «умным домом» — если потеряли смартфон или планшет, смените все логины-пароли-ID и прочие вещи, которые могут быть извлечены посредством утерянного гаджета;

- фишинг не дремлет: как и в случае с электронной почтой и мессенджерами, поменьше доверяйте сообщениям от незнакомцев и непонятным ссылкам.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: учебное пособие / Л.В. Астахова. – Челябинск, 2014. – 361 с.

2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита: учебное пособие.- М., Изд-во РИОР, Инфра-М.-2017.-324 с.

3. Барсуков В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М.: КУДИЦ – ОБРАЗ, 2016. – 496 с.

4. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов / В.И. Ярочкин - М.: Академический проект: Трикста, 2016. - 640 с.

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ ВОПРОСОВ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ «УМНЫХ ГОРОДОВ»

Плосконосов Даниил Алексеевич

Областное государственное бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»

Руководитель: Федорова Татьяна Викторовна

ВВЕДЕНИЕ

«Умный город» – сравнительно новая концепция благоустройства социального и экономического городского пространства. Цель внедрения технологии – улучшение условий жизни урбанизированного населения,

решение экологических, демографических проблем. В реализации таких программ помогают различные инновационные решения, чаще всего связанные с IT-сферой: цифровые метки, системы видеонаблюдения, централизованный общественный транспорт и т. д.

Мировые мегаполисы с каждым годом прилагают все больше усилий для создания по-настоящему умной среды жизни. Не отстают от них и большие российские города, в их числе Москва.

Умными в России считаются города, которые применяют инновационные подходы для улучшения условий окружающей среды и повышения уровня жизни населения.

Проблема исследования: внедрение технологии «умного города» влечет за собой множественные проблемы, одна из важнейших – проблема комплексной безопасности. Даже при реализации части отдельных технологий «умного города» вопрос о безопасности встает в полном объеме.

Цель работы: Использование современных технологий для решения вопросов комплексной безопасности «умных городов».

Методы исследования: анализ, синтез, изучение источников информации.

1. Современные стандарты для “Умного города”

В целях реализации пункта 1.13 раздела 4.3 паспорта национального проекта «Жилье и городская среда» , утвержденного в соответствующей редакции согласно протоколу заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 24 декабря 2018 г. № 16 и организации исполнения в Министерстве строительства и жилищно-коммунального хозяйства Российской Федерации паспорта ведомственного проекта по цифровизации городского хозяйства «Умный город», утвержденного приказом Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 27 декабря 2021 г. № 2014/пр.

Весьма вероятно, что «Приказ Минстроя России от 11 мая 2022 г. № 357/пр. Имеет непосредственное отношение к инициативе создания «национальной» версии международного стандарта ISO «Устойчивое развитие малых и средних городов», в разработке которого участвуют эксперты Технического Комитета (ТК) ISO ТК 465 «Строительство» и ООО «Русатом Инфраструктурные решения» совместно с ISO ТК 268 «Устойчивое развитие сообществ». Это направление стандартов делает акцент на потребителей-граждан, городское сообщество, а также на устойчивое развитие города.

Инициаторы разработки нового стандарта считают, что действующие стандарты:

ISO 37120:2014 «Устойчивое развитие сообщества. Показатели городских услуг и качества жизни» (идентичный ему ГОСТ Р ИСО 37120–2015 «Устойчивое развитие сообщества. Показатели городских услуг и качества жизни»).

ISO 37151:2015 «Интеллектуальные общественные инфраструктуры. Принципы и требования к системе рабочих показателей», а также находящиеся в разработке новые стандарты.

ISO 37122 «Устойчивое развитие в сообществах. Показатели для «умных городов».

ISO 37123 «Устойчивое развитие сообществ. Индикаторы для адаптивных городов» не в полной мере учитывают особенностей малых и средних городов, поэтому поставлен вопрос о разработке адаптированного стандарта.

С другой стороны, разработку национальных стандартов для «Умного города» начинал вести Технический комитет ISO ТК 194 «Кибер-физические системы», связанный с Российской венчурной компанией (РВК) и ДК «ТехНет» НТИ. Это направление стандартов связано с технологической, цифровой стороной «умного города».

2. Анализ технологий, которые делают города «умными»

Дата-центр

Благодаря единой базе данных появится возможность сопоставлять и применять различную информацию тогда, когда возникнет необходимость. В частности, при обращении в службу спасения будет известно местоположение человека, больница сможет получить данные из медкнижки пациента. В случае уличной стрельбы полиция сразу получит сигнал и изображение подозреваемого с камер наблюдения.

Универсальное городское приложение

Специализированная программа, основанная на концепции «умного города», может объединять в себе всю необходимую населению информацию. С ее помощью можно осуществить вызов такси, произвести оплату счетов, сообщить администрации о яме на дороге, выяснить, где в настоящий момент наблюдаются дорожные заторы, найти свободное место на парковке. Похожим приложением уже пользуются жители Чикаго.

Камеры

В Чикаго уличные фонари оборудовали камерами с высоким разрешением с целью обеспечить безопасность в многолюдных местах. В Сан-Антонио обустроили специальные будки с такими камерами, где могут отметиться судимые граждане без посещения здания суда.

Умный общественный транспорт

Технологии «умного города» предоставляют жителям не только интервалы движения общественного транспорта. К примеру, на московских остановках установлены специальные табло, отображающие время до прибытия нужного автобуса. «Яндекс.Транспорт» также отображает местоположение и перемещение автобусов, трамваев и т. д.

Противопожарные датчики

Принцип работы этих «умных» устройств не такой, как у классических датчиков дыма. В умные датчики помещены солнечные батареи. Чтобы огонь не успел перекинуться на соседние строения, с помощью встроенного

микрофона они ловят сигнал обычных датчиков и посредством модуля связи передают сообщение соседям и в пожарную службу.

Открытая информация

Концепция «умного города» предполагает открытый доступ к данным. Речь идет в том числе и о возможности обмена опытом, а также готовности предоставлять жителям города полученную информацию.

Мониторинг передвижений с помощью RFID

Система предполагает отслеживание объектов при движении с помощью радиочастотных меток (RFID) и беспроводных, мобильных или фиксированных сетей связи.

Эти метки можно прикрепить на форму, автомобили и инструменты работников обслуживающих инфраструктуру города компаний. Данная технология необходима умному городу: она позволяет вести учет и управлять доступом на объекты.

Движущиеся беспроводные сети

В процессе совершенствования беспроводной связи были разработаны движущиеся сети радиодоступа. Беспроводные точки размещают на общественном транспорте, такси, машинах коммунальных служб, беспилотниках.

В этом есть два важных преимущества: в транспортных средствах установлены бортовые источники питания, к которым подключаются эти устройства; кроме того, большое количество транспорта рассредоточено по всем автодорогам городских округов.

Взаимодействие движущихся точек доступа обеспечивает создание беспроводных самоорганизующихся сетей. Благодаря этому пассажиры могут использовать интернет, открывается доступ к данным, которые собирают бортовые датчики. Это позволяет оптимизировать маршруты, отслеживать местоположение общественного транспорта.

Контент для дополненной реальности

Такие цифровые технологии необходимы «умным городам». Возможность определения объекта и его параметров может быть полезно при строительстве, развитии муниципальной инфраструктуры, ее мониторинге. Данная технология позволяет идентифицировать объект, проанализировать его состояние, выявить потребность в ремонте или замене.

3. Практики внедрения стандартов и технологий безопасности в «умном городе»

Некоторые города, ожидающие потенциальную обратную сторону цифрового преобразования, уже внедрили меры предосторожности. Во многих городах используются сертифицированные биометрические системы, криптография и политика в области цифровой конфиденциальности, что создает культуру кибербезопасности.

Признание необходимости начинать с кибербезопасности, а затем составлять бюджет на нее в рамках общей инициативы «умного города» может помочь избежать дополнительных расходов, когда система уже установлена. Как и в случае с IoT в потребительских продуктах, для подключенных к городу систем также требуются протоколы безопасности.

Благодаря национальному институту стандартов и технологий недавно создана IoT с поддержкой смарт-городов для решения вопросов, связанных с кибербезопасностью, интеграции и обмена данными.

Слишком часто с IoT основное внимание уделяется преимуществам, при этом мало внимания уделяется рискам.

Создание политики в отношении конфиденциальности данных IoT и использования данных с самого начала может помочь предотвратить непреднамеренное неправильное использование. Надежная политика может помочь сотрудникам и пользователям стать более кибербезопасными.

Управление идентификаторами имеет решающее значение для всех подключенных систем. Каждый подключенный элемент инфраструктуры может иметь разные правила или стандарты для предоставления доступа, некоторые из которых слабее других. Синхронизируя учетные данные

доступа, устраняя таким образом слабые места, города могут помочь защитить личную информацию жителей.

Каждое подключенное устройство начинает генерировать данные с момента его подключения и каждую секунду после этого. Прежде чем система заработает, менеджеры «умного города» должны четко понимать масштабы собираемых данных, а также то, как они будут использоваться. Таким образом, оно может быть лучше защищено и надлежащим образом зашифровано с самого начала.

В настоящее время последствия для киберпреступлений ограничены и плохо определены. Санкции, штрафы должны быть обновлены, чтобы отразить последствия для нарушителей.

Каждый день злоумышленники пытаются найти еще неизвестные уязвимости в ИТ-подразделении организации. Непрерывное отслеживание этих проблем с внутренней (в рамках сети организации) и внешней точки зрения (из Интернета) является предпосылкой для обнаружения, отсутствующего или небезопасного шифрования.

Злоумышленник рано или поздно передаст данные. Это станет очевидным благодаря комплексному мониторингу безопасности всех систем, трафика данных и доступа ко всем чувствительным системам и данным. Передача данных с внутренних на внешние IP-адреса, с которыми не существует деловых отношений, должна незамедлительно выполняться и должна анализироваться экспертами. Это требует применения систем обнаружения вторжений и других инструментов, а также поддержки экспертов, которые правильно настраивают эти системы, адаптируют их к текущим условиям и анализируют их результаты.

ЗАКЛЮЧЕНИЕ

Хотя некоторые технологии «умного города» успешно применяются практически везде, полной реализации концепции удастся добиться нескоро. В РФ пока очень мало городов, в которых инфраструктура хотя бы на 2/3 соответствует принципам smart city. Конечно, такой масштабный проект не

может быть полностью реализован за короткое время. Важно, что у нашей страны есть все возможности для развития. Четкое следование к цели со временем приведет к тому, что мы будем жить в прогрессивных городах с инновационными технологиями.

Таким образом, можно сказать что в РФ полным ходом проводится переход на новые стандарты «умных городов», где жизнь людей будет намного лучше и безопаснее. Для этого применяются новые разработки в сферах IT и не только. Для «умных городов» были разработаны проекты, в которых самой главной целью является безопасность и комфортабельность жизни граждан. Говоря отдельно про безопасность граждан в «умном городе», хочется сказать, что профессионалы своего дела в разных сферах деятельности делают всё возможное для того, чтобы жизнь в «умном городе» была поистине прекрасна.

Список использованных источников и литературы

1.https://naukovedenie.ru/PDF/146EVN316.pdf

2.https://research-journal.org/archive/11-89-2019-november/cifrovaya-bezopasnost-umnyx-gorodov

3. https://dorians.ru/blog/umnyy-gorod/

4.https://vc.ru/future/82804-umnye-goroda-kakie-tehnologii-delayut-gorodskie-prostranstva-umnee

5. https://trasscom.ru/blog/umnyj-gorod

6. https://cyberleninka.ru/article/n/tsifrovaya-bezopasnost-umnyh-gorodov

НЕКОТОРЫЕ УЯЗВИМОСТИ В СИСТЕМЕ «УМНЫЙ» ДОМ

Никитин Данил Денисович, Ооржак Даваалан Алиевич

Областное государственное бюджетное профессиональное образовательное учреждение «Томский базовый медицинский колледж»

Руководитель: Фартушев Илья Викторович

Ключевые слова: цифровая безопасность, «умный» дом, уязвимости, данные, приватность, алгоритм, технологии, программное обеспечение. электронные системы.

Актуальность: довольно интенсивно на сегодняшний день в России, как и во всем мире, стала совершенствоваться концепция «умного» дома. Потенциал «умного» дома или квартиры огромны, а выгода, которую получает клиент, весьма значительна. К тому же, чтобы поддерживать комфорт, потребитель жилища бережет количество времени и материальные средства, потому что все функционирует на сохраняющих ресурсы режимах. Но в данной бочке мёда есть и большая ложка дёгтя. Цифровая безопасность оставляет желать лучшего, ведь всё, что связанны с цифрами можно взломать. Надеюсь, дальнейшие слова послужат доказательством данного выражения.

Цель нашей работы: рассказать о уязвимостях системы «умный дом» для тех, кто хочет ее приобрести или интересующихся.

Для начала стоит рассказать поподробнее про сам «умный» дом. Это не только роботы-пылесосы, умные кофеварки и голосовая колонка Алиса, которой можно давать команды. Это целая система, которая делает повседневную жизнь проще, и позволяет не переживать о незакрытой в спешке двери или не выключенном утюге. Эта система может сама принимать решения и выполнять определенные задачи, без участия человека. Вам остается лишь управлять дистанционно нажатием кнопок на пульте, гаджетах или голосовыми командами.

Представьте, вы просыпаетесь по сигналу умного будильника, для вас уже готов кофе и тосты, набрана ванна, играет приятная бодрая музыка. Вы уходите на работу, система ставит дом, на сигнализацию и вы можете дистанционно следить за тем, что происходит в доме.

Можно задать алгоритм, в соответствии с которым система будет включать или отключать разные приборы, бытовую технику, освещение, регулировать доступ в дом и выполнять другие важные функции. Иными

словами, умный дом подразумевает упрощение нагрузки в быту и делает дом удобным и комфортным.

Дыры в защите. В этой системе они есть и их довольно много, но мы пройдёмся по основным:

Наличие специально созданных уязвимостей в коде программы – «Бекдоров» оставленных разработчиками намеренно для получения данных о пользователе. И это очень серьёзная проблема, ведь эти бреши могут использоваться злоумышленниками для получения данных. С ними они могу получить доступ к системе, составить ваш распорядок дня, для успешного планирования кражи. С одной стороны, эту уязвимость устранить не просто, ведь чтобы понять ГДЕ, находится, а главное КАК залатать "Бекдор", нужна помощь специалиста, но, понятно, что это не очень хорошая идея. С другой стороны, это может и не являться проблемой вовсе, ведь разработчики программного обеспечения (ПО) могут не оставлять таких брешей, но не думаю, что это так.

Подключение к сети Интернет. Эта проблема частично связанна с предыдущей, но не полностью, поэтому мы посчитали нужным ее выделить. Помимо той же кражи данных, которую могут произвести через сеть, возможна и их подделка. Например, хакер подделал данные о состоянии вашей двери, и вы будете думать, что она закрыта, но это не так. Так же стоит выделить ещё одну опасную сторону данной бреши. Помимо кражи, они могут получить контроль над техникой, что в свою очередь позволяет настолько нагрузить систему, что может произойти возгорание. В этом случае возможны жертвы.

