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

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

СБОРНИК МАТЕРИАЛОВ

20 ноября 2024
Томск

В данном издании представлены работы участников двенадцатой региональной научно-практической конференции «Безопасность человека в информационном пространстве», состоявшейся 20 ноября 2024 г. на базе Томского индустриального техникума.

Материалы сборника сгруппированы по тематике секций конференции:

- Безопасность общества в информационном пространстве
- Современные средства защиты в информационном пространстве
- Полиграфическая продукция по теме «Информационная безопасность»
- Противодействие экстремизму и терроризму в сфере информационных технологий

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. БЕЗОПАСНОСТЬ ОБЩЕСТВА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ НА ПОРТАЛЕ ГОСУСЛУГ: ПЛЮСЫ И МИНУСЫ

Дереглазова Анастасия Алексеевна, Найдёнова Ксения Олеговна
Областное государственное бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»
Руководитель: Маслова Екатерина Константиновна

Современная демократия немыслима без процедуры голосования. Однако в современных условиях процедура выборов в Российской Федерации столкнулась с рядом серьезных вызовов, в том числе пандемия и угроза безопасности. Возможность модернизации процедуры позволяет значительно улучшить систему проведения голосования, повысив явку и уменьшив риски, связанные с большим скоплением людей. Поэтому изучение данной темы представляется нам как никогда *актуальным*.

В 2019 году Президентом Российской Федерации был подписан Федеральный закон «О внесении изменений в статьи 37 и 38 Федерального закона „Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации“», который сделал допустимым использование дистанционного электронного голосования при проведении выборов.

21 июля 2020 года Госдума РФ приняла закон, позволяющий проводить выборы в течение нескольких дней подряд, но не более трех, в избирательных кампаниях любого уровня. 24 июля того же года документ был одобрен Советом Федерации РФ, 31 июля 2020 года подписан главой государства.

Объект исследования – электронное голосование в РФ.

Предмет исследования – плюсы и минусы голосования на портале Госуслуг.

Гипотеза исследования состоит в том, что не все граждане нашей страны пользуются возможностью проголосовать на портале Госуслуг. В первую очередь, опасаясь нарушения анонимности процедуры. Ведь Тайное голосование, как символ демократического процесса, обеспечивает защиту личного выбора граждан. Это дает возможность свободно выражать свои взгляды без страха перед осуждением или репрессиями. Каждый избиратель чувствует себя в безопасности, зная, что его голос останется неприметным.

Методы, которые использовались в данном исследовании: анализ литературы и нормативно-правовых актов, социологический метод.

Данная тема изучалась в работах Киселевой Н.В.[1], Цаплина А.Ю.[2], Грачева М.Н.[3], Ерохиной О.В.[4] и других авторов.

На данный момент при выборах в органы государственной власти тайное голосование является общепринятым. В Законе говорится: голосование на выборах и референдуме является тайным, исключающим возможность какого-либо контроля за волеизъявлением гражданина[5]. В «Конвенции о стандартах выборов, избирательных прав и свобод» говорится: «ни один избиратель не может быть принужден кем бы то ни было объявить, как он намерен голосовать, или как он голосовал. Не допускается составление и (или) опубликование (распространение)

[1] Киселева Н.В Электронное голосование в России: понятие и виды // Актуальные проблемы теории и истории правовой системы общества. - №19. – 2020. – С. 36-43.

[2] Цаплин А.Ю. Перспективы дистанционного электронного голосования в России // Известия Саратовского университета. Новая серия. Серия Социология. Политология. – Т.16. – Вып. 3. – 2016. – С. 345-350.

[3] Грачев М.Н. Электронное голосование: «За» и «Против» // Известия Тульского государственного университета. Гуманитарные науки. – 2011. – С. 360-366.

[4] Ерохина О.В. Технологии электронного голосования в России//Вестник университета. 2019. – № 11. – С.5-11.

[5] Федеральный закон от 12.06.2002 N 67-ФЗ (ред. от 08.08.2024) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации».

персональных сведений об избирателях, принявших участие либо не принявших участие в голосовании» [6].

Тайное голосование обеспечивается использованием унифицированных избирательных бюллетеней и наличием на избирательных участках специальных обособленных комнат или кабин, в которых избиратели имеют возможность заполнить избирательные бюллетени. Однако каким способом обеспечивается анонимность онлайн-голосования не всем знакомо. В том числе этот фактор и порождает споры вокруг данного способа голосования.

Одним из основных аргументов сторонников дистанционного электронного голосования (ДЭГ) является его современность. Это утверждение действительно обоснованно. В условиях, когда жизнь все более цифровизируется, становится труднее объяснить, почему, если в интернете, возможно, совершать покупки, оплачивать налоги и получать государственные услуги, голосование не может осуществляться в том же формате. С точки зрения цифровой трансформации, переход к онлайн-голосованию представляется логичным и необходимым шагом.

Еще одним преимуществом ДЭГ является снижение затрат на организацию традиционных выборов. При этом речь идет не только о финансовых ресурсах. Для организации голосования требуется значительное количество человеческих ресурсов — в процессе участвуют десятки тысяч сотрудников участковых комиссий. Избирательные участки часто располагаются в образовательных учреждениях, что может нарушать учебный процесс, особенно в случае многодневных выборов. Использование ДЭГ позволяет избежать этих проблем.

Кроме того, электронное голосование предоставляет удобство для избирателей, что нельзя игнорировать. Проголосовать с помощью

[6] Конвенция «О стандартах выборов, избирательных прав и свобод» от 7 октября 2002 года, Ст. 8 «Свободные выборы»

смартфона или компьютера гораздо проще, чем тратить время на посещение избирательного участка. Это удобство теоретически может привлечь большее количество участников в избирательный процесс — главное, своевременно напомнить им о голосовании.

Наконец, с теоретической точки зрения, ДЭГ может считаться более надежной системой, поскольку она меньше подвержена человеческим ошибкам. Исключается возможность подброса бюллетеней, а подсчет голосов осуществляется машиной, а не уставшими членами комиссии.[7]

Как узнать, что голос учтён? Результаты волеизъявления участников ДЭГ незамедлительно зашифровываются и сохраняются в виде транзакций в блокчейн[8]. После отправки бюллетеня, система предоставляет избирателю «квитанцию», которая содержит данные о его транзакции, в том числе уникальный номер. По нему, с помощью специального сервиса на портале наблюдения ДЭГ, можно будет найти транзакцию и убедиться в ее наличии в блокчейн.

Тип транзакции «Принят бюллетень» будет означать, что транзакция содержит зашифрованный результат волеизъявления, а само наличие транзакции — факт ее учета.

Тайна голосования при ДЭГ обеспечивалась путем процедуры анонимизации, которая запускается после корректного ввода кода подтверждения вашей личности при голосовании на портале ДЭГ. Для обеспечения анонимности происходило отделение всех персональных данных избирателя и их замена на уникальный код, с помощью которого предоставляя доступ к электронному бюллетеню.

В момент голосования система знала ваш уникальный код, но не могла сопоставить его с вашими данными. При голосовании ваше волеизъявление

[7] Преимущества ДЭГ [Электронный ресурс] // Портал дистанционного электронного голосования ЦИК – https://России https://vybory.gov.ru/

[8] Блокчейн — это технология шифрования и хранения данных (реестра), которые распределены по множеству компьютеров, объединённых в общую сеть.

зашифровывалось на вашем личном устройстве и уже в зашифрованном виде передавалось в систему.[9]

Однако, несмотря на все преимущества, электронное голосование также вызывает множество вопросов и опасений. Одним из самых острых является проблема безопасности данных. В условиях растущей киберугрозы возникает закономерный вопрос: насколько надежно защищены персональные данные избирателей и как можно предотвратить возможные манипуляции с результатами голосования? Этот аспект требует тщательной проработки и постоянного обновления технологий, чтобы обеспечить доверие граждан к системе.

Кроме того, существует и другая сторона медали: не все избиратели имеют равный доступ к технологиям. Пожилые люди и жители отдаленных регионов могут испытывать трудности с использованием устройств, необходимых для онлайн-голосования. Это порождает необходимость в дополнительных мерах, направленных на инклюзию и обучение этих групп населения[10]

В итоге, пытаясь найти баланс между современными подходами и традиционными ценностями, важно учесть все аспекты перехода на электронное голосование. Только тогда можно будет говорить о том, что ДЭГ действительно отвечает как потребностям общества, так и требованиям безопасности и справедливости выборного процесса.

В рамках данного исследования был проведен опрос (приложение 1), направленный на изучение мнения граждан о голосовании через портал государственных услуг в электронном формате. Основной целью опроса являлось выявление факторов, влияющих на восприятие данной формы голосования, а также оценка уровня доверия к результатам, удобства процесса и перспектив его дальнейшего развития.

[9] Шустров Д.Г. Стадия избирательного процесса — голосование // Лекция 2020г.
[10] Все точки над ДЭГ: плюсы и минусы электронного голосования [Электронный ресурс] // Политсовет

Вопросы сформулированы таким образом, чтобы охватить различные аспекты электронного голосования и получить максимально полную информацию о мнении респондентов. Они затрагивают следующие темы:

1. Отношение к электронному голосованию
2. Технические аспекты
3. Будущее электронного голосования
4. Доверие и безопасность
5. Личное отношение
6. Манипуляции и фальсификации

Эти вопросы позволяют получить разнообразную информацию о мнении респондентов об электронном голосовании и его перспективах в нашей стране. Они могут быть полезны для анализа общественного мнения, разработки стратегий развития электронного голосования и повышения уровня доверия к нему.

В опросе приняли участие 58 человек в возрасте от 18 до 65 лет, включая как мужчин, так и женщин. Респондентам было предложено ответить на 10 вопросов, касающихся их опыта использования электронного голосования, уровня доверия к системе, а также восприятия возможных проблем и преимуществ данной формы участия в выборах.

Анализ полученных данных позволил выявить следующие ключевые аспекты общественного восприятия электронного голосования:

Уровень доверия к системе:

- 63.8% респондентов выразили доверие к честности системы электронного голосования.

- Однако 36.2% опрошенных выразили сомнения в безопасности данной системы.

Удобство и экономия времени:

- Большинство респондентов (58.6%) положительно оценили удобство и экономию времени, которые предоставляет электронное голосование.

- Возможность голосовать из любой точки мира также была отмечена как значительное преимущество.

Технические проблемы:

- 40.5% респондентов сталкивались с техническими неполадками на сайте или в приложении, что снижает их уверенность в надежности системы.

Перспективы развития:

- 72.4% опрошенных считают, что электронное голосование имеет перспективы развития.

Однако мнения разделились относительно дальнейшего использования данной формы голосования:

- 50% видят электронное голосование как дополнение к традиционному.

- 37.9% считают, что электронное голосование станет основным способом участия в выборах.

- 12.1% не верят в массовое распространение данной формы.

Результаты опроса свидетельствуют о наличии как положительных, так и негативных аспектов в общественном восприятии электронного голосования. Несмотря на определенные технические проблемы и сомнения в безопасности, большинство респондентов признают удобство и экономию времени, что делает данную форму голосования перспективной для дальнейшего развития.

Таким образом, можно сделать вывод об успешности относительно нового способа голосования – через портал Госуслуг. Однако необходимо информировать население о безопасности, анонимности, удобстве данного

вида голосования, не лишая граждан и возможности прийти на избирательный участок проголосовать традиционным способом.

СПИСОК ЛИТЕРАТУРЫ

1.Конвенция «О стандартах выборов, избирательных прав и свобод» от 7 октября 2002 года, Ст. 8 «Свободные выборы».

2.Федеральный закон № 67-ФЗ (ред. от 08.08.2024) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002.

3. Законопроект № 912249-7 «О внесении изменений в статьи 37 и 38 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» Архивная копия от 27 мая 2020 на Wayback Machine / Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество»).

4. Грачев М.Н. Электронное голосование: «За» и «Против» // Известия Тульского государственного университета. Гуманитарные науки. – 2011. – С. 360-366.

5.Ерохина О.В. Технологии электронного голосования в России//Вестник университета. 2019. – № 11. – С.5-11.

6. Как обеспечивалась тайна голосования при ДЭГ? [Электронный ресурс] // Портал дистанционного электронного голосования ЦИК России

7. Киселева Н.В Электронное голосование в России: понятие и виды // Актуальные проблемы теории и истории правовой системы общества. - №19. – 2020. – С. 36-43.

8. Преимущества ДЭГ [Электронный ресурс] // Портал дистанционного электронного голосования ЦИК России

9. Цаплин А.Ю. Перспективы дистанционного электронного голосования в России // Известия Саратовского университета. Новая серия. Серия Социология. Политология. – Т.16. – Вып. 3. – 2016. – С. 345-350.

Приложение 1: Опрос https://forms.yandex.ru/u/66ffd7ddd046880a320bf8

1. Ваш возраст:
   - 18-25
   - 26-35
   - 36-45
   - 46-55
   - 56-65
   - 65+

2. Ваш пол:
   - Мужской
   - Женский

3. Как вы относитесь к идее электронного голосования?
   - положительно
   - отрицательно
   - нейтрально

4. Доверяете ли вы результатам электронного голосования?
   - да, полностью доверяю
   - нет, не доверяю

5. Что вам кажется наиболее удобным в электронном голосовании? (можно выбрать несколько вариантов ответа)
   - возможность проголосовать из любой точки мира
   - экономия времени
   - простота процедуры
   - анонимность
   - другие варианты (указать)

6. С какими неудобствами вы сталкивались при электронном голосовании или слышали о них? (можно выбрать несколько вариантов ответа)
   - технические проблемы с сайтом или приложением
   - необходимость регистрации на сайте или в приложении
   - отсутствие возможности проверить правильность учёта голоса
   - другие варианты (указать)

7. Хотели бы вы использовать электронное голосование в будущем?
   - да
   - нет
   - затрудняюсь ответить

8. Каким Вы видите будущее электронного голосования в нашей стране?
   - Электронное голосование станет основным способом участия в выборах
   - Электронное голосование будет использоваться наряду с традиционным голосованием
   - Электронное голосование не получит широкого распространения

9. Считаете ли вы, что электронное голосование может быть подвержено манипуляциям или фальсификациям?
   - нет, это невозможно
   - возможно, но маловероятно
   - вполне возможно

10. Какое из следующих утверждений лучше всего описывает ваше личное отношение к электронному голосованию?
   - Я считаю электронное голосование удобным и надежным способом участия в выборах.
   - Я считаю электронное голосование удобным, но не до конца доверяю системе безопасности.
   - Я предпочитаю традиционное голосование на избирательных участках.
   - Я не уверен(а), что электронное голосование надежно, и предпочитаю не участвовать в нем.
   - Я считаю, что электронное голосование – это будущее демократии.
   - Другое (укажите ваше мнение)

КТО ТАКИЕ ДРОППЕРЫ, И КАК НЕ СТАТЬ ПРЕСТУПНИКОМ?

Вагин Владислав Вячеславович
Областное государственное бюджетное профессиональное образовательное учреждение «Шегарский техникум индустриальных технологий»
Руководитель: Тырышкина Елена Анатольевна

Кто такие дропперы?

Дроппер – это человек, которого используют мошенники для достижения своих целей. Он не является инициатором преступления, а выполняет указания, получая за это деньги.

Дропы участвуют во всех схемах по незаконному обналичиванию чужих денег. Схема довольна проста: дроппер предоставляет данные своей банковской карты, на которую переводят средства, добытые преступными способами. Затем он обналичивает сумму в банкомате, передает другим лицам и получает определенный процент со сделки.

Казалось бы, зачем усложнять работу и нанимать подставных людей? К услугам дропов обращаются, во-первых, чтобы самому мошеннику не засветиться и не получить наказание. Во-вторых, чтобы скрыть сам факт киберпреступления и сделать цепочку переводов более запутанной, ведь операции проводятся под разными именами.

Пример. Николаю К. поступил звонок. Неизвестный абонент предложил легкий заработок: оформить банковскую карту на свое имя и передать ее курьеру. За такую услугу Николаю К. пообещали 3 тыс. рублей. Мужчина выполнил все условия, и вскоре ему на счет перевели вознаграждение. Затем вновь позвонил абонент и пообещал платить по 2 тыс. рублей за каждого приведенного друга, который точно так же согласится открыть банковскую карту. Николай К. рассказал о ситуации своему коллеге Петру Н. Он не захотел отдавать физическую карту курьеру, но

согласился прислать ее реквизиты. За это Николай К., как и было обещано, получил 2 тыс. рублей, а Петр Н. – 3 тыс. рублей. Оба товарища стали дропперами.

В других случаях передавать свою карту либо делиться персональными данными вовсе не требуется. Заказчики просят лишь помогать с денежными переводами на другие счета либо со снятием средств в банкомате с дальнейшей передачей их курьеру. Иногда для привлечения дропперов придумываются целые легенды.

Бывает и так, что злоумышленники вовлекают в свои преступные схемы людей буквально силой: переводят деньги на карту либо пополняют счет мобильного телефона якобы по ошибке. Затем получателя средств просят их вернуть наличными или переводом на другую карту.

Целевая аудитория дропперов

Мошенники избирательно подходят к привлечению дропперов. Они намеренно выбирают тех людей, кто нуждается в деньгах и не будет особенно интересоваться их происхождением. Это могут быть, например, подростки. Им разрешено заводить банковскую карту начиная с 14 лет. Злоумышленники находят подростка в соцсетях и предлагают заработать, чтобы иметь возможность, например, самостоятельно купить приставку или компьютерную игру.

Не допустить вовлечения детей в преступные схемы – задача родителей. Перед тем, как выпустить ребенку банковскую карту, следует поговорить с ним о возможных рисках. Важны также доверительные отношения в семье – лучше если ребенок лишний раз посоветуется с родителем по тому или иному поводу (в данном случае о предложении заработать), нежели примет решение самостоятельно.

Также в группе риска:

- студенты;
- люди, получающие пособия или субсидии;

- приезжие, которые перебираются из небольших населенных пунктов в крупные города;
- клиенты банков с высокой кредитной нагрузкой;
- пожилые люди;
- люди, уже пострадавшие от уловок мошенников, и др.

Этим категориям предлагают быстро и легко заработать. Всего-то достаточно получить, а затем перевести деньги или снять наличные в банкомате. Даже если человек подозревает что-то неладное, он все равно соглашается попробовать, поскольку ему остро необходимы деньги.

Нужно учитывать, что вербовкой дропперов часто занимаются операторы колл-центров, которые прошли специальное обучение и обладают навыками убеждения. Отказать им непросто, поскольку на каждый ответ они готовы предоставить обоснованную аргументацию.

Способы обманов дропперов

Существует много схем для получения незаконного заработка. Перевод с одной пластиковой карточки на другую и затем снятие средств в банкомате – это, пожалуй, самый наглядный пример работы дропов и один из вариантов использования их труда.

Наверняка вам хотя бы один раз звонили и представились сотрудниками определенной банковской организации. Обычно они сообщают, что злоумышленники пытались списать средства со счета либо уже это сделали, а чтобы защитить ваши деньги, необходимо передать «сотрудникам» личные данные.

Если вы сообщите эту информацию, то мошенникам не составит труда украсть деньги с вашего счета.

Это один из способов черного заработка. Для звонков нанимают специальных людей (дропперов), а переводами, например, может заниматься другая группа.

Другой пример интернет-мошенничества – продажа товара по предоплате. Обычно это интернет-магазины, которые на первый взгляд кажутся официальными: реклама, все подтверждающие документы, отзывы от покупателей. Они регистрируются как ООО, а генеральным директором делают дропа.

Схема выманивания денег у лжепродавцов такова: они просят предоплату за товар, люди им отправляют деньги, но взамен не получают желанной покупки. Через некоторое время такие онлайн-платформы закрываются, и вернуть свои средства не получится.

Выяснить, кто являлся организатором дела, почти невозможно, а подставным лицом мог стать любой человек, даже сам того не подозревая.

Существует понятие «разводной дроппер», чьи конфиденциальные данные злоумышленники получают обманным методом. Например, они размещают вакансию курьера. Если кто-то откликается на нее, то его просят отправить сканы документов, обычно паспорт со СНИЛС, чтобы «пройти проверку службы безопасности».

Человеку не перезванивают насчет работы, а его данные мошенники могут использовать для любых целей.

Опрос среди учащихся ОГБПОУ «ШТИТ»

В нашем техникуме был проведен опрос среди студентов с первого по четвертый курс, в количестве 65 человек. Задавались такие вопросы, как:

1. Знаете ли вы кто такие дропперы?
2. Знаете ли вы как себя защитить от дропперства?

В ходе опроса было выявлено, что 38% студентов знали кто такие дропперы (это 25 человек). Из этих 38% студентов только один знал, как себя защитить от мошенников, остальные такой информацией не обладали.

Таким образом, мы видим, что большое количество студентов не знают, как себя защитить от мошенников, что делает их еще более уязвимыми для интернет-мошенников.

В связи этим мы распечатали и раздали студентам памятку-правило «Как защитить себя от дропперов?»

Памятка-правило «Как защитить себя от дропперов?»

Чтобы не стать жертвой дропперов, следуйте этим правилам:

1. Не сообщайте свои пароли, логины и другую личную информацию другим людям.

2. Используйте сложные пароли и регулярно их меняйте.

3. Не переходите по подозрительным ссылкам.

4. Не называйте коды из СМС и push-уведомлений.

5. Регулярно проверяйте свой кредитный рейтинг и кредитную историю.

6. Если вас просят перевести деньги по определённым реквизитам, свяжитесь с банком и оформите заявление на возврат средств.

7. Не сообщайте данные своей банковской карты незнакомым людям и не передавайте её третьим лицам.

8. Не соглашайтесь переводить деньги по реквизитам или снимать наличные в банкомате по просьбе незнакомых людей.

9. Если вам предлагают лёгкую работу или быстрый заработок, будьте осторожны и проверьте информацию.

10. Если вы подозреваете, что стали жертвой мошенничества, немедленно сообщите об этом в Банк России или полицию.

Заключение

Если человек стал дроппером по незнанию, ему очень трудно будет доказать факт своей неосведомленности. Поэтому будьте внимательны и осторожны при просмотре объявлений о работе, получении сообщений в социальных сетях,

разговорах по телефону, в которых обещают легкие деньги. Не поддавайтесь на уговоры работодателя о переводе чужих денежных средств на ваши банковские карты.

Помните, что обналичивание чужих денег в любом проявлении –это пособничество преступлению! Будьте бдительны!

Интернет - источники:

1.https://admmironovka.nso.ru/news/14918

2. https://economics.hse.ru/ecjourn/news/847434104.html

3. https://journal.uralsib.ru/hse/research/4

4. https://journal.sovcombank.ru/umnii-potrebitel/kto-takie-dropperi-i-chto-znachit-oformit-na-dropa.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ

Барсегян Марина Кареновна, Франк Евгения Витальевна

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

Руководитель: Илья Викторович Фартушев

Ключевые слова: информационно-психологическая безопасность личности, стресс, информационно-психологические проблемы и информационная культура личности.

