Департамент профессионального образования Томской области
Областное государственное бюджетное профессиональное образовательное учреждение
«Томский индустриальный техникум»

VIII ОТКРЫТАЯ НАУЧНО-ПРАКТИЧЕСКАЯ СТУДЕНЧЕСКАЯ КОНФЕРЕНЦИЯ «БЕЗОПАСНОСТЬ ЧЕЛОВЕКА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ»

СБОРНИК МАТЕРИАЛОВ

30 ноября 2020 г.

г. Томск, 2020

В данном издании представлены работы участников VIII открытой научно-практической конференции «Безопасность человека в информационном пространстве», состоявшейся 30 ноября 2020 г. в онлайн-формате 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»

ДИСТАНЦИОННОЕ ОБУЧЕНИЕ – ХОРОШО ИЛИ ПЛОХО?

Рачкова А. О.,
Кучерук Д.Я.
ОГБПОУ «Томский государственный педагогический колледж»
Руководитель: Кузьмина Е. А.

Актуальность: В современных условиях не снижается актуальность внедрения информационных и коммуникационных технологий в систему российского образования, растет количество учебных заведений, которые дополняют традиционные формы обучения дистанционными образовательными технологиями. Это тем более важно, что большинство современных молодых людей свободно владеют персональным компьютером, открывают для себя мир посредством Интернета и умело используют сведения, полученные из глобальной Сети. И тут появляется вопрос, связанные с мотивацией к обучению, успеваемости, качестве знаний, получаемых в рамках дистанционного образования, а также об информационной безопасности в сети Интернет.

Проблема: как повысить мотивацию к обучению и улучшить образовательные результаты во время дистанционного обучения?

Гипотеза: предположим, что мотивация к учению и качество знаний обучающихся в период дистанционного обучения понижается, а успеваемость повышается.

Тут следует обратить свое внимание на то, что образовательные программы дистанционного обучения полностью соответствуют обязательному минимуму содержания образовательных программ соответствующего уровня подготовки. Из чего можно сделать вывод, что качество образования нисколько не должно страдать. Но так ли это на самом деле?

Цель: изучение и анализ мотивации к учению, успеваемости и качества знаний.

Задачи:

1. Познакомить с определением “Дистанционное обучение”, достоинствами и недостатками такой формы обучения.
2. Провести анкетирование среди школьников “Как влияет дистанционное обучение на качество знаний?”
3. Создать и продемонстрировать уровневые задания, познакомить с различными образовательными платформами.

Дистанционное обучение - что это?

Термин «дистанционное обучение» использовался Университетом штата Висконсин начиная с 1892г. в каталоге заочных (корреспондентских) курсов. Под дистанционным понималось обучение, организованное на расстоянии.

В российском образовании понятие «дистанционное обучение» появилось в самом конце XX в. Благодаря работам Е.С.Полат, А.А.Андреева. Несмотря на авторитетные теоретические разработки в области дистанционного обучения, в России оно не является формой получения образования. Формой организации образовательного процесса в Российской Федерации признано обучение с использованием дистанционных образовательных технологий.

Еще одно определение, дистанционное обучение — технология целенаправленного и методически организованного руководства учебно-познавательной деятельностью учащихся (независимо от уровня получаемого ими образования), проживающих на расстоянии от образовательного центра. (Энциклопедический словарь Бим-Бада).

Достоинства дистанционного обучения

1. Обучение в индивидуальном темпе - скорость изучения

устанавливается самим учащимся в зависимости от его личных обстоятельств и потребностей.

2. Свобода и гибкость - учащийся может самостоятельно планировать время, место и продолжительность занятий.

3. Доступность - независимость от географического и временного положения обучающегося и образовательного учреждения позволяет не ограничивать себя в образовательных потребностях.

4. Мобильность - эффективная реализация обратной связи между преподавателем и обучаемым является одним из основных требований и оснований успешности процесса обучения.

5. Технологичность - использование в образовательном процессе новейших достижений информационных и телекоммуникационных технологий.

6. Творчество - комфортные условия для творческого самовыражения обучаемого.

Недостатки дистанционного обучения.

1. Отсутствие очного общения между обучающимися и преподавателем.

2. Необходимость наличия целого ряда индивидуально-психологических условий. Для дистанционного обучения необходима жесткая самодисциплина, а его результат напрямую зависит от самостоятельности и сознательности учащегося.

3. Необходимость постоянного доступа к источникам информации. Нужна хорошая техническая оснащенность: компьютер и выход в Интернет.

4. Как правило, обучающиеся ощущают недостаток практических занятий.

5. Отсутствует постоянный контроль над обучающимися, который является мощным побудительным стимулом.

Анкетирование студентов и диагностика ответов

Для решения данной проблемы, нами было принято решение провести

анкетирование среди обучающихся школ г.Томска (МАОУ СОШ №58, МАОУ СОШ №40, МАОУ «Перспектива», МАОУ «Заозерная СОШ №16»), в котором приняли участие 280 школьников с 1 по 4 класс. Мы проработали ответы на вопросы и получились следующие диаграммы.

Вопросы, которые предлагались школьникам:

1.В каком классе Вы обучаетесь?

2.Какая форма обучения Вам больше нравится?

3.Качество Ваших знаний при дистанционном обучении понизилось или повысилось?

4.Ваша успеваемость понизилась или повысилась?

5.Повысилась или понизилась у Вас мотивация к обучению?

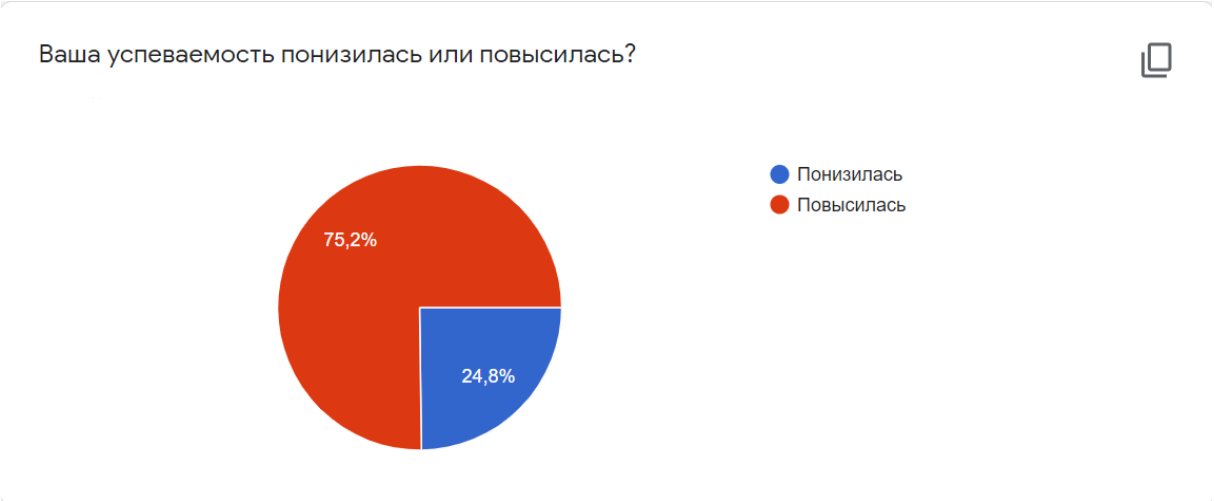
6.Возникли ли у Вас трудности в организации своей деятельности во время дистанционного обучения?

7. Были ли недопонимания в организации деятельности с педагогами онлайн?

Результаты анкетирования:

1. 61.8 % школьников считают, что качество их знаний на дистанционном обучении понизилось.

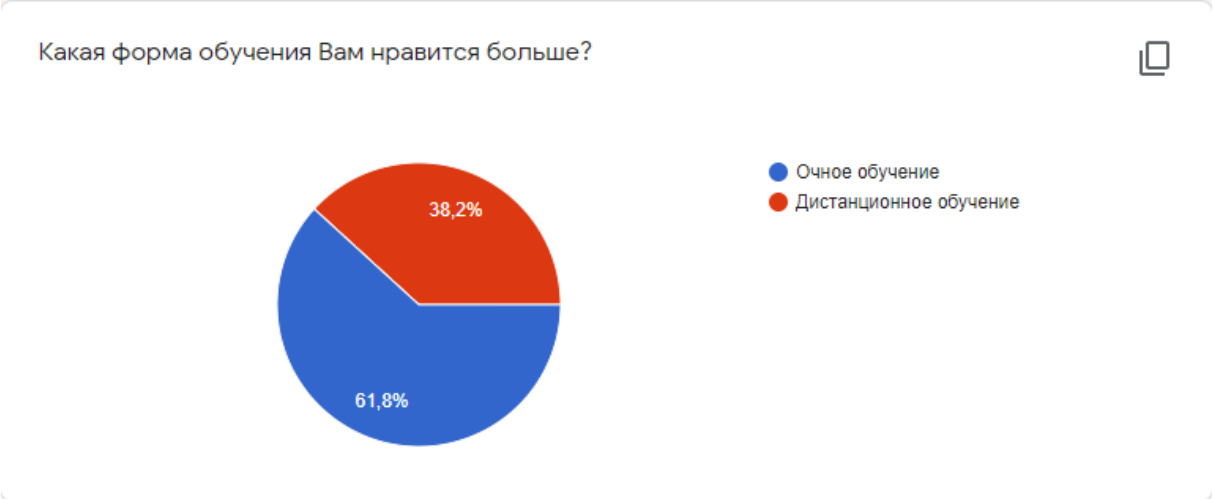
2. 75.2% школьников считают, что их успеваемость повысилась.



3. У 58.9 % школьников понизилась мотивация к обучению.

4. Большей половине школьников было трудно организовать свою деятельность на дистанционном обучении, а также у них были недопонимания в организации деятельности с педагогами онлайн.

5. 61% обучающимся нравится очное обучение больше, чем дистанционное.



Вывод: многие школьники считают, что достаточно сложно учиться во время дистанционного обучения, ведь весь материал необходимо прорабатывать самостоятельно, мотивация к учению понижается, качество знаний ухудшается, успеваемость повышается, соответственно, наша гипотеза подтвердилась.

Решение проблемы.