Отвлекаясь от столь тяжёлых дум, давайте лучше поговорим о электронной защите.

Электронные замки. Так как они электронные, то разные хакеры могут их взломать. Стоит выделить один способ обхода защиты такого замка. Как бы не было удивительно, но это голос. Подделать голос, для открытия замка, с современным оборудованием не составит труда. Надеюсь, столь очень краткое

пояснение показало небезопасность данной защиты, но думаю, лучше рассказать на примере, а также, показать ещё одну уязвимость электронных замков. Замок Tapplock открывающийся с помощью отпечатка пальца. Выяснилось, что API-сервер (API – это механизмы, которые позволяют двум программным компонентам взаимодействовать друг с другом, используя набор определений и протоколов. Например, система ПО метеослужбы содержит ежедневные данные о погоде. Приложение погоды на телефоне «общается» с этой системой через API и показывает ежедневные обновления погоды на телефоне) компании разглашает конфиденциальные данные пользователей. Любой посторонний человек может узнать не только о местонахождении замка, но и разблокировать его. Сделать это довольно просто: нужно завести аккаунт на Tapplock, взять ID аккаунта жертвы, пройти аутентификацию и захватить управление устройством. При этом на уровне back-end производитель не использует HTTPS. Даже не потребуется никакого взлома, потому что номера ID присваиваются аккаунтам по элементарной нарастающей схеме. Ягодка на торте — API не ограничивает количество обращений, поэтому можно бесконечно скачивать пользовательские данные с серверов, и эта проблема всё ещё не устранена.

К подобному можно отнести и Face ID. Просто показать чёткое видео с лицом человека и дверь откроется (конечно не всегда, но прецеденты были).

Упоминая о теме видео, не стоит забывать и о видеокамерах.

Общественные пространства современных мегаполисов обвешаны камерами. Причём они не просто получают живую картинку, но и разбираются в том, что на ней находится. Даже у нас в стране на ЧМ-2018 система распознавания лиц безошибочно отлавливала фанатов, которым был запрещён доступ на стадион.

Пока таким образом наша жизнь лишается какой-либо приватности, остаётся дожидаться, когда злоумышленники подберут ключи к камерам видеонаблюдения. И банальный вуайеризм будет не единственной и не

главной мотивация хакеров для взлома видеокамер. Часто, их ломают с целью создания ботнетов, используемых при проведении DDoS-атак.

Причин уязвимости у видеокамер несколько:

- слишком простой или морально устаревший механизм защиты;

- стандартные пароли, часто находящиеся в открытом доступе в интернете;

- при подключении к камерам через «облако» клиентские приложения шлют данные в незашифрованном виде;

- неизменяемый мастер-пароль от производителя.

Часто камеры атакуют методом man-in-the-middle, встраиваясь между клиентом и сервером.

Таким способом можно не только читать и изменять сообщения, но и подменять видеопоток. Особенно в тех системах, где не поддерживается протокол HTTPS.

Ещё одна угроза сохранности наших персональных данных кроется в «умных» телевизорах. Они теперь стоят почти в каждом доме. Причём ПО телевизора куда сложнее, чем у камер или замков. Следовательно, хакерам есть где разгуляться.

Допустим, на смарт-ТВ есть веб-камера, микрофон, а также веб-браузер, куда же без него? Как в таком случае могут навредить злоумышленники? Они могут воспользоваться банальным фишингом: встроенные в ТВ браузеры обычно слабо защищены, и можно подсунуть пользователю поддельные страницы, собирая пароли, информацию о банковских картах и прочие конфиденциальные данные.

Другой, в буквальном смысле, дыркой в безопасности является старый добрый USB. Скачали видео или приложение на ПК, воткнули потом флешку в телевизор – вот вам и зараза.

Кому может понадобиться знать, какие передачи пользователь смотрит и какие сайты посещает? Много кому, на самом деле. Аналитикам крупных корпораций, консалтинговых и рекламных компаний, например. И эта

информация стоит приличных денег, поэтому даже производители не брезгуют встраивать в свою продукцию приложения для сбора вашей статистики.

Угроза тут заключается в том, что данные пользователя могут уйти «налево» и попасть к злоумышленникам. Например, квартирный вор узнает, что с 9 утра до 18 вечера дома никого нет, так как у владельцев телевизора есть устойчивая привычка включать его, находясь дома. Соответственно, нужно отключить в настройках сбор лишней информации и прочее журналирование действий.

А такие закладки, как вы понимаете, это дополнительные бреши для проникновения. Известна история с телевизорами Samsung: пользователи жаловались на то, что встроенная система распознавания голоса позволяет следить за всеми их разговорами. Производитель даже указал в пользовательском соглашении, что слова, сказанные в присутствии телевизора, могут быть переданы третьей стороне. Как можно видеть, при создании системы «умного» дома стоит быть предельно внимательным к компонентам и их уязвимостям. Все устройства, подключенные к системе, так или иначе подвержены риску взлома. Инсталляторам и администраторам, а также продвинутым пользователям таких систем можно посоветовать следующее:

- внимательно изучите все возможности устройства: что оно делает, какие разрешения имеет, какую информацию получает и отправляет - отключите всё ненужное;

- регулярно обновляйте прошивку и встроенное ПО;

- используйте сложные пароли; везде, где можно, включайте двухфакторную аутентификацию;

- для управления «умными» гаджетами и системами используйте только те решения, что предлагают сами вендоры. Это не гарантирует отсутствия брешей, но хотя бы снижает вероятность их появления;

- закрывайте все неиспользуемые сетевые порты;

- «умное» устройство должно быть защищено от физического доступа посторонних.

Пользователям менее опытным? рекомендации такие:

- не доверяйте чужим людям устройства, с помощью которых вы управляете «умным домом» - если потеряли смартфон или планшет, смените все логины-пароли-ID и прочие вещи, которые могут быть извлечены посредством утерянного гаджета;

- фишинг не дремлет: как и в случае с электронной почтой и мессенджерами, поменьше доверяйте сообщениям от незнакомцев и непонятным ссылкам.

Перед окончанием стоит упомянуть и про исследовательскую часть данной темы. Мы провели ряд опросов среди своих одногруппников и получили следующие результаты:

1. Бывает ли вам скучно во время выполнения домашних дел? 50%- Да, 17%- Нет и 33%- Иногда.

2. У вас были ситуации, когда вы забыли что-то выключить и после этого произошло, что-то неприятное? 25%- Да, 75%- Нет.

3. Интересуют ли вас технологии "Умный дом"? 43%- Да, 57%- Нет.

4. Готовы ли вы платить за качественны и доступные решения в направлении «Умный» дом?. 57%- Да, 14%- Нет и 29%- Не задумывался.

5. Готовы ли вы приобрести робота помощника? 38%- Да, 37%- Нет, 25%- Не задумывался.

Цель нашей работы выполнена, надеемся информация была вам полезной.

Проблем при выполнении работы было не много, самая основная из них - заставить одногруппников пройти опросы.

Литература

1. Все публикации подряд/ Хабр - URL: https://habr.com/ru/company/trendmicro/blog/445538 Режим доступа: свободный – Текст: электронный.

2. Allbest – Выбери лучшее! - URL: https://otherreferats.allbest.ru/radio/00987600_0.html#text Режим доступа: свободный – Текст: электронный.

3. Вся недвижимость Москвы - URL: https://avaho.ru/articles/ns/umnyy-dom-chto-eto-takoe-zachem-nuzhen-i-kak-rabotaet-2332.html?ysclid=lajqgimqee784057486 Режим доступа: свободный – Текст: электронный.

4. Novainfo - URL: https://novainfo.ru/article/16545?ysclid=lalvhewxdj79942123 Режим доступа: свободный – Текст: электронный.

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ IOT ОБЪЕКТОВ

Михнюк Денис Алексеевич

Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум информационных технологий»

Руководитель: Смоляков Дмитрий Витальевич

Что такое IoT (Internet of Things)? В дословном переводе на русский это означает «Интернет вещей» так его везде и называют, но как по мне «интернет вещей» звучит не очень, для меня IoT в идеальной интерпретации на русский это «Интернет вещи» или хотя бы «Вещи интернета», ведь основная суть IoT-устройств, в том что они связанны с интернетом. Фитнес браслет, умный чайник, умная лампочка, станция «Алиса» от Яндекс, это все IoT-устройства.

С каждым годом восстание машин становится все более реальным, но не из-за чрезмерно быстро развивающихся Искусственных Интеллектов, а из-за быстро растущего количества IoT-устройств в нашей жизни. Большинство таких устройств имеют уязвимую прошивку и небезопасные или устаревшие компоненты, что в последствии может стать отличной «точкой входа» в систему устройства, для вируса или хакера и пока это не регулируется правительством, производители интернет вещей будут экономить на этом.

Так, например, в 2017 году вирус под названием «BrickerBot» вывел из строя более 2000 IoT-устройств и 60 000 модемов в Индии, тем самым он хотел показать незащищенность таких устройств и некоторых провайдеров. Сейчас место BrickerBot занял вирус «Silex», который направленно атакует Unix-системы и представляет опасность для серверов с операционной системой Linux.

Устройства интернет вещей собирают персональную информацию. И это не только логины и пароли, но и такие данные как отпечатки пальцев, голос, лицо, фото и другие биометрические данные. А с такими данными злоумышленники могут делать любые вещи от вашего лица, без вашего ведома.

IoT-устройства применимы в любой отрасли, где возможно автоматизирование. В сельском хозяйстве их применяют для улучшения качества и количества производимой продукции. От анализа почвы, до мониторинга состояния здоровья скота.

В здравоохранении устройства интернет вещей помогают выявлять и анализировать заболевания. Фитнес браслеты не единственные умные устройства, с помощью которых можно отслеживать показатели здоровья. Есть IoT-устройства, которые непрерывно мониторят уровень глюкозы владельца и отправляют информацию на смартфон, так же ей можно делиться с вашим лечащим врачом и членами семьи.

В городской среде IoT-решения позволяют управлять трафиком движения транспорта на дорогах, повысить уровень безопасности с помощью видеокамер, уменьшить количество ДТП и пробок, экономить на коммунальных услугах, путем отслеживания нужного количества электроэнергии, газа, воды. Можно использовать светофоры и камеры с датчиками, детекторы дорожного движения.

В промышленности IIoT-устройства (Industrial Internet of Things) подключаются к различным станкам и имеют выход в интернет, отслеживают состояние станков, количество изготовленных деталей и т. Так же устройства

IoT и IIoT используют для анализа и выявления неисправностей в двигателях и прочих сложных устройствах.

В электроэнергетике интернет вещей позволяет рационально распределять ресурсы и контролировать состояние оборудования. С помощью IoT можно дистанционно мониторить подстанции и линии электропередач.

Рынок интернет вещей это информационное месторождение нефти, золотая жила, ведь по данным аналитиков в сфере интернет вещей к 2025 году количество IoT-устройств в мире будет равняться 34 миллиарда единиц, а оценочная стоимость рынка будет 1,5 триллиона долларов.

И конечно это «Не паханные поля» для злоумышленников и факторы для их развития в этой сфере очень заманчивы.

Самый очевидный источник уязвимости IoT - это люди, которые ими пользуются. Простота использования IoT-устройств приводит к тому, что пользователи думают, что обычные бытовые приборы и не изучают приложенных к ним инструкции и даже не думают о том, что нужно изменить настройки поставленные на заводе. Взломать устройство с заводскими паролями для злоумышленника дело нескольких секунд.

Так же у производителей имеются проблемы при использовании IIoT. В начале этого года стало известно о семи серьезных уязвимостях, выявленных в ThingsPro Suite шлюзе IIoT и менеджере устройств, разработанном компанией Moxa. Задача ThingsPro Suite сбор данных с устройств технологической сети. Используя ошибки в прошивке, хакеры могут получить административный доступ к шлюзу и выполнять на нем любые команды.

Стремясь сделать применение IoT как можно более понятным, разработчики автоматизируют установку обновлений прошивки устройства. Конечно простота процедуры делает возможным замену исходного файла прошивки вредоносным. После установки обновления, которое было заменено, устройство может выйти из

строя или перейти под чужой контроль. Но в тоже время это позволяет своевременно устранять выявленные недоработки и уязвимости.

Компрометируя устройства IoT и IIoT, киберпреступники преследуют вполне понятные цели, связанные с коммерческим использованием захваченных ресурсов. Наиболее популярные варианты создание ботнетов для анонимной рассылки спама, организации DDoS-атак и распространения вредоносного ПО, промышленного шпионажа.

Подмена DNS это кибератака, с помощью которой хакер направляет трафик жертвы на вредоносный сайт. Злоумышленники используют метод «отравления» кэша DNS для перехвата интернет-трафика и кражи учетных данных или конфиденциальной информации. Отравление кэша DNS и подмена DNS синонимичные понятия. Хакеры хотят обманом заставить пользователей ввести личные данные на небезопасном сайте. Как у них это получается? С помощью отравления кэша DNS. Для этого хакеры подменяют или заменяют данные DNS для определенного сайта, а затем перенаправляют жертву на сервер злоумышленника вместо легитимного сервера. Таким образом хакеры добиваются своей цели, ведь перед ними открываются широкие возможности: они могут совершить фишинговые атаки, украсть данные или даже внедрить в систему жертвы вредоносные программы.

Большая часть IoT-устройств работает под управлением ОС Unix или Linux, богатый функциональность которых позволяет установить дополнительные компоненты.

Чтобы оставаться незамеченными хакеры устанавливают прокси-сервера SOCKS, который позволяет использовать устройство в качества анонимайзера и в последствие устраивать массовые рассылки спама и взламывать корпоративные сети. Самый популярный способ использования взломанных IoT-устройств организация ботнетов для проведения распределенных атак на отказ в обслуживании (DDoS). Эту задачу хакерам упрощают несколько факторов:

Все устройства IoT/IIoT подключены к интернет-каналу, часто с весьма высокой пропускной способностью. Протокол CoAP, который используется для взаимодействия с различными устройствами интернет вещей, идеален для организации DDos: он использует протокол UDP без установки соединения и предполагает отправку пакета данных в ответ на запрос.

IoT-устройства присутствуют во всех сферах человеческой деятельности, окружают нас дома и на работе. В этих обстоятельствах под угрозой оказываются практически все: от простых граждан до глав государств и прочих важных людей, в стороне не остались так же и различные компании, будь то небольшое ИП или огромная компания по международной торговле.

Захватив контроль над кардиостимулятором, преступники могут шантажировать родственников пациента, а организовав ботнет из умных лампочек заглушить все Wi-Fi-сети в городе. Учитывая эти обстоятельства, всем компаниям, использующим бытовые и промышленные IoT-устройства, необходимо уделять больше внимания к защите таких устройств. Рекомендации для бизнеса:

- Изучить актуальные новости информационной безопасности и отказаться от устройств, в которых обнаружены неустранимые уязвимости (например, пароль, который невозможно изменить).
- Придерживаться принципа «безопасность важнее стоимости».
- Организовать фильтрацию интернет-трафика к IoT-устройствам и от них, чтобы исключить возможность несанкционированного подключения.
- Запретить службам удаленного администрирования и доступ к ним из интернета.
- Регулярно обновлять прошивку на устройствах до актуальных версий из официального источника.
- Менять пароли по умолчанию и включать доступные настройки безопасности.