Актуальность: Проблема информационно-психологической безопасности личности достаточно актуальна в настоящее время, так как «производство» информации в современном мире неуклонно растет, и этот рост не соответствует потребностям и возможностям современного человека. Известную рекомендацию «Кто владеет информацией, тот владеет всем» порой трудно осуществить вследствие несогласованности процессов создания, доставки и усвоения информации. Телевидение, Интернет, радио и другие СМИ обрушивают на нас огромный поток

нужной и ненужной информации, порождая информационный стресс. Стресс проникает во все сферы нашей деятельности, становится частью нашей жизни. В этих условиях человек оказывается уже неспособным охватить всю поступающую информацию. Мало того, с этой задачей не всегда справляется даже программное обеспечение. Таким образом, большие объемы информации плюс высокопроизводительные сети дают в сумме так называемый информационно-психологический стресс, ликвидировать который не удается даже путем установки нового оборудования. Поэтому на современном этапе развития информационного общества возникла новая проблема - обеспечение информационно-психологической безопасности потребителя информации.

Цель нашей работы: изучить проблемы информационно-психологической безопасности личности в современном информационном пространстве и определить основные условия для предупреждения стрессовых ситуаций при взаимодействии человека с различными источниками информации.

Для начала нам нужно разобраться, что такое информационно-психологическая безопасность личности. Под информационно-психологической безопасностью личности в настоящее время принято понимать состояние защищенности граждан, их отдельных групп и социальных слоев, а также населения в целом от негативных информационно-психологических воздействий. К числу основных факторов информационно-психологического воздействия могут быть отнесены многие сравнительно недавно появившиеся в обществе тенденции и факторы, которые можно условно разделить на четыре основные группы:

1. Политические факторы

2.Социально-экономические факторы

3.Духовные факторы

4.Технологические факторы

Информационно-психологическая безопасность (ИПБ) личности как составная часть информационной безопасности связана в основном с отсутствием (недостатком) необходимой информации; нарушением прав личности в сфере доступа к информации; с воздействием информации сомнительного характера и другими информационными воздействиями на психику личности, что, бесспорно, ухудшает интеллектуальное, духовно-нравственное состояние человека и угрожает его здоровью.

Анализ научной литературы позволяет выделить некоторые из видов недоброкачественной («вредоносной») информации, которая способна привести к серьёзным отклонениям в психике человека. К видам такой информации следует отнести:

- информацию, порождающую воинственные настроения;

- информацию, содержащую элементы ненависти, вражды и превосходства;

- информацию, содержащую порнографию;

- информацию, содержащую посягательства на честь, доброе имя и репутацию личности;

- информацию, содержащую элементы неосознаваемого деструктивного воздействия на психику людей;

- рекламу заведомо ложную или содержащую элементы недобросовестности, недостоверности, неэтичности.

- недостаточно полная информация или отсутствие нужных сведений;

- ограничение прав и свобод личности в вопросах доступа к источникам информации;

- незаконное ограничение доступа к открытым информационным ресурсам;

- наличие информации, которая порождает социальную, расовую, национальную или религиозную ненависть, или пропагандирует насилие и жестокость;

- дезинформация, наличие непроверенной, ошибочной и искаженной информации;

Большой поток информации является пусковым механизмом для возникновения информационного стресса и формирует чувство тревоги и психической напряженности личности. как же справиться с этим?

На основании изученной литературы, нами были определены следующие основные условия для высокой эффективности усвоения информации и предупреждения стрессовых ситуаций при взаимодействии человека с различными источниками информации нужно:

1) *Желание усваивать новую информацию.* Это основной принцип успешной информационной деятельности. Человек должен уметь сознательно вызывать и поддерживать у себя желание учиться новому.

2) *Принцип радости.* Любую деятельность, в том числе и информационную, надо выполнять с внутренней радостью, в условиях внутреннего психологического комфорта, на фоне положительных эмоций. Только в таком состоянии человек способен легко усваивать и перерабатывать большие объемы информации.

3) *Принцип полного расслабления.* Излишнее внутреннее физическое и психологическое напряжение резко снижает эффективность любой деятельности, в том числе и интеллектуальной. В древности по этому поводу говорили: «Стоящий на цыпочках долго стоять не сможет». Если в процессе обучения научиться расслабляться, снимать мышечные зажимы (блоки), особенно в районе лица, шеи, плеч и кистей рук, которые максимально представлены в коре головного мозга, то можно добиться высоких результатов в усвоении нужной информации.

4) *Принцип тотального внимания или сосредоточенности* («Быть здесь и сейчас»). Основным условием эффективного усвоения информации является то, что в течение всего времени усвоения человек должен быть полностью сосредоточен на изучаемой информации, мысленно находиться в своем внутреннем пространстве.

Перед окончанием стоит упомянуть и про исследовательскую часть данной темы. Мы провели ряд опросов среди своей группы и получили такие результаты:

1. На сколько сильно вы подвергаетесь стрессу? Очень сильно-4% иногда бывает-64% очень редко-34%

2. Через какие средства информации чаще всего оказывают ипв на вас? Личное общение-42% образование 29% массовые коммуникации-29

3. Как часто вы сталкиваетесь с информационно-психологическим воздействием? Каждый день-12% раз в неделю-24% раз в месяц-64%

4. Как вы считаете обеспеченна ли ваша информационная безопасность? Да-50% нет-50%

Проанализировав информацию, полученную при опросе, можно сказать следующее: с информационно-психологическим воздействием, стрессом сталкиваются практически все люди. Поэтому знание своих индивидуально-психологических особенностей, видов и источников информационно-психологических угроз становится для человека в настоящее время не просто обязательным элементом его общей культуры, но и необходимым условием безопасности в социальном взаимодействии.

Цель нашей работы выполнена, надеемся информация была вам полезной.

Литература

1. https://almanah.su/tpost/soh6eyo6i1-filimonova-nv-informatsionno-psihologich
2. https://studfile.net/preview/16566604/page:8/
3. https://otherreferats.allbest.ru/psychology/00254720_0.html
4. https://ppt-online.org/1304518

ИНФОРМАЦИОННО- ПСИХОЛОГИЧЕСКАЯ УГРОЗА БЕЗОПАСНОСТИ ЛИЧНОСТИ

Бормотова Валерия Витальевна Ерофеева Валерия Алексеевна
Областное государственное бюджетное профессиональное образовательное учреждение «Колледж индустрии питания, торговли и сферы услуг»
Руководитель: Головина Нина Петровна

В эпоху цифровых технологий, когда информация становится все более доступной и распространяется с бешеной скоростью, возникают новые угрозы для безопасности личности. Одной из самых серьезных угроз является информационно-психологическая угроза, которая включает в себя использование информационных и психологических методов для повреждения психического здоровья.

Проблема информационно-психологической угрозы безопасности личности является одной из наиболее актуальных в современном мире. Она связана с возрастающей ролью информации в жизни каждого человека и общества в целом. Информационная среда стала мощным инструментом воздействия на сознание и поведение людей, что открывает возможности для манипуляций и злоупотреблений.

Предметом исследования является информационно-психологическая угроза безопасности личности, ее проявления, последствия и способы противодействия.

Объектом исследования является личность как субъект информационно-психологического воздействия в цифровой среде.

Цель: изучение информационно-психологической угрозы безопасности личности в условиях современного информационного общества, с определением ее характеристик, последствий, а также разработка рекомендаций по предупреждению и снижению ее влияния.

Задачи:

1. Проанализировать существующие теоретические концепции информационно-психологической безопасности личности.

2. Изучить основные проявления информационно-психологической угрозы в современном мире.

3. Провести опрос среди студентов ОГБПОУ «КИПТСУ», чтобы определить в какой степени проявляется информационно-психологическая угроза.

4. Оценить последствия информационно-психологической угрозы для личности.

5. Сделать выводы.

Методы исследования:

1. Анализ научной литературы по теме исследования.

2. Сбор и анализ статистических данных о проявлениях информационно-психологической угрозы.

3. Проведение социологических опросов

4. Анализ, сравнение и выводы.

Информационно-психологическая угроза безопасности личности - это воздействие на психику человека через информационные каналы с целью манипулирования его сознанием, поведением и эмоциональным состоянием для достижения определенных целей. Такие угрозы могут исходить от различных источников, включая СМИ, социальные сети, политические силы, террористические организации и даже отдельных людей.

В рамках информационно-психологической безопасности личности существует несколько ключевых концепций, каждая из которых рассматривает различные аспекты защиты психики индивида от негативного воздействия информации.

Рассмотрим некоторые из них:

1. Концепция информационного стресса.

Эта концепция предполагает, что чрезмерная информационная нагрузка может привести к стрессу у человека. Информационный стресс возникает тогда, когда человек сталкивается с большим количеством информации, которую он не способен

эффективно обработать. Это может приводить к когнитивным перегрузкам, эмоциональному выгоранию и снижению продуктивности.

2. Теория манипулятивного воздействия информации.

Эта теория акцентирует внимание на том, как информация может использоваться для манипуляции сознанием людей. Манипуляция осуществляется через скрытые методы влияния на восприятие, эмоции и поведение человека.

3. Модель психологической устойчивости к информационным угрозам.

Эта модель фокусируется на развитии психологических качеств, позволяющих человеку противостоять негативным информационным воздействиям. Устойчивость включает в себя способность сохранять душевное равновесие и рациональное мышление даже при воздействии деструктивной информации.

4. Концепция кибербезопасности личности.

В эпоху цифровых технологий особую роль играет защита от киберугроз, таких как фишинг, мошенничество, вирусные атаки и утечка персональных данных. Кибербезопасность личности связана с защитой психической сферы от негативных последствий этих угроз.

Все концепции указывают на важность защиты личности от информационно-психологических угроз. Однако, каждая концепция имеет свои ограничения и не полностью охватывает все аспекты проблемы.

Современный мир характеризуется высоким уровнем распространения информации, которая зачастую оказывает значительное влияние на психику человека. Информационно-психологические угрозы могут проявляться в различных формах и иметь разные последствия для общества и отдельных личностей. Вот основные проявления таких угроз:

1. Фейковые новости и дезинформация

Распространение ложной или искаженной информации с целью манипулирования общественным мнением и поведением. Фейки могут вызывать

панику, недоверие к официальным источникам, социальное напряжение и даже массовые беспорядки. Например, во время пандемии COVID-19 распространялись фейковые сообщения о «чудодейственных» лекарствах или методах лечения, что приводило к опасным последствиям для здоровья. Политически мотивированные фейки могут влиять на выборы и общественные настроения.

2. Кибербуллинг и травля в интернете.

Агрессивное поведение в отношении другого человека посредством интернета, включая оскорбления, угрозы и распространение личной информации. Кибербуллинг может нанести серьезный ущерб психическому здоровью жертвы, вплоть до депрессии и суицидальных мыслей. Например, распространение компрометирующих фотографий или видео без согласия человека, а также оскорбительные комментарии и угрозы в социальных сетях.

3. Информационные перегрузки (инфоглут)

Когда человек получает слишком много информации за короткий промежуток времени, это может привести к когнитивным перегрузкам, стрессу и ухудшению психического состояния. Постоянное пребывание в режиме многозадачности и необходимость обрабатывать большие объемы данных негативно сказываются на качестве жизни. Например, чрезмерное потребление новостных лент и социальных сетей или необходимость одновременно работать с несколькими проектами или задачами.

4. Социальные сети и зависимость от них

Зависимость от социальных сетей может привести к нарушению нормального режима сна, социальной изоляции, снижению самооценки и другим проблемам. Люди часто сравнивают свою жизнь с идеализированными образами, представленными в соцсетях, что вызывает чувство неудовлетворенности и тревоги.

5. Цифровое шпионство и нарушение приватности

Использование технологий для сбора и анализа персональной информации без ведома или с согласия человека. Это может включать слежку за активностью в интернете, сбор данных о местоположении, предпочтениях и поведении.

Примеры:

- Сбор данных пользователями приложений и сайтов для дальнейшей продажи рекламодателям.
- Хакерские атаки и кража личных данных.

6. Радикализация и экстремизм

Распространение экстремистских идей через интернет, что может привести к радикализации отдельных лиц и групп. Социальные сети и мессенджеры используются для вербовки новых членов террористических организаций и пропаганды насилия.

Эти примеры иллюстрируют разнообразие проявлений информационно-психологических угроз в современном мире. Они оказывают воздействие на индивидуальные и коллективные психические процессы, влияя на здоровье, благополучие и социальную стабильность.

Для того, чтобы определить уровень осведомленности студентов ОГБПОУ «КИПТСУ» о информационно-психологической угрозе безопасности личности в современном мире, оценить степень ее влияния на их жизнь и выяснить мнение о необходимости мер по защите от этой угрозы было проведено исследование.

Студентам ОГБПОУ «КИПТСУ» разных специальностей и курсов предлагалось пройти соцопрос, чтоб определить в какой степени проявляется информационно-психологическая угроза.

По результатам опроса было выявлено следующее:

1. 70% студентов знают о понятии «информационно- психологическая угроза безопасности личности», и даже с некоторыми проявлениями этой угрозы сталкивались, например кибербуллинг, фишинг или психологическое давление. 23%

опрошенных не знают о понятии «информационно- психологическая угроза безопасности личности», но сталкивались с ее проявлениями на просторах интернета, и лишь 7% никогда не сталкивались с этой угрозой. Можно сделать вывод, что большинство студентов осведомлены о понятии «информационно- психологическая угроза безопасности личности», только потому, что сталкивались с этой угрозой в разных проявлениях.

Диаграмма 1 Информационно- психологическая угроза безопасности личности

2. На вопрос, какие меры вы принимаете для защиты от информационно-психологической угрозы, мнения студентов выстроились следующим образом:

28% студентов используют фильтрацию контента, избегая создания или распространения контента, который может нанести вред психике пользователей или спровоцировать негативные эмоции.

25% студентов используют современные технологии для защиты данных и предотвращения несанкционированного доступа к ним.

24% -стараются проверять источники данных и учитывать контекст, чтобы минимизировать риск распространения дезинформации.

14%- студентов следуют принципам честности и уважения к пользователям, стараясь избегать манипуляций и давления.

И только 9% предложили обучение пользователей, как распознавать фейки и манипуляции, а также использование критического мышления при восприятии информации.

Диаграмма 2 Меры защиты от информационно- психологических угроз

Таким образом, для борьбы с информационно- психологическими угрозами необходимо развивать навыки критического мышления, повышать уровень медиаграмотности и использовать технологии для обеспечения безопасности в информационном пространстве.

Студенты колледжей являются одной из наиболее уязвимых групп для информационно-психологических угроз, так как они активно используют цифровые платформы и находятся в процессе формирования своих жизненных позиций и убеждений. Для предупреждения и снижения влияния этих угроз на студентов предложены специальные рекомендации:

1. **Интеграция медиаграмотности в учебный процесс**

Цель: Развить у студентов навыки критического анализа информации и умение распознавать манипуляции.

2. Информационная поддержка и консультирование

Цель: Предоставить студентам доступ к надежным источникам информации и профессиональной помощи.

3. Организация внеклассных мероприятий

Цель: Повышать уровень информированности и вовлеченности студентов в вопросы информационной безопасности.

4. Партнерства с организациями, работающими в сфере информационной безопасности

Цель: Расширить возможности взаимодействия студентов с экспертами и организациями, работающими в сфере информационной безопасности.

Информационно-психологическая угроза - это реальная опасность, которая может серьезно повлиять на жизнь каждого человека. Поэтому необходимо прилагать максимальные усилия для ее предупреждения и нейтрализации. Важно помнить, что информационно-психологическая безопасность - это не только забота о собственной безопасности, но и ответственность за безопасность окружающих.

Список литературы:

1. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2025. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528 (дата обращения: 09.11.2024). — Текст : электронный.

2. Литвинова, А. В., Проблемы психологической безопасности личности и образовательной среды : монография / А. В. Литвинова, А. В. Кокурин, М. И. Марьин, ; под общ. ред. А. В. Литвиновой, А. В. Кокурина, М. И. Марьина, Коллектив авторов. — Москва : Русайнс, 2022. — 189 с. — ISBN 978-5-466-02379-4. — URL: https://book.ru/book/948737 (дата обращения: 09.11.2024). — Текст : электронный.

3. Фейковизация как средство информационной войны в интернет-медиа: Практическое пособие / Е.И. Галяшина, В.Д. Никишин, К.М. Богатырев, Е.Г. Пфейфер — Москва : Проспект, 2023. — 144 с. — ISBN 978-5-6048622-5-4. — URL: https://book.ru/book/950056 (дата обращения: 09.11.2024). — Текст: электронный.

4. Белоусов, А.Д.. Угрозы сети Интернет для несовершеннолетних пользователей: психологический анализ и профилактика: Монография / А.Д. Белоусов — Москва: Проспект, 2019. — 76 с. — ISBN 978-5-392-29678-1. — URL: https://book.ru/book/937758 (дата обращения: 09.11.2024). — Текст: электронный.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ НА ЛИЧНОСТЬ И ЗАЩИЩЕННОСТЬ ОБЩЕСТВА

Пешков Алексей Алексеевич, Фирсов Артем Денисович
Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум информационных технологий»
Руководитель: Кирилова Анна Владимировна

Введение

Ежедневно человек получает, перерабатывает и обменивается информацией с обществом.

Информационная сфера – сфера деятельности субъектов общественной жизни, связанная с созданием, сбором, преобразованием, хранением, распространением и использованием информации.

Особый интерес приобретают формы оказания психологического воздействия в онлайн-пространстве. В современном мире, когда Интернет играет все более значимую роль, возникает множество новых возможностей для оказания психологического воздействия на людей через онлайн-каналы. Сегодня одними из наиболее распространенных форм психологического воздействия в Интернет-пространстве являются: Микротаргетированная реклама, фейковые новости и

дезинформация, виртуальный манипулятивный контроль, социальное подражание, кибершторминг. [7]

Актуальность исследования психологического воздействия на человека внешних факторов в информационном пространстве обусловлена рядом проблем, связанных с динамизмом и трансформацией современного информационного пространства.

Целью работы является изучение методов информационно-психологического воздействия на общество и определение путей защиты личности.

Задачи исследования для достижения поставленной цели:

- Изучить научную литературу касаемо информационно-психологического воздействия;

- Дать определение информационно-психологическому воздействию и выявить его методы влияния;

- Предложить пути решения проблем, связанные с правовой защитой деструктивно-информационно-психологического воздействия.

Методологическую основу работы составляет междисциплинарный подход к исследованию проблемы, который использует положение психологии, теории коммуникации, информационных систем.

Методы исследования: абстрагирование, анализ, синтез, аналогия, опрос, а также сравнение.

Гипотеза исследования: наряду с внешними социально-политическими и экономическими условиями, в качестве внутренних детерминант выступают психологические факторы и механизмы. Это предполагает использование междисциплинарного подхода в качестве системообразующего основания разработки проблемы информационно-психологической безопасности личности и общества.

Информационно-психологическое воздействие на человека

Для того чтобы определить концептуальные и смысловые границы понятия «психологическое воздействие», следует обратиться к определениям этого понятия. Наиболее обще и нейтрально, из исследованного нами научного массива, данный термин определяет Психологический словарь под ред. А. В. Петровского и М. Г. Ярошевского: «воздействие (в психологии) – целенаправленный перенос движения и информации от одного участника взаимодействия к другому».

Рассматривая предмет психологического воздействия, авторы выделяют: взгляды, мнения, отношения, установки (В.Н. Куликов,Ф. Зимбардо и М. Ляйппе, Г.Г. Романович); сознание человека (Е.В. Селезнева, А.В. Малько); психические состояния, чувства, мысли и поступки людей (Е.В. Сидоренко, А.В. Малько); [12]

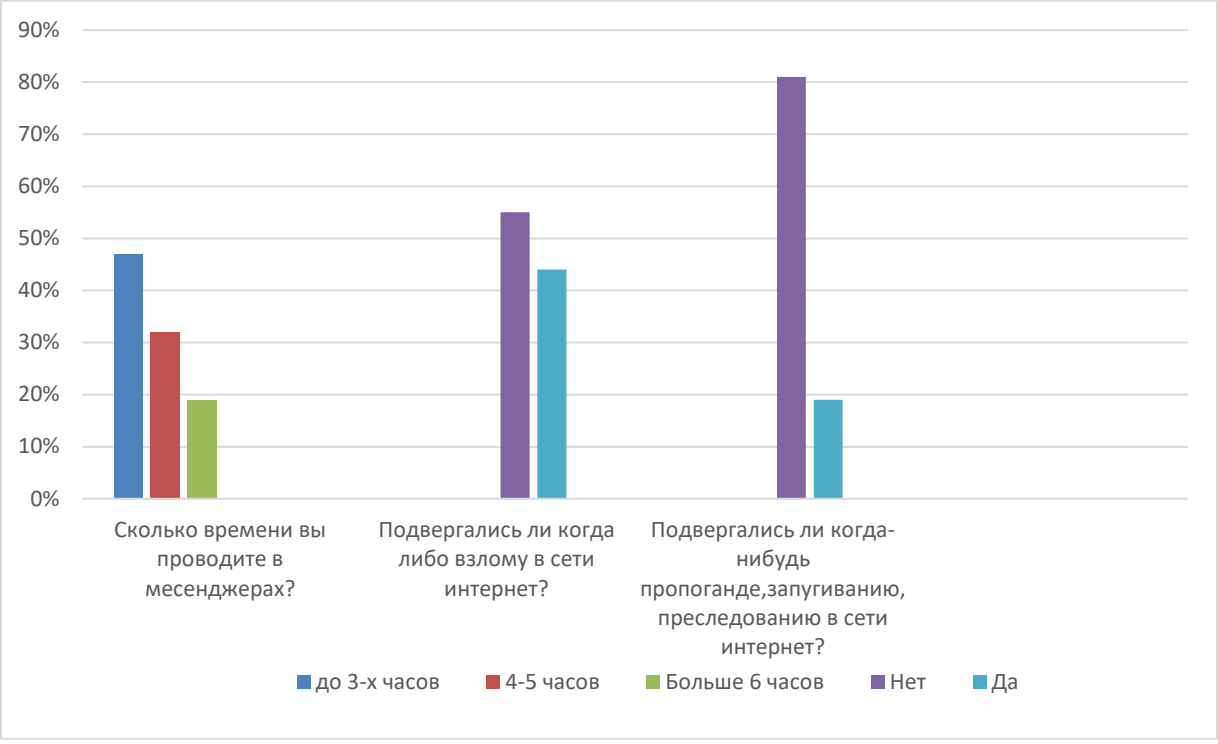
Анализ текущей практики Интернет-общения позволяет выделить такие формы и методы деструктивного психологического воздействия в онлайн-среде, как флейминг, киберхейт, троллинг, кибersталкинг, кибербуллинг (см. Таблица 1)

Таблица 1 Методы деструктивного психологического воздействия

Название	Описание	Сущность
Флейминг (flaming)	Разжигание спора между собеседниками	Деструктивная разновидность онлайн-коммуникации, реализуемая посредством агрессивных вербальных выпадов участников дискуссии; диалогический или полилогический кратковременный акт коммуникации.
Троллинг (trolling)	Привлечение внимания к собственной личности и снижение статуса собеседника	Вид коммуникации, восходящий к архетипу трикстера (шута) и продолжающий традиции карнавальной смеховой культуры, воссозданной в онлайн-пространстве; публикация провокативных комментариев с нарушением этических постулатов коммуникации.