Как всё-таки добиться улучшения результатов во время дистанционного обучения?

В настоящее время существуют различные методы по дистанционной работе с обучающимися. Но на наш взгляд, одной из самых продуктивных форм можно считать: уровневые учебные задания. Они помогаю разделить задания так, чтобы каждый смог выбрать то задание, которое подходит ему

по уровню. Также каждый педагог может создать такие задания самостоятельно, выбрав платформу, на которой ему будет удобнее работать, тем самым обеспечив безопасность ребенка в большой сети Интернет.

Продукт: уровневые учебные задания - https://rachkovanast.wixsite.com/konfa

Перспектива: дистанционное обучение в настоящий период актуально для всех участников образовательного процесса, поэтому мы не будем базироваться только школьниках, а будем продолжать наше исследование со студентами нашего колледжа и других учебных заведений.

Источники:

1.Айсмонтас, Б.Б. Личностные и мотивационные особенности студентов очного и дистанционного обучения (сравнительный анализ)/ Б.Б.Айсмонтас, Уддин Мд.Актхер. – М.: Изд-во МГППУ, 2014.

2. Информационные и коммуникационные технологии в дистанционном образовании: спец.учеб.курс: пер. с англ./М.Г.Мур, У.Макинтош, Л.Блек (и др.); под ред.М.Г.Мура; Ин-т ЮНЕСКО по информ.технологиям в образовании. – М.: Обучение-Сервис, 2006.

3. Маскаева, А.М. Использование веб-квестов при дистанционном обучении/ А.М.Маскаева, Н.В.Никуличева// Открытое и дистанционное образование. – 2013. - №2(50). – С.15-19.

4. Полат, Е.С. Современные педагогические и информационные технологии в системе образования: учеб.пособие для вузов/ Е.С.Полат, М.Ю.Бухаркина. – 3-е изд., стер. – М.: Академия, 2020.

5. Педагогические энциклопедический словарь/ гл.ред. Б.М.Бим-Бад. - 3-е изд., стер. – Москва: Большая российская энциклопедия, 2009.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И МЕТОДЫ БОРЬБЫ С НЕЙ

Гармашов С.А., Кошлец Д.А.
ОГБПОУ «Томский техникум информационных технологий»
Руководитель: Чувашов М. Д.

ВВЕДЕНИЕ

Формирование общественных отношений между особями человека разумного поспособствовало появлению слоев, честно зарабатывающих на свое существование и лиц, ищущих более простой, при этом нечестный способ улучшение собственного материального положения — мошенников, отнимающих блага у первых. Упоминания о актах мошенничества без труда можно найти в учебниках истории Древнего Рима, Древней Руси и античной Греции. Махинации купцов древности дошли и до наших дней, породив более жестокие и изощренные средства психологического воздействия на человека.

Широкое внедрение электронно-вычислительной техники во многие аспекты человеческой деятельности поспособствовало появлению преступной деятельности с применением компьютеров. Киберпреступления совершаются отдельными лицами, а иногда и группой лиц с целью получения прибыли за счёт пользователей. Пользователи в общем случае даже не представляют, что становятся жертвами своего доверия и базовых эмоций. Игры на доверии, страхе и жадности — любимые методы социальных инженеров.

ЦБ на конгрессе в Санкт-Петербурге в 2019 году выразил крайнюю обеспокоенность в связи с ростом киберпреступлений на основе социальной инженерии в России. Сам ЦБ связывает этот факт с низкой финансовой, цифровой грамотностью, а также с утечками баз данных госструктур. Например, в 2020 году СМИ обнаружили утечку почти 120 тысяч пользователей Сбербанка, в 2019 году утекла информация о пользователей портала Госуслуг. Утекают данные других банков, интернет-магазинов и

даже данные с серверов игровых компаний. По данным «РБК» лишь в 2016 россияне потеряли 650 млн. рублей с собственных карт. По данным «Коммерсанта» в 2019 году российские компании потеряли на социальной инженерии 1,26 млрд. рублей.

Во время пандемии, когда наша страна переживает экономические проблемы, вопрос социальной инженерии стоит ещё острее. По данным всё того же «РБК» в период самоизоляции на 76% выросло число дел о киберпреступлениях.

Целью работы является изучение методов социальной инженерии и её воздействия.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1) Используя литературу, изучить инструменты социальной инженерии.

2) Провести опрос лиц, столкнувшихся лицом к лицу с социальными инженерами, выявить нанесенный ущерб.

3) Выявить наиболее подверженные к действиям социальной инженерии категории и дать рекомендации к предотвращению её воздействия.

Объектом исследования являются методы социальной инженерии и конкретные социальные общности.

Предметом исследования является анализ собранных данных.

Метод исследования: теоретический, статистический.

ОБЩИЕ ПОНЯТИЯ И ПОДХОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В информационной безопасности слабейшим звеном всегда по определению выступает человек. Используя чувства и переживания человека проще совершить атаку, нежели попытаться обмануть бесчувственную машину. Приёмы социальной инженерии не новы и довольно удивительно, почему же до сих пор люди не научились противостоять злоумышленникам.

Общаясь в сети Интернет, люди не видят и не слышат своего собеседника. Сложно сразу догадаться, что в деньги «в долг» просит незнакомый человек. При использовании средств телефонной связи также сложно понять действительно ли человек по ту сторону тот, за кого себя выдает.

Одно из любимых орудий социального инженера – *шантаж*. Получив доступ к аккаунту или любому другому средству, где может храниться компрометирующая информация, с высокой долей вероятности злоумышленник ею воспользуется. Однако шантаж в большинстве случаев дело наказуемое. На смену шантажу приходит другое оружие – *игра на чувствах*. Найдя подход к жертве и установив контакт, социальный инженер обязательно пожалуется на свое трудное положение и в «беде» не останется.

Социальный инженер может получить доступ к аккаунту просто *подсмотрев или выманив* пароль, или используя другой метод, сочетающий в себе социальную инженерию и высокие компьютерные навыки – *фишинг*. Злоумышленник может качественно повторить сайт любой компании, а невнимательный пользователь (или пользователь, не имеющий определенных знаний) вероятно не заметит, что вводит свои конфиденциальные данные на сайте, ссылка на который ведёт на IP адрес вместо домена.

Базы данных с номерами телефонов гуляют по интернету. Обычно такие базы интересны компаниям по предоставлению услуг, однако они могут попасть и в руки социального инженера. Под видом службы технической поддержки злоумышленник способен совершить различные манипуляции с аккаунтом пользователя его же руками или вовсе представиться сотрудником банка и рассказать о подозрительных операциях, которые владелец карты «совершил» (на самом деле они и не совершены вовсе). Испуганный клиент без своего печального опыта или историй от знакомых с большой вероятностью воспользуется помощью «оператора», а в качестве оплаты предоставит ему данные для получения несанкционированного доступа, ответив на пару безобидных вопросов. На

языке социальной инженерии это называется *«Кви про кво»* («Услуга за услугу»).

Социальные инженеры эффективно используют человеческую ревность, злость, предлагая свои услуги «взлома аккаунтов», где заказчик по итогу одномоментно сам становится «взломанным».

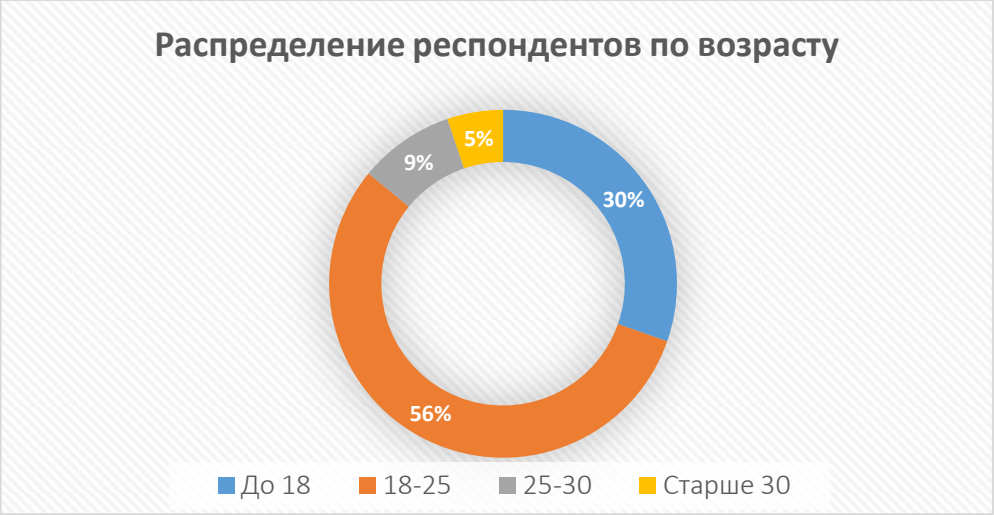
Отсутствие денежных средств, алчность или любопытство заставляют человека перейти по соблазнительной ссылке, например, с «ключом активации программы». Это очередная уловка умелых социальных инженеров: вместо желаемого программного продукта по ссылке находится вирус, использующий ресурсы компьютера жертвы и наносящий ему вред. Такой метод социальной инженерии называется «*Троянским конем*». Почему-то именно он стал камнем преткновения между злоумышленниками и сотрудниками компаний, которые по итогу терпят убытки. Порой люди забывают, где на самом деле бесплатный сыр.

Мы перечислили лишь самые распространенные методы, на деле о инструментах социальной инженерии можно говорить бесконечно.

1. АНАЛИЗ ВОЗДЕЙСТВИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Изучение воздействия социальной инженерии проводилось методом опроса 135 респондентов с использованием инструментов создания форм Google.