- Обратиться к специалистам для поиска уязвимостей используемых в компании.

Использование незащищенных устройств может нанести непоправимый финансовый и репутационный ущерб, который будет значительно больше разницы в стоимости на обеспечение безопасности компании.

Как итог могу сказать, что Io-устройства – это будущее, от прогресса ни куда не деться, технология эта весьма нужная и полезная не смотря на ее потенциальную небезопасность, умные станции дома, IIoT-станки на производстве очень экономят время и ресурсы, что с каждым годом становиться лишь актуальнее.

БЕЗОПАСНОСТЬ СИСТЕМЫ «УМНОГО ДОМА»

Никитин Никита Владимирович
Шералиев Рустам Антонович
Областное государственное бюджетное
профессиональное образовательное учреждение
«Томский индустриальный техникум»
Руководитель: Петруша Мария Анатольевна

Актуальность: одно из наиболее перспективных направлений развития технологий – это Интернет вещей, а «умный дом»– его особенно приоритетная сфера. Возможность комплексно решить вопрос автоматизации инженерных систем, освобождение времени, которое раньше тратилось на рутинные бытовые процессы – все это серьезно повышает качество жизни, делает ее более благоустроенной и современной. С «умным домом» наша жизнь станет более беззаботной и комфортной. Однако у всякой медали есть и обратная сторона. В интернете много опасностей, и все устройства, подключенные к сети, становятся уязвимыми.

Цель: изучить систему «умный дом».

Задачи:

1. познакомиться с научной литературой по теме;

2.определить каким типам киберугроз подвергается система «умный дом»;

3. рассмотреть средства безопасности система «умный дом»;

4. сделать выводы и рекомендации.

Объект исследования: «умный дом».

Метод работы:

— анализ литературных источников;

— теоретические;

— наблюдение;

— обобщение полученных результатов.

Подбор материала по выбранной теме: Интернет-источник, научная и дополнительная литература.

История появления «умного дома»

Домашняя автоматизация (англ. home automation), или «умный дом»» (англ. smart house) — система домашних устройств, способных выполнять действия и решать определённые повседневные задачи без участия человека.

История возникновения «умного дома» зародилась в начале 60-х годов, когда появился на свет диммер — прибор для регулировки яркости света. Авторами этого приспособления стала чета Спира. Это было первым шагом к реализации идеи автоматизации дома.

В 70-х годах некоторые богатые граждане Соединённых Штатов задумались о том, как сделать свою жизнь комфортнее. Тогда и появилась идея передачи информации для управления приборами по одному кабелю. Учитывая, что именно в этот период технологии шагнули далеко вперед, каждое новое кабельное внедрение устаревало еще до того, как здание переходило в эксплуатацию.

В 1987 году в СССР был разработан проект радиоэлектронного оснащения жилища «СФИНКС», по своей сути напоминающий идею современного «умного дома». Главной изюминкой проекта был главный центральный процессор, состоящий из нескольких блоков, а также пульты управления — «малый» пульт со съемным дисплеем и большой с псевдосенсорными клавишами. Как ручной, так и большой пульт содержали микрофоны управления голосом.

Однако в России «умными» называют чайники, утюги, холодильники — вообще любую технику с немного расширенным функционалом. Классический «умный дом» — это набор гаджетов, которые автоматизируют те или иные действия в доме. Самый простой пример — включение и выключение света в определенное время. Более сложный — активация камеры безопасности при открытии входной двери. Совсем сложный — включение и выключение обогревателя и управление окнами и шторами при достижении определенной температуры.

Согласно дорожной карте Москвы до 2030 года – «умный дом» является одним из направлений развития «умного города».

«Умный город» (Smart city) – это взаимосвязанная система коммуникативных и информационных технологий с интернетом вещей, благодаря которой упрощается управление внутренними процессами города и улучшается уровень жизни населения.

Принцип работы «умного дома»

Устройства Интернета вещей имеют доступ к сети, и внутри них есть небольшой встроенный компьютер. В современном доме такими свойствами могут обладать как обычные бытовые приборы (например, кофеварка), так и целые системы (например, отопление).

Они используют интернет-протокол для связи и подключаются к единому центру управления (контроллеру). Это может быть, например, роутер или смартфон.

В отличие от пульта для телевизора контроллер собирает информацию об использовании устройства, о ваших привычках и предпочтениях. Такие данные могут храниться на самом устройстве либо в сети. Чем больше устройств «умном доме», тем больше информации о хозяине он запоминает. А ведь это конфиденциальные данные, которые преступники могут использовать в своих целях.

Поэтому при создании «умного дома» нужно учесть, что его устройства могут быть уязвимы.

Типы киберугроз для «умного дома»

«Умный дом» подвержен сразу нескольким типам киберугроз.

Во-первых, отдельные устройства могут быть небезопасны сами по себе. Некоторые производители стараются как можно быстрее продвигать на рынок новые IoT-устройства и не слишком заботятся об их безопасности. В некоторых руководствах пользователя нет информации о конфиденциальности данных или о безопасности устройства. А ведь киберпреступники часто взламывают, например, «радионяни» и камеры, чтобы наблюдать за происходящим в доме.

Многие эксперты полагают: имеет смысл заранее продумать, что делать, когда вашу IoT-технику взломают. Именно «когда», а не «если»: большинство устройств Интернета вещей защищено очень слабо, и злоумышленники легко могут получить к ним доступ.

Во-вторых, Wi-Fi тоже может быть защищен не очень надежно. Если злоумышленники получат доступ к нему, у них окажутся все данные, которые ваши контроллеры хранят в сети. А это ценная информация для преступника. Данные об использовании устройств в доме, например, покажут ему, когда хозяина обычно нет дома.

Допустим, Wi-Fi в доме управляется из основной учетной записи в интернете. В этом случае риску подвержены не только данные, которые собирали ваши IoT-устройства. Взломав домашнюю сеть, преступники могут

добраться до электронной почты хозяина, аккаунтов в соцсетях и даже до учетных записей в платежных системах.

Многие управляют «умным домом» со смартфона. Он автоматически становится ценным источником данных для злоумышленников. Если смартфон взломают, украдут или будут прослушивать, личные данные окажутся в большой опасности. То есть всего одно уязвимое IoT-устройство может поставить под угрозу личную информацию, которая хранится в домашней сети.

Обеспечение безопасности «умного дома»

Первый шаг – создать отдельную сеть для устройств умного дома. Это довольно просто: нужно просто настроить для них гостевые сети. Это не защитит само IoT-устройство: холодильник по-прежнему можно будет взломать и сделать частью ботнета, который рассылает спам или майнит криптовалюты. Но преступники не смогут добраться до электронной почты или банковского счета – ведь взломанный холодильник хранит данные в гостевой сети, из которой нельзя попасть в домашнюю.

Второй шаг – защитить все устройства, которые обрабатывают данные: умные колонки, роутер, компьютер, смартфон и другую умную технику. Если смартфон взломают или украдут, вся домашняя сеть может быть скомпрометирована. А ее безопасность – главный приоритет. Чтобы защитить смартфон, необходимо приобрести надежное защитное решение для Android или для устройств на базе iOS.

— Необходимо установить блокировку экрана на смартфоне, чтобы никто не мог воспользоваться им, пока хозяев нет.

— Поставить пароль на все компьютеры и мобильные устройства, используя надежные пароли, которые трудно подобрать. Нежелательно использовать комбинации слов и цифр, которые легко угадать (например, имя или дата рождения).

— Необходимо убедиться, что основная учетная запись на компьютере не корневая и не имеет прав администратора. Даже если хакер проникнет в компьютер, он мало что сможет сделать без прав администратора.

— Нужно поменять имя пользователя и пароль, заданные по умолчанию на роутере, изменить учетные данные роутера, это не позволит злоумышленникам войти в домашнюю сеть. Для защиты Wi-Fi необходимо использовать протокол шифрования WPA.

— Использовать сетевые экраны на всех компьютерах и на роутере. В большинстве маршрутизаторов есть встроенный сетевой экран, но, чтобы он заработал, пользователь должен включить его.

— Если роутер недостаточно защищен, лучше заменить его более надежным.

— Использовать надежное защитное решение на всех компьютерах и мобильных устройствах, чтобы на них не попали вирусы и вредоносные программы. Установить антивирус «Лаборатории Касперского» или пакет Total Security – решение для защиты всего умного дома от киберугроз.

— Всегда устанавливать актуальные исправления безопасности и обновления. В устаревшем программном обеспечении есть уязвимости, которыми легко могут воспользоваться хакеры.

Необходимо учитывать, что при подключении к публичному Wi-Fi с ноутбука или телефона существует риск утери данных даже при соблюдении всем советам, которые написаны выше. Если сеть не требует авторизации, в нее беспрепятственно смогут войти хакеры. Поэтому при регулярном использовании публичного Wi-Fi, необходимо включать VPN (Virtual Private Network), чтобы защитить умный дом и личные данные.

Обеспечение безопасности отдельных устройств «умного дома».

— Необходимо поменять все пароли, установленные по умолчанию. Пока стоит пароль, установленный по умолчанию, любой обладатель такой же модели сможет получить доступ к вашему устройству.

— Менять пароли целесообразно раз в полгода: это сильно повышает уровень защиты.

— При пользовании устройствами, которые управляются голосом (например, умные колонки), необходимо поменять фразу активации «*OK Google*» или «*Hey Alexa*». Новая фраза должна быть известна только пользователю или членам его семьи, тогда посторонний не сможет воспользоваться системой.

— Прежде чем приобретать новое устройство, нужно найти информацию о его уровне безопасности. Например, выпускает ли производитель регулярные обновления прошивки. В мире Интернета вещей полгода – уже довольно большой срок, ведь новые угрозы появляются постоянно. При покупке устройства, которое должно прослужить десяток лет, нужно быть уверенным в его безопасности.

— Приобретать устройства известных производителей с хорошей репутацией, например, Samsung, LG, Google или Amazon.

— Перед покупкой устройства ознакомиться с политикой конфиденциальности. Как производитель собирается распоряжаться личными данными пользователей? К какой информации будет иметь доступ это устройство? В случае, если голосовая активация не используется, отключить микрофон: так никто не сможет подслушивать и транслировать разговоры.

— Не забывать обновлять устройства с помощью автоматического обновления или вручную. Возможно, их нужно будет скачивать на компьютер с сайта производителя. Хакеры постоянно изобретают новые способы компрометации IoT-техники. При установке исправлений устройство будет защищено от свежих угроз.

— Определить, какие устройства действительно нужно подключать к сети. Если возможности кофеварки или плиты, для которых нужен интернет, не используются, лучше и дальше пользоваться ими автономно.

— Отключить Universal Plug & Play (UPnP). Почти вся IoT-техника поддерживает эту возможность: она позволяет находить похожие устройства и подключаются к ним. Однако протоколы UPnP уязвимы для внешних атак. Взломав одно устройство умного дома, преступник может получить контроль и над другими.

— Проверить разрешения приложений, запущенных на устройствах. Все приложения, которые запрашивают разрешение на изменение настроек роутера, – потенциальная угроза безопасности.

— С осторожностью относиться к облачным хранилищам. Для загрузки и выгрузки данных IoT-устройству нужно подключение к облаку. Это хранилище можно взломать и получить доступ к индивидуальной сети. Если все же используются облачные технологии, необходимо позаботиться о защите конфиденциальности и сохранности данных.

Необходимо помнить, что каждое новое устройство – еще одна лазейка в сети, ею могут воспользоваться незваные гости.

Используемая литература:

1. Безопасность «умных» домов https://www.kaspersky.ru/resource-center/threats/how-safe-is-your-smart-home

2. Системы безопасности «умного» дома https://www.eremont.ru/enc/engineer/clever/security-system-smart-home.html

3. Все про «умный» дом https://avaho.ru/articles/ns/umnyy-dom-chto-eto-takoe-zachem-nuzhen-i-kak-rabotaet-2332.html

НЕГОТОВНОСТЬ СЕТЕЙ ИНФРАСТРУКТУРЫ К МОЩНЫМ DOS/DDOS-АТАКАМ

Краснов Константин Дмитриевич

Областное государственные бюджетное профессиональное образовательное учреждение «Томский механико-технологический техникум»

Руководитель: Самия Салим Викторович

Введение

В наши дни у многих компаний основной бизнес-процесс связан с сервисами, которые должны быть постоянно доступны клиентам, это могут быть веб-сайты, личные кабинеты, облачные хранилища и т.п.

И все они подвержены Dos/DDos-атакам. Что вообще значит Dos/DDos-атака, она переводится как Distributed Denial of Service или же хекерская атака на сервер с целью вывести его из строя.

После это атаки, доступ на сервер затруднён или вообще не доступен некоторое время. В настоящее время Dos/DDos-атаки наиболее популярны, так как могут позволяют довести до отказа практически любую плохо написанную систему3 не оставляя юридически значимых улик.

Цели и задачи исследования:

- Узнать актуальность Dos-атак в 2022 году;
- Понять в чём разница Dos и DDos атак;
- Общая защита от атак;
- Понять причины их использования Dos/DDos-атак;
- Узнать классификацию Dos/DDos-атак;
- Как их выявить;
- Как защититься от Dos/DDos-атак;
- Самые крупные Dos/DDos- атаки.
- Источники

Актуальность Dos/DDos-атак в 2022 году

В 2022 году актуальность Dos/DDos-атак ни кдуа не исчезла, до сих поо многие корпорации, бизнес как большие, так и малые и даже страны подаержены им. В 2022 году основная чать атак приходилась на США, меньше же всего пострадал Сингапур. 16,35% атак проводиль в всокресенье. Почти 90% атак длились меньше 4 часов, а самая долга атака длилась 549 часов, чуть менее 23 суток. Так же, основная чать Dos/DDos-атак производилась из Китая.

Основаня аткивность была в январе этого года, 2.250 атак, основной вид атак был UPD.

В чём разница Dos и DDos-атак?

Отличие Dos от DDos в количестве задействованных устройств.

В случае классической Dos для атаки одной цели используется одно устройство. DDos-атака, как правило используется несколько устройств для атаки цели, распределяя по ним большое количество атакующих операций.

Общая защита от атак

Для общей защиты от сетевых атак применяются сетевые фильтры, подключаемых к интернет каналу с большой пропускной способностью. Фильтры анализируют проходящий трафик и выявляют нестандартную активность сети и ошибки. В нестандартную активность входят все неизвестные на сегодняшний день методы атак. Фильтры могут реализоваться на уровне маршрутизаторов, управляемых свичей, так и специализированными аппаратными средствами.

Причины спользования Dos/DDos- атак

Специалисты в области защиты информации выделяют несколько причин использования Dos/DDoS-атак.