Киберхейт (hate, cyberhate)	Пропаганда ненавистнических идей	Осуждение или оскорбление, направленное против какой-либо группы, вызванное социальной активностью адресата хейта.
Кибербуллинг (cyberbulling)	Запугивание партнера по коммуникации	Агрессивные, умышленные, продолжительные во времени действия, совершаемые группой лиц или одним лицом
Кибersталкинг (cyberstalking)	Преследование сообщениями или звонками, вызывающими страх и тревогу	Повторяющиеся действия, характеризующиеся вторжением в личную жизнь жертвы, угрозы жертве.

Изучив информацию об информационной безопасности, угрозах и методах защиты, в рамках данной работы проведено анонимное тестирование студентов, в возрасте от 15 до 23 лет. Мы выявили, что: большинство молодых людей (47%) от 15 до 23 лет проводят в мессенджерах до 3-х часов, 32% 4-5 часов и больше 6 часов-19 % опрошенных. На вопрос «Подвергались ли вы когда-нибудь взлому в сети



интернет?» 44% студентов ответили положительно, а 19% - подвергались пропаганде, запугиванию, преследованию в сети интернет. (Рис. 1)

Рисунок 1 Опрос студентов ТТИТ «Личная безопасность в сети интернет»

Защита личности от информационно-психологического воздействия

Обеспечение информационно-психологической безопасности – это предотвращение или парирование опасностей и угроз, связанных с информационно-психологическими воздействиями на индивидуальное, групповое, массовое и общественное сознание, а также ликвидация последствий целенаправленного негативного информационно-психологического воздействия. Выполнение указанных функций должно осуществляться системой обеспечения информационно-психологической безопасности государства, а также личной ответственностью каждого человека [3]

Психологическая защита личности – это сложная многоуровневая система социальных, социально-психологических и индивидуально-личностных механизмов. Можно выделить три основных уровня организации психологической защиты человека и, соответственно, три основных направления ее формирования и функционирования:

1) Социальный (в масштабах общества в целом). На этом уровне в качестве субъектов психологической защиты личности выступают государство и общество. Защита реализуется через регулирование и организацию информационных потоков

2) Социально-групповой – осуществляется в рамках различных социальных групп и разнообразных форм социальных организаций. Психологическая защита реализуется посредством распространения и использования внутригрупповых информационных потоков и источников, а также специфических для конкретных социальных групп и организаций способов социального взаимодействия, переработки и оценки информации

3) Индивидуально-личностный. Осуществляется посредством образования, самообразования, прохождения специальных тренингов под руководством опытных психологов.

Заключение

Осознание грозной реальности существования информационно-психологических воздействий вызывает необходимость внимательного рассмотрения проблем обеспечения защиты индивидуального, группового, массового и общественного сознания от подобных воздействий, имеющих негативный (деструктивный) характер. Благодаря исследованию, мы выяснили, что студенты все чаще подвергаются воздействию в сети интернет, что сказывается отрицательно как на психологическом состоянии отдельной личности, так и групповом сознании. Поэтому развитие междисциплинарной взаимосвязи информационных систем и психологии.

Список литературы:

1. Астахова Л. В. Информационно-психологическая безопасность в регионе: культурологический аспект // Вестник УрФО. Безопасность в информационной сфере. 2011. № 2. С. 40–47.

2. Басанова Т. А. К вопросу обеспечения информационно-психологической безопасности студентов вуза // Известия ЮФУ. Технические науки. 2006. № 13. С. 311–316.

3. Баришполец В.А. Информационно-психологическая безопасность: основные положения // журнал Радиоэлектроника. Наносистемы. Информационные технологии. 2013. №2. С. 65-105

4. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М.: Изд-во РАГС, 1998. 125 с.

5. Ежевская Т. И. Психологическое воздействие информационной среды на современного человека // Психопедагогика в правоохранительных органах. 2009. № 2. С. 38–41.

6. Иванов С. В. Правовое регулирование информационной безопасности личности в Российской Федерации // Вестник Екатерининского института. 2014. № 1 (25). С. 50.

7. Исакович Е.И., Кошелев Д. В. Современные методы и технологии психологического воздействия на человека // Журнал Вестник Университета российского инновационного образования. 2023. №1 С.27-39

8. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия – Телеком, 2004. 208 с.

9. Рыбалкин О. Р. Феномен безопасности // Вестник Московского университета. 2003. № 5. С. 35–42.

10. Рощин С. К., Соснин В. А. Психологическая безопасность: новый подход к безопасности человека, общества и государства // Российский монитор. 1995. № 6. С. 133–146.

11. Рерке В. И., Бубнова И. С. Психологическая безопасность образовательной среды школы: изучение и прогноз // Казанский педагогический журнал. 2016. № 3. С. 150–155.

12. Стуканов В.Г. К уточнению понятия «информационно-психологическое воздействие // Вестник московского университета МВД России. 2014. №5. С. 224-226

13. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ. URL: http://www.consultant.ru

КИБЕРПРИСТУПНОСТЬ

Кабанов Николай Николаевич
Областное государственное бюджетное профессиональное образовательное учреждение «Томский аграрный колледж»
Руководитель: Клевцова Ольга Александровна

Введение

Моя работа посвящена киберприступности. Я выбрал эту тему, потому что киберпреступностью это достаточно сильная проблема в современном мире. Однако, несмотря на это с киберпреступностью бороться можно и в домашних условиях.

Актуальность этой темы бесспорна так как немалое количество наших соотечественников подвергаются угрозам кибер атак. Обработав результаты опроса, я увидел что эта тема интересна моим друзьям, близким, родственникам и знакомым. Поэтому **целью** моей работы стало: изучить информацию по данному вопросу и выявить средства борьбы с киберприступниками.

Задачи:

1. Изучить что такое киберприступность и ее виды.
2. Провести классный час по этой теме.
3. Выявить наиболее эффективный способ борьбы с хакерами.

Методы исследования: поиск информации в сети Интернет, анкетирование, анализ, проведение опроса, составление мониторинга.

Объект: Отношение людей к данной проблеме.

Предмет исследования: материал в сети Интернет о киберприступности.

Гипотеза: Я считаю, что знание о киберприступниках и их преступлениях необходимо для работы с информацией в современном мире.

Глава I. Теоретическая часть.

1.1. Киберпреступность.

Так что же такое Киберпреступность? Это различные противомерные действия в виртуальном пространстве.

1.1.1. Виды киберпреступности.

В ходе исследования я выделил несколько основных видов киберпреступлений. Среди них:

- Спам
- Фишинг
- Похищение цифровой личности
- Инсайдинг
- Телекоммуникативные преступления

Фишинг- это интернет мошенничество, когда всеми возможными правдами и неправдами у вас пытаются узнать различные персональные данные (пароли, логины, номера банковских карт и счетов). Смысл заключается в том, чтобы побудить вас перейти на фишинговой ссылке на поддельную страницу, визуально похожую на настоящую, например банка, где под различными предлогами выудить персональную информацию.

Похищение цифровой личности - неправомерное завладение профилем, в социальной сети, с целью рассылки спама (Использование личных данных), шантажа, выманивания денежных средств.

Спам - это нежелательные рекламные объявления и сообщения, предназначенные для распространения рекламных объявлений или вредоносных программ. Они доставляют пользователям не удобства и опасность, так как авторы спама имеют множества средств, для получения новых адресов электронной почты и способов нелегальной рассылки сообщений.

Инсайдинг - инсайдер (Освобожденный сотрудник компании) является потенциальным преступником. Он знает тонкости компьютерной системы компании, имеет неограниченный доступ к ним с целью незаконного вмешательства в работу в

автоматизированных электронно-вычислительных машин и компьютерных сетей. С целью незаконного завладения информацией, которая является собственностью компании. Наиболее известным преступлением является атака с целью перегрузить оборудование жертвы и помешать использовать его нормально (DDOS-атака).

1.2. Кто такие киберпреступники.

И так мы выяснили что киберпреступник - это человек, который совершает те или иные не правомерные действия в виртуальном пространстве.

1.2.1. Какие существуют наказания для киберпреступников?

Давайте разберёмся, какие существуют наказания для киберпреступников. Согласно уголовному кодексу Российской Федерации предусмотрено наказание по "УК РФ статья 272, 273, 274"

УК РФ 272 "Неправомерный доступ к компьютерной информации". Наказания: Штраф в размере до 2 тыс. руб.,

либо исправительные работы на срок до 1 года, либо ограничением свободы на срок до 2 лет, Либо лишением свободы на тот же срок.

УК РФ 273 "Создание, использование и распространение вредоносных компьютерных программ". Наказания: ограничение свободы на срок до 4 лет, либо принудительными работами на срок до 5 лет, либо лишением

свободы на срок до 5 лет, со штрафом в размере от 100. тыс. руб. до 200 тыс. руб.

УК РФ 274 "Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей".

Наказания: Штраф в размере до 500 тыс. руб., либо исправительными работами на срок до 6 месяцев до 1 года, либо ограничением свободы до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок.

1.3. Противостояние хакерам в домашних условиях.

Итак, позвольте представить - первоочередные шаги для повышения безопасности:

- Устанавливать качественное антивирусное и антишпионское ПО;
- Устанавливать спам-фильтр в почтовые программы;
- Не открывать писем от незнакомых пользователей;
- Не переходить по ссылкам на известные сайты;
- Храните несколько резервных копий важных данных;
- Обращайте внимание, если ваши знакомые начинают вести себя необычно - игнорируйте их просьбы одолжить денег, или предоставить другие ресурсы;
- Установка надежных паролей;
- Подключение только проверенных USB-устройств;
- Установка лицензионного ПО;

А так же советую пользоваться проверенными WEB-браузерами, посещать сайты только по оригинальной ссылке.

Глава II. Практический этап исследования.

2.1. Анкетирование в колледже

При изучении данной темы мною был проведен опрос среди студентов группы МС-205П Томского аграрного колледжа Первомайского филиала (приложение 1), респондентов было 25 человек.

По результатам опроса было выявлено, что: 40% учащихся подвергались заражению их устройств вирусами, и еще 12% подверглось краже финансовых средств при сталковении с фишингом, так же 16% подвергалось хищению цифровой личности, 32% из опрошенных подвергалось спаму в соц.сетях. (приложение 2).

Вывод: По результатам данного тестирования видно, что эта тема довольно актуальна, так как большая часть моих знакомых уже подверглись угрозам кибер-атак. И для них будет полезно ознакомиться с правилами безопасности в сети Интернет.

2.2. Столкновение с киберпреступностью на моем личном опыте.

Так же киберприступности был подвержен и я сам. Мое устройство было заражено вирусом при скачивании программы из неофициальных и непроверенных источников. Помимо этого я был подвержен спаму на электронной почте, что доставляло много неудобств.

Рекомендации: Я бы хотел порекомендовать владельцам смартфонов на операционной системе Android, установить бесплатный антивирус *Dr.Web Light*. Вы можете установить его, введя в строку поиска в приложении Play Market, нажав на кнопку "Установить".

пойдет им на пользу.

Заключение

В данной работе, проанализировав изученный материал, я пришёл к выводу, что действительно уже сейчас стоит защититься от киберпреступников в домашних условиях.

И так мне удалось рассказать о таком явлении как киберпреступность. О том кто такие киберпреступники, о видах киберпреступности , о средствах защиты от кибер-атак в домашних условиях.

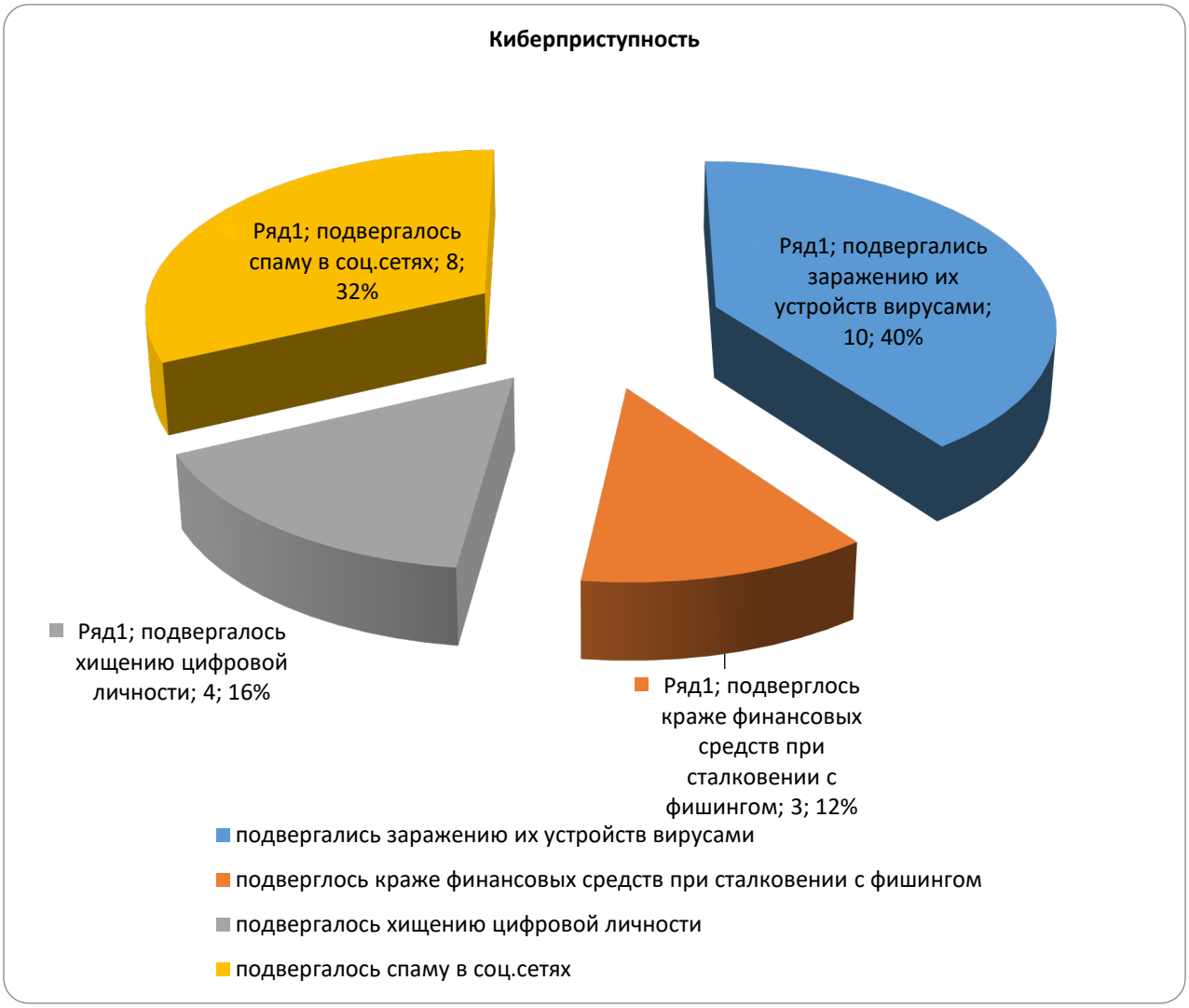
Используемая интернет-ресурсы.

- https://wikipedia.org/wiki/Претсупления_в_сфере_информационных_технологий
- https://urist.one/dolzhnostnye-prestupleniya/kiberprestupnost/kiberprestuplenie.html
- https://sledcomrf.ru/news/311007-profilaktika-kiberprestupleniy.html

Приложение 1

№	Вопрос	Кол-во студентов	%
1	Подвергались заражению их устройств вирусами	10	40
2	Подверглось краже финансовых средств при столкновении с фишингом	3	12
3	Подвергалось хищению цифровой личности	4	16
4	Подвергалось спаму в соц.сетях	8	32

Приложение 2



ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ

Батовский Игорь Алексеевич
Стрежевской филиал Областного государственного бюджетного профессионального образовательного учреждения «Томский промышленно-гуманитарный колледж»
Руководитель: Коледина Арина Фёдоровна

ВВЕДЕНИЕ

Поговорка «если тебя нет в социальных сетях, то тебя нет и в реальной жизни» появилось совсем недавно, но она показывает суть человеческой сущности сегодня. Ведь, сегодня практически половина населения земного шара расходует свое время иногда с пользой, а зачастую впустую «сидя» в социальных сетях. Информация в социальных сетях небезопасна.

Актуальность исследования заключается в том, что в условиях информационных войн, глобальных угроз и постоянного роста цифровых технологий возникла острая потребность в формировании комплексной системы защиты от информационно-психологических угроз. Эти угрозы могут проявляться в виде манипуляций общественным мнением, распространения фейковых новостей, воздействия на психоэмоциональное состояние индивидов и групп через медиа платформы.

Цель исследования: исследовать проблемы информационно-психологической безопасности личности.

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

1) Определить основные виды информационно-психологических угроз безопасности личности и общества;

2) Изучить роль международного сотрудничества в сфере защиты от информационно-психологических угроз;

3) Разработать рекомендации для защиты от негативного влияния информации в интернете.

Гипотеза исследования: разработка и внедрение методов информационно-психологической защиты помогут повысить личную устойчивость и благополучие человека в условиях интенсивной информационной среды.

Методы исследования проекта: поисковой, анализ литературы, синтез, разработка.

1.Теоретические основы информационно-психологической безопасности

1.1 Основные виды информационно-психологических угроз безопасности личности и общества

Информационно-психологическая безопасность — это концепция, охватывающая защиту личности, общества и государства от различных информационно-психологических угроз, способных нарушить стабильность и гармоничное развитие социальной среды.

Сегодня специалисты по информационной безопасности востребованы практически во всех сферах деятельности человечества. Все сферы деятельности человека в любом современном государстве нуждаются высококвалифицированных специалистах по защите информации.

В наше время информация обеспечивает жизнедеятельность любой организации, учреждения, компании, фирмы, гражданина. И там есть своя опасность (Рис.1).

Рисунок 1- Виды информационных угроз

Хотя организации с квалифицированными специалистами по информационной безопасности имеют определенный уровень защиты, обычный пользователь сетей передачи данных остается самым уязвимым звеном в системе безопасности. Пользователи без специального образования и навыков работы с компьютером и интернетом особенно подвержены угрозам информационной безопасности и часто оказываются беззащитными перед ними (Рис.2).

Рисунок 2- Пирамида цифровых угроз

Анализируя вышесказанную информацию, можно выделить следующие виды информационно-психологических угроз для личности:

1) кибербуллинг и психологическое давление. Это нападения с целью причинения психологического вреда, осуществляемые через различные информационные платформы, могут нанести ущерб психическому здоровью и

самооценке жертвы. Эти угрозы особенно опасны для подростков и молодежи, склонных к уязвимости в интернете;

2) манипулятивное воздействие: намеренное искаженное представление информации с целью изменить восприятие, поведение или эмоциональное состояние людей. Это включает дезинформацию, фейки, пропаганду и использование когнитивных искажений для влияния на убеждения и решения;

3) информационная перегрузка: избыточное количество информации, которое затрудняет фильтрацию и осмысление данных, вызывает тревожность, усталость, снижает способность к критическому мышлению и повышает вероятность принятия ошибочных решений;

4) пропаганда радикальных и экстремистских идей: распространение радикальных идей, направленных на насилие, расизм или дискриминацию. Вовлечение в подобные группы угрожает личной безопасности и способствует росту социальной напряженности и конфликтов;

5) социальная инженерия и мошенничество: методы психологического воздействия, используемые для получения конфиденциальной информации, манипуляции действиями жертвы или кражи данных. Это может включать фишинг, телефонные мошенничества и другие формы обмана.

1.2 Роль международного сотрудничества в сфере защиты от информационно-психологических угроз

Международное сотрудничество играет ключевую роль в противодействии информационно-психологическим угрозам, поскольку современные угрозы в этой сфере зачастую не ограничиваются границами отдельных государств и требуют координированных усилий на глобальном уровне. Основные направления международного сотрудничества включают:

- разработка и согласование международных стандартов: Установление единых подходов к защите данных, регулированию распространения дезинформации и

созданию этических норм помогает странам синхронизировать усилия в защите от манипуляций и вредоносного воздействия;

- обмен информацией и опытом: Международные партнерства позволяют обмениваться передовыми методами и успешными практиками в области защиты от информационных угроз, что повышает эффективность национальных мер и ускоряет реакцию на новые виды киберугроз и психологических атак;

- создание совместных программ и инициатив: Организации, такие как ООН, НАТО и Евросоюз, разрабатывают глобальные проекты для защиты информационного пространства и создания инструментов противодействия кибербуллингу, пропаганде и экстремизму, что помогает формировать более устойчивую среду для всех стран-участников;

- обучение и повышение осведомленности: Совместные образовательные программы и информационные кампании, проводимые на международном уровне, способствуют повышению осведомленности общества об информационно-психологических угрозах и формируют навыки критического мышления, необходимые для защиты от манипуляций.

- координация реагирования на кризисные ситуации: В условиях информационных атак или кибератак, которые могут дестабилизировать общества и вызывать массовые психологические последствия, международные альянсы позволяют быстрее реагировать на кризисные ситуации и поддерживать друг друга в восстановлении информационной безопасности.

Таким образом, международное сотрудничество позволяет государствам объединять ресурсы и усилия, обеспечивая более надежную защиту личности и общества от информационно-психологических угроз, укрепляя доверие и содействуя формированию устойчивой цифровой среды.

2. Практические разработки для защиты общества

2.1 Разработка рекомендаций для защиты от негативного влияния информации в интернете

Развивайте критическое мышление: Не принимайте информацию за правду сразу, особенно если она вызывает сильные эмоции. Старайтесь проверять факты и избегать поспешных выводов.

Ограничьте потребление информации: Регулярные перерывы от социальных сетей и новостей помогают поддерживать эмоциональную устойчивость. Старайтесь избегать «информационного переедания» и тщательно выбирайте источники информации.

Проверяйте источники: Пользуйтесь авторитетными сайтами и проверяйте новости через несколько независимых источников. Предпочтение стоит отдавать СМИ с хорошей репутацией, избегая анонимных и не проверенных каналов.

Отписывайтесь от токсичных страниц и аккаунтов: Если какой-то контент или аккаунт вызывает у вас негативные эмоции, тревожность или стресс — отписывайтесь. Создавайте в соцсетях здоровую и позитивную информационную среду.

Ограничьте личные данные в соцсетях: Не делитесь в сети лишней личной информацией, чтобы снизить вероятность манипуляций. Убедитесь, что в настройках конфиденциальности указано, кто может видеть ваши публикации и личные данные.

Обучайтесь распознаванию манипуляций: Изучайте методы, которые используют в манипулятивных новостях и рекламных материалах. Это поможет вам лучше фильтровать информацию и не поддаваться на попытки влиять на ваше мнение.

Используйте программы для блокировки контента: Установите расширения для браузеров, которые блокируют нежелательный контент, рекламу и сайты с сомнительной репутацией. Это уменьшит риск столкнуться с фейковыми новостями или нежелательной информацией.

Занимайтесь цифровой грамотностью: Изучите базовые принципы кибербезопасности, например, как отличить фейковую страницу от настоящей, как распознавать фишинг, и защитите свои аккаунты двухфакторной аутентификацией.