Диаграмма 1

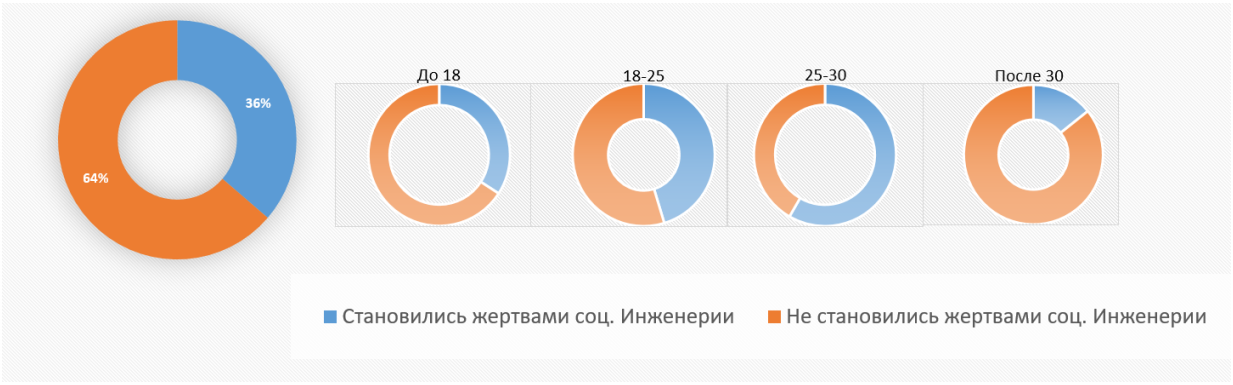


Большая часть опрошенных находятся в возрасте от 15 до 25 лет (86%). По уровню образования наблюдается следующая картина:

Диаграмма 2

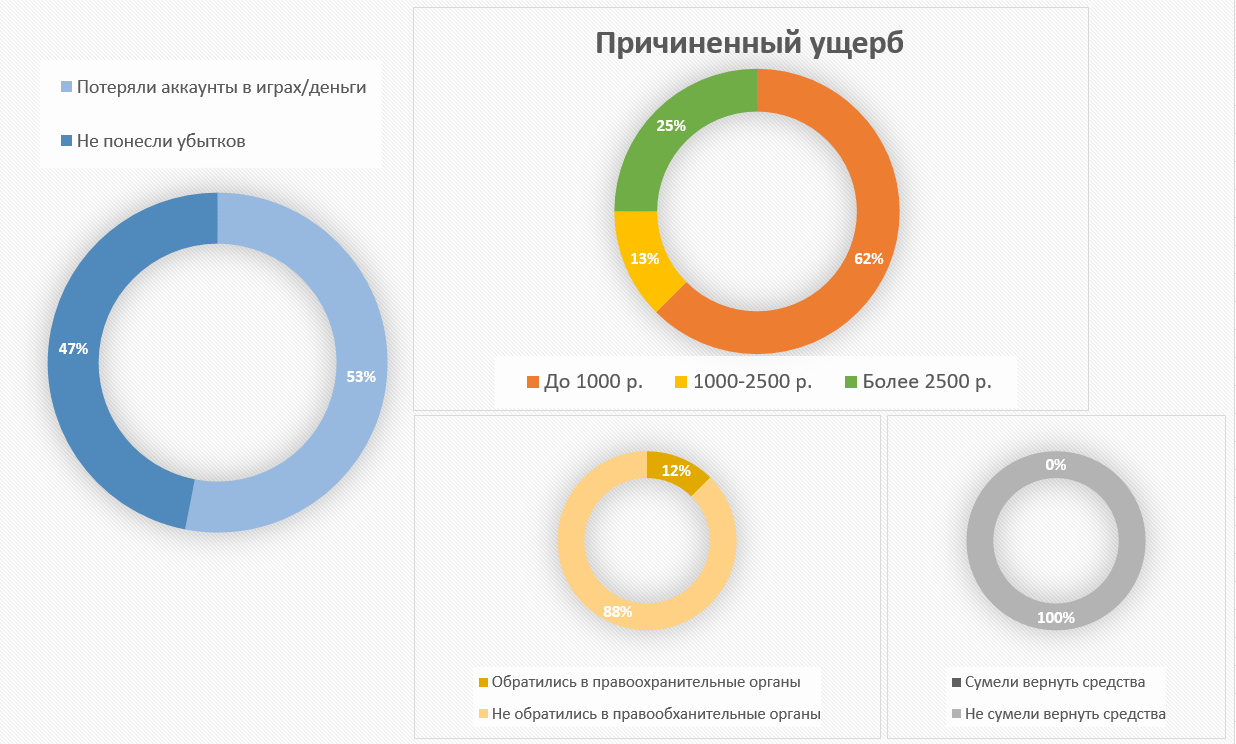
Респондентам было рассказано о социальной инженерии и основных подходах, используемых злоумышленниками. После чего было предложено ответить на вопрос «Становились ли Вы жертвами социальной инженерии?». В результате оказалось, что 36% респондентов так или иначе коснулась данная проблема, а 12% опрошенных и вовсе сами использовали подобные уловки с целью получения несанкционированного доступа к аккаунтам знакомых.

Диаграмма 3



Среди 49 респондентов, ставшими жертвами социальной инженерии 26 человек потеряли ценные аккаунты или денежные средства. В соответствии с 159.6 УК РФ уголовная ответственность за кражу в сети Интернет наступает при причинении ущерба на сумму более 1000 рублей.

Диаграмма 4



Исходя из результатов опроса, 38% респондентов, понесших убытки, могли обратиться в правоохранительные органы, а обратились лишь 12%. Вернуть средства не удалось никому.

Люди, аккаунты которых использовались с целью хищения денежных средств у их знакомых указывают, что в среднем среди 60 человек находится 1-2 небезразличных, теряющих от 1000р. до 3000р.

Каким образом злоумышленник получал доступ к аккаунту? На данный вопрос мы получили множество вариантов ответов. Первые стали жертвой фишинга, вторые в силу ощущения мнимой безопасности использовал слабые пароли и попались на брут-форс атаку, прочие сетуют на использование одинаковых паролей на различных web-ресурсах или вовсе не понимают, как это могло произойти.

ЗАКЛЮЧЕНИЕ

Актуальность социальной инженерии никогда не пропадёт: развитие технологий происходит с невероятной скоростью, а это в свою очередь влечет появление новых методов психологического воздействия на человека

с целью получения выгоды. До сих пор мы не упомянули, что жертвами социальных инженеров стали люди, имеющие высшее образование, а также люди, квалификация которых напрямую связана с информационной безопасность. Ошибки, невнимательность и наивность присущи каждому. Универсального оружия против социальной инженерии нет: среди преступников находятся люди с огромным талантом, способные обхитрить любого. Каждая ситуация требует индивидуального подхода и изучения.

Изучая методы социальной инженерии, мы решили грубо предположить, что основы этих методов со временем остаются одинаковыми. И ключ решения проблемы – жесткая дисциплина. Её отсутствие порождает дыры безопасности. Стоит помнить, что на данный наша страна является раем для социальных инженеров в связи с поразительной мягкостью наказания за подобные преступления и отсутствием достаточных мощностей у правоохранительных органов в этой отрасли. На своей безопасности нельзя экономить, а к любому действию в интернете следует относиться с осторожностью.

Банк никогда не попросит пароль через электронную почту, а лицензионные соглашения в играх не написаны ради забавы. Секретный код, который просят «никому не передавать» обязан быть сохранен в тайне. Если действительно следовать инструкциям компании, которые прописаны системой её безопасности, если проверять всю информацию, которую с легкостью можно «подсунуть под нос» в интернете или слепом звонке, то социальная инженерия окажется просто бессильной.

СПИСОК ЛИТЕРАТУРЫ

1. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 12.11.2018) // Собрание законодательства РФ, 17.06.1996, N 25, ст. 2954

2. Kevin D. Mitnick The Art of Deception / Kevin D. Mitnick, William L. Simon // John Wiley & Sons. – 2002. – P. 304

3. Кузнецов М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов // СПб.: БХВ-Петербург, 2007. – 368 с.

4. Katharina Krombholz Advanced Social Engineering Attacks / Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl // Journal of Information Security and Applications. – 2014. – P. 11

5. Касперски, К. Секретное оружие социальной инженерии [Электронный ресурс] / Крис Касперски. - 11 с. Режим доступа: http://www.gumer.info/bibliotek_Buks/Econom/Article/kasp_sekret.php

ВИДЫ И ИСТОЧНИКИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ УГРОЗ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Добровольский И. М.
ОГБПОУ «Томский аграрный колледж»
Руководитель: Клевцова О. А.

Введение

В современных реалиях информация несёт большую ценность, так как способна приносить существенные доходы и равным образом нести проблемы. Как следствие информационный ресурс нуждается в защите, а именно от возможного разглашения информации, утечки и несанкционированного доступа к охраняемым сведениям, предотвращении противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации. Защита информации нужна для сохранения государственной тайны, конфиденциальности документированной информации в соответствии с законодательством.

В свете вышеперечисленных данных и нарастающих как снежный ком проблем в связи с неверным использованием информационных ресурсов, повсеместных нарушений законов о защите информации мы поставили **целью исследования** рассмотрение особенности информационной безопасности личности в современном мире.

Для достижения данной цели необходимо решить следующие **задачи**:

- исследование нормативно-правовых документов по регулированию безопасности личности;

- определение основных целей и объектов информационной безопасности личности, источников угроз информационной безопасности и основных задач обеспечения информационной безопасности личности.

Объектом исследования является информация в современном мире.

Предметом исследования являются методы и средства защиты информации, а так же борьбы с угрозами информационной безопасности.

Методы исследования. В исследовании использовался методологический инструментарий, интегрирующий исследовательские возможности методов философии, социологии, психологии, управления и ряда других наук, объединенных принципами и подходами междисциплинарного, структурно-функционального, сравнительно-исторического, комплексного и системного изучения исследуемой проблемы

1. Нормативно-правовые документы по регулированию безопасности личности

1.1 Законы, регламентирующие защитную функцию информационной среды и информационных ресурсов на территории РФ

На территории РФ от 7 декабря 2010 года действует Федеральный закон «о безопасности», дающий чёткое понимание того, как важно защищать жизненно важные интересы личности, общества и государства.

Правительство нашей страны, ставит перед собой задачу обеспечить безопасность в этих сферах от информационных угроз.

Что входит в понятие защита информационной среды, отвечает Федеральный закон «Об информации, информатизации и защите информации» (ст. 20):

- Любая утечка информации, любое незаконное вмешательство в информационные ресурсы.
- Конституционные права граждан дают право на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах.