- **Личня неприязнь:**
  - Эта причина нередко служит поводом для атак на крупные коммерческие и правительственные организации и компании. Так в 1999 году были атакованы Web-узлы ФБР, которые впоследствии были недоступны в течение нескольких недель. Мотивом послужил недавний рейд ФБР против хакеров.
- **Развлечение:**
  - В настоящее время всё больше людей интересуются DoS-атаками, и все хотят попробовать себя в этом деле. Поэтому многие начинающие злоумышленники осуществляют DoS-атаки ради развлечения. После успешно проведённого нападения они смотрят масштабы своих разрушений.
- **Политический протест:**

- Эта причина используется чаще выборах, чтобы помочь кому-то из кандидатов выбиться по очкам. Реже же используется для обрушения экономики какой-либо страны.

- **Недобросовестная конкуренция:**
  - Осуществляются по зкаказу каких либо компаний, для устранения конкурентов.

- **Вымогательство или шантаж:**
  - В настоящее время всё больше людей интересуются DoS-атаками, и все хотят попробовать себя в этом деле. Поэтому многие начинающие злоумышленники осуществляют DoS-атаки ради развлечения. После успешно проведённого нападения они смотрят масштабы своих разрушений

Классификация Dos/DDos-атак

Хакеры разделили Dos/DDos-атаки на множество разных типов, чтобы знать какую и когда атаку применять. Есть 4 основных вида атак, это:

- **HTTP-флуд и ping-флуд**
- **Smurf-атака (ICMP-флуд)**
- **Атака Fraggle (UDP-флуд)**
- **Атака с помощью переполнения пакетами SYN (SYN-флуд)**

HTTP-флуд и ping-флуд - Это самый примитивный вид DoS-атаки. Насыщение полосы пропускания можно осуществить с помощью обычных ping-запросов только в том случае, если канал атакующего намного шире канала компьютера-жертвы. Но такая атака бесполезна против сервера, так как тот, в свою очередь, обладает довольно широкой полосой пропускания. Для атаки на сервер обычно применяется HTTP-флуд. Атакующий шлёт маленький по объёму HTTP-пакет, но такой, чтобы сервер ответил на него пакетом, размер которого в сотни раз больше. Для того, чтобы ответные HTTP-пакеты не отказали у хакера, он каждый раз подменяет свой ip-адрес на ip-адреса узлов в сети.

Smurf-атака (ICMP-флуд) - один из самых опасных видов DoS-атак, Злоумышленник использует широковещательную рассылку для проверки работающих узлов в системе, отправляя ping-запрос. Очевидно, атакующий в одиночку не сможет вывести из строя компьютер жертвы, поэтому требуется ещё один участник — это *усиливающая сеть*. В ней по широковещательному адресу злоумышленник отправляет поддельный ICMP пакет. Затем адрес атакующего меняется на адрес жертвы. Все узлы пришлют ей ответ на ping-запрос. Поэтому ICMP-пакет, отправленный злоумышленником через усиливающую сеть, содержащую 200 узлов, будет усилен в 200 раз. Для такой атаки обычно выбирается большая сеть, чтобы у компьютера-жертвы не было никаких шансов

Атака Fraggle (UDP-флуд) - Атака Fraggle является полным аналогом Smurf-атаки, где вместо ICMP пакетов используются пакеты UDP, поэтому её ещё называют UDP-флуд. Принцип действия этой атаки простой: на седьмой порт жертвы отправляются echo-команды по широковещательному запросу. Затем подменяется ip-адрес злоумышленника на ip-адрес жертвы, которая вскоре получает множество ответных сообщений. Их количество зависит от числа узлов в сети. Эта атака приводит к насыщению полосы пропускания и полному отказу в обслуживании жертвы.

Атака с помощью переполнения пакетами SYN (SYN-флуд) - До появления атаки Smurf была широко распространена атака с помощью переполнения пакетами SYN, также известная под названием SYN-флуд. Как она работает: Хакер с системы A отправляет пакет SYN системе B, но предварительно поменяв свой IP-адрес на несуществующий. Затем, ничего не подозревая, компьютер B отправляет ответ SYN/ACK на несуществующий IP-адрес и переходит в состояние SYN-RECEIVED. Так как сообщение SYN/ACK не дойдет до системы A, то компьютер B никогда не получит пакет с флагом ACK. Данное потенциальное соединение будет помещено в очередь. Из очереди оно выйдет только по истечении 75 секунд. Этим пользуются злоумышленники и отправляют сразу несколько пакетов SYN на компьютер

жертвы с интервалом в 10 секунд, чтобы полностью исчерпать ресурсы системы. Определить источник нападения очень непросто, так как злоумышленник постоянно меняет исходный IP-адрес.

Выявление Dos/DDos-атак

В основном Dos/DDos-атаки невозможно не заметить, однако наблюдались довольно удачные атаки, их последствия замечали только через 2-3 дня. Флуд-атаки обычно находились после того, как пользователю приходил большой счёт за интернет. Кроме того, многие методы обнаружения атак неэффективны вблизи объекта атаки, но эффективны на сетевых магистральных каналах. В таком случае целесообразно ставить системы обнаружения именно там, а не ждать, пока пользователь, подвергшийся атаке, сам её заметит и обратится за помощью.

Есть три метода обнаружения Dos/DDos- атак:

Сигнатурные — основанные на качественном анализе трафика.

Статистические — основанные на количественном анализе трафика.

Гибридные — сочетающие в себе достоинства обоих вышеназванных методов.

Защита от Dos/DDos-атак

Полностью защититься от Dos/DDoS-атак на сегодняшний день невозможно, так как совершенно надёжных систем не существует. Здесь также большую роль играет человеческий фактор, потому что любая ошибка системного администратора, неправильно настроившего маршрутизатор, может привести к весьма плачевным последствиям.

Меры противодействия Dos/DDoS-атакам можно разделить на пассивные и активные, а также на превентивные и реакционные:

- **Ответные меры:** Применяя технические и правовые меры, нужно как можно активнее воздействовать на источник и организатора Dos/DDoS-атаки. В настоящее время даже существуют специальные фирмы, которые

помогают найти не только человека, который провел атаку, но даже и самого организатора.

- **Программное обеспечение.** На рынке современного программного и аппаратного обеспечения существует и такое, которое способно защитить малый и средний бизнес от слабых Dos/DDoS-атак.
- **Фильтрация и блэкхолинг.** Блокирование трафика, исходящего от атакующих машин. Эффективность этих методов снижается по мере приближения к объекту атаки и повышается по мере приближения к атакующей машине. В этом случае фильтрация может быть двух видов: использование межсетевых экранов и списков ACL. Использование межсетевых экранов блокирует конкретный поток трафика, но не позволяет отделить «хороший» трафик от «плохого». ACL списки фильтруют второстепенные протоколы и не затрагивают протоколы TCP. Это не замедляет скорость работы сервера, но бесполезно в том случае, если злоумышленник использует первостепенные запросы.
- **Обратный DDOS:** перенаправление трафика, используемого для атаки, на атакующего. При достаточной мощности атакуемого сервера позволяет не только успешно отразить атаку, но и вывести из строя сервер атакующего.
- **Устранение уязвимостей:** Не работает против *флуд*-атак, для которых «уязвимостью» является конечность тех или иных системных ресурсов. Данная мера нацелена на устранение ошибок в системах и службах.
- **Наращивание ресурсов:** Абсолютной защиты, естественно, не дает, но является хорошим фоном для применения других видов защиты от DDoS-атак.
- **Рассредоточение:** Построение распределённых и дублирование систем, которые не прекратят обслуживать пользователей, даже если некоторые их элементы станут недоступны из-за DoS/DDos-атаки.

- **Уклонение:** Увод непосредственной цели атаки подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью атаки.
- **Активные ответные меры:** Воздействие на источники, организатора или центр управления атакой, как техногенными, так и организационно-правовыми средствами.
- **Использование оборудования для отражения Dos/DDoS-атак:** Например, DefensePro® (Radware), SecureSphere® (Imperva), Периметр (МФИ Софт), Arbor Peakflow®, Riorey, Impletec iCore и от других производителей. Устройства развёртываются перед серверами и маршрутизаторами, фильтруя входящий трафик.
- **Приобретение сервиса по защите от DDoS-атак.** Актуально в случае превышения флудом пропускной способности сетевого канала.

Самые крупные Dos/DDos-атаки

- **2012 год - Атака на Банки Америки**
  - под обстрел попали сразу 6 банков – Bank of America, JPMorgan Chase, US Bank, Citigroup, Wells Fargo и PNC Bank. Злоумышленники использовали разные способы, проверяя, от какого типа атаки банки менее всего защищены.
- **2017 год - Атака на Google**
  - сервисы Google работали без сбоев, данные пользователей не пострадали.
  - На данный момент это самая мощная DDoS-атака в истории. По данным Google Threat Analysis Group (TAG), источником атаки был Китай. Аналитики возложили ответственность за нее на «правительственных хакеров».
  - Атака мощностью 2.54 Тбит/с стала кульминацией полугодичной кампании, которую хакеры вели против Google. В течение 6 месяцев злоумышленники использовали разные методы в попытках подорвать работу инфраструктуры корпорации.

- **2020 год - Атака клиента Amazon Web Services**
  - Представители Microsoft сообщили, что атака продолжалась 9 минут и велась силами примерно 70 000 устройств из Азиатско-Тихоокеанского региона. Были замечены хосты из Малайзии, Вьетнама, Тайваня, Японии, Китая, США.
- **2007 год – Атака на Эстонию**
  - пострадала торговля – были проблемы с кассовым, платежным оборудованием, системы работали со сбоями. Злоумышленники практически вывели из строя электронные почтовые сервисы, каналы передачи информации были забиты спамом.
  - Исчерпывающей информации о мощности атаки нет. Но поражает другое – время активности атакующих. Около 3 недель ботнеты рассылали огромные объемы спама, заваливая эстонскую сеть запросами.

Источники

SECURELIST: https://securelist.ru/ddos-attacks-in-q1-2022/105045/

Комьюнити: https://timeweb.com/ru/community/articles/samye-gromkie-ddos-ataki-v-istorii

ВикипедиЯ: https://ru.wikipedia.org/wiki/DoS-атака

РБК: https://trends.rbc.ru/trends/industry/62a758bf9a794772a846f917

CISOCLUB: https://cisoclub.ru/top-5-problem-setevoj-bezopasnosti-v-2022-godu-i-varianty-borby-s-nimi/

StromWall: https://stormwall.pro/knowledge-base/termin/ddos-protection

СЕКЦИЯ 3. ЗАЩИТА ПРАВ И ИНТЕРЕСОВ ГРАЖДАН В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

МЕТОДЫ ИДЕНТИФИКАЦИИ ПОДДЕЛЬНЫХ ДОКУМЕНТОВ И ДЕНЕЖНЫХ ЗНАКОВ, ПРИМЕНЯЕМЫЕ В ОТРАСЛИ ПОЧТОВОЙ СВЯЗИ

Максименкова Анастасия Викторовна
Областное государственные бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»
Руководитель: Ротару Алеся Семеновна

Введение

Тема: Методы идентификации поддельных документов и денежных знаков, применяемые в отрасли почтовой связи.

Актуальность: подделка документов и денежных знаков очень распространена в России. В современном обществе постоянно появляются новые и все более эффективные методы подделки и распространения этих предметов.

Гипотеза: я предполагаю, что почтовая связь использует методы идентификации поддельных документов и денежных знаков.

Цель: изучить методы идентификации поддельных документов и денежных знаков, применяемые в отрасли почтовой связи.

Задачи:

1. Подобрать литературу и отобрать необходимую информацию по данной теме.
2. Обработать полученную информацию, систематизировать полученные знания.

3. Представить результат проделанной работы в виде исследовательской работы.

Объект исследования: отрасль почтовой связи.

Предмет исследования: методы идентификации подлинных документов и денежных знаков.

Метод исследования: теоретический метод: аналогия; индукция; классификация; изучение и анализ источников.

Практическая значимость исследовательской работы: распространение знаний об элементах защиты банкнотных изделий и ценных бумаг от подделки.

1. Понятия «подделка документа» и «подделка денежных знаков»

Подделка документа — это изготовление полностью фальсифицированного документа, либо частичное фальсифицирование реквизитов подлинного документа путём внесения в текст документа заведомо недостоверных сведений, исправлений, фальсификация подписей или иных реквизитов документа.

Подделка денежных знаков – это изготовление с целью выпуска в обращение или сбыта в виде промысла поддельной металлической монеты, денежных знаков, государственных ценных бумаг.

2. Основные методы идентификации подделки документов

Подчистки: заключается в механическом удалении части текста, путем стирания резинкой или выскабливания острым предметом с нарушением поверхностного слоя бумаги. Признаками подчистки являются: взъерошенность волокон поверхностного слоя бумаги, изменение глянца поверхности бумаги, уменьшение толщины бумаги в месте подчистки, расплывы чернил нового текста, остатки красителя штрихов подчищенного текста. Химическое травление текста: текст документа полностью или

частично подвергается обесцвечиванию или смыванию каким-либо химическим реактивом (кислотой, щелочью). Признаками химического травления являются: изменение оттенка бумаги, расплывы чернильных штрихов нового текста вследствие нарушения проклейки бумаги, хрупкость, ломкость бумаги при травлении концентрированными реактивами. Дописки, допечатки, исправления текста: основными признаками произведенной дописки являются различия в общих и частных признаках почерка в сравниваемых частях текста (размер букв, разгон почерка толщина штрихов признаки замедленности движений, остановок в дописанных буквах). Признаками допечатки на пишущей машинке являются несовпадения горизонтальности расположения печатных знаков в строке, различия размера и рисунка одноименных печатных знаков, различия в цвете красителя ленты и различия в дефектах шрифта, если допечатка производилась на другой пишущей машинке. В исправленных (измененных) письменных знаках наблюдаются сдвоенные, утолщенные штрихи, излишние элементы, оставшиеся от прежнего знака. Замены частей документа (фотокарточки, листов в многостраничных документах): при подделке документов могут заменяться фотокарточки, листы, номера документов. Замена фотокарточки производится в документах, удостоверяющих личность. Признаками переклейки фотокарточки являются отслоение поверхностного слоя бумаги у краев фотокарточки, наличие двух по составу клеев под фотокарточкой и вокруг нее, несовпадение по содержанию, размеру и рисунку букв текста в оттиске печати на фотокарточке и бумаге документа, отсутствие разрыва в оттиске печати у края фотокарточки на бумаге. При замене листов в многостраничных документах могут наблюдаться различия вставленных листов по размеру, оттенку цвета, линии обреза, несовпадения мест проколов со скрепками (лишние отверстия в месте сгиба), порядка нумерации страниц, серии и номера документа. Подделки подписей, оттисков печатей и штампов: подписи в документе могут подделываться различными способами путем подражания подлинной подписи лица или путем копировки с применением

технических средств. Имитация подписи и исполнитель ее (подделыватель) устанавливаются почерковедческой экспертизой путем сравнительного исследования сомнительной подписи с образцами подписи и почерка подозреваемого в подделке лица. Подделка подписи может быть установлена визуально по наличию расположенных рядом со штрихами обводки частично не перекрытых штрихов подготовки, по признакам замедленности движений в штрихах обводки.