Научитесь управлять своими эмоциями: Не позволяйте страху или гневу влиять на ваше восприятие новостей.

Эти меры помогут снизить негативное воздействие интернета и социальных сетей на ваше психологическое состояние и защитить ваше личное пространство от нежелательных информационных влияний.

ЗАКЛЮЧЕНИЕ

Проект на тему «Информационно-психологическая безопасность личности» позволил всесторонне рассмотреть и проанализировать аспекты защиты человека от негативных информационно-психологических воздействий. В современных условиях стремительного развития информационных технологий и медиа, личность становится особенно уязвимой к манипуляциям, дезинформации, кибербуллингу и другим видам психологического давления. Поэтому обеспечение информационно-психологической безопасности становится важным направлением как на государственном уровне, так и в контексте личной ответственности и осознанности.

Исследование показало, что информационно-психологическая безопасность подразумевает не только защиту от негативного информационного влияния, но и развитие у личности навыков критического мышления, эмоциональной устойчивости и цифровой грамотности. Эффективная система защиты предполагает комплексный подход, включающий правовое регулирование, образовательные программы, формирование навыков информационной безопасности, а также разработку этических норм для интернет-сообщества.

В рамках проекта были предложены рекомендации по повышению уровня информационно-психологической безопасности, включая улучшение законодательной базы, повышение осведомленности пользователей, создание

программ по формированию устойчивости к манипуляциям и психологическому давлению. Принятые меры будут способствовать формированию безопасной и комфортной информационной среды, в которой личность сможет полноценно развиваться и реализовывать свои потенциалы без угроз со стороны внешних воздействий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Акулич, М.М. (2022) Троллинг в социальных сетях: возникновение иразвитие. Электронный ресурс. // journals.rudn.ru › sociology › article.

2. Бабенко, М. Скрытые угрозы в социальных сетях. Электронный ресурс.http://cripo.com.ua/processes/skrytye-ugrozy-v-sotsialnyh-setyah/

3.Зона беззащитности. Скрытые угрозы, которым дети и взрослыеподвергаются в социальных сетях. Электронный ресурс.https://osvitanova.com.ua/posts/2389-zona-bezzashchytnosty-skrytye-uhrozy-kotorym-dety-y-vzroslye-podverhaiutsia-v-sotsyalnykh-setiakh

4.Виды онлайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка. Электронный ресурс.https://74205s25.edusite.ru/DswMedia/vidy_onlajn-ugroz.pdf

5.Информационно-психологическая безопасность несовершеннолетних в сети Интернет. Электронный ресурс.https://infourok.ru/informacionnopsihologicheskaya-bezopasnost-nesovershennoletnih-v-seti-internet-1798086.html

6.Ишимбаев,Э. Угрозы информационной безопасности. Тенденции, пути,средства и методы борьбы с ними. Электронный ресурс.http://infocom.uz/2009/12/02/ugrozyi-informatsionnoy-bezopasnosti-tendentsii-puti-sredstva-i-metodyi-borbyi-s-nimi/

7.Ковалева, Н.Н.(2023) Информационное право России (Учебное пособие).Электронный ресурс. https://knigi.news/informatsionnoe/informatsionnoe-pravo-rossii-uchebnoe.html

9.Ненашев, С.М. (2020) Информационно-технологическая иинформационно-психологическая безопасность пользователей социальных сетей. Электронный ресурс. https://cyberleninka.ru/article/n/informatsionno- setey.

ВЛИЯНИЕ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ УГРОЗ НА ПСИХИКУ ЧЕЛОВЕКА

Демлер Алексей Дмитриевич

Областное государственное бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»

Руководитель: Захарова Анна Павловна

Гейнц Юлия Владимировна

Введение

В современном мире сложно найти человека, который бы не пользовался интернетом, социальными сетями и мессенджерами. Однако далеко не все задумываются о безопасности при использовании различных способов общения и передачи информации. Информационное развитие и цифровизация общества приводят к увеличению числа кибератак и взломов. Эти угрозы могут иметь серьезные последствия, как для отдельных пользователей, так и для организаций. Каждый второй сталкивался с различными видами кибератак, которые могут привести к финансовой потери, ущербу репутации, утечки конфиденциальной информации и пр. Последствия взлома в сети могут быть разрушительными и многогранными.

Актуальность данной работы заключается в том, что с развитием цифровых технологий такие информационные угрозы, как недостоверная информация, кибербуллинг и онлайн-мошенничество, становятся серьезной проблемой. С одной

стороны, с появлением новых информационных угроз разрабатываются все более эффективные методы защиты данных и создаются различные инструкции, позволяющие своевременно распознать преступника. С другой стороны, внимание к психологическим аспектам и последствиям, возникающим в результате подобных мошенничеств, остается недостаточным. Психологические последствия информационных угроз разнообразны и могут привести к повышению уровня стресса и тревоги, усилению чувства уязвимости и психологической травме.

В работе рассматривается ***проблема*** влияния различного рода информационных угроз на психику человека, что позволяет заранее оценить потенциальные риски и выработать стратегии для их минимизации.

Объектом исследования является анализ существующих методов психологической защиты личности от негативного влияния информационных угроз на основе полученных статистических данных. Практическая важность этой работы заключается в разработке рекомендаций по повышению информационной грамотности и психологической устойчивости личности при воздействии информационных угроз (***продукт исследования***).

Таким образом, ***цель исследования*** заключается в анализе влияния информационных угроз на психику человека, направленном на выявление психологических механизмов реакции, разработку мероприятий по защите от негативных последствий и повышение уровня осведомленности в области информационной безопасности. Достижению цели способствуют представленные ниже ***задачи исследования***:

1. Определить основные виды информационно-психологических угроз и их влияние на восприятие реальности и принятие решений.
2. Рассмотреть последствия кибербуллинга на психическое здоровье жертв, а также изучить воздействия онлайн-мошенничества на эмоциональное состояние пострадавших.

3. Осуществить сбор статистической информации, которая касалась влияния информационно-психологических угроз на психику человека.

4. Разработать рекомендации по повышению уровня информационной грамотности и психологической устойчивости личности в условиях воздействия информационно-психологических угроз.

К ***методам исследования***, используемым в данной работе можно отнести:

5. Проведение литературного обзора по теме информационно-психологических угроз безопасности личности;

6. Опрос участников для сбора статистической информации о влиянии информационно-психологических угроз на психику человека;

7. Анализ существующих методов защиты личности от информационно-психологических угроз.

Виды информационно-психологических угроз

Информационно-психологические угрозы — это угрозы, связанные с воздействием на психику и поведение людей через информационные каналы. Они могут иметь различные формы и проявляться в разных контекстах.

Основные виды информационно-психологических угроз включают:

1. Кибербуллинг - агрессивное поведение в интернете, такое как травля, запугивание или унижение. Жертвы кибербуллинга могут испытывать стресс, тревогу, депрессию и низкую самооценку.

2. Дезинформация и фейковые новости - распространение ложной информации может привести к панике, недоверию и паранойе среди населения. Люди могут начать сомневаться в достоверности информации, что негативно влияет на их психическое состояние.

3. Угрозы конфиденциальности - потеря личных данных или утечка информации может вызывать у людей страх, тревогу и чувство уязвимости. Это может также привести к паранойе и недоверию к окружающим.

4. Социальная изоляция - чрезмерное использование социальных сетей или технологий может привести к социальной изоляции, так как люди начинают избегать реальных взаимодействий. Это может способствовать развитию депрессии и тревожных расстройств.

5. Негативное влияние контента - контент, содержащий насилие, ненависть или другие негативные темы, может оказывать вредное воздействие на психику, особенно на молодых людей. Это может привести к формированию агрессивного поведения или снижению уровня эмпатии.

6. Зависимость от технологий - чрезмерное увлечение интернетом и цифровыми устройствами может привести к зависимости, что негативно сказывается на межличностных отношениях и психическом здоровье.

7. Угрозы безопасности - кибератаки, фишинг и другие формы мошенничества могут вызывать у людей страх за свою финансовую безопасность и личные данные, что приводит к повышенной тревожности.

Психологические аспекты воздействия информационно-психологических угроз на человека.

Кибербуллинг — это форма агрессии, которая осуществляется через цифровые технологии, такие как социальные сети, мессенджеры и онлайн-игры. Последствия кибербуллинга могут быть серьезными и разнообразными, особенно для психического здоровья жертвы. Вот некоторые из основных последствий:

- Депрессия: жертвы кибербуллинга часто испытывают чувство беспомощности, безнадёжности и никчёмности. Эти чувства могут привести к длительной депрессии и повлиять на способность жертвы функционировать в повседневной жизни.
- Тревога: люди, подвергшие кибербуллингу, могут испытывать тревогу и страх перед возможностью новых нападок. Они могут избегать социальных ситуаций

и изолироваться от своих сверстников, что приводит к чувству одиночества и изоляции.

- Низкая самооценка: жертвы кибербуллинга часто испытывают чувство стыда и смущения, что может привести к негативному самовосприятию. Такое самовосприятие может повлиять на способность формировать позитивные отношения и привести к социальной изоляции и замкнутости.
- Суицидальные мысли и самоповреждение: исследования показали, что жертвы кибербуллинга подвержены повышенному риску суицидальных мыслей и самоповреждений.
- Расстройства сна: хроническая бессонница или гиперсомния могут развиться как реакция на постоянный стресс.

Влияние онлайн-мошенничества на эмоциональное состояние пострадавших заключается в том, что жертвы могут испытывать чувство смущения, стыда и вины. В экстремальных ситуациях без должной помощи это может привести к депрессии и мысли о причинении себе вреда. Последствия обмана могут влиять на психику в течение многих лет.

Опрос, целью которого является сбор статистических данных о влиянии информационно-психологических угроз на психику человека.

Проведён опрос в виде анкетирования с целью выявления уровня влияния информационно-психологических угроз на психику человека среди студентов техникума. На диаграммах ниже, представлены результаты опроса.

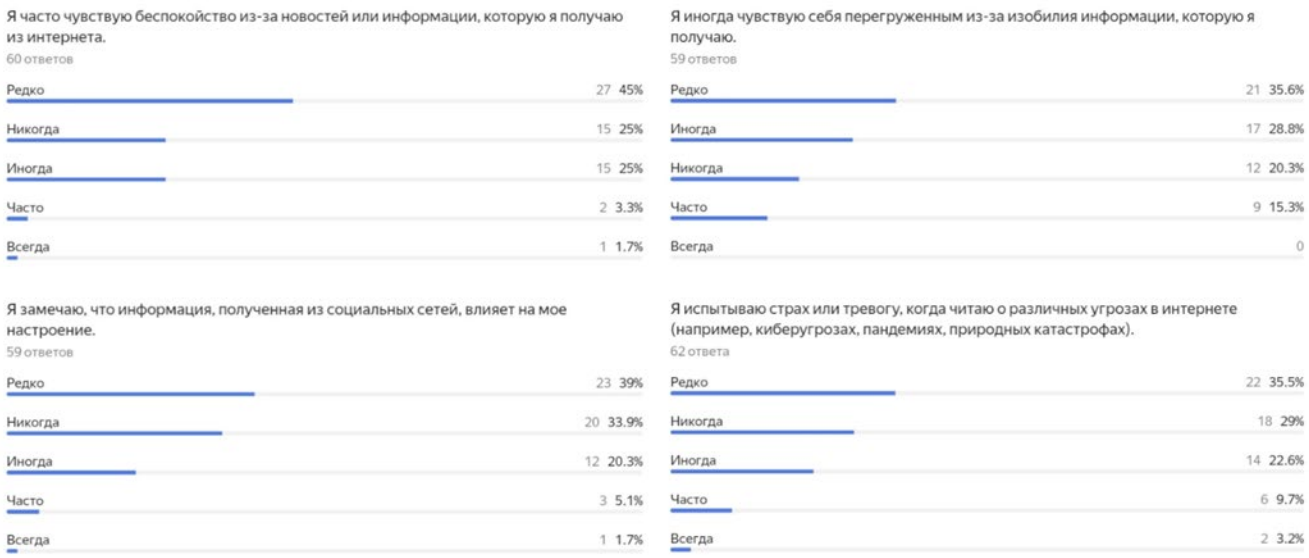


Рисунок 1.

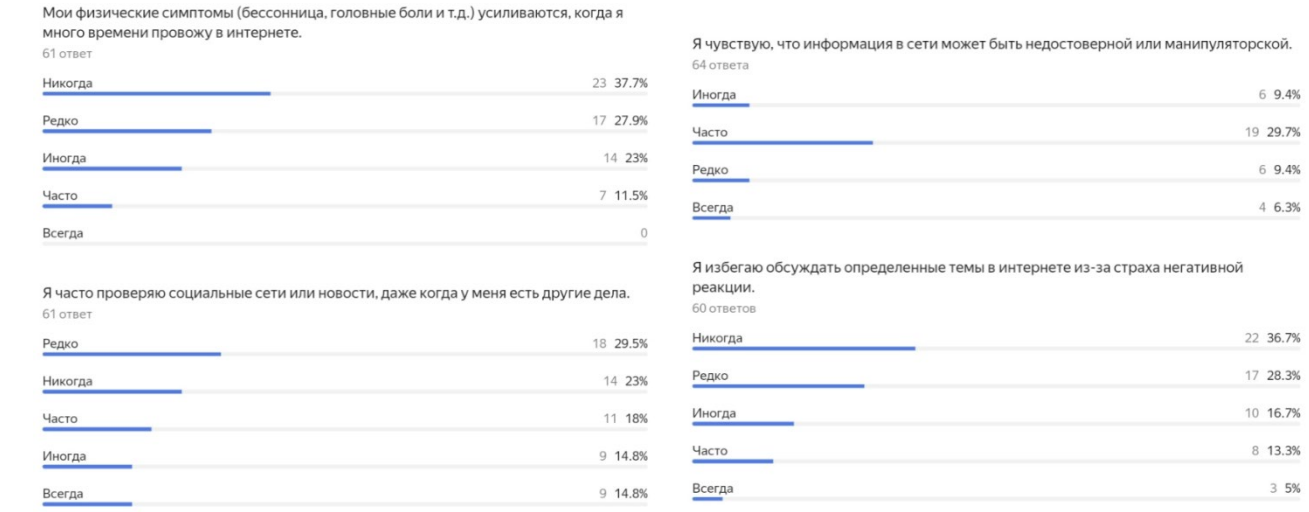


Рисунок 2.

Полученные статистические данные предоставляют ценную информацию, в том числе о том, насколько молодое поколение осведомлено о рисках, связанных с онлайн-пространством. По полученным данным можно сделать следующий вывод, что большинство опрошенных обладают общими сведениями о информационно-психологических угрозах, фильтруют полученную информацию из медиа пространства, а также понимают, что информация в сети может быть недостоверной или нести манипуляторный характер.

Таким образом, важно осознавать психологические последствия от различного рода информационно-психологических угроз.

Результаты опроса показывают насколько студенты считают важным обучение по вопросам информационной безопасности и психологии.

Рекомендации, позволяющие снизить влияние информационных угроз на психику человека

Собранные статистические данные также могут быть использованы для разработки рекомендаций, которые помогут снизить влияние информационных угроз на психику человека, а также для создания более безопасной онлайн-среды:

1. Не воспринимать получаемую информацию как истину в конечной инстанции. Важно научиться интерпретировать её, понимать суть, принимать личностную позицию по отношению к скрытому смыслу.

2. Развивать информационную культуру. Нужно уметь находить требуемую информацию в различных источниках, систематизировать её, находить ошибки в получаемой информации, воспринимать альтернативные точки зрения и высказывать обоснованные аргументы, устанавливать связи, вычленять главное в информационном сообщении.

3. Ограничивать информационную нагрузку. При длительном воздействии информационной нагрузки, превышающей допустимый для конкретного человека предел, развивается информационная перегрузка. В этом случае наблюдается ослабление сопротивляемости организма, нарушение нормальных физиологических функций, снижение работоспособности, появление чувства беспомощности и внушаемости.

4. Знать свои индивидуально-психологические особенности. Это не только обязательный элемент общей культуры, но и необходимое условие безопасности в социальном взаимодействии, в различных межличностных коммуникативных ситуациях.

Заключение

В заключение хотелось бы отметить, что влияние информационных угроз на психику человека является многогранным и требует внимательного подхода. Понимание этих рисков и активные меры по их минимизации помогут сохранить психическое здоровье в условиях современного информационного общества.

Изучение влияния информационных угроз на психическое здоровье становится все более актуальным в нашем быстро меняющемся цифровом мире. Защита личности и повышение информационной грамотности не только способствуют улучшению психоэмоционального состояния, но и помогают создать более безопасное и поддерживающее онлайн-пространство.

Список использованных источников

1. Ежевская Т.И. Психологическое воздействие информационной среды на современного человека // Психопедагогика в правоохранительных органах, 2012. № 3 (27).

2. Емелин В.А., Рассказова Е.И., Тхостов А.Ш. Психологические последствия развития информационных технологий // Национальный психологический журнал, 2012. № 1 (7).

3. Аносов В.Д., Лепский В.Е. Исходные посылки проблематики информационно— психологической безопасности // Проблемы информационно— психологической безопасности / под ред. А.В. Брушлинского, В.Е. Лепского. М., 2009.

4. Виноградова С.М., Мельник Г.С. Психология массовой коммуникации // Учебник для бакалавров. М.: Издательство Юрайт, 2017.

РЕАЛЬНАЯ ОПАСНОСТЬ. ДЕСТРУКТИВНЫЙ КОНТЕНТ

Дранов Егор Игоревич

Областное государственное бюджетное профессиональное образовательное учреждение «Колпашевский социально- промышленный колледж»

Руководитель: Криницкая Наталья Александровна

«…российское общество должно быть эффективно защищено от различных отрицательных проявлений»

В. В. Путин

Все материалы, распространяющиеся в сети Интернет, которые могут негативно повлиять на пользователей относятся к деструктивному контенту.

Опрос Всероссийским центром изучения общественного мнения[11] о восприятии россиянами Интернета выявил, что 32% опрошенных считают, что Интернет приносит вред обществу; 35% – что Интернет – угроза семейным ценностям; 35% – что он может угрожать политической стабильности в стране; 50% – что зарубежные страны используют Интернет против России; 46% – что Интернет значительно увеличивает количество самоубийств.

По результатам опроса можно сделать вывод, что существует проблема распространения деструктивного контента в сети Интернет.

Цель исследования: анализ и обоснование негативного воздействия на пользователей сети Интернет деструктивного контента.

Задачи

1. Проанализировать источники рунета о понятии, техниках вовлечения и маркерах деструктивного контента.

2. Создать тест в программе PowerPoint, протестировать обучающихся на предмет знакомства с маркерами деструктивного контента.

3. Выполнить анализ результатов тестирования и разработать пост- памятку по правилам общения в Интернете.

[11] Что такое интернет и какая информация там распространяется? URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-i-deti-vozmozhnosti-i-ugrozy (дата обращения: 05.11.2024).

Методы исследования: синтез и анализ информации, тестирование, моделирование.

Гипотеза: предположим, что большинство обучающихся знакомы с маркерами деструктивного контента, и это оказывает на них негативное воздействие.

Деструктивный контент, что это?

Деструктивный или опасный контент - любой контент, который может нанести вред человеку или сподвигнуть его к причинению вреда другому. Деструктивные культы призывают к разрушению, убийству, аутоагрессии.

Социальные сети являются самым эффективным и широким по охвату инструментом, с помощью которого злоумышленники могут вербовать пользователей в разные преступные организации[12].

Деструктивные сообщества могут:

- нанести непоправимый вред психическому и физическому здоровью ребенка;
- сформировать не традиционные духовно-нравственные ценности, опасные взгляды и убеждения, основанные на насилии и мизантропии;
- заставить пользователя причинить вред себе или окружающим.

В случае, если пользователь столкнулся с деструктивным контентом, он может сделать самую простую, но очень важную вещь - нажать кнопку «Пожаловаться» на публикации в соцсетях. В форме жалобы необходимо указать категорию такого контента (насилие, пропаганда наркотиков и т.п.).

Пользователь может обращаться в ораны власти. Направление обращений в органы власти - это право по закону. Никто не может в этом ограничить пользователей сети Интернет[13]. В обращении указывается конкретная ссылка на

[12] В российском сегменте соцсетей около 25 млн аккаунтов с деструктивным контентом. URL: http://rapsinews.ru/human_rights_protection_news/20190530/299835996. html (дата обращения: 05.11.2024).

[13] «Деструктивный контент» - повод для ограничения Интернета? URL: https://rus.azattyq.org/a/destruktivniy-kontent-internet-ogranichenia/27739890.html (дата обращения: 06.11.2024).

аккаунт, группу, сообщество, чат или список таких ссылок. Желательно также прикладывать скриншоты самих публикаций, так как часто они бывают удалены, заблокированы или скрыты к моменту рассмотрения письма.

Если были установлены факты распространения детской порнографии, призывов к суициду, рекламы азартных игр (онлайн-казино), склонения несовершеннолетних к противоправным действиям, по всем этим темам нужно обращаться в Роскомнадзор. Заявление в Роскомнадзор можно отправить через Госуслуги или Единый реестр запрещённых сайтов (https://eais.rkn.gov.ru/feedback/).

Чем больше обращений будет подано, тем быстрее социальные сети будут очищены от противоправного контента.

Телефоны служб, которые могут помочь

- Всероссийский телефон доверия: 8 800 2000 122.
- Телефонная линия «Ребенок в опасности» Следственного комитета РФ 8-800-200-19-10.
- Горячая линия Дети России Онлайн: 8-800-25-000-15 (с 9:00 до 18:00 по рабочим дням, время московское, бесплатно, анонимно, конфиденциально).

Техники вовлечения подростков в деструктивные группы в сети

Вербовка - процесс привлечения участников, включающий обещание помощи, поддержки, предложение развлечений.

Манипуляция, включающая искажение информации, использование эмоций, давление на чувство вины, стыда, страха.

Воронки вовлечения[14] включают последовательность действий: знакомство с информацией, вызывающей интерес; участие в обсуждениях, дискуссиях; выполнение заданий, поручений; переход к более активным действиям.

[14] Дети в Интернете. Скрытая угроза. URL: https://narasputye.ru/archives/10631(дата обращения: 06.11.2024).

Маркеры проявления деструктивных сообществ в сети Интернет

1. Маркеры склонности к ультраправой идеологии (Рисунок 1)

· Публикация в социальных сетях статусов, содержащих в себе критику и оскорбления других людей по признаку национальности, религии, социального статуса.

· Подписки на сетевые сообщества, в название которых входят слова и словосочетания типа «ультра», «ультраправые», «белая раса» и др., и контент которых характеризуется материалами, содержащими оправдание действий и романтизацию поступков националистов.

· Тематические татуировки, отсылающие к таким символам, как свастика, иные солярные символы, «1488» (как «закодированное приветствие «Хайль Гитлер»), собственно изображения нацистских лидеров и т.д.

· Пропаганда насилия.

· Оценка человеческих качеств и ценности личности.

Рисунок 1. Маркеры склонности к ультраправой идеологии

2. Маркеры склонности к псевдорелигиозному экстремизму (Рисунок 2)

· Непризнание традиционных религиозных институтов и их лидеров.

· Непризнание основ светского государства.