Выделяются три направления правовой защиты. В первом направлении рассматривают защиту чести. Во втором направлении при защите информации ограничивается доступ к разному рода тайн, технологиям, средствам связи и телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц. В третьем направлении защищаются информационные права и свободы личности. Для обеспечения

работы первого направления действуют информационно-правовые нормы Конституции РФ.

- П. 5 ст. 29 Статья 29 гарантируется свобода массовой информации. Цензура запрещается.
- В п. 3 ст. 41 Конституции РФ указано, что личность и общество могут быть защищены от сокрытия опасной информации в соответствии с федеральным законом.
- Статья 29 «Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства».

Что можно отнести к возможной недоброкачественной информации:

- Заведомо ложную рекламу (ст.182);
- Злоупотребления любого характера при эмиссии (выпуск ценных бумаг, ст. 185);
- Заведомо ложные сообщения об актах терроризма попадают под статью 207;
- Ст. 237 поясняет незаконность сокрытия информации об обстоятельствах, создающих опасность для жизни или здоровья людей;
- По ст. 242 запрещается распространять порнографические материалы или предметы;
- Под запрет попадают публичные призывы к насильственному изменению конституционного строя РФ (ст.280), возбуждение национальной, расовой или религиозной вражды (ст.282), публичные призывы к развязыванию агрессивной войны (ст.354).

Согласно статье 23 у каждого из нас есть право на хранение личной и семейно тайны, на защиту своей чести и доброго имени. Сюда же входят « право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений...». Никто не имеет право собирать информацию о гражданах без их согласия

Таким образом, мы видим, что любая защита вышеперечисленных сведений защищается на основании законодательства РФ.

1.2. Информатизация общества и проблема информационной безопасности

Под информатизацией общества понимают совокупность социально-экономического и научно-технического процесса создания оптимальных условий для удовлетворения информационных потребностей и реализации прав.

Большие потоки информации сложны в плане обработки, но их образование имеет под собой весомое основание:

- постоянно растёт число документации в любом виде и направлении;
- увеличивается печатная и электронная периодика в разных областях человеческой деятельности;
- включение разных научных данных (метеорологии, геофизики, медицины, экономики и др.), которые ранее записывались на магнитные ленты, а сейчас попадают на электронные ресурсы;

резкое повышение темпа появления новой информации. Если к начала прошлого века сумма знаний росла медленно, удваивавшись, раз в 50 лет, то с 1990 года такое удвоение идёт ежегодно.

1.3. Виды информационной безопасности

Информационная безопасность личности

Информационная безопасность личности - это состояние и условие жизни личности, при которой реализуются ее права и свободы.

Информационно психологическая безопасность личности

Информационно-психологическая безопасность личности - это состояние защищенности личности и возможностей ее развития, обеспечивающее ее целостность как активного социального субъекта в условиях информационного взаимодействия с окружающей средой. **Информационная безопасность личности и государства** в юридической и

политической литературе выделяют такие понятия, как информационная безопасность личности и государства.

1.4 Источники угроз информационной безопасности

Исходя из понимания жизненных интересов личности, следует понимание смысла фразы «угроза информационной безопасности».

Угрозами информационной безопасности личности являются:

• нормативные акты, которые противоречат конституционным правам граждан;

• отказ в праве граждан на неприкосновенность частной жизни;

• ограничение доступа к открытой информации также неправомерно;

• любое нарушение прав граждан в области СМИ;

• использование специальных средств, которые воздействуют на сознание человека;

• манипулирование информацией.

Сегодня вырос объём и влияние информации, предлагаемой личности и обществу, что сопоставимо с влиянием семьи, школы или социальной группы.

Порой посторонние лица осуществляют разными способами проникновение в базы данных посредством компьютерных сетей, компьютерных вирусов.

Даже если адрес этого сайта сначала мало, кому известен, то существование так называемых поисковых систем - Яндекс, Рамблер, Google и других, делает эту информацию доступной для запроса по каким-либо ключевым словам или фразам документа, по фамилиям людей. На сторонних сайтах тем же способом может появиться конфиденциальная информация об организации. Таким образом, государство должно проводить единую политику с целью обезопасить информационную среду принятием мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства, направленных на выявление, предупреждение угроз извне и

изнутри. Если за информационную безопасность будут сражаться со всех сторон, постепенно исключая источники скрытых и открытых угроз, жизнедеятельность человека станет вне такой опасности, которая грозит ей сейчас.

Во второй части исследовательской работы, будем проводить анализ по выяснению осведомлённости студентов и педагогов о вопросах информационной безопасности

2. Основные задачи обеспечения информационной безопасности личности и способы их решения

2.1 Исследовательская работа по выяснению осознания учащимися колледжа угрозы информационной безопасности

Исследование по вопросам информационной безопасности проводилось на территории Областного государственного бюджетного профессионального образовательного учреждения «ТОМСКИЙ АГРАРНЫЙ КОЛЛЕДЖ» Первомайского филиала. Исследовательская работа включала в себя три этапа: анкетирование и обработка полученных данных, классный час по теме информационной безопасности и обсуждение, повторное анкетирование. Обработка полученных результатов и анализ проведённого исследования.

Первый этап исследования

На первом этапе было проведено тестирование(ссылка на тест https://forms.gle/maZC5sbuXA7f5U6v5) учащихся, среди студентов 1 курса, 2 курса и 3 курса, преподавателей.

Второй этап исследования

Классные часы по теме информационной безопасности и обсуждение. Классный час проводился в трех группах (ТВ-195, ТВ-193, МС-187) разного курса (1 курса, 2 курса, 3 курса)

Третий этап исследования

На этом этапе было проведено повторное тестирование, напрямую касающихся темы информационной безопасности личности.

В тестировании приняло 55студентов и 10 преподавателей

Итого, в третьем этапе исследования участвовали:

- 20 студенты1курса
- 18 студенты 2 курса
- 17 студенты 3 курса
- 10 преподавателей

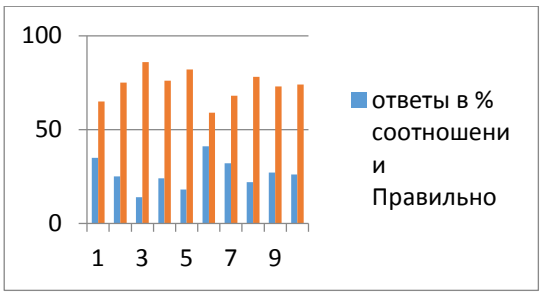
Анкетирование было направленно на выяснение знаний по теме информационная безопасность личности, на пробелы в данной теме. Повторное анкетирование показало, что всё равно эта тема вызывает недопонимание учащихся. Сложности были выявлены как в ответах студентов, так и в ответах преподавателей.

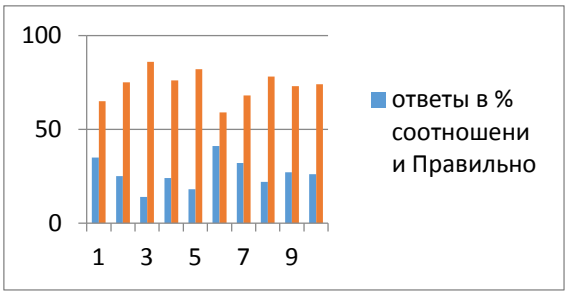
После анкетирования и обработки полученных данных был проведен классные часы по теме информационной безопасности и обсуждение. Наиболее уязвимым местом оказалась сеть интернет.

Для более простого разъяснения правил поведения в сети интернет, студенты и преподаватели были ознакомлены с памятками, а так же была создана стенд - газета.

2.2 Обработка результатов исследования

Каждый этап показал определённые результаты, которые было необходимо обработать и учесть в исследовании. Результаты анкетирования представлены в виде графиков.





первый этап опроса третий этап опроса

Вывод: Для того, чтобы повысить грамотность в данной деятельности, требуется гораздо больше времени уделять таким важным вопросам современного образа жизни и всеобщей компьютеризации и информатизации.

Заключение

Итак, в ходе работы над темой исследования были достигнуты все поставленные задачи и цель:

1) Было проведено исследование нормативно-правовых документов по регулированию безопасности личности;

2) Дано определение основных целей и объектов информационной безопасности личности, источников угроз информационной безопасности и основных задач обеспечения информационной безопасности личности;

3) На примере экспериментальной работы по теме исследования были получены сведения о состоянии информационной безопасности личности на примере учащихся колледжа и педагогического.

Я считаю, что цели и задачи данной работе достигнуты.

Список литературы

1. Конституция Российской Федерации. М.: Юридическая литература,1996.

2. Закон РФ "О федеральных органах правительственной связи и информации". №4524-1 от 19.02.93 // Ведомости Совета Народных Депутатов и Верховного Совета РФ. 1993. - №12. - Ст.423.

3. Федеральный закон "О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации" №7-ФЗ от 13.01.95 // Собрание законодательства РФ. 1995. - №3. Ст. 170.

4. Федеральный закон "Об информации, информатизации и защите информации" №24-ФЗ от 20.02.95 // Собрание законодательства РФ. 1995. - №8. - Ст. 609.

5. Федеральный закон "Об участии в международном информационном обмене" №85-ФЗ от 04.07.96 // Собрание законодательства РФ. 1996. -.№28. - Ст.3347.

6. Федеральный закон "О государственной поддержке средств массовой информации и книгоиздания Российской Федерации" №159-ФЗ от 22.10.98.

СЕКЦИЯ 2. «СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ «IoT» ОБЪЕКТОВ»

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

Савин Д.Д.

ОГБПОУ «Молчановский техникум отраслевых технологий»

Руководитель: Литвинов А. С., Смирнов Я. В.

ВВЕДЕНИЕ

Актуальность исследования**:** Стандарты, реализации и концепции умных городов построены на применении быстро развивающихся цифровых и иных технологий и нацелены на экономические, социальные, экологические и иные положительны эффекты при их применении в городах. Внедрение таких инноваций, трансформирует городской уклад жизни невероятно быстрыми темпами и сопровождается цифровыми угрозами и опасностями. Эта тема требует и особого внимания и множества исследований. В приоритете при выборе решений в сфере городской безопасности защита инфраструктуры и проживающих людей. Создать комфортные и удобные условия для существования становится сверхзадачей. А удобство, комфорт и безопасность – это неразделимые понятия.