3. Основные защитные элементы, применяемые в современной банкнотной продукции

1. Муаровые полосы. При наклоне на однотонном поле банкноты появляются радужные полосы.

2. Для печати банкнот крупных номиналов часто используются для печати оптически изменяющиеся краски, имеющие металлический блеск и способные менять цвет при изменении угла зрения.

3. Использование латентных эффектов. КИПП-эффект - способ создания скрытых изображений при использовании металлографской печати. При рассматривании изображения под прямым углом изображение является невидимым, а при изменении угла на острый скрытое изображение становится видимым.

4. Защитная нить. Часто в бумагу бумажных купюр вводят пластиковые, металлизированные или металлические нити, иногда выходящие на поверхность денежного билета с лицевой стороны. Нить может иметь магнитные свойства или флуоресцировать под воздействием УФ-излучения, при этом свечение может быть как одноцветным, так и многоцветным. Обычно нить содержит повторяющийся микротекст.

5. Метка для людей с ослабленным зрением. Имеет повышенную рельефность, которая воспринимается на ощупь.

6. Водяные знаки. На полях видно число купюры, на одной стороне изображён портрет, на другой город.

Для защиты современных ценных документов применяется также голография. Данная группа защитных признаков представлена в виде фольги для: горячего тиснения, ламинационных материалов, самоклеющихся этикеток и т. п. В настоящее время изготовление голограмм является достаточно доступным и наилучшим его решением - совмещение голограммы с другими методами защиты.

Как видно из выше представленных элементов защиты от подделки, для создания большинства элементов используется металлографская печать, что отводит ей одну из ведущих ролей при изготовлении высокозащищенной полиграфической продукции. Следует отметить, что данный способ защиты банкнотных изделий и ценных бумаг используется более ста лет, и соответствует рекомендациям международной организации криминальной полиции Интерпол. Помимо визуально и тактильно воспринимаемых элементов защиты от подделки, элементы металлографской печати обладают признаками определения подлинности на уровне эксперта. Для широкой публики главное в металлографской печати — это рельеф, который можно осязать при прикосновении. Специалистам металлографская печать может сказать значительно больше. Например, вытеки краски, образуемые при металлографской печати (так называемые «усики»), в некоторых случаях дают бесценную информацию. Вытеки краски делают каждую банкноту уникальной, а повторяемость одних и тех же рисунков «усиков» со всей очевидностью свидетельствует о подделке. «Усики» сложно воспроизвести офсетом: они частично теряются при копировании или сканировании. В то же время «усики», воспроизведенные офсетом, оказываются одинаковыми на всех банкнотах, отпечатанных с одной формы. Повторяемость одних и тех же комбинаций вытеков краски дает основание причислять поддельные банкноты к одной группе, а затем использовать эту информацию в сочетании с другими сведениями для выявления происхождения фальшивок.

Как видно из изложенного материала, использование металлографской печати в высокозащищенной полиграфической продукции является приоритетным, несмотря на долгий временной интервал ее использования.

Поскольку, в настоящее время на рынке появляется большое количество наименований новых запечатываемых материалов: полимерных субстратов, бумаги с полимерными включениями, композиционных материалов; что ставит задачу, направленную на повышение качества оттисков. Ведь от этого зависит не только визуальные характеристики элементов, но и потребительские свойства изделий, такие как, стойкость к истиранию, светостойкость, стойкость к воздействию горячих кислых или щелочных сред, стойкость к смятию и многие другие.

Для проведения исследования я обратилась за помощью в отделение почтовой связи №15 города Томска.

Было установлено, что в отделениях Почты России проверяются документы и денежные знаки, в основном, с помощью детектора документов и денег, детектора банкнот. Сотрудники почтовой связи изучают основные защитные элементы, применяемые в современной банкнотной продукции, и опираясь на эти знания, с успехом применяют на практике.

Сотрудник почтовой связи в случае обнаружения поддельного документа или поддельного денежного знака в виде денежной купюры, должен сообщить старшему по смене, либо начальнику отделения, тот в свою очередь, должен сообщить в Службу безопасности Почты России, либо в полицию.

Каждый клиент, пользующийся услугами почтовой связи, проверяется по базе террористов в соучастии в запрещённых террористических группировках Российской Федерации. Данный список обновляется раз в 1-3 месяца.

Сотрудник почтовой связи всеми возможными путями обязан задержать клиента до приезда полиции.

Заключение

В ходе проведенного исследования было установлено, что в отрасли почтовой связи существуют методы идентификации поддельных документов и денежных знаков.

Более того, при обнаружении поддельных документов и денежных знаков клиенту грозит штраф или уголовная ответственность.

Подделка документов наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо арестом на срок до шести месяцев (УК РФ Статья 327. Подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков).

Подделка денежных знаков наказываются лишением свободы на срок до двенадцати лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового и с ограничением свободы на срок до одного года либо без такового (УК РФ Статья 186. Изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг).

Список используемых источников:

1. Виды подделки документов: как распознать «липовую» бумагу [Электронный ресурс] // URL: https://studfile.net/preview/4649613/page:21/ (дата обращения 04.11.2022).

2. Процедура проверки фальшивых денег и действия кассира при их обнаружении [Электронный ресурс] // URL:

https://www.ekam.ru/blogs/pos/proverka-falshivyh-deneg-deystviya-kassira (дата обращения 04.11.2022).

3. Распознание подделок документов [Электронный ресурс] // URL: https://www.profiz.ru/sr/4_2003/1494/ (дата обращения 05.11.2022).

4. Способы подделки документов и способы их распознания [Электронный ресурс] // URL: https://ruadvocate.ru/vidy-prestuplenij/vidy-poddelki-dokumentov-kak-raspoznat-lipovuyu-bumagu/ (дата обращения 05.11.2022).

5. Обзор элементов защиты от подделки, предназначенных для идентификации населением, применяемых в настоящее время. А. Б. Сорокин. Известия ТулГУ. Технические науки. 2013. Вып. 3 [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/obzor-elementov-zaschity-ot-poddelki-prednaznachennyh-dlya-identifikatsii-naseleniem-primenyaemyh-v-nastoyaschee-vremya/viewer (дата обращения 06.11.2022).

6. Уголовный Кодекс Российской Федерации [Электронный ресурс] // URL: https://rulaws.ru/uk/(дата обращения 06.11.2022).

7. Дубина Н. Полиграфические методы защиты // КомпьюАрт. 2002. № 1 С. 28-33. (дата обращения 06.11.2022).

8.Бумажные деньги России [Электронный ресурс] // Металлографская печать: [сайт]. URL: http://bummoney.narod.ru/metall.html (дата обращения 06.11.2022).

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПОЧТОВОЙ СВЯЗИ

Михайлова Анастасия Сергеевна

Областное государственные бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»

Руководитель: Ротару Алеся Семеновна

Введение

Тема: Современные информационные технологии в почтовой связи.

Актуальность: в настоящее время в условиях свободной конкуренции организации федеральной почтовой связи предпринимают шаги и активизируют усилия по техническому и интеллектуальному перевооружению объектов почтовой связи на основе внедрения современных технологий. В результате развивается новый сегмент рынка услуг почтовой связи на основе информационных и инфокоммуникационных технологий. Информационная безопасность в современных условиях становится важнейшим базовым элементом всей системы национальной безопасности российского государства.

Цель: изучить основные современные информационные технологии в почтовой связи.

Задачи:

1. Подобрать и изучить источники с информацией по теме.

2. Проанализировать и систематизировать подобранную информацию о современных информационных технологиях в почтовой связи.

3. Оформить проект и компьютерную презентацию по теме.

Объект исследования: почтовая связь.

Предмет исследования: современные информационные технологии.

Гипотеза: я предполагаю, что почтовая связь обеспечивает достаточную защиту личных данных и информации о почтовых отправлениях пользователей её услуг.

Методы исследования: Теоретические (аналогия; индукция; классификация; изучение и анализ источников); качественные.

1. ИНФОРМАЦИОННЫЕ СИСТЕМЫ, ИСПОЛЬЗУЕМЫЕ В ПОЧТОВОЙ СВЯЗИ

1.1. ЕАС ОПС (единая автоматизированная система отделения почтовой связи)

Данная система предназначается для автоматизации операционной деятельности ОПС. Назначение ЕАС ОПС – повышение эффективности оказания услуг за счёт создания единого решения для автоматизации деятельности отделений почтовой связи.

1.2. АИС СЦ (автоматизированная информационная система «сортировочный центр»)

Данная информационная система автоматизирует производственный процесс по обработке почты в сортировочных центрах, местах и пунктах международного почтового обмена. Система позволяет формировать сведения для взаиморасчетов за международный почтовый обмен с иностранными почтовыми администрациями и между филиалами ФГУП «Почта России». Система позволяет обрабатывать рекламации, заявления и запросы по розыску международных почтовых отправлений.

1.2.1. Модули системы

Администрирование. Данный модуль позволяет управлять правами доступа пользователей системы и предоставляет возможность раздачи или снятия разрешений на работу пользователей или групп с различными модулями системы.

Ведение нормативно-справочной информации. Адресная информация, включающая информацию об объектах почтовой связи и административно-территориальном делении, загружается и регулярно обновляется из централизованного источника. Система позволяет вести экспортный план направлений и плана отправки почты по стране. Экспортный план ведется централизовано.

Обработка почты. Система позволяет обрабатывать почту и формировать сопроводительные документы в соответствии с внутренними регламентирующими документами РФ и международными стандартами (стандарты ВПС). Реализована возможность воспроизведения звука для подачи звуковых сигналов и голосовых команд. На таких рабочих местах возможно использование радио-сканера.

Участки регистрации входящей почты. Система позволяет регистрировать входящую почту внутренних и международных типов. Информация о регистрируемых объектах заносится в полуавтоматическом режиме.

Участки таможенного контроля. Система позволяет в полуавтоматическом режиме формировать списки, по которым подаются отправления на таможенный досмотр с последующей их обработкой.

Участки детальной сортировки (формирования исходящей почты). Система позволяет формировать емкости и сопроводительные документы согласно внутренним и международным правилам.

Транспортные участки. Система позволяет осуществлять регистрацию и отправку емкостей, формирование сопроводительных документов согласно внутренним и международным правилам.

Мониторинг прохождения почты. Система позволяет просматривать статистику прохождения почты внутри сортировочного центра за заданный период времени с детализацией до информации об объектах обработки (отправлениях/емкостях/документах).

Ведение рекламаций. Система позволяет вести учет и контроль рекламаций от клиентов и запросов от международных почтовых операторов, формировать документы согласно внутренним и международным правилам. Сбор статистики за месяц/квартал/год.

1.3. ИС контроля доступа

Аппаратно-программный комплекс автоматизированного контроля и управления доступом на охраняемую территорию и учета времени

нахождения служащих на ней построен по принципу модульной конструкции, состоящей из ядра и адаптируемой оболочки.

Ядро комплекса включает в себя аппаратную и программную части.

В состав аппаратной части входят сервер, станция администратора, станции охранников и сетевые средства связи.

Программная часть состоит из трех модулей: серверного модуля, модуля автоматизированного рабочего места охранника и административного модуля.

Серверный модуль, включающий в себя операционную среду, необходимые сетевые ресурсы и реляционную базу данных комплекса, располагается на сервере.

В комплексе могут быть установлены следующие аппаратно-программные модули оболочки:

1. Модуль идентификации личности в момент прохода через КПП;

2. Модуль обработки телесигналов;

3. Модуль обработки внешних сигналов;

4. Модуль дистанционного управления электромеханическими устройствами.

1.4. ИС почтового отделения

Информационная система почтового отделения предназначена для автоматизированного оформления, учета и первичной обработки почтово-кассовых операций по услугам, предоставляемым предприятиями Федеральной службы почтовой связи РФ. Система состоит из программного обеспечения (ПО) и аппаратных средств.

Должностные и иные лица, работники организаций почтовой связи, допустившие нарушения указанных положений, привлекаются к ответственности в порядке, установленном законодательством Российской Федерации.

2. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОЧТОВОЙ СВЯЗИ

В федеральном законе от 17.07.1999 N 176-ФЗ «О почтовой связи», Глава II «Услуги почтовой связи общего пользования» содержит статью 15 «Тайна связи», которая гласит о том, что:

1. Тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, гарантируется государством;

2. Осмотр и вскрытие почтовых отправлений, осмотр их вложений, а также иные ограничения тайны связи допускаются только на основании судебного решения;

3. Все операторы почтовой связи обязаны обеспечивать соблюдение тайны связи;

4. Информация об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и иные сообщения являются тайной связи и могут выдаваться только отправителям (адресатам) или их представителям.

Все почтовые отправления, почтовые переводы, документы находятся в закрытом доступе. Почтовые отправления хранятся в специально оборудованных хранилищах отделений почтовой связи, закрыты в железных шкафах или сейфах.

3. ИССЛЕДОВАНИЕ КАЧЕСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мною было проведено исследование качества защиты личных данных и информации, содержащейся в почтовых отправлениях пользователей услуг почтовой связи на примере программы ЕАС ОПС.

Данная программа была установлена нам для её практического изучения. При попытке входа в систему необходимо выбрать ФИО оператора, после чего ввести пароль, без которого нельзя получить доступ к каким-либо данным программы. Система автоматически блокирует работника ОПС после 100 неудачных попыток пароля подряд в течении рабочего дня. Для разблокировки необходимо обратиться к администратору или в службу технической поддержки.

Срок действия пароля составляет не более 90 дней. Система сообщает об истечении срока действия пароля за 10 дней до окончания срока действия пароля, при каждом успешном входе в систему до окончания срока действия пароля. По окончании срока действия пароля появляется сообщение о принудительной смене пароля.

При удачной попытке входа мы можем получить доступ к списку услуг, оказываемых в отделении почтовой связи, но доступ к данным клиентов, их отправлений и финансовым операциям нам закрыт.

Заключение

В данной работе были рассмотрены основные современные информационные системы объектов почтовой связи, такие как ЕАС ОПС, ИАС СЦ, ИС контроля доступа, ИС почтового отделения и их основные задачи.

Говоря о сохранности личных данных и информации о почтовых отправлениях, то она обеспечивается на государственном уровне.

Мною была выдвинута гипотеза о том, что почтовая связь обеспечивает достаточную защиту личных данных и информации о почтовых отправлениях пользователей её услуг. Проведя исследование на примере программы ЕАС ОПС, я могу сказать, что моя гипотеза подтвердилась: наличие пароля, его регулярная смена, а также отсутствие доступа к финансовым операциям даже для студентов специальности «Почтовая связь», изучающим эту программу,

показывает, что почтовая связь обеспечивает достаточную защиту данных своих пользователей.

Список использованных источников:

Инфопедия [Электронный ресурс] // Краткая инструкция пользователя для работы в системе ЕАС ОПС, 02.07.2021. URL: https://infopedia.su/25x640d.html (дата обращения: 08.11.2022).

Судебные и нормативные акты РФ [электронный ресурс] // Статья 15. Тайна связи, 27.12.2019. URL: https://sudact.ru/law/federalnyi-zakon-ot-17071999-n-176-fz-o/glava-ii/statia-15/?ysclid=la2htf0sm6868679688 (дата обращения: 04.11.2022).