· Чрезмерный интерес к идеологии «конца света» и т.д.

· Критика, запреты касающиеся одежды, еды и т.п.

· Публикация в социальных сетях статусов, критикующих и оскорбляющих других людей по признаку национальности, религии, социального статуса.

· Использование радикальной религиозной и псевдорелигиозной лексики.

· Позитивные упоминания о тех или иных представителях запрещенных в России псевдоисламских экстремистских течений.

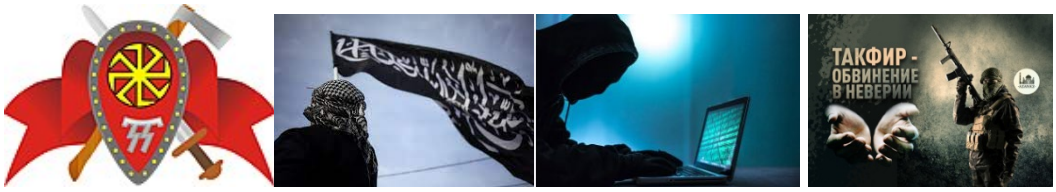


Рисунок 2. Маркеры склонности к псевдорелигиозному экстремизму

3. Маркеры склонности к политическому экстремизму (Рисунок 3)

· Непризнание органов государственной власти, государственных праздников РФ.

· Публикация в социальных сетях статусов, материалов и комментариев, критикующих и оскорбляющих государственные органы власти, ВС РФ, патриотические организации.

· Акцент на агрессивном отказе России в статусе тысячелетней цивилизации и самом праве на государственность.

· Отрицание территориальной целостности России

Рисунок 3. Маркеры склонности к политическому экстремизму

4. Маркеры вовлеченности в околокриминальную субкультуру (Рисунок4)

· Использование специфического слэнга.

· Наличие соответствующих татуировок.

· Выраженный интерес к криминальному миру.

· Демонстративно негативное отношение к правоохранительным органам и их сотрудникам.

· Гипертрофированный интерес к околокриминальной музыкальной субкультуре.

Рисунок 4. Маркеры вовлеченности в околокриминальную субкультуру

5. Маркеры склонности к совершению акций типа «Колумбайн» и (или) террористическим актам (Рисунок 5)

· Проявление особого, пристрастного интереса к темам насилия и убийств.

· Речевые маркеры, указывающие на пренебрежительное отношение к ценности жизни.

· Речевые маркеры, одновременно указывающие на сильные чувства обиды, ненависти, страха и апатии.

· Демонстрация тех или иных атрибутов «Колумбайна».

· Проявление деструктивной агрессии (вербальной и невербальной).

· Отказ от общения с семьей и близкими людьми.

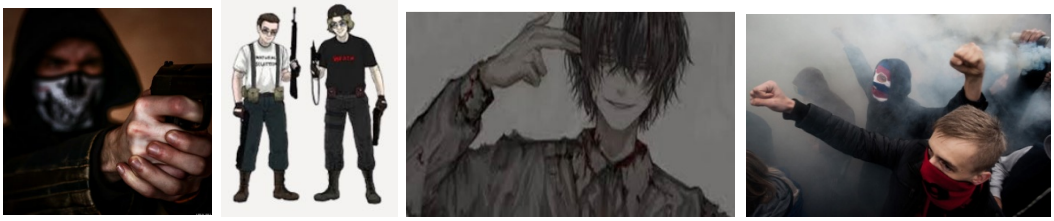


Рисунок 5. Маркеры склонности к совершению акций типа «Колумбайн» и (или) террористическим актам

Тест «Маркеры деструктивного контента»

Для выявления осведомленности обучающихся первого курса колледжа о маркерах проявления деструктивного контента, разработан тест «Маркеры деструктивного контента», созданный в программе PowerPoint (Рисунок 6). Тест содержит три слайда. На первом слайде размещены: инструкция по прохождению

теста, таблица из 36 ячеек со словами и числами, две управляющие кнопки. Из 36 ячеек 17 являются маркерами деструктированного контента. Обучающимся предлагается выбрать маркеры, с которыми они знакомы. Цвет текста в выбранных ячейках меняется с черного на красный. После выбора известных маркеров необходимо кликнуть кнопку «Проверь себя». На таблицу накладывается трафарет, скрывающий ячейки, не содержащие деструктивные маркеры. Открытыми остаются 17 маркеров деструктивного контента. Количество ячеек с текстом красного цвета является результатом прохождения теста. При клике на кнопку «Помощь» пользователь может перейти на следующие слайды и узнать значение слов на ячейках таблицы, в том числе значение слов и чисел, которые являются маркерами деструктированного контента.

Ссылка для скачивания теста:

https://vk.com/s/v1/doc/op4coEu66NEGuW4tYiMh4dEVCn0GPxj28SKLPQGtSlTeq-6BkE0 .

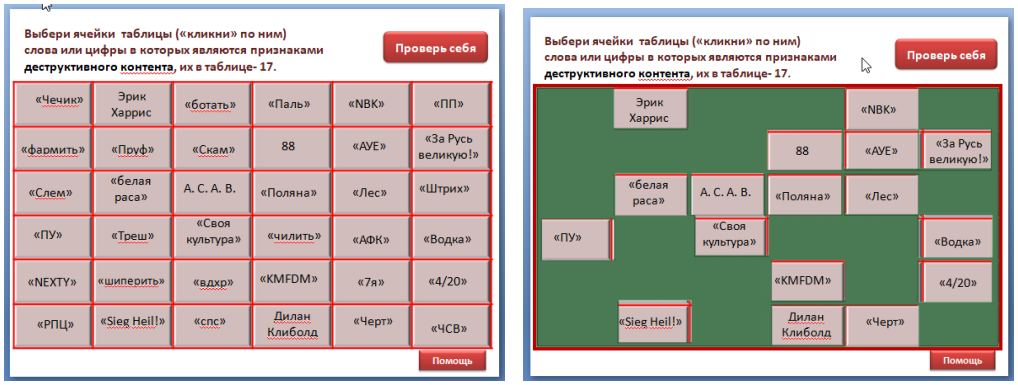


Рисунок 6. Окно интерактивного теста «Маркеры деструктивного контента».

Анализ тестирования обучающихся ОГБПОУ «КСПК»

В тестировании принимали участие 55 первокурсников. По результатам тестирования составлена таблица (Таблица 1).

Таблица 1

Результаты прохождения теста среди первокурсников ОГБОУ «КСПК»

Маркеры	NBK	ПУ	Водка	KMFDM	88	Своя культура	белая раса	4/20	А. С. А. В.	За Русь великую!	Поляна	Лес	Черт	Эрик	Дилан	А.У.Е.	«Sieg Heil!»
Число совпадений	8	8	7	1	9	4	2		4				2	4	1	1	9
% выбора	3	3	1	8	5	5	0	1	4	6	6		8	5	0	5	5

Результаты тестирования показывают, что большая часть обучающихся знакомы со значением девиза криминальной субкультуры и российского неформального объединения банд «А.У.Е.» – 75% респондентов. 58% обучающихся знакомы со словом «Черт» - жертва оффников[15] , намеченная предварительно и приглашенная на забив[16]. Наименьший выбор: «Лес» - место для «забивов», часть культа оффника, составил 7%.

Средние результаты таблицы показывают, что первокурсники колледжа знакомы с маркерами склонности к: террористическим актам - 30%; ультраправой идеологии - 29%; псевдорелигиозному экстремизму - 25%; околокриминальной субкультуре - 40%; политическому экстремизму - 16%.

В результате анализа сделаны выводы, что студенты первого курса мало используют деструктивный контент, о некоторых маркерах они не знают.

С целью предостережения от вовлечения молодежи в деструктивный контент создан постер-памятка (Рисунок 7) по правилам общения в Интернете. Печатный

[15] Околофутбольные фанаты- российская молодёжная субкультура, выделяющаяся среди других своей показной агрессивностью. URL: https://life.ru/p/1571590 (дата обращения: 05.11.2024).

[16] организованная драка между враждующими группировками футбольных фанатов/ URL: https://sinonim.org/t/%D0%B7%D0%B0%D0%B1%D0%B8%D0%B2 (дата обращения: 05.11.2024).

вариант памятки получили участники тестирования, электронный вариант размещен на странице в Контакте. Ссылка: https://vk.com/wall235201735_713 .

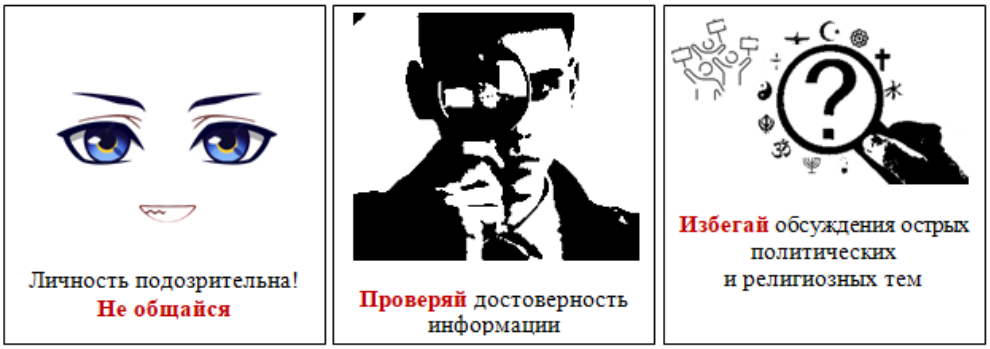


Рисунок **7.** Постер-памятка по использованию деструктивного контента

Постер- памятку, можно использовать в мероприятиях, посвященных информационной безопасности личности.

Среди видов контента, распространяемого в сети Интернет, значительную опасность представляет деструктивный контент, который является угрозой для достижения общественно-полезных целей и решения задач государственного управления, а также способствующий вовлечению пользователей сети Интернет в совершение противоправных и антиобщественных действий.

Объемы деструктивного и противоправного контента в социальных сетях растут вместе с объемами информации, которые «постят» пользователи. Запрещенный контент, угрожающий жизни или здоровью граждан России, направленный против традиционных нравственных ценностей или призывающий к противоправным действиям, появляется не на личных страницах в соцсетях, а в специально сформированных для его распространения информационных каналах.

При анализе результатов тестирования в колледже установлено, что не все обучающиеся знакомы с маркерами деструктивного контента, в среднем правильный выбор маркеров деструктивного контента составил 32%, что частично опровергает выдвинутую гипотезу.

Работа будет продолжена автором. На следующий год исследование уровня знаний студентами маркеров деструктивного контента будет дополнено анализом материалов об изменениях в законодательстве, ведь до сих пор не установлено на законодательном уровне четкого определения понятия деструктивный контент[17].

Список литературы

1. ВЦИОМ. Что такое интернет и какая информация там распространяется? [сайт]. 2019- 2024. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-i-deti-vozmozhnosti-i-ugrozy (дата обращения: 05.11.2024).

2. Лига безопасного Интернета. Деструктивный контент. [сайт]. 2011- 2024. URL: https://ligainternet.ru/ (дата обращения: 23.10.2024г.)

3. АО «Газета.Ру». Тонкая грань дозволенного: что такое деструктивный контент и почему его хотят регулировать. [сайт].1999-2024. URL: https://www.gazeta.ru/comments/2023/06/23_a_17180996.shtml (дата обращения: 23.10.2024г.)

4. РАПСИ. Новости. [сайт]. 2024. URL: http://rapsinews.ru/human_rights_protection_news/20190530/299835996.html (дата обращения: 05.11.2024).

5. На распутье. Дети в Интернете. Скрытая угроза. [сайт].2017-2024. URL: https://narasputye.ru/archives/10631 (дата обращения: 06.11.2024).

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ: СПАМ И ФИШИНГ

Глухов Максим Сергеевич

Областное государственное бюджетное профессиональное образовательное учреждение «Колпашевский социально- промышленный колледж»

[17] «...важно на законодательном уровне закрепить понятие "деструктивный контент"- вице-спикер ГД Анна Кузнецова. URL: https://ria.ru/20241026/kontent-1980302231.html .

Руководитель: Чемекова Ольга Валентиновна

Введение

Человек и информационная система — это два важных элемента в современном мире, которые взаимодействуют между собой. Человек использует информационные системы для получения, обработки и передачи информации. Информационные системы, в свою очередь, обеспечивают человеку доступ к большому объему данных и помогают принимать обоснованные решения.

Проблема и актуальность

Важно, чтобы информационная система была удобной и эффективной для пользователя, учитывая его потребности и способности. В свою очередь, человек, чтобы обезопасить свои персональные данные, должен быть грамотным пользователем информационных систем, уметь эффективно работать с данными и анализировать полученную информацию. Но интернет-мошенники умеют пользоваться разными способами для того, чтобы похитить персональные данные. И делают они это разными способами: от рассылок на почту до создания фальшивый новостей в игровых событиях. Многие люди пострадали от их действий.

В 2023 году «Лаборатория Касперского»[18] предоставила отчет о спаме и фишинге:

— 45,60% писем по всему миру и 46,59% писем в Рунете были спамом;

— 31,45% всех спамовых писем были отправлены из России;

— антивирус заблокировал 135 980 457 вредоносных почтовых вложений;

— система «Антифишинг» предотвратила 709 590 011 попыток перехода по фишинговым ссылкам.

[18] Securelist by Kaspersky: Спам и фишинг в 2023 году, 07.03.2024: Доступ: свободный/URL: https://securelist.ru/spam-phishing-report-2023/109104/ (дата обращение: 01.11.2024 г.)

— компонент «Защита чатов» мобильных решений «Лаборатории Касперского» предотвратил более 62 тысяч переходов по фишинговым ссылкам из Telegram.

Данные показывают, как много блокируют антивирусные программы вредоносной информации. Тем не менее, очень много людей попадаются на их уловки? Большая часть информации размещена на сайтах в виде рекламы, в играх, в виде анонса игрового события. Антивирусные программы не могут заблокировать абсолютно все, ведь поток информации огромен. Причем, фишингу и спаму подвержены люди всех возрастных групп. А это значит, что абсолютно всем пользователям сети Интернет, как говорится, «от мала до велика» нужно уметь защитить персональную информацию свою и своих родных

Цель проекта

Повышение осведомленности людей о фишинге и спаме через создание и размещение в социальных сетях информационных ресурсов «Информационно-психологическая безопасность» студентами специальности «Преподавание в начальных классах»

Задачи проекта

1. Анализ источников информации о спаме и фишинге как угрозе информационно-психологической безопасности.
2. Подготовка материалов для информационных ресурсов о способах защиты от мошенничества размещение их в социальной сети ВКонтакте.
3. Создание банка онлайн-ресурсов «Информационно-психологическая безопасность личности».

Продукт проекта

Продуктом проекта являются информационные ресурсы (буклеты, памятки, баннеры), разработанные студентами специальности 44.02.02 Преподавание в начальных классах.

Ссылка на продукты проекта: https://disk.yandex.ru/d/YQFLRmS383GMFA

Уникальность и значимость работы

Конечно, можно прийти в каждую группу, в любое место и рассказать им о фишинге и спаме, о том, какие последствия могут быть от них, о том, как это может изменить жизнь (не в лучшую сторону, как могут говорить и что показывать мошенники). Тут уместно вспомнить известное изречение Конфуция «Я слышу и забываю. Я вижу и запоминаю. Я делаю и понимаю».

Люди послушают о фишинге и спаме и забудут… Каждый думает, что это не про него, что его это не коснётся, а значит ему не нужна защита. Следуя «по Конфуцию» нужно, чтобы каждый что-то сделал своими руками, чтобы осознать, принять проблему и научиться не пускать ее в свою жизнь. Основная идея проекта заключается в том, что обучающиеся колледжа на занятиях самостоятельно разработают информационный ресурс, разместят его в социальных сетях. А для охвата большего количества людей указать #хэштеги. Реализация идеи целесообразна и эффективна, так как обучающиеся – пользователи социальных сетей – самостоятельно находят информацию, анализируют и структурируют для создания собственного информационного ресурса.

Этапы работы над проектом

1. Подготовительный этап – работа с источниками информации: выбор источников, анализ, обобщение, синтез.

2. Основной этап – о разработка информационных ресурсов на онлайн-платформе Supa и размещение готовых разработок в социальную сеть ВКонтакте.

3. Заключительный этап – создание банка онлайн-ресурсов «Информацинно-психологическая безопасность личности».

Описание продукта проекта

При разработке информационных ресурсов, студенты 2 и 3 курсов использовали онлайн-платформу Supa. Данная платформа позволяет творчески,

красочно и информативно оформить буклеты, плакаты и баннеры. Для разработки онлайн ресурсов была определена тема «Информационно-психологическая безопасность: спам и фишинг».

Пример 1.

Студент 3 курса отобрал основную информацию и выделил следующее:

- необходимо использовать проверенные социальные сети;
- не переходить по незнакомым ссылкам;
- создавать надежные пароли;
- использовать официальное программное обеспечение.

Создана памятка «Защитись от фишинга» https://disk.yandex.ru/i/qQIjD7tzQnc0Zw

Пример 2.

Студент 2 курса сделал вывод о том, что необходимо проверять систему антивирусов и игнорировать SMS от спамеров.

Создан плакат «Осторожно, подделка». https://disk.yandex.ru/i/IGvJmKgIp_vR2A

Пример 3.

Студент 1 курса в буклете расскажет о том, что необходимо создавать надёжные пароли. Это основа вашей безопасности!

Буклет «Как избавиться от спама» https://disk.yandex.ru/i/J1fIn7C1AZtblg

Все работы студентов специальности 44.02.02 «Преподавание в начальных классах» собраны в банк онлайн-ресурсов «Информационно-психологическая безопасность личности». Ссылка на банк онлайн-ресурсов: https://disk.yandex.ru/d/YQFLRmS383GMFA

Банк онлайн-ресурсов будет дополнятся другими информационными ресурсами. В дальнейшем студенты и преподаватели могут воспользоваться материалом банка при организации урока, студенты специальности 44.02.02 «Преподавание в начальных

классах» могут использовать материалы при прохождении учебной и производственных практик, чтобы научить безопасному поведению в информационном пространстве младших школьников. Ссылки на материалы могут быть размещены в групповые чаты обучающихся колледжа.

Заключение

Знание о защите от фишинга и спама в социальных сетях важно, потому что это помогает предотвратить кражу личной информации, финансовые потери и вероятность мошенничества. Умение распознавать подозрительные сообщения и ссылки снижает риски попадания в ловушки злоумышленников и обеспечивает безопасность личных данных и аккаунтов. Необходимо пользоваться только проверенными сайтами, вступать в переписку с проверенными аккаунтами, не вестись на рекламу и акции. И всегда помогать своим близким! И тогда информационно-психологическая безопасность гарантирована!

Источники информации

1. Securelist by Kaspersky: Спам и фишинг в 2023 году, 07.03.2024: Доступ: свободный/URL: https://securelist.ru/spam-phishing-report-2023/109104/ (дата обращения: 01.11.2024 г.)
2. Skillbox Media: Что такое фишинг и как от него защититься, 2023. Доступ: свободный: URL: https://skillbox.ru/media/code/slezhka-za-kulturoy-chat-boty-v-policii-i-otravlenie-kesha/ (дата обращения: 01.11.2024 г.)
3. Skillbox Media: Важное о спаме для пользователя и маркетолога: какой бывает спам и что грозит нарушителям, 2023. Доступ: свободный: URL: https://skillbox.ru/media/marketing/vazhnoe-o-spame-dlya-polzovatelya-i-marketologa-kakoy-byvaet-spam-i-chto-grozit-narushitelyam/ (дата обращения: 01.11.2024 г.)

БЕЗОПАСНОСТЬ ОБЩЕСТВА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Ушеренко Степан Денисович
Областное государственное бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»
Руководитель: Пальцев Вячеслав Владимирович

Одновременно с информатизацией возникают угрозы, связанные с противоправным использованием достижений в области информационных технологий. Становится актуальной проблема обеспечения информационной безопасности общества, которая признается всем мировым сообществом.

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудования, предназначенных для использования, сбережения и передачи этой информации.

Общество сегодня зависит от надежности и защищенности информационных систем, которые обеспечивают передачу критически важной информации. Поскольку такие системы все чаще становятся объектами атак, вопросы информационной безопасности становятся приоритетными для государства, бизнеса и каждого отдельного гражданина. Защита информации и создание безопасной информационной среды становятся необходимыми условиями для устойчивого развития и нормального функционирования общества.

Цель данной работы состоит в том, чтобы рассказать о возможных угрозах безопасности общества в информационном поле и методах предосторожности нужных чтобы не допустить утечки личных данных.

Я считаю, что в России стоит повысить осведомленность граждан о возможных угрозах в информационном поле.

Для этого необходимо проводить регулярные тренинги и обучения чтобы граждане лучше заботились о своих данных.

В 2023 году в Сеть было слито 1,12 млрд персональных данных, что почти на

60% выше показателя 2022-го, говорится в исследовании InfoWatch. Всего из российских компаний утекло 95 крупных баз данных. При этом в исследовании InfoWatch пришли к выводу, что истинный масштаб ущерба может быть существенно недооценен, так как более чем в 35% случаях утечек объем украденных данных остался неизвестен.

Эксперт связал этот тренд с появлением крупных хранилищ персональных данных на фоне ускоренной цифровизации экономики. Сейчас основными мишенями для кибератак становятся социальные сервисы, операторы связи, маркетплейсы и другие подобные платформы, в ближайшем будущем к ним могут добавиться федеральные ресурсы.

Согласно этой статистике можно понять насколько важно заботиться о своих данных, ниже я приведу в пример несколько распространенных способов мошенников украсть личные данные пользователей, а также решения которые помогут повысить безопасность данных.

Самые распространенные способы мошенников заполучить личные данные пользователя:

1. Фишинг – Мошенники отправляют поддельные электронные письма или сообщения, маскируясь под какие либо организации (например, банки, социальные сети). В таких сообщениях содержатся ссылки на фальшивые веб-сайты, которые копируют страницы настоящих компаний. Пользователь, введя свои учетные данные на таких сайтах, передает их мошенникам.

2. Слабые пароли, их подбор и отсутствие двухфакторной аутентификации – Использование слабых и легко угадываемых паролей (по типу, "123456789", "password", “qwerty”) может привести к тому, что мошенники смогут воспользоваться методом перебора, чтобы угадать пароль и получить доступ к учетной записи.

3. Трояны или Кейлоггеры – Вредоносное ПО установленное на компьютере пользователя (через поддельные приложения или вложения в письмах). Кейлоггеры

записывают нажатия клавиш, что позволяет злоумышленникам узнать, какие пароли вводит пользователь.

4. СМС или Voice фишинг – Мошенники звонят жертве, выдавая себя за представителей банка или службы поддержки. Они могут запрашивать личные данные или ввод на телефоне кода подтверждения, который был отправлен пользователю (то есть обходить с вашей помощью двухфакторную аутентификацию).

5. Использование общественных WIFI сетей – Подключение к незащищенным сетям Wi-Fi может позволить злоумышленникам перехватить данные, передаваемые между устройством пользователя и серверами, включая логины и пароли.

6. Утечки баз данных легитимных организаций – происходит взлом базы данных определенных организаций работающий с личными данными клиентов через ошибки и уязвимости в коде корпорации (Ситуация со сдеком в мае 2024 г.)