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 без опасности встает в полном объеме.

Цель исследования – анализ вызовов «умным городам» и современных технологий организации комплексной безопасности.

Задачи исследования:

1. Изучить современные данные по теме исследования

2. Проанализировать и систематизировать полученную информацию

3. Выявить технологии комплексной безопасности.

Методы исследования: исторический анализ, сопоставительный анализ, социологическое исследование, аналитико-синтетический.

1.ОБЗОР ЛИТЕРАТУРЫ О БЕЗОПАСНОСТИ УМНЫХ ГОРОДОВ

По данным ABI Research, к 2024 году будет около 1,3 миллиарда подключений к интеллектуальным городам в глобальных сетях. Ожидается, что почти 50% этих подключений будут LPWA-LTE и LPWA. Некоторые протоколы LPWA, такие как NB-IoT, пытаются решить хотя бы некоторые проблемы цифровой и коммуникационной безопасности.

В России с 2014 года действует концепция построения и развития АПК «Безопасный город» (Распоряжение Правительства РФ от 03.12.2014 №2446-р), а в 2018 году Минстроем России утвержден паспорт ведомственного проекта «Умный город».

Составляющая национальных интересов включает развитие современных информационных технологий, отечественной индустрии информации, телекоммуникации и связи, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. Только на этой основе можно решать проблемы создания наукоемких технологий.

Создание базовой системы зашиты информации в ИС основывается на следующих принципах:

1. Комплексный подход к построению системы защиты при ведущей роли организационных мероприятий. Он означает оптимальное сочетание программных аппаратных средств и организационных мер защиты, подтвержденное практикой создания отечественных и зарубежных систем защиты.

2. Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки. Пользователям

предоставляется минимум строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей.

3. Полнота контроля и регистрации попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ИС без ее предварительной регистрации.

4. Обеспечение надежности системы защиты, т.е. невозможность снижения ее уровня при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала.

5. Обеспечение контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты.

6. «Прозрачность» системы защиты информации для общего, прикладного программного обеспечения и пользователей ИС.

7. Экономическая целесообразность использования системы защиты. Стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту

Smart Cities - это набор технологических инновации и инициатив, использования датчиков и использование большей возможности подключения для увеличения сбора данных. Основная цель: «Умный город» должен улучшить жизнь граждан более эффективным использованием данных, позволив лучше и устойчивее управлять инфраструктурой и услугами. «Умные города» должны обеспечить безопасность и эти соображения являются краеугольным камнем их системы.

Очень интересная и, по нашему мнения, модельная система для России, есть инициатива по созданию общей городской платформы.

Проект предполагает построение иерархической комплексной информационной системы уровня «дом-район (город)». В проекте

выделяются следующие пять основных компонентов комплексной системы «Безопасный интеллектуальный город:

1. Техногенная безопасность. Назначение – обеспечение защищенности граждан и городских объектов, в том числе ГИОП, от воздействия опасных процессов, вызванных повреждениями и разрушениями конструкционных, тепловых, водных, энергетических систем, ошибками в эксплуатации и несанкционированными воздействиями.

2. Экологическая безопасность. Назначение – мониторинг экологического состояния воздушной среды и водного бассейна для обеспечения защищенности граждан и природной среды от возможного негативного воздействия хозяйственной деятельности

3. Транспортная безопасность. Назначение – обеспечение защищенности граждан на транспорте, объектов транспортной инфраструктуры и транспортных средств от незаконного вмешательства.

4. Общественная безопасность. Назначение – обеспечение личной защищенности граждан в местах проживания, на придомовых территориях, в местах массового отдыха, на культурных и архитектурно-исторических объектах.

5. Энергоэффективность и ресурсосбережение. Назначение – обеспечение оптимизации затрат и потребления энергоресурсов, водных ресурсов, тепловых ресурсов социальными, жилищно-коммунальными и иными объектами.

2. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ КОМПЛЕСНОЙ БЕЗОПАСНОСТИ

Основные задачи, проекта «Безопасный город»:

Наладка видеонаблюдения за общественным порядком в людных местах, документальное фиксирование произошедших событий, а также для визуального наблюдения за отдельными лицами;

- Контролирование и охрана культурно значимых объектов, с целью выявить и зафиксировать на видео акты вандализма;

- Контролирование ситуации на автомобильных дорогах;
- Проведение розыска транспортных средств;
- Контроль правонарушений на дорогах;
- Контролирование состояния улиц, а также выявление локации аварии на объектах ЖКХ и контроль пожарной ситуации в городе;
- Наблюдение за объектами городской инфраструктуры с целью их защиты.

При организации городской системы безопасности не возможно пройти мимо этих факторов. Поэтому принимаемые решения должно быть разумными и взвешенными, принятые с мыслью о защите и комфорте граждан. Кроме этого важна их прогрессивность и экономическая эффективность.

Автоматизированная система камер видеонаблюдения «Безопасный Город» способна повысить эффективность работы всех муниципальных служб, а именно:

- Охрана общественного правопорядка и безопасности;
- Эффективность взаимодействия и реагирования всех экстренных служб;
- Контроль и выявление социально опасного поведения и вандализма;
- Оперативное получение данных и доступ к видеоархиву;
- Защита стратегически значимых объектов в пределах города;
- Эффективная работа системы оповещения граждан о возникновении опасных ситуаций.

Внедрение централизованной городской системы безопасности позволяет значительно снизить уровень преступности и риск терактов, улучшить координацию действий правоохранительных органов и экстренных служб, а также предотвращать или уменьшать последствия крупных аварий. Комплексная городская система безопасности строится на базе единого городского ситуационного центра, в функции которого входит:

- мониторинг загрязненности окружающей среды;
- мониторинг значимых инфраструктурных, административных, культурных объектов (СМИС и СМИК)
- прием сигналов с тревожных кнопок;
- прием экстренных вызовов с автоматическим определением местоположения абонента;
- обработка данных об обнаружении опасных грузов на транспорте;
- обработка данных камер видеонаблюдения, видеоаналитика;
- Оповещение населения.

Какие решения востребованы сейчас в образовательных учреждениях? В первую очередь, системы обеспечения безопасности.

Сегодня в системах контроля и управления доступом в основном используется барьерный. Сейчас существуют более продвинутые бесконтактные интеллектуальные системы. Они основаны на принципе распознавания и идентификации на основе биометрических данных: по отпечаткам пальцев или по лицам.

К сожалению, эти системы пока крайне дороги и не получили широкого распространения. Уверен, что первый успешный проект внедрения подобной «умной безопасной школы» способствовал бы его тиражированию в регионе.

Умные города все чаще подвергаются атакам различных угроз. К ним относятся сложные кибератаки в критически важной инфраструктуре, приведение промышленных систем управления в тупик, злоупотребление маломощными глобальными сетями (LPWAN), угрозы блокировки системы, вызванные вымогательством, манипуляции с данными датчиков, (например, системы обнаружения стихийных бедствий), а также незаконное получение личных данных. В этом все более и более связанном технологическом ландшафте каждая услуга «умного города» так же надежна, как и ее самое слабое звено.

Международная электротехническая комиссия ведет разработку интеллектуальных стандартов городов для электротехнологий, чтобы помочь интеграции, взаимодействию и эффективности городских систем. Власти всех стран стараются разрабатывать стандарты и руководящие принципы, но многое еще предстоит сделать.

Некоторые города, ожидающие потенциальную обратную сторону цифрового преобразования, уже внедрили меры предосторожности. 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.

В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

ЗАКЛЮЧЕНИЕ

Продвижение в области цифровой техники, информации и коммуникационных технологий являются важными для этих изменений. Однако более широкое использование и зависимость от этих технологий, особенно когда они применяются в сочетании с гораздо более широким использованием и применением городских данных и информации, а также новые модели предоставления услуг, также создает значительные уязвимости и связанные с ними проблемы с безопасностью.

Поэтому подход умного города, ориентированный на безопасность, отличается от любых политик и процессов по безопасности, которые могут уже существовать в пределах отдельных местных органов власти или другой

службы поскольку он должна реагировать на новые или расширенные уязвимости, созданные изменениями существующих способов работы.

Важно, чтобы для любого отдельного и особенного города, ориентированного на этот подход к безопасности он являлся уместным и пропорциональным рискам и не мешал реализации целей города. Кроме того, индивидуальные организационные стратегии и процессы, ориентированные на безопасность следует, в случае необходимости, поддерживать и дополнять этот более широкий подход.

Развитие в России цифровой экономике определено решениями Президента РФ, и тема умных городов уже вошла в программы ее развития. Вместе с тем, авторам представляется, что в этом, безусловно, важном и нужном деле необходим всесторонний учет уже достигнутого в мире и быстрое освоение необходимого.

Проблемы цифрой экономики России - это общие проблемы всех нас, и их необходимо обсуждать и решать сообща.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2020. – 400 с.

2. Безопасный город https://www.intelvision.ru/services/safe-city.

3. Дрожжинов В.И., Куприяновский В.П., Намиот Д.Е., и д.. Умные города: модели, инструменты, рэнкинги и стандарты. https://cyberleninka.ru/article/n/umnye-goroda-modeli-instrumenty-renkingi-i-standarty.

4. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2019. – 64 с.

5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2020. — 280 с.

6. Намиот Д.Е., Куприяновская Ю.В. Цифровая безопасность умных городов https://cyberleninka.ru/article/n/tsifrovaya-bezopasnost-umnyh-gorodov.

7. Намиот Д.Е., Шнепс-Шнеппе М.А. Об отечественных стандартах для Умного Города. https://cyberleninka.ru/article/n/ob-otechestvennyh-standartah-dlya-umnogo-goroda.

8. Панин Д.Н., Железнова П.В.' , Лапаева О.С., Новикова Д.Д. Цифровая безопасность умных городов https://research-journal.org/technical/cifrovaya-bezopasnost-umnyx-gorodov.

9. Партыка Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум, 2019. – 88 с.

10. Умный город – основной принцип и технологические задачи https://www.intelvision.ru/services/smartcity

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

КИБЕРПРЕСТУПНОСТЬ

Варламов А. А.