Referat911 [Электронный ресурс] // Современные информационные технологии почтовой связи и их место в развитии отрасли, 22.09.2014. URL: https://www.referat911.ru/Kommunikacii-i-svyaz/sovremennye-informacionnye-tehnologii-pochtovoj-svyazi/518645-3218961-place1.html (дата обращения: 04.11.2022).

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Клейменов Артём Юрьевич

Зырянский филиал ОГБПОУ «Асиновский техникум промышленной индустрии и сервиса», с. Зырянское Зырянского района Томской области

Руководитель: Смокотина Анна Алексеевна

Ключевые слова: информационная безопасность, правонарушения, правоприменительная практика, государственная политика, федеральные законы, нормативно-правовые акты, информационное законодательство.

Актуальность и проблема. Процесс скоротечной информатизации современного общества приводит к усилению значимости необходимого уровня информационной безопасности как в государстве в целом, так и

отдельного гражданина Российской Федерации. Проблема обеспечения защиты информации от посторонних лиц возникла давно. С развитием информатизации информация приобретает цену. Ценной становится та информация, обладание которой позволит ее владельцу получить какую-либо выгоду. В данном контексте неважно, о какой именно информации (тайне) идет речь, государственной, коммерческой, персональной или личной. Государству и гражданам Российской Федерации гораздо важнее, чтобы эта информация (тайна) не была передана третьим лицам, а в случае, если такое произошло, то лицо или группа лиц в обязательном порядке должны быть привлечены к ответственности, что в настоящее время довольно затруднительно. Вместе с тем, низок уровень правового сознания граждан и правовой культуры юристов в сфере защиты информации от несанкционированного доступа. Все это наносит немалый ущерб гражданам и государству в целом.

Целью исследования является анализ законодательства и правоотношений возникающих в сфере информационной деятельности, направленной на обеспечение информационной безопасности.

Для достижения поставленной цели необходимо решить следующие *задачи*:

- проанализировать структуру правовой защиты информации;

- исследовать статистические данные привлечения к ответственности за нарушения в сфере обеспечения информационной безопасности;

- сформулировать проблемы и предложения по корректировке и определить основные тенденции развития информационного законодательства Российской Федерации.

Для решения задач используются *методы*: анализ и синтез, сравнение, статистический метод, визуализация.

Под информационной безопасностью Российской Федерации в целом понимается состояние защищенности её национальных интересов в

информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

На сегодняшний день существует множество правонарушений в информационной сфере, которые, на наш взгляд, вызваны следующими факторами:

1) несовершенство нормативной правовой базы, регулирующие отношения в области обеспечения информационной безопасности, а также недостаточная правоприменительная практика;

2) отсутствие единой государственной политики в области обеспечения информационной безопасности;

3) низкий уровень информатизации государственных и коммерческих структур;

4) недостаточный контроль за развитием информационного рынка со стороны государственных структур и общества;

5) низкий уровень защищенности интересов физических и юридических лиц в информационной сфере;

6) сращивание государственных и коммерческих структур в области кредитно-финансовой сферы с криминальными структурами;

7) получение доступа злоумышленников к конфиденциальной информации;

8) усиление влияния организованной преступности на жизнь общества;

9) нелицензионное программное обеспечение;

10) низкий уровень правовой культуры граждан Российской Федерации в области информационной безопасности.

Угрозами же безопасности информационных систем могут быть:

- разработка и распространение программ, нарушающих нормальное функционирование информационных систем, в том числе систем защиты информации;

- утечка информации;

- противоправный сбор и использование информации;

- перехват информации в сетях передачи данных и на линиях связи;

- несанкционированный доступ к информации, находящейся в банках и базах данных;

- нарушение законных ограничений на распространение информации.

Формирование информационного законодательства Российской Федерации осуществляется достаточно быстрыми темпами, что подтверждает значительное количество принятых нормативных правовых актов в этой сфере за последние несколько лет.

Информационную безопасность регулирует:

- Конституция Российской Федерации;
- «Доктрина информационной безопасности Российской Федерации», которая определяет цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации;
- Уголовный кодекс Российской Федерации;
- Кодекс об административных правонарушениях;
- Гражданский кодекс Российской Федерации;
- Федеральный закон "Об информации, информационных технологиях и о защите информации",
- Федеральный закон "О связи";
- Федеральный закон "О средствах массовой информации";
- Федеральный закон "О государственной тайне";
- Федеральный закон "О коммерческой тайне";
- Федеральный закон "О персональных данных";
- И множество других законодательных актов

Целью правового регулирования является обеспечение защиты прав и законных интересов лиц при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную

тайны. Основная угроза безопасности этих прав и свобод, как правило, исходит от неправомерного использования собираемых персональных данных различными структурами, в том числе некоммерческими организациями. Федеральный закон «О персональных данных» устанавливает общие принципы и условия обработки персональных данных, права субъектов персональных данных, обязанности оператора при сборе персональных данных, а также порядок осуществления контроля и надзора за обработкой персональных данных.

Тем не менее, мы констатируем тот факт, что становление законодательства в области информации, информационных технологий все еще отстает от развития информационных ресурсов, информационных услуг и средств информационного производства в стране.

В данной сфере правового регулирования существуют пробелы, которые должны быть устранены на законодательном уровне. Информация в базах данных, с одной стороны, обладает высокой стоимостью, а с другой - использование сведений конфиденциального характера не уполномоченными на то лицами способно причинить существенный вред правам и свободам человека и гражданина, общественному порядку и безопасности.

Если государственную и коммерческую тайну законодательство в области информатизации еще «как-то» защищает, то персональные и личные данные отдельного гражданина практически нет… Преступлений в области информационной безопасности «заявляется» все больше, а раскрывается все меньше, ущерб растет, но, получается, не возмещается.

Об этом свидетельствует статистика, приведенная Главным Управлением правовой статистики информационных технологий при Генеральной Прокуратуре Российской Федерации. Ущерб составил 150 млрд рублей по итогам 2021 года. В 2022 году люди «живут в состоянии неопределенности перспектив, с одной стороны, и постоянно растущих цен — с другой». В этой связи россияне стараются максимально сэкономить средства, чем злоумышленники, в свою очередь, активно злоупотребляют.

В целом на деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, по-прежнему приходится одно из четырех регистрируемых преступлений. Число преступлений в IT-сфере ежегодно вырастает более чем в полтора раза. За последние пять лет число таких преступлений увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8 % до 25 %.

В январе - декабре 2021 года зарегистрировано 517,7 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 1,4% больше, чем за аналогичный период прошлого года, но сразу в 1,8 раза превосходит показатель 2019 года.[1]. В общем числе зарегистрированных преступлений их удельный вес увеличился с 25% в январе - декабре 2020 года до 25,8%. Больше половины таких преступлений (55,7%) относится к категориям тяжких и особо тяжких (288,3 тыс.; +7,7%), более двух третей (67,9%) совершается с использованием сети «Интернет» (351,5 тыс.; +17,0%), почти половина (42,0%) – средств мобильной связи (217,6 тыс.; -0,5%). Из них раскрыто лишь 118920 преступления, что составляет 25,3%.[2]

В январе - декабре 2020 года показатель составлял (+73,4 %, 510,4 тыс.). Большинство «киберпреступлений» были совершены с использованием сети «Интернет» (300,3 тыс.) или при помощи средств мобильной связи (218,7 тыс.).[3]

За январь – декабрь 2019 года зарегистрировано 294 409 (+68,5 %) преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации,

[1] Число киберпреступлений в России (tadviser.ru)
[2] Состояние преступности в России 2021 год sb_21_12.pdf (tinkoffjournal.ru) Показатели сформированы в соответствии с Перечнем № 25, введенным в действие указанием Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» от 29 декабря 2021 г. № 790/11/1.
[3] Состояние преступности в России 2020 год <32305FC5E6E5ECE5F1FFF7EDFBE95FF1E1EEF0EDE8EA5FF15F30395F32303230> (d-russia.ru) Показатели сформированы Главным управлением правовой статистики и информационных технологий при Генеральной прокуратуре Российской Федерации

предварительно расследовано – 65 238 (+50,4 %). Ущерб от преступлений в 2019 году составил 627 697 445 тыс. рублей, что на 11,5 % больше аналогичного показателя 2018 года.[4]

На наш взгляд это вызвано отставанием финансирования правоохранительных органов в области технических средств и информационных ресурсов.

Кроме того, сведения, опубликованные Роскомнадзором, свидетельствуют, что в 2018-2021 году количество нарушений обработки персональных данных (ПД), варьирует на уровне 2018 года, что свидетельствует о том, что граждане перестают обращаться за помощью, чувствуя безнаказанность злоумышленников. В 2018 году – 39300 правонарушений, в 2019 году - 50300[5], в 2020 году – 39795, а в 2021 году – 38000. В 2021 году составлено лишь 220 протоколов об административном нарушении. Фактически, по оценкам экспертов, о каждом гражданине РФ, в зависимости от его активности в сети «Интернет», содержатся записи в среднем от 10 до 100 и более базах данных. В общей сложности это почти 13 млрд записей с персональными данными граждан. Результатом неисполнения операторами баз данных требований действующего законодательства в сфере персональных данных являются регулярные утечки ПД граждан. Граждане, чьи ПД оказываются в свободном доступе, всё чаще получают навязчивые рекламные сообщения и звонки, становятся жертвами телефонных мошенников. Всего более 3,7 млн подобных звонков за 2021 год.[6]

Наибольшее число составов в области информации и средств связи сосредоточено в гл. 13 «Административные правонарушения в области связи и информации» (ст. 13.2–13.49) кодекса Российской Федерации об Административных правонарушениях. Среди них отдельно следует выделить такие, как нарушение законодательства Российской Федерации в области

[4] https://genproc.gov.ru/smi/news/regionalnews/news-1844096/
[5] www.finmarket.ru/news/5159900
[6] Роскомнадзор - Подведены итоги работы Роскомнадзора в 2021 году по защите прав и интересов граждан в сфере персональных данных (rkn.gov.ru)

персональных данных (ст. 13.11); разглашение информации с ограниченным доступом (ст. 13.14). Административная ответственность за совершение правонарушения в области персональных данных предусмотренная, к примеру, ст. 13.11 до 2021 года имела максимальный размер штрафа для физических лиц четыре тысячи рублей и для юридических лиц 70 тысяч рублей (за исключением повторности). Федеральный закон от 24.02.2021 № 19-ФЗ внёс изменения в КоАП РФ, в том числе и в части административной ответственности за нарушение законодательства Российской Федерации в области персональных данных (ст. 13.11). Новые штрафы действуют с 27 марта 2021 года. На физических лиц максимальный размер штрафа 10 тысяч рублей, а для юридических лиц 100 тысяч рублей (за исключении ем повторности). Ранее за совершение некоторых нарушений можно было избежать штрафа, отделавшись предупреждением. Теперь такая норма отсутствует. Но, на наш взгляд, не смотря на изменения, совершенно очевидно, что состав действующей ст. 13.11 КоАП РФ все еще не в полной мере учитывает негативные последствия совершенных правонарушений. Следствием этого станет продолжение увеличения роста количества жалоб и обращений граждан на незаконные действия операторов, осуществляющих обработку персональных данных с нарушением законодательства Российской Федерации в области персональных данных и, соответственно, количества выявленных нарушений.

Длительная, установленная процедура собирания материалов по ст. 13.11 КоАП РФ делала затруднительным привлечение операторов к установленной законом административной ответственности, для которой был установлен 3-месячный срок давности. Благодаря вступившим в силу изменениям №19-ФЗ от 24.02.2021 оштрафовать теперь можно в течение года, что безусловно повлияет статистику по итогам конца 2021 года.

Согласно Федеральному закону от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» с 1 марта 2021 года каждый человек сам решает, какие сведения о себе он публикует в

свободном доступе, предоставляет неопределенному кругу лиц, т.е. распространяет, и для каких целей. При этом все остальные лица не вправе использовать их по своему усмотрению. Любые данные о человеке можно распространять только с его прямого согласия. Исключения возможны для случаев, где имеется государственный, общественный и публичный интерес. Согласно тому же закону исправлена коллизия, что оператор доступа к использованию сети не несет ответственность за соответствие распространяемой пользователями информации. В соответствии с ранее действующим законодательством ответственность несло лицо, непосредственно распространившее информацию, оператор же к таковым не относился.

В Уголовном кодексе Российской Федерации и вовсе отсутствует статья, предусматривающая ответственность за преступления совершенные в сетях общего доступа по распространению личной и персональной информации (в том числе в сети «Интернет»).

В *итоге* представляется необходимым дальнейшее усовершенствование правовой базы, при этом в первую очередь необходимо достижение единства норм различных отраслей права, максимальное уменьшение их несбалансированности.

Можно выделить несколько *способов*, заключающихся в повышении эффективности действующих норм права путем:

- дифференцирования составов правонарушений с учетом ущерба, причиненного нарушителем;
- существенного увеличения размеров штрафных санкций, как в плоскости административной ответственности, так и в качестве уголовного наказания в области распространения личной и персональной информации;
- наделения органов государственной власти дополнительными полномочиями в области административного производства;
- повышения уровня правовой сознательности граждан;

- увеличения финансирования правоохранительных органов, в том числе в части оснащенности современными техническими средствами и информационными ресурсами.

Список использованных источников

1. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" / КонсультантПлюс (consultant.ru)
2. "Уголовный кодекс Российской Федерации" (УК РФ) от 13.06.1996 N 63-ФЗ (последняя редакция) / КонсультантПлюс (consultant.ru)
3. "Кодекс Российской Федерации об административных правонарушениях" (КОАП РФ) от 30.12.2001 N 195-ФЗ (последняя редакция) / КонсультантПлюс (consultant.ru)
4. Гражданский кодекс Российской Федерации (ГК РФ) / КонсультантПлюс (consultant.ru)
5. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция) / КонсультантПлюс (consultant.ru)
6. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 (последняя редакция) / КонсультантПлюс (consultant.ru)
7. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (последняя редакция) / КонсультантПлюс (consultant.ru)
8. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) / КонсультантПлюс (consultant.ru)
9. Российская газета (rg.ru)
10. Число киберпреступлений в России (tadviser.ru)
11. Состояние преступности в России 2021 год (tinkoffjournal.ru)
12. Состояние преступности в России 2020 год (d-russia.ru)
13. https://genproc.gov.ru/smi/news/regionalnews/news-1844096/
14. www.finmarket.ru/news/5159900

15. Итоги работы Роскомнадзора в 2021 году по защите прав и интересов граждан в сфере персональных данных (rkn.gov.ru)

РАСПРОСТРАНЁННЫЕ ВИДЫ МОШЕННИЧЕСТВА

Коробкин Руслан Владиславович
Сороколетов Денис Александрович
Областное государственное бюджетное
профессиональное образовательное учреждение
«Томский индустриальный техникум»
Руководитель: Петруша Мария Анатольевна

Актуальность*:* В уголовном праве Российской Федерации под мошенничеством понимается хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием лица. Казалось бы, сейчас все уже знают все о мошенниках, каким образом они работают и как их распознать. Но читая новости на просторах интернета и в социальных сетях, мы натыкаемся на заголовки новостей такого формата: «34-летняя томичка стала очередной жертвой мошенников, пытаясь обезопасить денежные средства…, женщина из Томска доверилась мошенникам и перевела на 12 номеров телефонов более 1.2 млн. рублей…, пожилая жительница Томска перевела более 2.2 млн. рублей лжетрейдеру.» Это говорит лишь о том, что тема мошенничества всегда актуальна, на уловки мошенников могут попасть как подростки, так и взрослые люди, пенсионеры. Видов мошенничества очень много на данный момент, и с каждым годом появляется что-то новое, от самых банальных до весьма изощренных.