Решения для обеспечения большей безопасности общества в информационном пространстве:

1. Двухфакторная аутентификация аккаунта – самый надежный и легкий вариант обеспечения дополнительной защиты аккаунта.

2. Регулярная смена пароля – лучше всего каждые полгода менять пароль и не хранить его в веб ресурсах и приложения предлагающих хранение ваших паролей.

3. Антивирусные программы – установка и обновление антивирусного ПО на устройствах.

4. Регулярно проверять утечки паролей в открытых каналах – например при утечке паролей, украденные будут отображаться в вкладке “пароли” на Iphone.

5. Не использовать слабые пароли – включать в пароль цифры и прочие знаки, дополнительно использовать пароли от 16 символов.
6. Не отвечать на какие-либо звонки с незнакомых номеров. Не говорить код из СМС посторонним людям.

Вывод: Информатизация всех сфер жизни создает как возможности, так и новые вызовы. Угрозы, связанные с киберпреступностью, манипуляцией данными и распространением дезинформации, требуют комплексного подхода к обеспечению безопасности. Стоит более серьезно подходить к вопросу обеспечения собственной информационной безопасности и регулярно изучать новые методы мошенников чтобы не попасться на эту удочку и не потерять личные данные.

Список использованных источников

1. Статья об утечках личных данных Россиян https://www.rbc.ru/society/11/03/2024/65ec41e89a7947dc41bd43f9

2. Учебные и научные издания Научно-издательского центра https://book.uraic.ru/files/news/102020/spisok_inform_bezop.pdf

3. Утечки информации в мире, 2022–2023 годы https://ict.moscow/research/utechki-informatsii-v-mire-2022-2023-gody/

4. Обеспечение информационной безопасности https://digital.gov.ru/ru/activity/directions/466/

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ПСИХЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЖИТЕЛЕЙ РОССИИ

Круценко Ульяна Евгеньевна

Парабельский филиал областного государственного бюджетного профессионального образовательного учреждения «Томский политехнический техникум»

Бучельников Виктор Сергеевич

Введение

Отличительной чертой развития современного этапа общества является его тотальная цифровизация и информатизация. Помимо неоспоримых преимуществ эти два процесса имеют ряд существенных проблем.

Сегодня человек находится в непрерывном потоке информации, источники которой могут быть как внутренними: анализ собственного опыта, личное общение, так и внешними: чтение книг, газет и журналов, просмотр телепередач, прослушивание радиопрограмм и конечно же это получение информации с помощью Интернета, для чего сегодня активно применяются не только компьютеры, но и мобильные телефоны.

Актуальность: для обеспечения национальной безопасности необходим охват всех областей государственного устройства, при этом нельзя забывать и о важных психологических аспектах, основой которых выступаю информационные потоки. А как известно, воздействие информации не только влияет на принятие решений государственного значения, но и может выступать одним из факторов, влияющих на эмоциональный настрой в обществе. В связи с этим крайне важно обеспечивать необходимый уровень психологического равновесия в обоестве.

Цель работы – рассмотреть современное состояние информационно-психологической безопасности в Российской Федерации и выделить основные направления её дальнейшего развития.

Задачи:

1 – Ознакомиться с основными вопросами информационно-психологической безопасности России;

2 – Собрать и проанализировать информацию об имеющихся проблемах в этой области;

3 – Сделать выводы по проделанной работ

1. Человек в условиях информационного общества

Качественная и дозированная информация, несомненно помогает регулировать поведение личности, поддерживать коммуникативную связь с миром, а также помогает адаптироваться к изменяющимся условиям среды и т. д.

Однако в любом обществе всегда существует экономическая и политическая конкуренция, где простой человек становится объектом манипуляций различных структур, которые пытаются за счёт психологического воздействия на людей добиться так называемой «добровольной подчиняемости».

Используя различные методы влияния на общественное сознание, «информаторы» стремятся заглушить возможность к самостоятельному осмыслению выданной информации, её анализу, обобщению, сравнению и конкретизации, а также формулированию выводов.

Отсутствие критичности мышления делает человека и общество в целом крайне уязвимыми.

Ещё премьер-министр Великобритании, Уинстон Черчилль утверждал: «Кто владеет информацией, тот владеет миром».

В погоне за достижением поставленных целей, чтобы добиться власти над людьми, заинтересованные структуры и службы всегда стремятся выдать информацию в выгодной для себя свете, что в дальнейшем может использоваться ими при политических манипуляциях.

СМИ традиционно выступают в роли главного формирующего инструмента, управляющего общественным мнением, поэтому крайне важно, чтобы их возглавляли честные, порядочные и беспристрастные люди, желающие доносить объективную информацию, которая дает каждому человеку возможность делать собственные выводы и форировать своё отношение к чему-либо.

Ещё в 2000 году была принята Окинавская «Хартия глобального информационного общества», в которой отмечалось, что мировое сообщество должно предпринимать максимальные усилия, способствующие развитию глобального информационного общества, что требует согласованных действий в борьбе с преступностью в киберпространстве. Этот вид преступности отнесен к сфере транснациональной организованной преступности. Информационно-

коммуникационные технологии названы в Хартии «одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. ИТ быстро становятся жизненно важным стимулом развития мировой экономики».

Возникающие на постоянной основе геополитические угрозы требуют незамедлительного решения, поскольку имеют долгосрочный негативный результат.

2. Россия перед лицом информационно-психологической угрозы

На протяжении нескольких десятков лет наша страна находится в поле внимания тех, кто не заинтересован в том, чтобы Россия была сильным, независимым, экономически развитым государством, и в первую очередь это пытаются сделать путём влияния на общественное мнение. Это потребовало ответных действий.

В 2016 году была утверждена «Доктрина информационной безопасности России», в которой были чётко сформулированы основные информационные угрозы:

1. Использование возможностей трансграничного оборота информации для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

2. Наращивание рядом зарубежных стран возможностей информационно-технического воздействия, включая техническую разведку, на информационную инфраструктуру России в военных целях.

3. Использование специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира, и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.

4. Использование различными террористическими и экстремистскими организациями механизмов информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников.

5. Рост масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере; увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны.

6. Применение отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников, и представляющих угрозу международному миру, глобальной и региональной безопасности.

7. Постоянное повышение сложности, увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усиление разведывательной деятельности иностранных государств в отношении Российской Федерации.

8. Недостаточный уровень развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

9. Недостаточная эффективность научных исследований, направленных на создание перспективных информационных технологий, низкий уровень внедрения отечественных разработок и недостаточное кадровое обеспечение в области информационной безопасности, а также низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование с использованием отечественных информационных технологий и отечественной продукции, зачастую не имеют комплексной основы.

10. Стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.

11. Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, что затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

Заключение

Долгое время в России существует переизбыток «грязной информации», задачей которого является разрушение общественного строя, усиление разобщенности населения, подрыв морали, и нравственных устоев общества.

Сегодня крайне важно формировать новую единую национальную идею, которая будет основана на традиционных ценностях народов, живущих на территории Российской Федерации, кроме того, необходимо формирование научных институтов, которые будут разрабатывать решения вопроса повышения психологической стабильности в нашем обществе.

Всё это требует разработки мощной государственной программы обеспечения информационно-психологической безопасности.

Список использованных источников

1. Жохова Н.Н., Овсяник О.А., Дежкина Ю.А. Проблема информационно-психологической безопасности общества в современных условиях // В сборнике: Безопасная образовательная среда в изменяющихся условиях современного общества. Сборник материалов II Международной научно-практической конференции. Под научной редакцией О.И. Щербаковой, Л.В. Шукшиной. 2017. С. 126-130.

2. Лукин В. Н., Мусиенко Т. В. Информационная безопасность: геополитический аспект // Философия и гуманитарные науки в информационном обществе. – 2019. – № 1. – С. 68–88.

3. Лызь Н.А., Веселов Г.Е., Лызь А.Е. Информационно-психологическая безопасность в системах безопасности человека и информационной безопасности государства // Известия ЮФУ. Технические науки. 2014. № 8 (157). С. 58-66.

4. Лупанов Д.Ю. Понятие информационно-психологической безопасности личности // В сборнике: Актуальные проблемы самореализации личности в современном обществе. Материалы Международной научно-практической конференции. Под редакцией Д.Я. Грибановой. 2017. С. 182-189.

5. Манжуева О.М., Некрасов С.И., Некрасова Н.А. Информационно-психологическая безопасность - важнейший аспект безопасности государства // Инновации в гражданской авиации. 2017. Т. 2. № 3. С. 28-34.

СЕКЦИЯ 2: СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

ДЕФЕКТЫ БЕЗОПАСНОСТИ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ, СВЯЗАННЫЕ С ПЕРЕПОЛНЕНИЕМ БУФЕРА

Волков Алексей Дмитриевич
Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум информационных технологий»
Руководитель: Жабин Дмитрий Иванович

Буфер — участок памяти, выделяемый программой. Ошибка переполнения буфера (buffer overflow) — попытка поместить данные в заполненный буфер, то есть за его пределами. Подобные ошибки являются дефектами безопасности. В таких языках, как C и C++, следить за этим должен разработчик программы, языки не обеспечивают такой защиты из соображений производительности. То есть от разработчиков требуется определённая дисциплина.

Гипотеза проекта предполагает, что дефекты безопасности устройств интернета вещей, связанные с переполнением буфера, могут привести к повреждению данных или раскрытию чувствительных данных, то есть серьёзных атакам и их последствиям, поэтому важной является проблема их предотвращения.

Актуальность проекта обусловлена распространением устройств интернета вещей и используемых в них программ и библиотек, которые могут содержать дефекты безопасности, в том числе один из распространённых — переполнение буфера.

Основные методы исследования — анализ, классификация, эксперимент. Творческий подход автора состоит в связывании теории с практикой.

Анализ литературы

Существует перечень дефектов безопасности под названием CWE (Common Weakness Enumeration, Общий перечень дефектов/недостатков безопасности) [1,

с.39]. В этом перечне есть коды дефектов, которые связаны с переполнением буфера [3], они перечислены в таблице 1.

Таблица 1

Код дефекта	**Описание дефекта**
CWE-119	Неправильное ограничение операций в границах буфера
CWE-121	Переполнение буфера к стеке
CWE-122	Переполнение буфера к куче
CWE-125	Чтение за пределами границ буфера
CWE-131	Некорректное вычисление размера буфера

Программа rlogin для установления удалённой сессии пользовательского терминала в UNIX-подобных системах содержала указанный дефект. Из-за неограниченного копирования строки, содержащей переменную среды TERM, в массив из 1024 символов разрушался стек. Другой пример — свободная реализация сетевого протокола аутентификации Kerberos, где в ранних версиях злоумышленник мог получить по сети доступ с правами суперпользователя [2, с.127].

Практическая часть исследования

В листинге 1 представлен исходный код программы на языке C++, который содержит минимально воспроизводимый пример. В нём объявляются константа N для размера массива и сам массив str символьного типа, затем из стандартного потока ввода в этот массив считываются данные.

Листинг 1 — Минимально воспроизводимый пример

```
#include <iostream>

int main()
{
   const size_t int N = 8;
   char str[N];
   std::cin >> str;
}
```

На сайте compiler-explorer.com можно посмотреть, какой получается ассемблерный код (см. листинг 2). Во время выполнения программы в автоматическую область памяти, которая называется стеком, сохраняются адрес возврата, определяемый операционной системой, и содержимое регистра RBP (64-битный базовый указатель). Затем идут объявленная переменная и массив.

Листинг 2 — Пролог и эпилог функции после компиляции

```
push    rbp
mov     rbp, rsp
sub     rsp, 16
mov     qword ptr [rbp - 8], 8
...
add     rsp, 16
pop     rbp
ret
```

Функция ввода не контролирует выход за пределы массива. Если вместо восьми символов (фактически семи, поскольку один символ отводится под признак конца строки — нулевой символ) ввести больше, то «лишние» данные запишутся поверх других данных. В нашем случае это, в частности, RBP вызывающей функции и адрес возврата. В конце работы программы управление должно быть корректно передано по этому адресу. Если подобрать входные данные так, чтобы на месте адреса возврата

оказался адрес возврата произвольной функции, которую хочет выполнить злоумышленник, поведение программы будет отличаться от задуманного.

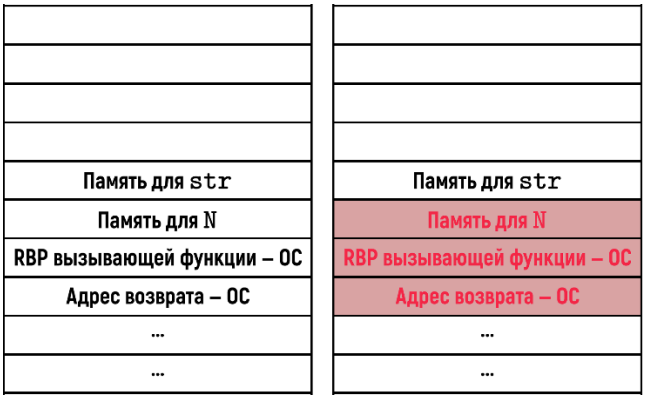


Рисунок 1 – Состояние стека, справа показан повреждённый стек

При сборке в отладочном режиме обычно есть предупреждение о том, что стек повреждён (см. рисунок 2), без отладочного режима предупреждения нет (см. рисунок 3), но стек всё ещё повреждён.

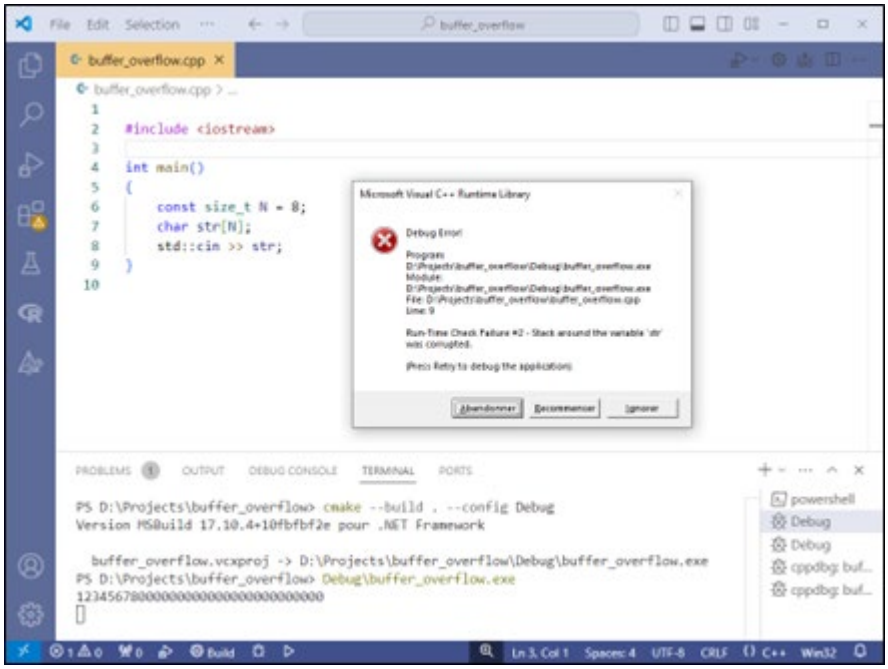


Рисунок 2 – Предупреждение о повреждении стека при сборке в отладочном режиме

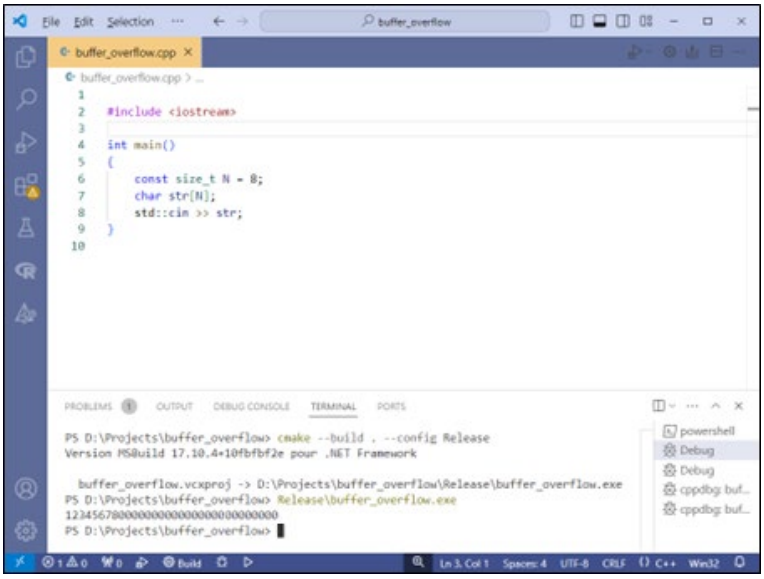


Рисунок 3 – При сборке без отладочного режима предупреждения нет

Причины, по которым устройства интернета вещей особенно подвержены дефектам типа переполнения буфера [3], перечислены в таблице 2.

Таблица 2 – Причины подверженности устройств интернета вещей дефекту

Причина	**Объяснение**
Необходимость эффективно использовать память	Устройства интернета вещей часто имеют ограниченную память и вычислительные ресурсы, что вынуждает разработчиков создавать буферы ограниченного размера (подверженные переполнению)
Использование языков C и C++	Языки C и C++ не имеют встроенной защиты против доступа или перезаписи данных в любой части памяти
Использование стандартных программ и библиотек	Если какая-либо стандартная программа или библиотека содержит дефект переполнения буфера, это потенциально может увеличить риск атаки сразу на множество устройств

Контрмеры

Меры борьбы с дефектом переполнения буфера различаются по сложности использования и переносимости. Это проверка входных данных; функции из новых стандартов, которые проверяют размеры (gets_s(), strcpy_s() и т. п.); динамическое выделение памяти; проверки времени выполнения (библиотеки Libsafe и Libverify), стековые «канарейки» (с помощью ключей и директив у отдельных компиляторов); рандомизация схемы адресного пространства (сложнее угадать адреса), технику W^X («запись либо исполнение» — предотвращение выполнения данных) [2, с.89—122]. В листинге 3 показано, как следовало бы организовать ввод в программе из указанного примера, а именно установить длину считываемых в буфер данных.

Листинг 3 — Контроль за границами буфера

```
std::cin >> std::setw(N - 1) >> str;
```

Результаты и выводы

Дефекты безопасности устройств интернета вещей, связанные с переполнением буфера, могут привести к серьёзных атакам, в литературе описаны инциденты. В ходе исследования были изучены причины переполнения буфера, что происходит во время переполнения и к каким последствиям это приводит, а также меры борьбы с переполнением. Устройства интернета вещей особенно подвержены такому дефекту из-за своей специфики — частого использования буферов фиксированного размера, использования языков без встроенной проверки границ буферов, а также возможных дефектов в стандартных программах и библиотеках. Откуда следует, что следует использовать функции, возможности компиляторов и библиотек, отслеживающие переполнение.

Список использованных источников

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учеб. пособие для СПО / О. В. Казарин, И. Б. Шубинский. — М. : Издательство Юрайт, 2019. — 342 с. — (Серия: Профессиональное образование).

2. Сикорд, Роберт С. Безопасное программирование на C и C++, 2-е изд.: Пер. с англ. — М.: ООО «И.Д. Вильямс», 2015. — 496 с. : ил. — парал. тит. англ.

3. What is a Buffer Overflow Attack. [Электронный ресурс]. 2023. URL: https://sternumiot.com/iot-blog/buffer-overflow-attack/ (дата обращения: 31.10.2024).

БЕЗОПАСНОСТЬ ЛИЧНЫХ ДАННЫХ В ИНТЕРНЕТЕ КАК ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мелентьева Валерия Валерьевна

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

Руководитель: Кушеева Мария Николаевна

Введение

В настоящее время проблема безопасности личных данных стала особенной острой в связи с развитием современных технологий. В современном информационном обществе персональные данные стали особенно ценным активом. Компании, органы власти и обычные граждане хранят и обрабатывают огромные объёмы личной информации. Однако с возрастающей важностью персональных данных возрастает и необходимость обеспечения их безопасности. Кража или неправомерный доступ к такой информации может привести к серьезным последствиям, включая финансовые потери, утрату доверия клиентов и штрафы за нарушение законодательства.

Для начала, что же такое личные данные? Личные, или персональные, данные — это любая информация, которая прямо или косвенно относится к человеку. Пример персональных данных — фамилия, имя и отчество пользователя, дата его рождения, домашний адрес, e-mail, номер телефона, фото и ссылки на профили в соцсетях.

Пользователи активно делятся информацией о себе, когда заказывают одежду и продукты, ищут вторую половинку или смотрят кино онлайн. Благодаря данным,

которые собирают сайты, пользователям не приходится каждый раз заново вводить номер телефона или искать музыку под настроение. А вот в руках злоумышленника личные данные становятся опасным оружием, готовым навредить не только тем, у кого их украли, но и их близким, знакомым и т.д.

Поэтому целью данной работы является выявление основных средств защиты личных данных, которые должен знать и применять в обыденной жизни простой пользователь сети Интернет.

Для достижения данной цели были поставлены и решены следующие задачи:

1. изучить предметную область;
2. выявить и описать опасности от кражи личных данных;
3. определить способы защиты, доступные обычному пользователю.

Основная часть

Чем опасна кража личных данных? Из-за хакерских атак на организации личные данные могут оказаться у мошенников. В зависимости от полученных данных (логин, паспортные данные или личные фото) мошенники могут использовать их несколькими способами:

- оформить на имя жертвы кредит;
- «повесить» долги или оформить фирму-однодневку;
- совершить незаконные сделки с недвижимостью;
- подобрать или перехватить пароль от вашего банковского приложения;
- вывести средства с банковского счета;
- открыть на ваше имя электронный счет, который впоследствии может быть использован, например, для покупки или продажи запрещенных товаров;
- зарегистрироваться в онлайн-казино или на сайте знакомств;
- шантажировать;
- совершать мошеннические действия от вашего лица;
- надоедать звонками и письмами в попытках навязать свои услуги.

Самая желанная цель злоумышленника — это реквизиты банковской карты. Как правило, мошенники используют стандартные схемы для похищения информации. В таблице 1 представлены самые известные мошеннические схемы и уязвимости.

Таблица 1 – Способы кражи личных данных

Способ	Уязвимость
Взлом аккаунта	Ненадежный пароль — это самый простой путь к утечке, так как существуют специальные программы, способные подобрать комбинацию методом перебора. Чем меньше в пароле символов, чем они однообразнее, тем быстрее злоумышленники получат доступ к данным
Фишинговая ссылка	Преступники копируют целые сайты или отдельные страницы, чтобы украсть реквизиты банковской карты. Посетитель думает, что оплачивает заказ в интернет-магазине, но по факту он отдает данные карты прямиком мошенникам
Незащищенные страницы	Если в адресной строке в браузере нет символа с замочком, на этом сайте не действует защита. Любая внесенная информация может быть легко похищена
Обман и вымогательство	Для кражи информации или денег мошенники прибегают к обману. Например, представляются сотрудниками банка или сообщают о трагедии в семье

Для сохранения конфиденциальной информации в тайне важно следовать правилам безопасности в интернете. Что нужно делать в первую очередь обыкновенному пользователю?