ОГБПОУ «Томский техникум информационных технологий»

Руководитель: Слепухина Н. С.

Введение

Мы живем в век информационных технологий, когда ПК охватывает всю жизнедеятельность человека и государства. В наше время актуальна проблема с киберпреступностью. Почти у каждого из нас есть телефон или ПК. Более 70 процентов населения земли не могут обойтись без своего телефона или ПК. Сегодня ПК используется во всех сферах жизни, в проведение досуга или для работы. Быстрое развитие персональных компьютеров и быстро увеличивавшейся рынок новых электронных устройств изменили и способы проведения досуга, и методы ведения бизнеса.

Сегодня мы храним всю информацию на ПК или другом устройстве и хотим защитить ее от кражи. В данное время, как не когда ранее актуальна проблема зашиты своих данных. По мене развития технологий развевается и способ защиты информации, но также и растет и количество преступлений по кражи информации или других данных. Невозможно создать идеальную систему зашиты. В любые системы есть уязвимость.

Объект исследования – киберпреступность, ее виды и особенности, структура и способы борьбы с ней.

Цель: Изучить проблемы развития киберпреступности в мире и России и найти способы ее профилактики

Задачи:

1. Провести опрос на знание киберприступности
2. Изучить понятие киберпреступности, основные виды преступления в сфере информационных технологий, ущерб, наносимый киберпреступностью.
3. Рассмотреть виды киберпреступлений.
4. Найти примеры киберпреступлений в мире, России.
5. Дать рекомендации противостояния хакерам в домашних условиях.

Описание

Мною был проведен опрос, вопросами которого являлись два вопроса:

1. Встречались ли вы с киберпеступностью?
2. Как защититься от киберпреступников?

Опрос проводился в соц. сетях, участвовало 100 человек (студенты моей группы, друзья родственники). Результаты опроса показали, что многие не знают, что такое киберпреступность и как с ней борется.

Что же такое киберприступность?

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Есть несколько видов киберпреступлений:

1. Кража аккаунтов

2. Номеров кредитных карт

3. Распространение вирусов или вирусных программ

Сейчас большинство киберпреступлений совершается в сети Интернет. Так вложив деньги в какой-либо сайт в сети интернет вас могут обокрасть и забрать все ваши деньги. Так же еще одним видом мошенничества является аукцион, на котором сами продавцы поднимают цены на товар.

Один из видов киберпреступления – это разнесение вредных компьютерных вирусов. Компьютерный виру – вид вредоносного программного обеспечения, он способен создавать копии самого себя, внедрятся в код других программ, в системе области памяти, в загрузочные секторы, а также способен распространять свои копии по разным каналам связи.

Распространяются вирусы, встраивая свой код в код другой программы для выполнения последующих не разрешённых действий. Внедряясь в другие программы вирус может управлять всеми возможностями программы вплоть для удаления файлов и данных, причем даже абсолютно изничтожить операционную систему устройства. Примером может послужить вирус под названием “LoveLetter” который в 2000 году за небольшой промежуток времени заразил более миллиона портативных компьютеров.

Год за годом растет количество покушений на безопасность сайтов. В последние пару лет ООН (Организация Объединённых Наций) обеспокоено в увеличении киберпреступлений в сфере информационных технологиях, что показывает, что проблемы информационной безопасности переходит на международный уровень.

Интернет не тот что был несколько лет назад. Сейчас в интернете больше возможностей чем раньше. Киберпреступники тоже не стоят на месте, они становятся умнее и хитрее. Но люди только сейчас начали беспокоится и уделять внимание этой угрозе. Если раньше стоило

беспокоится только о зашите своих данных, то сейчас надо думать о защите секретных баз и компьютерных систем.

С хакерами начали появляется и группы хакеристов – хакер который причиняет ущерб не только ради денег, но и ради и идеи. Пентагон показывает группу хакеристов под названием “Anonymous”, как пример серьезной угрозы для всех. Anonymous известна по взлому госструктур и нападению на разные крупные корпорации. Атаками подверглись не только госструктуры, но и различные компании и корпорации по произведению оружия или атомных ректоров. Все это может привести к кибервойнам.

Быстрому развитию киберприступлений способствует безнаказанность и доступу в Интернет, а также не способность полиции вычислить такого преступника.

Киберприступники не могут использовать обычный Интернет, так как из-за него их могут вычислить и пойманы полицией. Они использует Глубинный Интернет.

Глубокая паутина - часть веб-страниц Всемирной паутины, не индексированная поисковыми системами.

Весь доступный обычному пользователю Интернет составляет только пару процентов. Считается что этот вид Интернета самым безопасным, поэтому там много преступников

Ущерб от Киберпреступности

В России ущерб от киберпреступности составляет около двух миллиардов долларов в год.

В 2011 году ущерб мировой экономики составил примерно 2.5 миллиардов долларов, а в 2012 году около 18 миллиардов. В 2019 году от киберпреступности пострадало около 600 миллионов пользователь

различных устройств, которым более 60 лет, это больше населения европейского союза.

Оборот киберпреступности

В год киберпреступники списывают со счетов более 388 миллионов долларов, это больше оборота на черном рынке, на котором оборот составляет около 299 миллионов долларов

Если знать правила технической, и не только, самозащиты, то будешь в безопасности.

Как защититься от киберпреступников:

1. Используйте виртуальные карты
2. Храните номер карточки и ПИН–коды в тайне
3. Поставьте лимит на сумму списаний или перевода в банке
4. Регулярно проверяйте состояние своих банковских счетов
5. Устанавливайте надежную антивирусную программу на электронные носители
6. Используйте сложные электронные пароли в различных онлайн-сервисах и они не должны совпадать
7. Не нужно вестись на тонкие психологические приемы киберпреступников.

Заключение

В последние годы преступления в сфере информационных технологиях стали опасны для общества. Несмотря что киберпреступность появилась недавно она очень быстро развивается. Из-за неподготовки полиции к такому роду преступления и скрытность самих преступников способствует развитию киберпреступности. Киберпреступность сильно отличается от традиционных

видов преступлений. Из-за этого появляется ряд проблем по развитию зашитых мер от кражи информации, с дальнейшем ее использованием и распространение вирусных программ, которые нарушают работу компьютера. Считаю, что поставленные цель и задачи проекта достигнуты. При работе над проектом узнал много нового, интересного и полезного. Думаю, представленная информация пригодится в жизни. Чем сильнее мы зависим от компьютерных систем, тем опаснее уязвимость от всевозможных киберприступников. О безопасности нужно думать всегда.

Литература

1. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия, М., 1996г 182

Интернет ресурсы:

1. Киберперступность: http://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%EF%F0%E5%F1%F2%F3%EF%ED%EE%F1%F2%FC/

2. Компьютерные вирусы: http://dic.academic.ru/dic.nsf/ruwiki/977057

3. Википедия. Преступления в сфере информационных технологий: https://ru.wikipedia.org/wiki/Преступления_в_сфере_информационных_технологий

КАК ЗА НАМИ СЛЕДЯТ

Попкова К. В., Лузин К. В.

ОГБПОУ «Томский индустриальный техникум»

Руководитель: Алькова М. А.

ВВЕДЕНИЕ

Аннотация: для современных людей существует множество причин сокрытия от опознания при нахождении в сети интернет. Таковыми являются: контроль правоохранительных органов, работодателей и администрации учебных заведений. Наблюдается тенденция усиления контроля сети интернет российскими правоохранительными организациями. Кроме того, многим людям просто нравится ощущение анонимности и свободы общения, это их право. Право, защищенное 23 и 24 статьями Конституции РФ.

На сегодняшний день почти каждый человек, независимо от возраста проводит время в интернете. В качестве исследовательской работы был проведён онлайн-опрос, в котором участвовало 110 человек. В ходе опроса было выявлено, что большинство человек проводит время в интернете каждый день, и только 10,9% посещает интернет время от времени.

ВОЗМОЖНОСТЬ КРИПТЫ

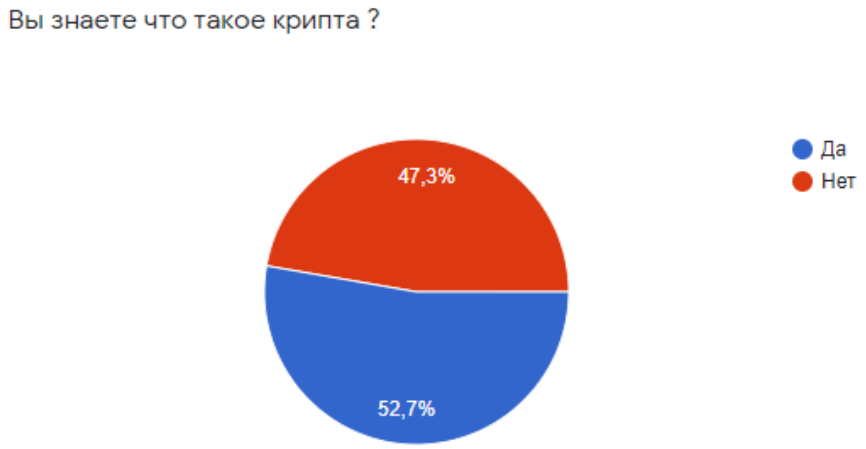
Благодаря Крипте каждый из миллионов людей, которые заходят на сайты сервисов Google и его партнёров, видит на их страницах предложения, которые могут быть актуальны именно для него. Другими словами, эта технология даёт рекламодателям возможность показывать свои объявления только тем, на кого они рассчитаны, например людям определенного возраста, дохода и привычек, которые живут в конкретном районе города. Выяснить, принадлежит ли пользователь к такому сегменту.

Система специально устроена так, что Крипта не получает личной информации о людях и тем более не передаёт её рекламодателям. Каждый пользователь для неё — это набор идентификаторов. Крипта может с высокой вероятностью предположить, что пользователю с таким-то идентификатором может быть интересно такое-то предложение, — но кто этот человек, как его зовут и тому подобное, она не знает.

Крипта работает на основе различных методов машинного обучения. Чтобы установить признаки, по которым человека можно отнести к какой-либо группе, она исследует сетевое поведение её типичных представителей: какие слова они используют в запросах, сколько запросов задают за сессию, какие сайты посещают, в какое время суток выходят в интернет и т. д. — всего около 300 факторов.