Цель: на примере Томской области рассмотреть распространенные виды мошенничества и предостеречь людей не поддаваться обманам мошенников.

Задачи:

- изучить виды мошенничества;
- изучить меры предосторожности.

Методы мошенничества всегда идут в ногу со временем и быстро адаптируются к любым изменениям в мире — появление новых коммуникационных технологий, новых сфер деятельности или продуктов. Мошенничество в интернете оказывает наибольшее влияние на жизнь современных людей, так как многие существующие методы обмана людей в Интернете имеют целью непосредственное получение денег или имущества от жертв. Зачастую целью являются персональные данные — логины, пароли, файлы — доступ к которым предоставляет мошеннику возможность шантажировать, вымогать что-либо или же распоряжаться полученной информацией на свое усмотрение не позволяют пользователям, особенно старшему поколению, быть готовыми и правильно реагировать на уловки мошенников.

Основные виды мошенничества в финансовой сфере:

1. фишинг;
2. вишинг;
3. смишинг.

Фишинг (от англ. «fishing» – уловка) – введение пользователя в заблуждение при помощи поддельного сайта, визуально имитирующего сайт банка или иной интернет-системы, предполагающей идентификацию пользователя. Главная задача фишера – заманить пользователя на сайт-ловушку и каким-либо образом убедить его сообщить идентификационные данные. Для решения такой задачи фишеры обычно применяют одну из следующих методик:

- Спам
- Рассылка поддельных писем от имени банка или некого провайдера услуг с просьбой уточнить номер счета, логин/пароль и прочие персональные данные, отправив их по указанному адресу
- Реклама неких товаров или услуг, которые можно приобрести в интернет-магазине или же ознакомиться об услуге на сайте, причем в рекламе обязательно приводится ссылка на данные сайты. Вместо сайта магазина

пользователь может попасть на сайт фишеров или на сайт созданного мошенниками магазина-однодневки

- Применение троянской программы
- Выуживание у пользователя отсканированных копий его документов. В частности, имея ксерокопию паспорта и образец подписи, теоретически можно оформить кредит от имени пользователя.

Таблица 1. Примеры фишинга на территории Томской области за период с сентября по ноябрь 2022 год

Ситуация	Статья УК РФ	Рекомендации	Итог
В полицию Томска обратился местный житель, рассказав, что он совершил сделку в Интернете, перевел денежные средства, но потом не получил заказанное устройство - снегоход. Возбуждено уголовное дело по факту мошенничества. "Мужчина решил приобрести снегоход посредством одной популярной Интернет-площадки частных объявлений, нашел подходящий для него вариант, затем связался с продавцом и обсудил условия сделки", - уточняет УМВД. Также добавляется, что после оплаты снегохода, продавец перестал выходить на связь.	В отношении неизвестного заведено уголовное дело, предусмотренное частью 2 статьи 159 УК РФ «Мошенничество ».	Быть внимательными к совершению денежных операций в Интернете и не переводить средства через банкомат неизвестным личностям и не участвовать в предложенных схемах.	Преступление не раскрыто
Томич хотел купить кроссовки, но отдал мошеннику 20 тысяч рублей. Молодой человек решил приобрести обувь через интернет. Найдя продавца, он перевел ему деньги, однако товар так и не получил. Об этом сообщает пресс-служба УМВД по Томской области. По данным ведомства, в мае текущего года в полицию обратился учащийся одного из высших учебных заведений Томска. Молодой человек рассказал, что заказал кроссовки в группе в социальных сетях, с полной предоплатой. В указанный продавцом срок и после него товар так и не пришел, материальный ущерб составил 20 тысяч рублей.			В октябре 2022 года оперативниками был установлен злоумышленник, похитивший деньги. Им оказался житель города Пермь, 1999 года рождения. В отношении подозреваемого избрана мера пресечения в виде подписки о невыезде»
Жительница Томской области, пытаясь заработать на инвестициях, перевела мошенникам более 6 миллионов рублей. Об этом сообщает пресс-служба регионального УМВД.			Преступление не раскрыто

По данным ведомства, 44-летняя жительница Стрежевого в интернете увидела рекламу брокерской компании и оставила заявку на обратный звонок. Ей перезвонил менеджер и предложил создать аккаунт на сайте компании, после чего скинул в мессенджере ссылку на уже зарегистрированный личный кабинет и убедил пополнить счет для начала введения финансовых операций на сумму 100 евро. Спустя несколько недель стрежевчанке на банковскую карту поступил первый "заработок" в сумме более 80 тысяч рублей, после которого она поверила в надежность брокерской компании, вновь взяла кредит на сумму 3 миллиона рублей и перевела на счет личного кабинета. Таким образом стрежевчанка за месяц перевела мошенникам более 6,4 миллиона рублей.			
Жительница Томского района, желая продать шкаф через интернет, стала жертвой аферистов. Как сообщает пресс-служба регионального УМВД, женщина, перейдя по ссылке, ввела данные карты и лишилась почти 60 000 рублей. По данным ведомства, жительница поселка Зональный разместила объявление о продаже шкафа на одной из интернет-площадок частных объявлений. После чего ей написал потенциальный покупатель, который захотел приобрести мебель и выслал женщине ссылку для осуществления сделки.			Преступление не раскрыто
Томичка отправила аферистам более 140 тысяч рублей во время онлайн-собеседования "с работодателем" Томичка отправила аферистам более 140 тысяч рублей во время онлайн-собеседования "с работодателем". Об этом сообщает пресс-служба УМВД по Томской области. По предварительным данным, желая подработать, 48-летняя томичка разместила свое резюме на одном из сервисов по поиску работы. Через некоторое время ей позвонил мужчина, представился менеджером и предложил пройти собеседование по видеосвязи.			Преступление не раскрыто

Сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые якобы отправлены из официального банка, могут сообщать пользователям о необходимости позвонить по определённому номеру для решения проблем с их банковскими счетами. Эта техника называется **вишинг** (голосовой фишинг). Позвонив на указанный номер, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести номер своего счёта и PIN-код. К тому же вишеры могут

сами звонить жертвам, убеждая их, что они общаются с представителями официальных организаций, используя фальшивые номера. В конечном счёте, человека также попросят сообщить его учётные данные.

Таблица 2. Примеры вишинга на территории Томской области за период с сентября по ноябрь 2022 год

Ситуация	Статья УК РФ	Рекомендации	Итог
Томичка перевела мошеннику 350 тысяч рублей, поверив, что ее аккаунт на "Госуслугах" взломан Поверив, что аккаунт на сайте "Госуслуг" взломан, 61- летняя томичка попалась на уловку телефонного мошенника. Как сообщает пресс-служба УМВД по Томской области, женщина перевела ему 350 тысяч рублей. Полицейские выяснили, что жительнице Совествкого района на мобильный телефон позвонил неизвестный и представился сотрудником сайта «Госуслуги». Он сказал, что аккаунт женщины "взломан" и сейчас заблокирован, а через личный кабинет неизвестный сделал заявку на получение кредита в банке.	В отношении неизвестного заведено уголовное дело, предусмотренное частью 2 статьи 159 УК РФ «Мошенничество».	Быть предельно внимательными, ни при каких обстоятельствах не сообщать незнакомым людям, в том числе по телефону, персональные данные, реквизиты банковских карт, защитный код на оборотной стороне, а также коды подтверждения операций, пришедших Вам посредством SMS-сообщений. Ни в коем случае не совершать какие-либо финансовые операции по указанию незнакомцев по телефону, кем бы они не представлялись! В случае поступления звонка с сообщением о безопасности Ваших денежных средств на банковских счетах и картах - немедленно прекратите разговор и самостоятельно перепроверьте информацию в названном Вам	Преступление не раскрыто
Жительница города Томска перевела денежные средства на "безопасный счет" мошенников и лишилась 2,5 млн рублей. Об этом сообщает пресс-служба УМВД по Томской области. Как уточняется, в полицию обратилась 59-летняя томичка с заявлением о хищении денежных средств. В одном из мессенджеров женщине поступил звонок от "сотрудника банка". Он сообщил, что потерпевшей одобрен кредит, а также от ее лица подана заявка на смену номера телефона, привязанного к банковской карте. *«Томичка уточнила, что никаких заявок не подавала, в ответ на это злоумышленник сказал, что в отношении женщины совершаются мошеннические действия, и пояснил, что для "аннулирования кредита" необходимо оформить другой, а полученные деньги перевести на "безопасный счет" банка. Действуя по указаниям лжесотрудника банка, женщина оформила кредит и перевела на указанный ей счет более 2,5 млн рублей».*			Преступление не раскрыто
38-летний житель Томска лишился почти 1,4 млн рублей из-за телефонных мошенников. Они представлялись сотрудниками полиции. Об этом сообщает пресс-служба регионального УМВД. Выяснилось, что в текущем месяце в течение суток на мобильный телефон жителю Октябрьского района поступали звонки от неизвестных лиц, которые представлялись сотрудниками правоохранительных органов города Москвы и сообщали, что по паспортным данным томича через банк осуществлен перевод на сумму 100 000 рублей. *«Для предотвращения мошеннических действий"лжеправоохранители" предложили мужчине взять в разных банках кредиты и*			Преступление не раскрыто

перевести денежные средства на так называемый "безопасный счет", что потерпевший и сделал. Всего он перевел на счёт аферистов через различные терминалы оплаты денежные средства на сумму 1 374 600 рублей»		банковском учреждении.	
Трое жителей Томской области перевели на «безопасные счета» аферистов более 4,8 миллионов рублей. Об этом сообщает пресс-служба регионального УМВД. Уточняется, что накануне, в дежурную часть поступили заявление от трех местный жителей о хищении денежных средств обманным путем. Всем гражданам звонили на сотовые телефоны и говорили, что мошенники пытаются оформить кредит на их персональные данные. После чего, следуя указаниям звонящих лиц, граждане оформляли на свое имя кредиты и перечисляли денежные средства якобы на «безопасные счета».			Преступление не раскрыто

Набирает свои обороты и SMS-фишинг, также известный как **смишинг**. Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, - входя на него и вводя свои личные данные, жертва аналогичным образом передает их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем».

Таблица 3. Примеры смишинга на территории Томской области за период с сентября по ноябрь 2022 год

Ситуация	Статья УК РФ	Рекомендации	Итог
Молодой томич стал жертвой мошенников, познакомившись с девушкой в одном из популярных приложений. Об этом сообщает пресс-служба регионального УМВД. Как уточняется, 24-летний местный житель в одном из популярных приложений для знакомств познакомился с девушкой, которая после недолгого общения предложила сходить в театр и направила ссылку для покупки билетов. *«Доверившись незнакомке, томич перешел по ссылке, где указал реквизиты своей банковской карты, после чего с банковской карты произошло списание денежных средств в сумме более 2 000 рублей, однако на сайте отобразилась ошибка и билеты не были предоставлены. Тогда молодой человек написал в чат поддержки сайта, где для устранения неполадки ему вновь скинули ссылку»* Повторив операцию и указав данные карты произошло повторное списание денежных средств в сумме более 2 000 рублей, а новая знакомая перестала выходить на связь.	В отношении неизвестного заведено уголовное дело, предусмотренное частью 2 статьи 159 УК РФ «Мошенничество».		Преступление не раскрыто
Пытаясь устроиться на работу, 26-летний житель Томска лишился крупной суммы денег. Как	По данному факту следователями по	Не переходите по незнакомым	Преступление не раскрыто

сообщает пресс-служба регионального УМВД, у него было похищено около миллиона рублей. Житель областного центра рассказал, что с целью поиска работы размещал своё резюме на различных Интернет-сервисах. Далее ему на телефон поступило сообщение о дистанционной работе, для которой необходимо было зарегистрироваться в приложении для осуществления видеозвонков и следовать поступающим инструкциям. *«Действуя указаниям «работодателей» томич внес первоначальный взнос для дальнейшей работы в сумме 7 000 рублей, а после якобы «активации личного кабинета» ещё 120 000 рублей. Затем менеджер сообщил о необходимости оформления кредита в сумме 700 000 рублей, которые в последствие также были списаны в пользу «нанимателя». Таким образом было похищено 827 000 рублей».*	Советскому району возбуждено уголовное дело по статье «Кража»	ссылкам и не вводите никакие свои персональные данные и данные банковских карт.	

Томичи потеряли более 380 млн рублей за девять месяцев 2022 года (с января по октябрь), поверив мошенникам. Почти 2500 раз обманули жителей Томской области за девять месяцев текущего года с помощью интернет-мошенничества. Злоумышленники похитили более 380 миллионов рублей у доверчивых граждан. Такие цифры в программе «Открытая студия» привёл замначальника отдела по противодействию преступлениям, совершенным с использованием IT-технологий УМВД России по Томской области Сергей Изосимов.

Среди наиболее популярных способов обмана можно выделить дистанционное мошенничество. Напомним, это мошенничество с помощью средств мобильной связи.

«За 9 месяцев текущего года, на территории Томской области зарегистрировано 2423 преступления с использованием IT-технологий. Из них 772 – хищение со счетов и 1651 связано с дистанционным мошенничеством. Раскрыто 563 преступления, раскрываемость составляет 25%», – сказал Сергей Изосимов.

Также он отметил, что основной сложностью в раскрытии подобных преступлений является местоположение злоумышленников, которое в большинстве случаев находится за пределами Томской области и Российской Федерации.

Вывод.

Мошенники стремятся получить секретные данные карты — трёхзначный код CVC/CVV с обратной стороны, коды подтверждения из SMS, логины и пароли от интернет-банков. Настоящие сотрудники банка никогда не запрашивают эту информацию — для обеспечения безопасности они используют отдельные технические средства. Для отправки платежа нужен только номер карты — другие данные для этого не нужны.

Как составить заявление по факту мошенничества по телефону?

Если пользователь столкнулся с телефонным мошенничеством, необходимо как можно скорее обратиться в полицию, даже если пользователь не отправлял деньги или данные карты. В заявлении нужно подробно описать обстоятельства происшествия — время звонка номер телефона, ФИО и «должность» звонящего, содержание и итог разговора, в случае перевода денег — отправленную сумму. В качестве основания - указать статью 159 УК РФ (если мошенник смог получить деньги) и часть 3 статьи 30 УК РФ (если этого сделать не удалось). Если есть запись звонка (его можно записать с помощью специального приложения) — приложить ее к заявлению.

Заявление будет рассматриваться в течение 10-30 дней. По итогам будет принято решение о возбуждении уголовного дела. В случае отказа , то можно обжаловать его в прокуратуре — для этого потребуются копия заявления и постановление об отказе.