1. *Использовать длинные пароли.* Они должны состоять из цифр, строчных и заглавных латинских букв, специальных символов. Для каждого ресурса должен быть свой пароль.

2. *Подключить двухфакторную аутентификацию*. После введения логина и пароля система попросит дополнительно подтвердить вход — например, через пароль по СМС.

3. *Периодически очищать куки и кеш.* Лучше ввести данные повторно, чем позволить мошенникам украсть сведения и использовать их против вас.

4. *Минимизировать информацию о себе в открытых ресурсах*. Сделать соцсети закрытыми для посторонних, не привязывать лишний раз номер телефона или электронную почту в магазинах, не выкладывать в сеть фото документов.

5. *Отзывать подозрительные разрешения для приложений*. Для пользователей мобильных устройств iOS и Android включена функция разрешения или запрета получения приложением персональных данных. Важно только не лениться и периодически проверять, к каким сведениям получает доступ скачанное приложение или игра. При появлении подозрительных запросов рекомендуется отказаться от установки и использования такого приложения.

Однако, методов стопроцентной защиты не существует. Но можно минимизировать риски. Как правило, мошенники не взламывают аккаунты целенаправленно — трудозатраты могут просто не оправдаться. Преступники выискивают уязвимости и используют их для получения доступа. Основные правила защиты помогают минимизировать эти уязвимости и тем самым оградить себя от потенциального мошенничества. Так что же нужно делать?

- Будьте осторожны при переходе по сомнительным ссылкам на посторонние сайты. Также воздержитесь от посещения непроверенных и незащищённых сайтов.
- Личные данные, связанные с социальными сетями, не предоставляйте третьим лицам (пароли, логины, номера карт, т.д.)

- При утере смартфона или других гаджетов, в которой есть личная информация о вас, нужно в первую очень защитить данные (завершить все сеансы, проверить время последнего подключения, сменить пароли).
- Иметь всегда актуальные средства восстановления (почту, номер телефона, и др.) Также может помочь сайт с apple id или же google аккаунтом для быстрого отслеживания устройства.

Заключение

Компьютерные технологии не только улучшили жизнь обычных людей, но и упростили жизнь мошенникам и злоумышленникам. Каждый год появляются новые схемы кражи личных данных и использования их в корыстных целях. Совместно с потенциальными преимуществами от использования сети Интернет комбинированно присутствуют повышенные угрозы вредоносного проникновения третьих лиц или вирусного взлома с последующим причинением вреда.

Применяя описанные выше предложения, пользователи смогут защитить себя от основных видов угроз, и практически исключить возможное зловредное проникновение. Важно быть внимательными к себе, своим данным и своим действиям.

Список используемых источников

1. Бачило, И.Л. Персональные данные в структуре информационных ресурсов. Основы правового регулирования /И.Л. Бачило, Л.А. Сергиенко, Б.А. Кристальный., А.Г. Арешев // Информационное право. — 2016. — N 3

2. Трофимова, И.А. Обработка и хранение персональных данных/ И.А. Трофимова // Делопроизводство.- 2015. — № 3. — С. 107 — 110

3. Яковец, Е.Н. Своеобразие состава защищаемой конфиденциальной информации / Е.Н. Якрвец // Право и кибербезопасность. — 2014. — № 2. — С. 51 — 58.

4. Защита персональных данных. [Электронный ресурс]. URL: https://6alsah-school.ru/p33aa1.html (дата обращения: 10.11.2024)

5. Как обеспечить безопасность обработки персональных данных в организации [Электронный ресурс]. URL: https://cryptoarm.ru/news/personal-data-security/ (дата обращения: 10.11.2024)

6. Как защитить личные данные в интернете [Электронный ресурс]. URL: https://www.vtb.ru/articles/kak-zashchitit-lichnye-dannye-v-internete/ (дата обращения: 10.11.2024)

7. Защита персональных данных в интернете [Электронный ресурс]. URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-internete/ (дата обращения: 10.11.2024)

АНТИВИРУСНЫЕ ПРОГРАММЫ: ЗАЩИТА В ЦИФРОВОМ МИРЕ

Илюшников Иван Николаевич, Бехов Кирилл Евгеньевич

Областное государственное бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»

Руководитель: Симонов Андрей Юрьевич

Введение:

Актуальность: Введение подчеркивает, что защита данных становится одной из главных проблем в современном обществе, где информационные технологии занимают центральное место. Вредоносные программы представляют серьезную угрозу, которая может привести к потере данных, финансовым потерям, и нарушению конфиденциальности.

Роль антивирусов: Антивирусные программы выступают в роли первой линии защиты от вредоносных программ. Они выполняют важную роль в обеспечении

безопасности пользователей, защищая их от угроз, которые могут проникнуть в их устройства и сети.

Цели и задачи:

Изучение функций: Проект ставит целью детальное изучение основных функций антивирусных программ, таких как обнаружение угроз, удаление вредоносного ПО, защита в реальном времени, обновление баз данных и защита личных данных.

Виды антивирусов: Рассмотрение различных видов антивирусов, включая настольные, серверные, облачные, мобильные и для интернет-шлюзов, с описанием их отличий и особенностей.

Принципы работы: Проект изучит различные принципы работы антивирусного ПО, включая сигнатурный метод, эвристический анализ, анализ поведения, использование искусственного интеллекта и применение облачных технологий.

Актуальные угрозы: Определение основных актуальных угроз, таких как вирусы, черви, трояны, шпионские программы, руткиты и фишинг, а также методы защиты от них.

Сравнительный анализ: Проведение сравнительного анализа популярных антивирусных решений, таких как Norton, Kaspersky, McAfee, Bitdefender, Avast и ESET NOD32, для выявления их сильных и слабых сторон.

Глава 1: Основные функции антивирусных программ:

1.1. Обнаружение вредоносных программ:

Методы:

Сравнение с базой сигнатур: Антивирус сравнивает код файлов с базой известных вирусов. Если совпадение обнаружено, файл блокируется.

Эвристический анализ: Антивирус использует алгоритмы для поиска подозрительных паттернов в коде, которые могут указывать на наличие вредоносного ПО.

Анализ поведения: Антивирус отслеживает действия программ, ищет подозрительное поведение, например, необычный доступ к файлам, попытки отправить данные на неизвестные серверы.

Важность обновления: База данных вирусов должна постоянно обновляться, чтобы антивирус мог эффективно бороться с новыми угрозами.

1.2. Удаление вирусов и вредоносного ПО:

Процессы:

Изоляция: Зараженный файл изолируется, чтобы предотвратить дальнейшее заражение системы.

Удаление: Зараженный файл удаляется из системы.

Восстановление: Поврежденные данные, если возможно, восстанавливаются.

Дополнительные инструменты: Специальные инструменты для глубокого сканирования и очистки системы могут быть использованы для удаления упрямых вирусов.

1.3. Защита в реальном времени

Принцип: Антивирус постоянно мониторит активность в системе, сканирует загружаемые файлы, блокирует подозрительные действия.

Предотвращение новых угроз: Эта функция позволяет защитить систему от новых угроз, еще не внесенных в базы данных.

1.4. Обновление баз данных вирусов:

Необходимость: Регулярные обновления баз данных позволяют антивирусу эффективно бороться с новыми угрозами.

Методы: Обновления могут быть получены автоматически или вручную.

1.5. Защита личных данных и конфиденциальности:

Функции:

Защита от фишинга: Антивирус может блокировать доступ к фишинговым сайтам, предотвращая кражу личных данных.

Блокировка доступа к веб-сайтам: Антивирус может блокировать доступ к опасным веб-сайтам, которые могут содержать вредоносное ПО.

Шифрование данных: Антивирус может шифровать данные, чтобы защитить их от несанкционированного доступа.

Комплексный подход: Защита конфиденциальности должна быть комплексной и включать не только использование антивируса, но и соблюдение правил безопасности в интернете, использование надежных паролей, осторожность при открытии вложений в электронных письмах.

Глава 2: Виды антивирусов:

2.1. Настольные антивирусы:

Описание: Устанавливаются на отдельные компьютеры, обеспечивают защиту от широкого спектра угроз.

Преимущества: Обширная функциональность, глубокая интеграция с системой.

Недостатки: Могут быть ресурсоемкими, требуют регулярных обновлений.

2.2. Серверные антивирусы:

Описание: Предназначены для защиты серверов, обеспечивают безопасность данных и сетевых ресурсов.

Преимущества: Высокая производительность, специализированные инструменты для управления безопасностью сети.

Недостатки: Требуют специализированных знаний для настройки и обслуживания.

2.3. Облачные антивирусы:

Описание: Работают в облачной среде, обеспечивают защиту данных, хранящихся в облаке.

Преимущества: Доступность с любого устройства, автоматическое обновление, отсутствие нагрузки на ресурсы компьютера.

Недостатки: Зависимость от интернет-соединения, могут быть менее эффективными при защите локальных данных.

2.4. Мобильные антивирусы:

Описание: Предназначены для защиты мобильных устройств (смартфонов, планшетов), блокируют вирусы, защищают личную информацию.

Преимущества: Компактность, относительно низкие требования к ресурсам.

Недостатки: Могут иметь ограниченный функционал, зависят от операционной системы устройства.

2.5. Антивирусы для интернет-шлюзов:

Описание: Устанавливаются на устройства, обеспечивающие доступ к сети, отфильтровывают вредоносный трафик, защищают от внешних угроз.

Преимущества: Централизованная защита сети, предотвращение распространения вирусов внутри сети.

Недостатки: Требуют специализированных знаний для настройки, могут быть дорогими.

Глава 3: Принципы работы антивирусного ПО:

3.1. Сигнатурный метод обнаружения:

Описание: Сравнивает файлы с базой данных сигнатур известных вирусов. Если совпадение обнаружено, файл блокируется.

Преимущества: Эффективен для известных угроз, относительно прост в реализации.

Недостатки: Неэффективен против новых угроз, требует постоянного обновления баз данных.

3.2. Эвристический анализ:

Описание: Анализирует подозрительные действия программ, используя алгоритмы для поиска подозрительных паттернов.

Преимущества: Эффективен для обнаружения новых угроз, не зависит от наличия сигнатур.

Недостатки: Может давать ложные срабатывания, требует больших вычислительных ресурсов.

3.3. Анализ поведения:

Описание: Отслеживает поведение программ, анализирует их взаимодействие с системой, выявляет подозрительные действия.

Преимущества: Эффективен для обнаружения сложных угроз, не зависит от сигнатур или алгоритмов.

Недостатки: Может быть ресурсоемким, требует тщательной настройки для избегания ложных срабатываний.

3.4. Использование искусственного интеллекта:

Описание: Использование машинного обучения для автоматизации анализа данных, повышения эффективности обнаружения угроз.

Преимущества: Автоматизация процесса, снижение ложных срабатываний, постоянное обучение на новых данных.

Недостатки: Требует больших объемов данных для обучения, может быть сложным в реализации.

3.5. Облачные технологии в антивирусах:

Описание: Использование облачных платформ для обмена информацией, анализа данных, обновления баз сигнатур.

Преимущества: Повышение эффективности обнаружения угроз, упрощение управления, снижение нагрузки на устройства.

Недостатки: Зависимость от интернет-соединения, могут быть проблемы с конфиденциальностью данных.

Глава 4: Актуальные угрозы:

4.1. Вирусы и черви:

Описание: Программы, распространяющиеся через сеть, могут повредить файлы, уничтожить данные, нарушить работу системы.

4.2. Трояны:

Описание: Скрытно проникают в систему, выполняют действия без ведома пользователя, могут красть данные, управлять компьютером удаленно.

4.3. Шпионские программы:

Описание: Тайно собирают информацию о пользователях, отслеживают действия, передают данные третьим лицам.

4.4. Руткиты:

Описание: Скрываются в операционной системе, предотвращают обнаружение вредоносного ПО, могут управлять системой удаленно.

4.5. Фишинг и социальная инженерия:

Описание: Мошенники, использующие обман, для получения доступа к данным, могут отправлять фишинговые письма, использовать поддельные сайты, манипулировать пользователями.

Глава 5: Сравнительный анализ популярных антивирусных решений:

5.1. Norton:

Описание: Предоставляет комплексную защиту от широкого спектра угроз, высокая эффективность, широкий функционал.

Преимущества: Надежная защита от различных видов вредоносных программ, включая вирусы, трояны, шпионские программы.

Недостатки: Может быть ресурсоемким, требует регулярных обновлений.

5.2. Kaspersky:

Описание: Известен своей надежностью и эффективностью, предоставляет защиту от различных угроз, имеет широкий набор функций.

Преимущества: Сильная защита от вирусов, троянов, шпионских программ, фишинга.

Недостатки: Может быть дорогостоящим, иногда может давать ложные срабатывания.

5.3. McAfee:

Описание: Предлагает комплексные решения для защиты устройств и сетей, высокая эффективность, сильная защита от вирусов и троянов.

Преимущества: Надежная защита от различных видов вредоносных программ, широкий набор функций, включая защиту от фишинга.

Недостатки: Может быть ресурсоемким, иногда может давать ложные срабатывания.

1 https://www.kaspersky.com/about/policy-blog

2 https://ru.norton.com/

3 https://www.mcafee.com/ru-ru/antivirus.html

5.4. Bitdefender:

Описание: Известен высокой скоростью сканирования, эффективной защитой от zero-day угроз, имеет широкий набор функций.

Преимущества: Очень высокая скорость сканирования, предоставляет защиту от новейших угроз.

Недостатки: Может быть дорогостоящим, не всегда подходит для всех типов устройств.4

5.5. Avast:

Описание: Предоставляет бесплатную версию с базовыми функциями, имеет платную версию с более широким функционалом, оптимизирован для быстрого сканирования.

Преимущества: Доступная цена, широкий набор функций, включая защиту от фишинга.

Недостатки: Бесплатная версия может иметь ограниченный функционал, иногда может давать ложные срабатывания.

5.6. ESET NOD32:

Описание: Известен высокой эффективностью, низким потреблением ресурсов, предоставляет надежную защиту от широкого спектра угроз.

Преимущества: Высокая эффективность, низкое потребление ресурсов, хорошая защита от различных угроз.

Недостатки: Может быть менее функциональным, чем другие антивирусы, требует регулярных обновлений.

4 https://tele2.ee/ru/teenused/mugavusteenused/viirusetorje

5 https://support.avast.com/ru-ru/#android

6 https://pro32.com/ru/home/pro32-antivirus/

Заключение:

1.Важность антивирусных программ: Подводя итоги, можно отметить, что антивирусные программы играют ключевую роль в обеспечении безопасности пользователей в цифровом мире.

2.Выбор надежного решения: Важно выбирать надежное антивирусное решение, которое соответствует вашим потребностям, и регулярно обновлять его.

3.Комплексный подход: Защита информации должна быть комплексной и включать не только использование антивируса, но и соблюдение правил безопасности в интернете, использование надежных паролей, осторожность при открытии вложений в электронных письмах.

Список использованных источников:

1)https://www.kaspersky.com/about/policy-blog

2)https://ru.norton.com/

3)https://www.mcafee.com/ru-ru/antivirus.html

4)https://tele2.ee/ru/teenused/mugavusteenused/viirusetorje

5)https://support.avast.com/ru-ru/#android

6)https://pro32.com/ru/home/pro32-antivirus/

ТЕХНОЛОГИИ ДОВЕРЕННОГО ВЗАИМОДЕЙСТВИЯ

Грунвальд Борис Дмитриевич

Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум водного транспорта и судоходства»

Руководитель: Хуснутдинова Лариса Равильевна

Выбор

Я выбрал эту тему по причине своего же интереса в данной технологии, другим людям или поставщикам

Технологии доверенного взаимодействия

Технологии доверенного взаимодействия — технологический пакет, обеспечивающий базовые сервисы информационной безопасности и надёжного хранения данных. Проще говоря, решения, позволяющие защитить информацию на всем протяжении цепочки обмена данными как снаружи, так и внутри любой организации.

Это основа для защиты любых данных, которыми обмениваются организации и сервисы у себя внутри (между сотрудниками, отделами) и снаружи — между компаниями, структурами.

Что входит в сквозную технологию

Блок аналитики –

- технологии оценки безопасности информационного окружения и входящих в него устройств на основе собираемых интеллектуальными агентами данных;

- технологии оценки безопасности трафика и используемых для передачи информации сервисов;
- построение прогнозных моделей о текущем уровне опасности среды.

Блок технологий-

- квантовое шифрование;
- блокчейн;
- технологии анализа больших данных.

Эти технологии нужны для обработки технологической информации, чтобы определять уровень доверия субъектов информационного взаимодействия, находить отклонения от принятых и опубликованных политик безопасности. Они обеспечат безопасный и доверенный обмен информацией в цифровом виде, то есть создадут чистую среду для одной или нескольких компаний.

Суть технологии

Создание инфраструктуры и технологических пакетов, обеспечивающих соответствие уровня доверия и непрерывности функционирования создаваемых информационных систем требованиям регуляторов РФ по охране прав субъектов персональных данных

Цель технологии

Создание кибербезопасной среды доверенного обмена данными по открытым каналам связи (защита ПО, каналов связи, устройств хранения и обработки информации), поддерживающей интеграцию с системами анализа и корреляции событий для оперативной оценки подлинности контрагента.

Создание технологических пакетов, обеспечивающих снижение инвестиционных рисков, связанных с обеспечением защиты прав человека и выполнением законодательных требований стран (с учетом специфики конкретных рынков НТИ).

Национальная технологическая инициатива (НТИ) — это объединение представителей бизнеса и экспертных сообществ для развития в России перспективных технологических рынков и отраслей, которые могут стать основой мировой экономики в ближайшие 15–20 лет.

Цель этой инициативы — добиться не абстрактного научного-технологического прорыва, а точечно нащупать «пустоты» на глобальном рынке будущего, чтобы их занять.

Пример

Томская судоходная компания «ТСК» решила выйти на связь с Московской судоходной компании «Астрол» для интересного предложения в сторону компании «Астрол», создание нового вида транспортировки груза, внутреннего формата в международный формат. Компании полностью защищённо могут договориться заниматься таким видом деятельности. Для этого нужен защищённый формат предложения и реализации идеи. Именно поэтому использую технологии доверенного взаимодействия, обе стороны будут в полном спокойствие за информацию передаваемую друг другу

Пример: надо как-то по ярче изобразить может корабль навстречу кораблю, или схему типа такой, надо подумать.

Вывод

Полностью рассказав тему, я для себя понял окончательно что же это такое и дал понять слушателям.

Использовать технологию доверенного взаимодействия могут абсолютно любые компании для безопасного взаимодействия друг с другом.

Литература, интернет ресурсы

Запись в соц. сети Вконтакте - https://vk.com/wall-193945498_3719 НТИ Тусур - https://nti.tusur.ru/

ЧТО ТАКОЕ ИНТЕРНЕТ ВЕЩЕЙ, И КАК ИХ ОБЕЗОПАСИТЬ

Хлебников Влад Михайлович, Соколовская Дарья Викторовна
Областное государственное бюджетное профессиональное образовательное учреждение «Томский политехнический техникум»
Руководитель: Лапов Антон Владимирович

Интернет вещей (IoT, Internet of Things) — это концепция сетевой инфраструктуры, которая объединяет физические устройства («вещи») с возможностью обмена данными через интернет. Эти «умные» устройства могут взаимодействовать друг с другом без участия человека, собирая данные о своем состоянии и окружающей среде, а также выполняя различные задачи автоматически.

Примеры устройств Интернета вещей:

1. Умный дом:

- Умная колонка может управляет освещением, температурой, музыкой и другими функциями дома через голосовые команды;

- Умные лампы могут изменять яркость и цвет освещения, включаться и выключаться по расписанию или командам через приложение;

- Умные термостаты регулируют температуру в доме на основе данных о погоде и вашем присутствии.

2. Носимые устройства:

- Фитнес-браслеты и смарт-часы собирают информацию о физической активности, сне, пульсе и передают её для анализа через приложения;

- Устройства мониторинга здоровья измеряют уровень сахара в крови, артериальное давление и другие показатели здоровья, отправляя их врачу или храня в облаке.

3. Транспорт:

- Автомобили с подключением к интернету: современные автомобили могут обмениваться информацией с облачными сервисами, обновлять карты навигации, диагностировать неисправности и даже самостоятельно парковаться.

- Система управления городским транспортом: Интернет вещей помогает отслеживать движение автобусов, трамваев и троллейбусов, оптимизируя маршруты и расписание.

4. Сельское хозяйство:

- Датчики влажности почвы и температуры воздуха помогают фермерам точно определять оптимальное время полива и внесения удобрений;

- Мониторинг состояния животных: специальные метки и датчики контролируют здоровье скота, предупреждая фермеров о возможных проблемах.

5. Энергетика:

- Смарт-счетчики электроэнергии автоматически передают показания энергопотребления поставщикам услуг, позволяя более эффективно распределять ресурсы;

- Интеллектуальные сети: системы управления электросетями, которые адаптируются под изменения нагрузки и предотвращают аварии.

6. Безопасность:

- Камеры видеонаблюдения с аналитикой: камеры могут распознавать лица, номера автомобилей и отправлять уведомления при обнаружении подозрительной активности;

- Беспроводные системы сигнализации: охранные системы, которые уведомляют владельца о вторжении через мобильное приложение.

Эти примеры показывают, насколько разнообразны возможности применения Интернета вещей. Он охватывает практически все сферы жизни, начиная от повседневных задач и заканчивая сложными промышленными процессами.

Для обеспечения комплексной безопасности IoT объектов необходимо интегрировать несколько технологий и подходов:

1. Шифрование данных: Применение современных методов шифрования, таких как AES и TLS, для защиты передаваемой информации;

2. Идентификация и аутентификация: Использование многофакторной аутентификации и цифровых сертификатов для подтверждения подлинности устройств и пользователей;

3. Системы обнаружения вторжений (IDS): Разработка и реализация систем, которые могут выявлять несанкционированные попытки доступа и вмешательства в сети IoT;

4. Технологии блокчейн: Использование блокчейн-технологий для децентрализованного хранения данных и подтверждения транзакций, что значительно усложняет возможность их мошеннического изменения или удаления;

5. Облачные сервисы: Хранение данных и вычислений в облаке (с должными мерами безопасности) для повышения доступности и интеграции различных IoT устройств.

Искусственный интеллект в защите IoT

Искусственный интеллект (ИИ) играет решающую роль в современных системах защиты IoT. За счёт своей способности к анализу больших объёмов данных, ИИ может:

1. Анализировать аномалии: Используя алгоритмы машинного обучения, ИИ может выявлять аномальные действия в сети, что позволяет быстро реагировать на потенциальные угрозы;

2. Автоматизировать реагирование: Системы на основе ИИ способны автоматически блокировать подозрительные подключения или активировать протоколы безопасности, минимизируя временные затраты на реагирование;

3. Прогнозировать угрозы: Анализируя предыдущие инциденты, ИИ может прогнозировать возможные атаки и заблаговременно рекомендовать меры предосторожности;

4. Фильтровать данные: Технологии ИИ помогают в фильтрации несанкционированного доступа к данным, позволяя определить, какие данные могут быть подвержены утечкам.