Затем Крипта рассчитывает значимость каждого фактора для конкретного сегмента пользователей. В итоге получается формула, с помощью которой вычисляется вероятность принадлежности пользователя к данной группе. Эти данные пересчитываются каждый день, чтобы успевать реагировать на изменения в интересах людей.

По данным опроса про технологию «крипта» знают 52,7% опрошенных.



1.1. РЕКЛАМА

Технология крипта, позволяет настраивать рекламу и показывать объявления, которые будут интересны именно вам. Социальные сети делают также, например, INSTAGRAM. Обычный разговор о новогодних украшениях в direct, до покупки в магазине «Пятёрочка».

И в опросе на эту тему большинство людей ответило согласием:

ХРОНОЛОГИЯ В GOOGLE КАРТАХ

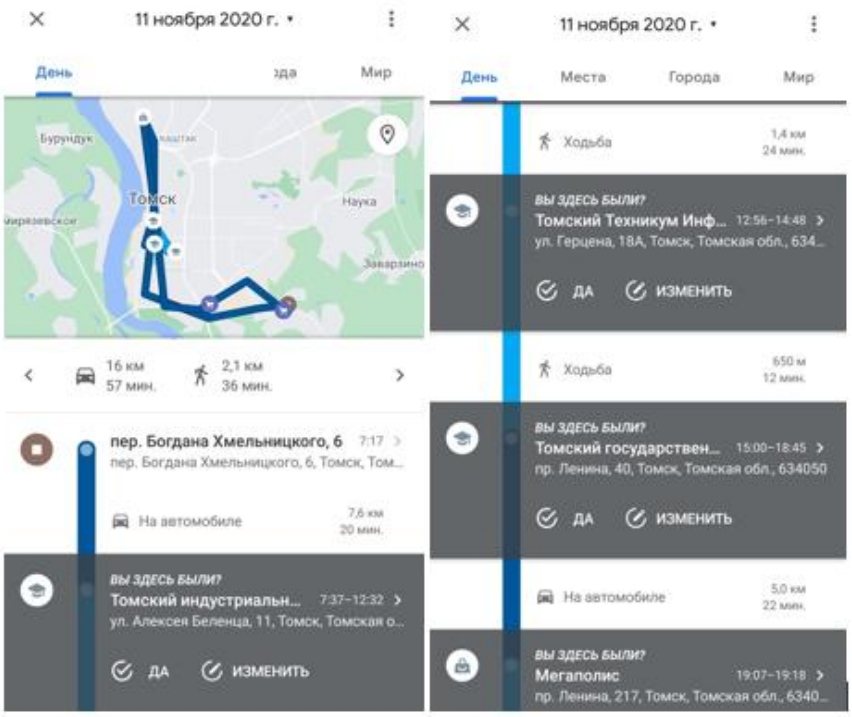
Просмотреть свою историю местоположений и изменить соответствующие настройки можно с помощью хронологии в Google картах.

В хронологии можно изменять отдельные записи из истории местоположений, а также удалять информацию за определенные периоды или же в полном объеме.

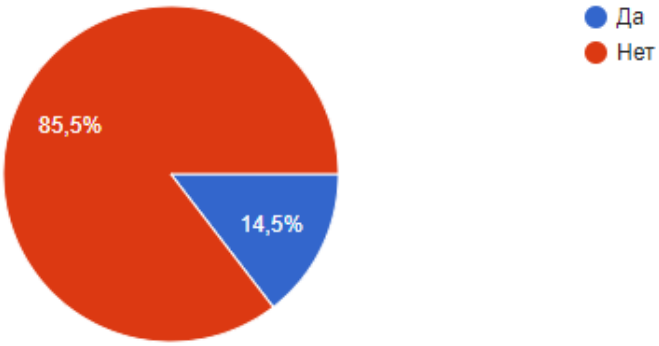
Если включена история приложений и веб-поиска и, приостановить историю сохранения местоположения, то геоданные могут по-прежнему сохраняться в аккаунте при использовании других сайтов, приложений и сервисов Google.

Например, при включенной истории приложений и веб-поиска данные о местоположении могут сохраняться в результате действий в Google Поиске и на картах и в зависимости от настроек камеры добавляться в сведения о фото.

А также опрошенным был задан вопрос «Просматриваете ли Вы свою хронологию в google картах?» и результаты были такие: 85,5% опрошенных ответили, что не просматривают, а 14,5% опрошенных смотрят свою хронологию.



Просматриваете ли вы свою хронологию в Google картах?



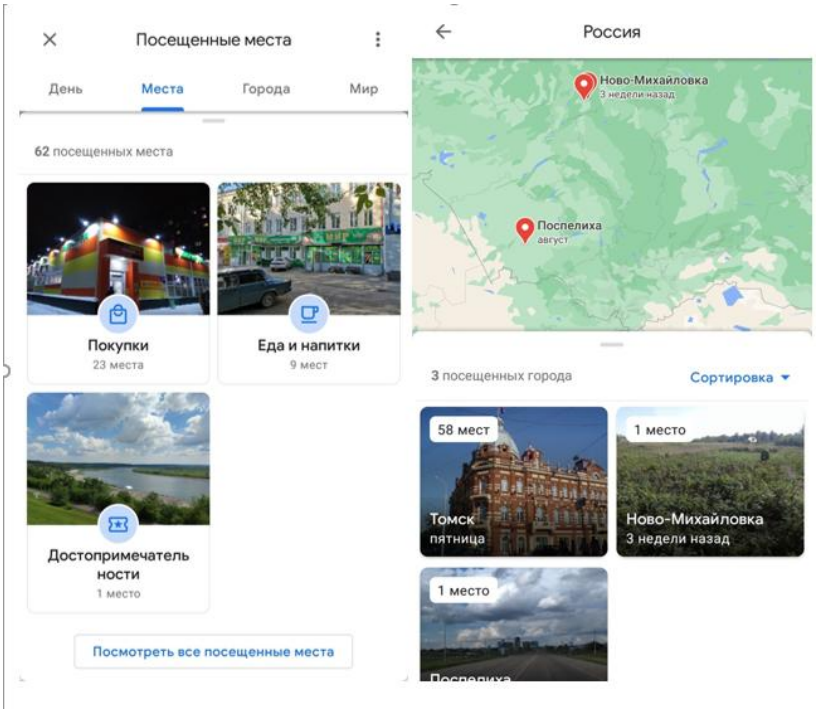
1.1. Зачем Google использует данные о местоположении?

Google стремится предоставлять пользователям самую актуальную и полезную информацию, и данные о местоположении играют при этом важную роль. Зная, где находится пользователь, google может предлагать маршруты проезда, результаты поиска, включающие места поблизости и подробные сведения о них. Данные о местоположении также помогают в работе базовых функций продуктов, позволяя показывать сайты на нужном языке и защищать сервисы Google.

В опросе про геолокацию и про онлайн – карты, были выведены следующие данные:

1.2. Как Google определяет местоположение?

В зависимости от того, какие продукты пользователи используют и какие настройки выбирают, можно передавать в google разные типы информации о местоположении, которая нужна для работы одних сервисов и делает полезнее другие. Местоположение может определяться по сигналам в режиме реального времени, таким как IP-адрес или местоположением устройства, а также по истории действий на сайтах и в сервисах Google, позволяя персонализировать работу с ними с учетом контекста.



ЗАКЛЮЧЕНИЕ

В качестве заключения нашего исследования был задан последний и важный вопрос: «Вы догадывались, что Google за вами следит?!»

Мнения разделились, но преобладание неизвестности в слежке google всё же перевалило больше всего.

СЕКЦИЯ 4. «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ПЛАКАТАХ»

Митькина В. В.

ОГБПОУ «Томский индустриальный техникум»

Руководитель: Абатуров И. А.

Глевицкая А. А.

ОГБПОУ «Томский аграрный колледж»

Руководитель: Горбунова Т. С.

Кусмарцева А.А.

ОГБПОУ «Колпашевский социально- промышленный колледж»

Руководитель: Криницкая Н. А.

Тыхеева А. И.

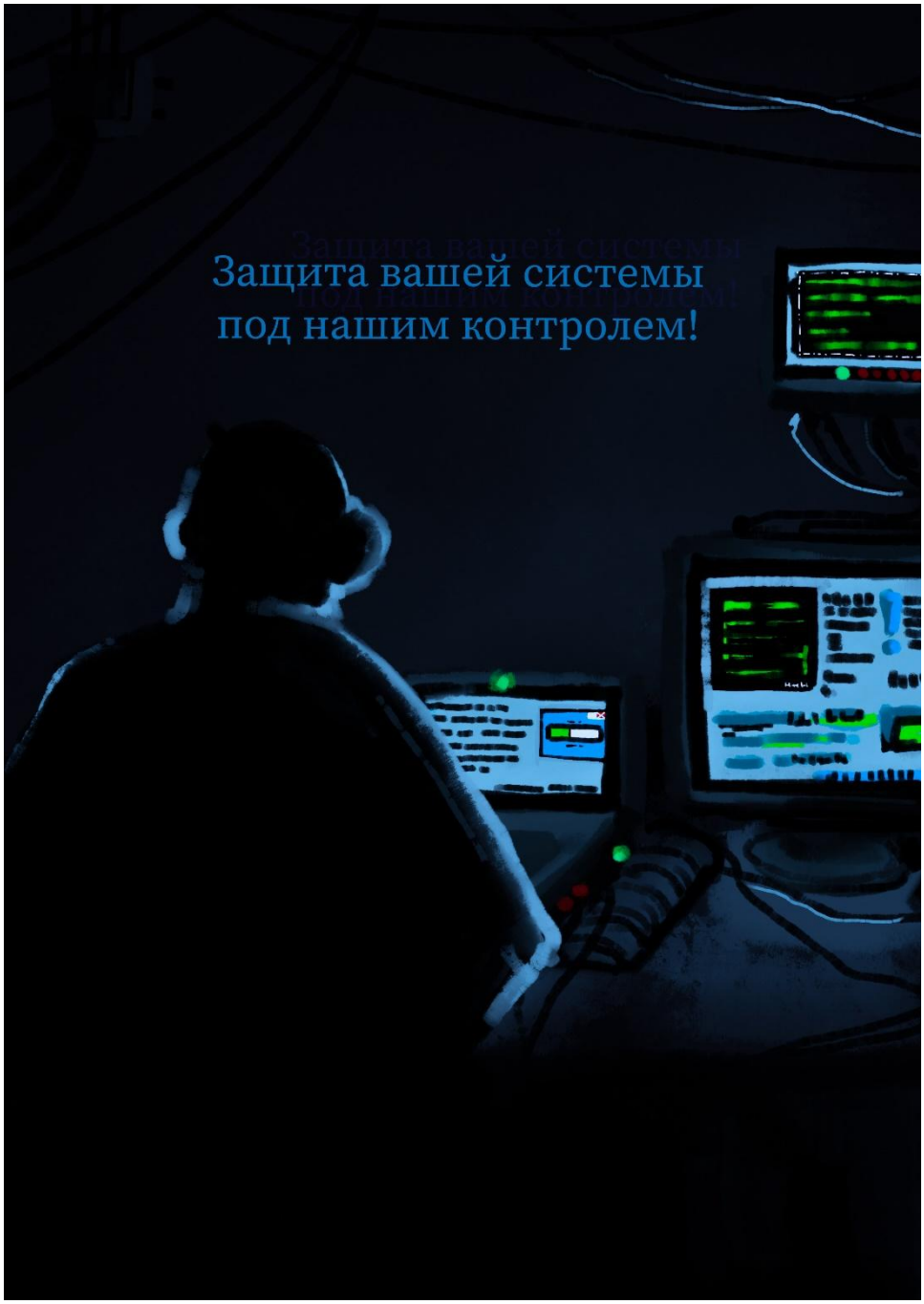
ОГБПОУ «Томский индустриальный техникум»