Главное: Если во время звонка неизвестный представляется сотрудником банка или органов внутренних дел, следует немедленно прекратить разговор. А при совершении интернет-покупок необходимо пользоваться отдельной банковской картой.

Все данные о мошенничестве в Томской области взяты с открытых источников:

1. Вести – Томск https://www.tvtomsk.ru/tags/мошенничество/
2. БеZформата https://tomsk.bezformata.com/word/moshennichestvo/10092/
3. Комсомольская правда https://www.tomsk.kp.ru/online/news/5018102/

СЕКЦИЯ 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ПЛАКАТАХ

Фофанова Ульяна Олеговна

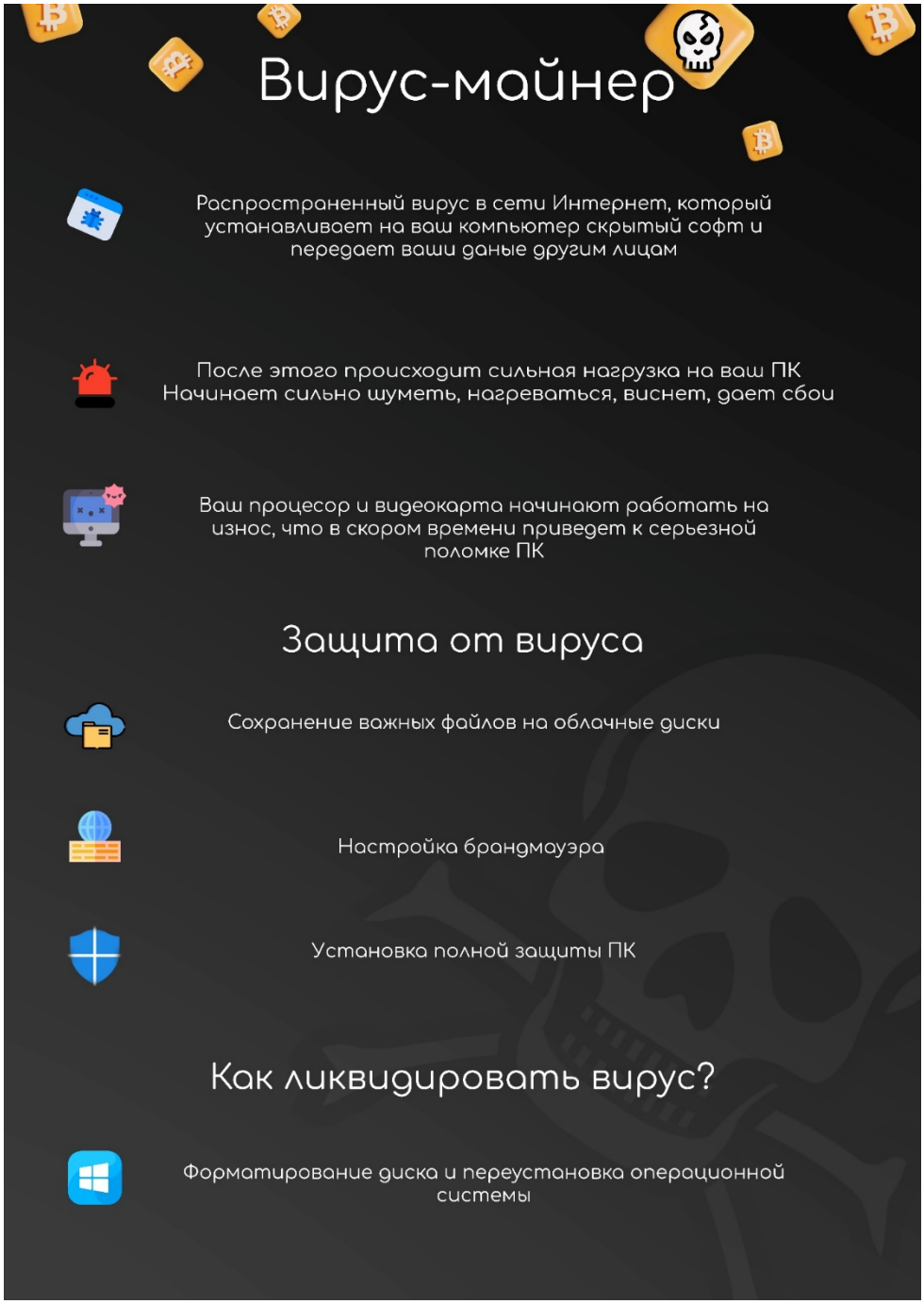
Областное государственное бюджетное

профессиональное образовательное учреждение

«Томский индустриальный техникум»

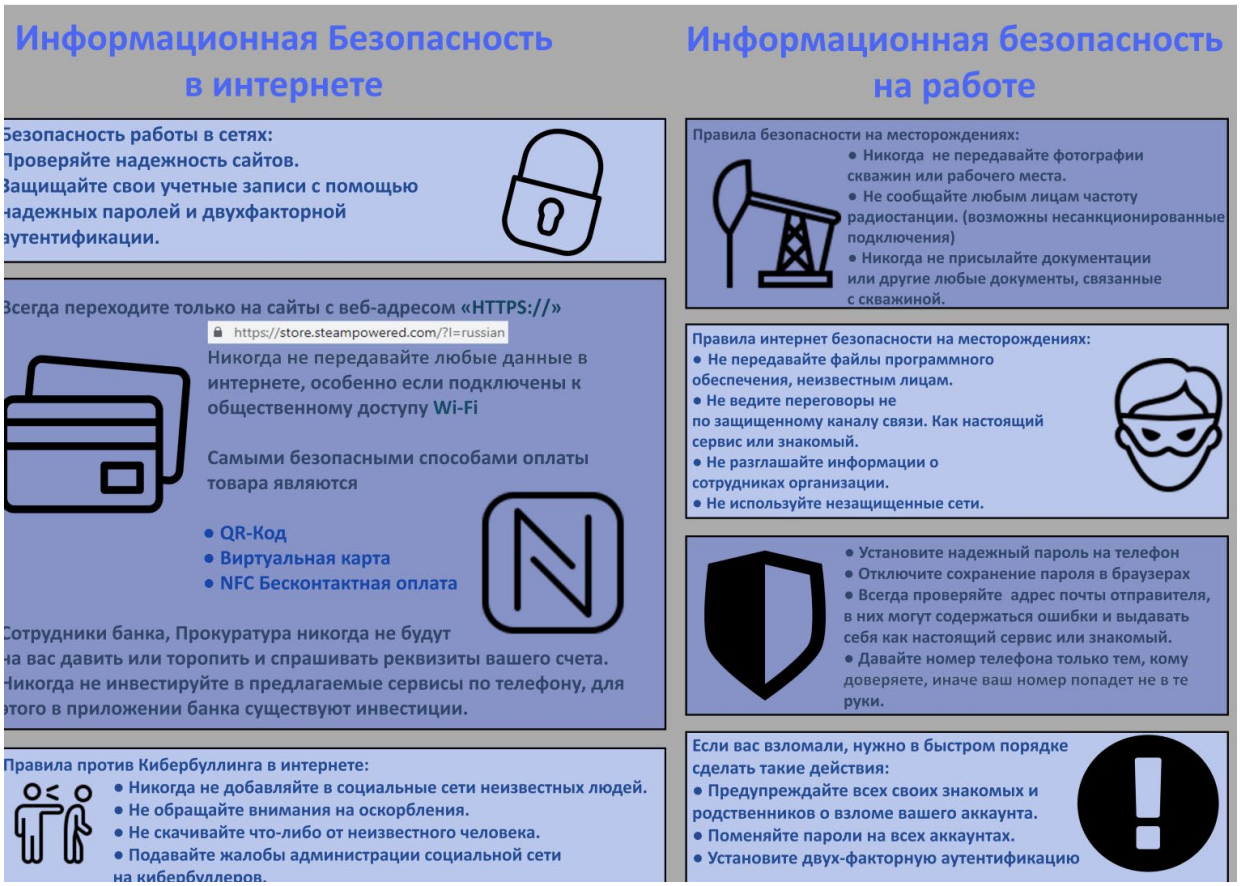
Руководитель: Мазенина Александра Николаевна

Азаров Денис Андреевич
Областное государственное бюджетное
профессиональное образовательное учреждение
«Томский индустриальный техникум»
Руководитель: Асадулина Галия Спартаковна



Марченко Максим Сергеевич
Областное государственное бюджетное
профессиональное образовательное учреждение
«Томский техникум водного транспорта и судоходства»
Руководитель: Осипова Татьяна Викторовна

Томашев Дмитрий Алексеевич
Областное государственное бюджетное
профессиональное образовательное учреждение
«Томский политехнический техникум»
Руководитель: Шабалин Вадим Сергеевич



Лебедев Дмитрий Витальевич
Областное государственное бюджетное
профессиональное образовательное учреждение
«Томский механико-технологический техникум»
Руководитель: Самия Салим Викторович

Бекк София Владимировна
Областное государственное бюджетное
профессиональное образовательное учреждение
«Колледж индустрии питания, торговли и сферы услуг»
Руководитель: Дозморова Татьяна Васильевна

Ващенко Александр Максимович
Областное государственное бюджетное
профессиональное образовательное учреждение
«Асиновский техникум промышленной индустрии и сервиса»
Руководитель: Смокотина Анна Алексеевна

Информационная безопасность

Социальные сети

ПРАВИЛА:

1) Ограничивать список друзей.

2) Защищать частную информацию (пароли, номера телефонов, адреса и т.д.).

3) Защищать свою репутацию. Дважды думать перед загрузкой чего-либо в социальные сети.

4) Скрывать личную информацию при общении с незнакомыми людьми.

5) Не размещать в соц.сети изображение, где по местности можно определить место жительства.

6) Использовать сложные пароли при регистрации.

Электронные деньги

ПРАВИЛА:

1) Привязывать к счету мобильный телефон. Это самый быстрый способ восстановить доступ к счету.

2) Использовать одноразовые пароли.

3) В случае использования постоянного пароля, использовать максимально сложный.

4) Не вводить свои данные на сайтах, которым нет доверия.

Электронная почта

ПРАВИЛА:

1) Выбирать правильный почтовый сервис.

2) Не указывать в адресе почты личную информацию.

3) Использовать двухэтапную авторизацию.

4) Выбирать сложный пароль.

5) Использовать секретные вопросы.

6) Не открывать подозрительные файлы и другие вложения, даже если они пришли от друзей.

7) Выходить из аккаунта после окончания работы в сервисе.

Защита от вирусов

ПРАВИЛА:

1) Использовать современные операционные системы.

2) Постоянно обновлять операционную систему.

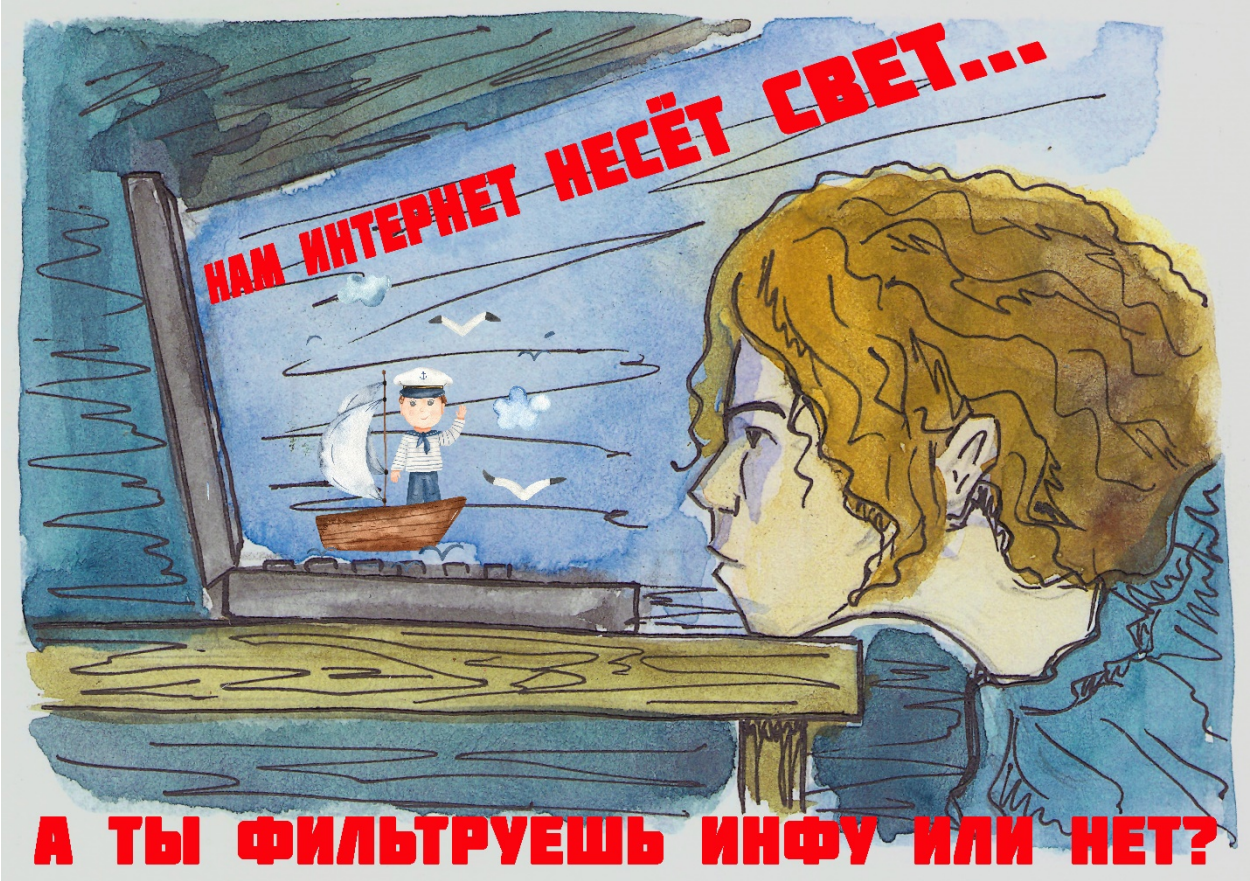
3) Использовать ПК под правом пользователя, а не администратора.

4) Использовать проверенные, лицензионные антивирусные программы.

5) Ограничивать физический доступ к компьютеру посторонних лиц.

6) Не открывать и не устанавливать файлы полученные из неизвестного источника.

Кузьмин Виталий Лазаревич
Областное государственное бюджетное
профессиональное образовательное учреждение
«Томский техникум водного транспорта и судоходства»
Руководитель: Киселева Елена Викторовна



Кужугет Кежик Эртинеевич, Ооржак Ангыр Аясович
Областное государственное бюджетное
профессиональное образовательное учреждение
«Томский техникум водного транспорта и судоходства»
Руководитель: Киселева Елена Викторовна

Воробьева Ксения Андреевна

Областное государственное бюджетное

профессиональное образовательное учреждение

«Томский индустриальный техникум»

Руководитель: Мазенина Александра Николаевна