Руководитель: Тумакова Н. А.

Аверкиева С. А.

ОГБПОУ «Томский индустриальный техникум»

Руководитель: Пургина М. В.



Кривошеин К. Д.

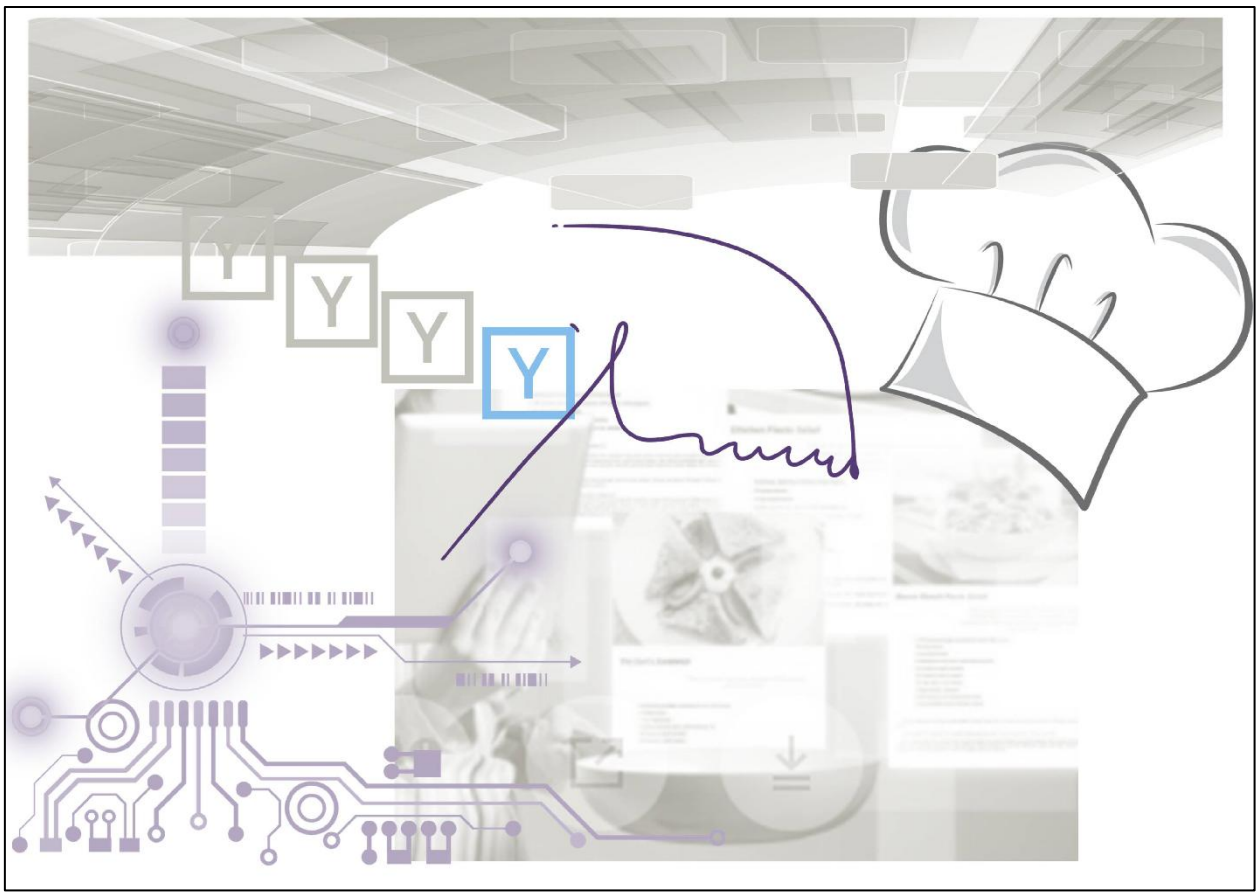
ОГБПОУ «Колпашевский социально- промышленный колледж»

Руководитель: Криницкая Н. А.

Сухушина М. И.

ОГБПОУ «Колпашевский социально- промышленный колледж»

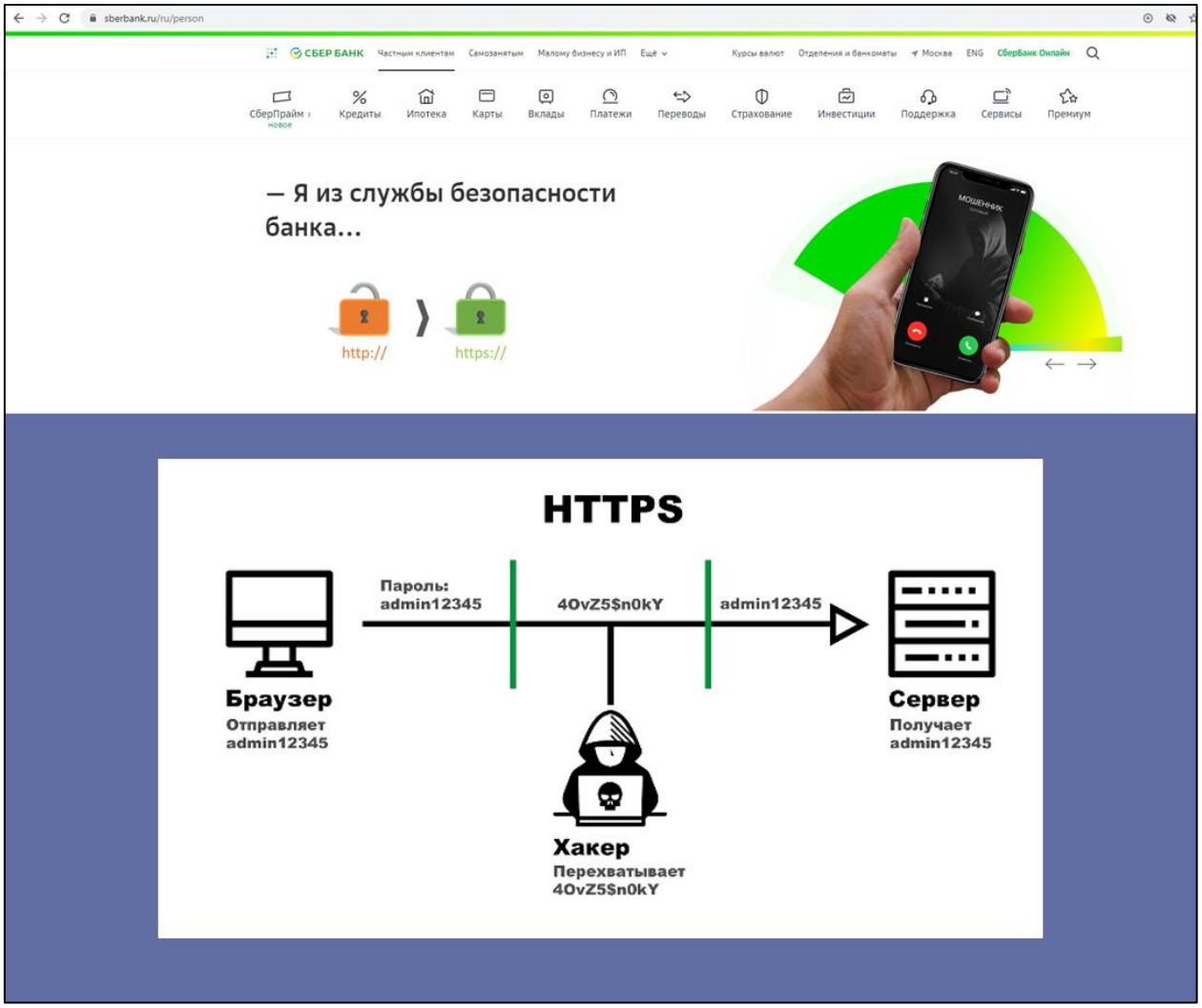
Руководитель: Криницкая Н.А.



Березин Д. А.

ОГБПОУ «Томский индустриальный техникум»

Руководитель: Асадулина Г. С.



Алексеенко Ю. А.

ОГБПОУ «Колледж индустрии питания, торговли и сферы услуг»

Руководитель: Элис Т.В.

Папкина П. В.

ОГБПОУ «Томский индустриальный техникум»

Руководитель: Мазенина А. Н.

Фёдоров П. В.

ОГБПОУ «Томский индустриальный техникум»

Руководитель: Вернигора А. М.