С учётом постоянного роста числа IoT объектов значимость современных средств защиты, таких как искусственный интеллект, культура информационной безопасности и внедрение современных технологий, будет только расти. Всесторонняя стратегия безопасности, которая сочетает в себе все эти компоненты, необходима для защиты как отдельных пользователей, так и организаций в целом. Обеспечение безопасности IoT — это не только защита устройств, но и формирование надежной и устойчивой экосистемы, способной справляться с современными вызовами и угрозами.

Предстоящие исследования и практические подходы должны сосредоточиться на интеграции этих компонентов, что позволит создать более безопасное и устойчивое будущее для IoT технологий.

Список литературы:

1. Кириллов, И. А. (2017). "Интернет вещей: от концепции к практике."

2. Павлова, Е. В., & Кузнецов, С. В. (2019). "Интернет вещей: современные технологии и тенденции."

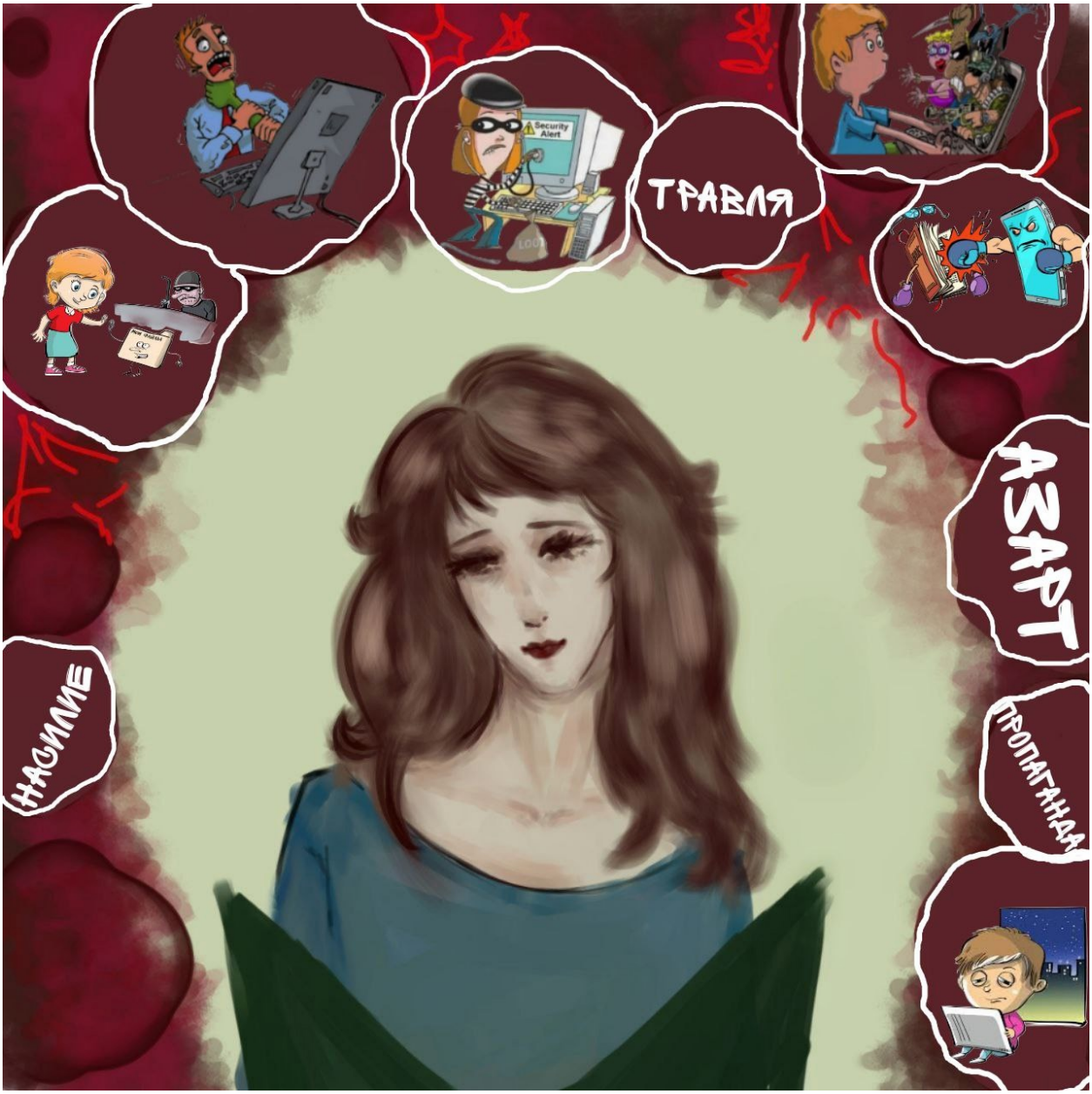
3. Семёнов, И. В. (2020). "Искусственный интеллект в системах защиты Интернета вещей."

СЕКЦИЯ 3. ПОЛИГРАФИЧЕСКАЯ ПРОДУКЦИЯ ПО ТЕМЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Мерзликина Анастасия Ивановна, Сухушина Дарья Михайловна

Областное государственное бюджетное профессиональное образовательное учреждение «Томский лесотехнический техникум»

Руководитель: Думан Юрий Владимирович

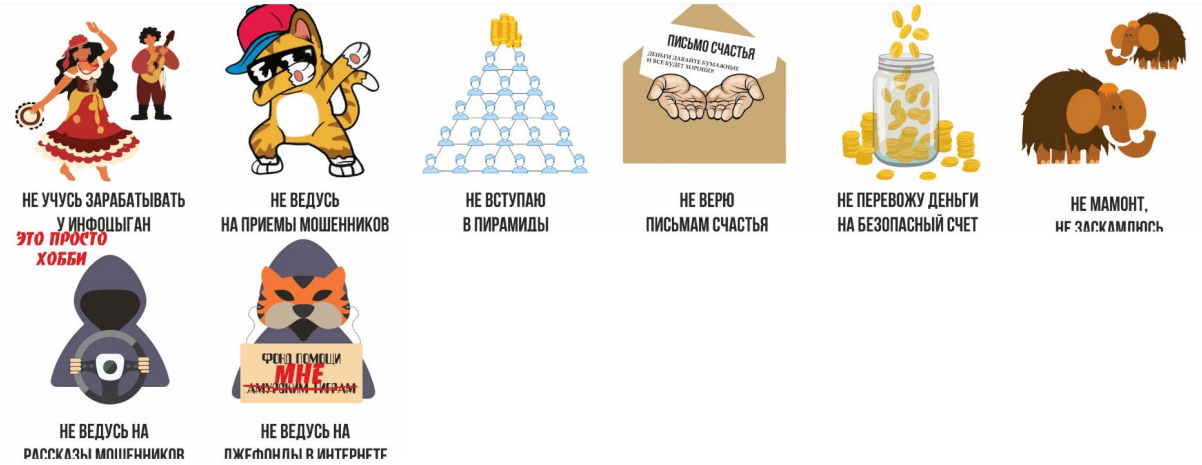


Алтынцева Жанна Руслановна

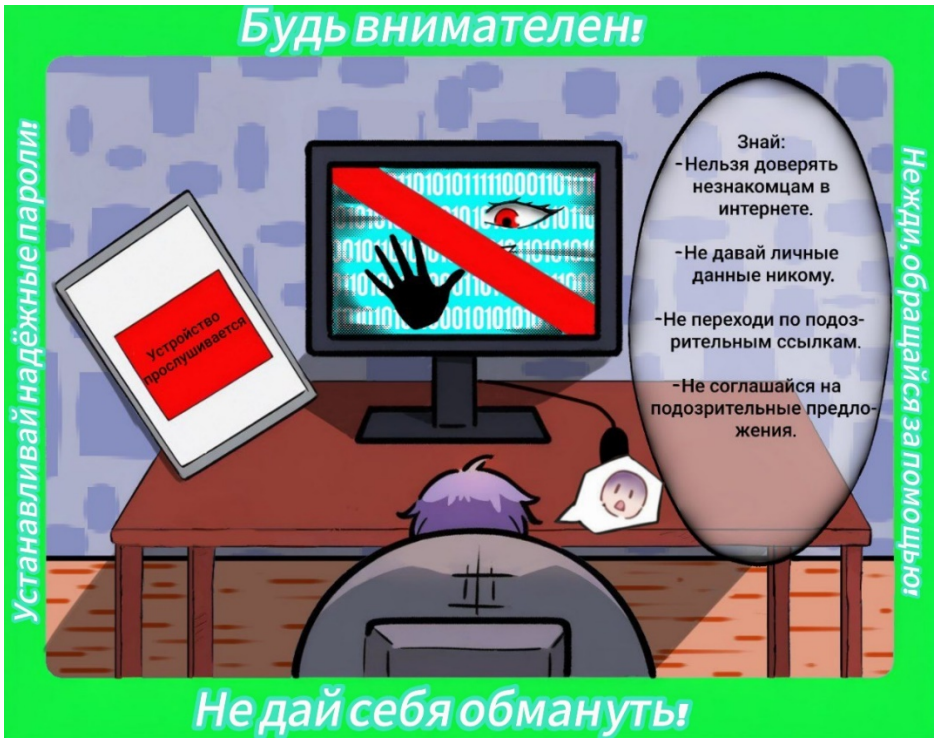
Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум социальных технологий»

Руководитель: Якимова Юлия Владимировна

Семенова Екатерина Павловна
Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум социальных технологий»
Руководитель: Якимова Юлия Владимировна



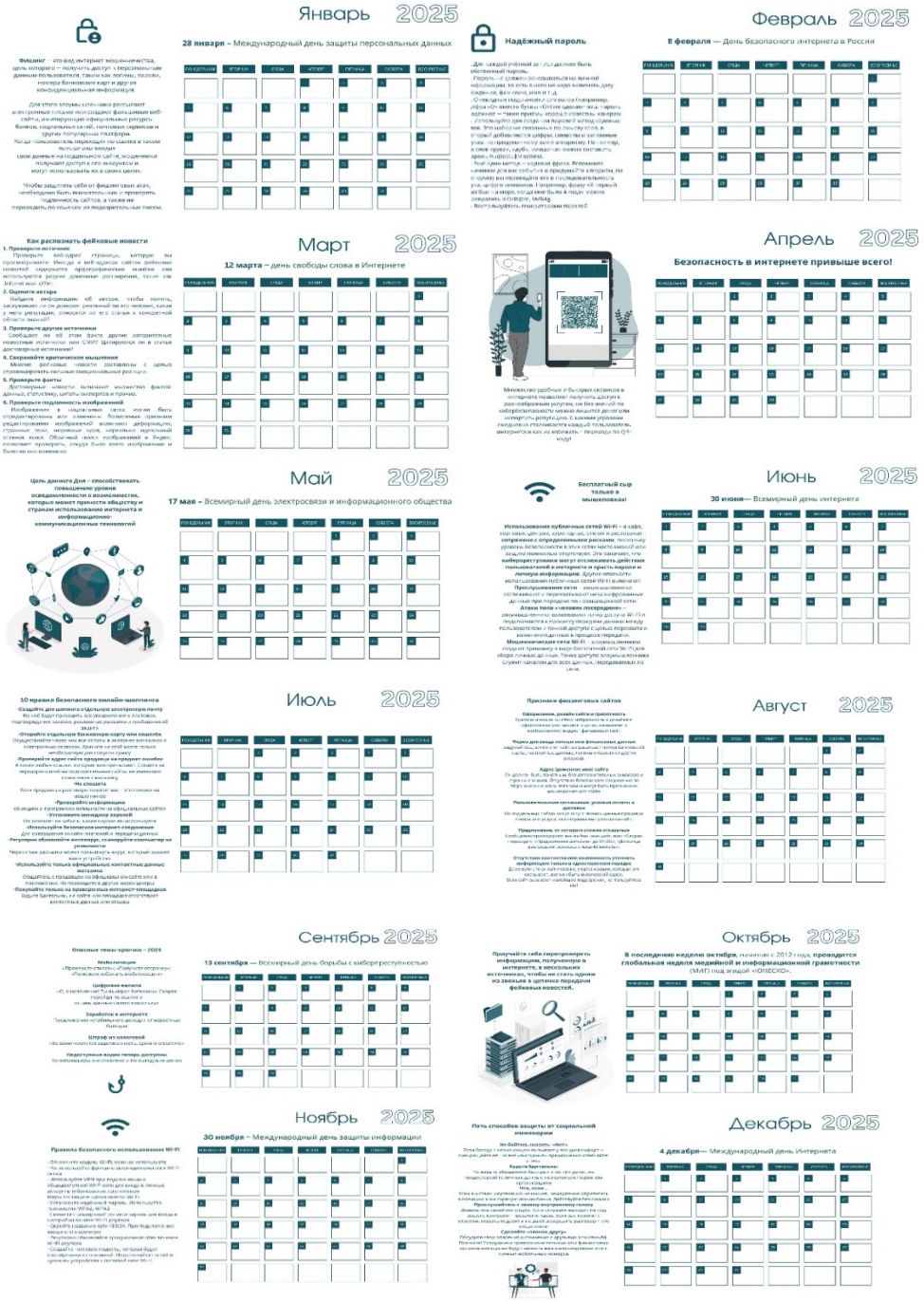
Кайгородова Ксения Николаевна
Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум информационных технологий»
Руководитель: Кабикова Алина Владимировна



Акименко Максим Викторович

Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум водного транспорта и судоходства»

Руководитель: Мезенцев Станислав Васильевич



Климова Надежда Алексеевна
Областное государственное бюджетное профессиональное образовательное учреждение «Колледж индустрии питания, торговли и сферы услуг»
Руководитель: Дозморова Татьяна Васильевна

Бабина Полина Вячеславовна, Агалин Родион Алексеевич
Областное государственное бюджетное профессиональное образовательное учреждение «Колледж индустрии питания, торговли и сферы услуг»
Руководитель: Кузенкова Ольга Зинуровна

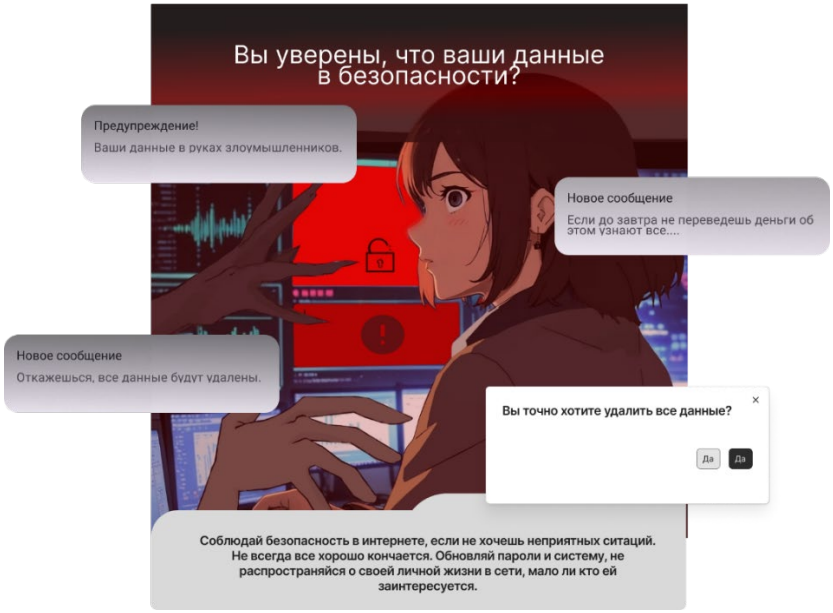
Козлов Иван Алексеевич

Областное государственное бюджетное профессиональное образовательное учреждение «Томский политехнический техникум»

Руководитель: Горяинова Светлана Владимировна

Метленко Сергей Александрович
Областное государственное бюджетное профессиональное образовательное учреждение «Томский политехнический техникум»
Руководитель: Шабалин Вадим Сергеевич

Шамилова Лия Магомедовна
Областное государственное бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»
Руководитель: Пальцев Вячеслав Владимирович



СЕКЦИЯ 4. ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ОБЛАЧНЫХ СИСТЕМ ХРАНЕНИЯ В БОРЬБЕ С ТЕРРОРИЗМОМ

Филиппи Данила Андреевич, Новосёлова Алина Михайловна
Областное государственное бюджетное профессиональное образовательное учреждение «Томский техникум информационных технологий»
Руководители: Кирилова Анна Владимировна, Нестерова Екатерина Михайловна

Введение

В настоящее время, в эпоху цифровых технологий, интернет имеет большую значимость. С помощью него можно делать все: искать нужную информацию, использовать в личных целях.

Чем уязвимы информационные системы? Негативные последствия террористической атаки на информационную сферу предугадать практически невозможно, а последствия таких атак могут принять статус катастрофических.

Используя личные данные, с помощью сетей можно шантажировать, распространять ложную информацию. Кроме того, интернет используют и в целях информационного терроризма.

Актуальность рассматриваемой проблематики обусловлена тем, что в настоящее время ситуация в сфере информационного противодействия терроризму требует принятия более усиленных мер безопасности.

Гипотеза: Облачные системы хранения как изначально наиболее уязвимые объекты могут стать достаточно серьезным оружием в борьбе с информационным терроризмом.

Цель: Исследование преимуществ и недостатков облачных систем хранения в борьбе с информационным терроризмом.

Задачи:

1. Изучить материал о информационном терроризме

2. Изучить материал о структуре облачных систем хранения

3. Проанализировать, какими методами пользуются создатели облачных хранилищ для защиты данных пользователей.

4. Выделить преимущества облачных систем хранения

Введение в проблему информационного терроризма

В условиях нынешней цифровизации, автоматизации, информатизации и компьютеризации с учетом темпа развития информационных технологий все больше процессов происходят с использованием сети интернет. Люди заносят большое количество информации о себе и своей жизни в различные социальные сети, оставляют информационные следы во всемирной паутине. Все это приводит к тому, что различная информация используется против людей с корыстными целями и с целью получения выгоды. Угроза информационного терроризма увеличивается с каждым годом.

Информационный терроризм – это целенаправленное прямое воздействие на людей, их психику, сознание и поведение с целью внушения определенный идей, мнений и действия для достижения определенных действий.

Терроризм многообразен. В. П. Емельянов сравнивает понятие «террор» с такими, как «агрессия», «геноцид», «война», считая террор массовым насилием, применяемым субъектами власти, и в связи с этим рассматривает понятия «идеологический террор», «государственный террор», «внесудебный террор», «административный террор». Основу рассматриваемых явлений составляет терроризирование (фр. terroriser), под которым понимается преследование с угрозами расправы, насилия; запугивание, держа кого-либо в состоянии страха

Выделяются следующие виды информационного терроризма:

1. Терроризм информационно-психологического характера. Осуществляется путем манипулирования СМИ для того, чтобы дезинформировать

общество, запугивать, а также для демонстрации обществу мощность террористических организаций.

2. Терроризм информационно-технического характера. Основная цель: наносить ущерб информационным государственным структурам, использую вирусные программы, чтобы вызвать разрушение системы; осуществление дистанционного управления объектами биологического и химического оружия [1].

Таким образом можно сделать вывод, что с каждым годом растет число жертв информационного терроризма. Исправить сложившуюся ситуацию представляется возможным только при введении соответствующего закона, а также проведения профилактических мероприятий для населений, то есть государство должно сформулировать ясные, четкие, справедливые правила взаимодействия в информационном поле.

Алгоритмы шифрования у разных облачных систем хранения.

К 2025 году общий объем данных в мире достигнет 175 зеттабайт, и все их нужно где-то хранить. Облачное хранилище — виртуальный ящик для хранения файлов в интернете. Вы можете загрузить документы и другие данные и получать к ним доступ по интернету. Как и обычное на компьютере, облачное хранилище позволяет работать с файлами: просматривать, редактировать и удалять. Но в отличие от локальных накопителей, данные хранятся не на устройстве, а на сервере провайдера.

Примеры популярных облачных хранилищ: Google Drive; Dropbox; iCloud; OneDrive; pCloud; Яндекс

Как работает технология облачного хранилища?

Распределенное хранение: Данные разбиваются на фрагменты и распределяются по множеству серверов. Это обеспечивает отказоустойчивость и быстрый доступ.

Виртуализация: используется для создания абстрактного уровня хранения, независимого от физического оборудования.

Дедупликация: Технология, позволяющая избежать хранения дублирующихся данных, что экономит место и ресурсы.

Кэширование: Часто используемые данные хранятся в быстрой памяти для ускорения доступа.

Синхронизация: Изменения в файлах отслеживаются и распространяются на все устройства пользователя через протоколы delta-sync, передающие только измененные части файлов.

Балансировка нагрузки: Распределяет запросы между серверами для оптимизации производительности.

API интеграция: Позволяет разработчикам создавать приложения, взаимодействующие с облачным хранилищем.

В начале 2010-х, в условиях нестабильности в публичном облачном пространстве, когда появлялись новые облачные провайдеры, внедрение облаков переходило от ситуативного к стратегическому. ИТ-руководители поняли, что мультиоблачность была — и будет оставаться — жизнеспособным и желательным подходом для их ИТ-комплексов будущего.

В том самом первом опросе, проведенном в апреле 2012 г., 68% респондентов указали, что их организация полагается на мультиоблачный подход. Среди организаций с 1000 и более сотрудников число тех, кто использует этот подход, с годами значительно росло: с 77% в 2013 г. (когда он был назван «стратегией выбора для предприятий») до 82% в 2015-м. Сегодня 92% предприятий используют мультиоблачную стратегию, при этом ожидается, что в ближайшие 12 месяцев 55% корпоративных рабочих нагрузок окажутся в публичном облаке.

Как выбрать безопасное облачное хранилище? При выборе провайдера обратите внимание на:

1. Наличие E2EE и шифрования с нулевым знанием.

2.Соответствие стандартам безопасности (например, ISO 27001).

3. Прозрачность политики конфиденциальности.

4. Возможности контроля доступа и аудита.

5. Репутацию провайдера и отзывы пользователей.

6. Двухфакторная аутентификация.

Проблемы и риски облачного хранилища:

1. Утечка информации. Облачная инфраструктура подвергается все тем же угрозам, что и традиционная физическая. И чаще всего компании сталкиваются с потерей или утечкой конфиденциальной информации. Проблема часто возникает по вине самих сотрудников, однако не стоит забывать и о возможных атаках со стороны злоумышленников.

2. Взлом интерфейсов и API. Очень часто при взаимодействии с третьей стороной применяются интерфейсы API, из-за которых безопасность хранилища может оказаться под угрозой. Связано это с тем, что для входа в систему потребуется предоставить дополнительную информацию, включая логин/пароль.

3. Обход аутентификации. Проблема утечки данных нередко становится следствием пренебрежительного отношения к используемым механизмам проверки подлинности. В том числе, могут применяться слабые пароли, ненадежные сертификаты, непроверенные ключи шифрования и т. д.

4. Кража учетных записей. Опасность для облачной инфраструктуры может представлять и фишинг. Также в эту категорию стоит отнести эксплойты, манипуляции с транзакциями и изменениями данных. Очень часто злоумышленники рассматривают облако как наиболее удачную площадку для совершения таких атак.

5. Недостаточная осведомленность. Провайдеру важно предоставить полную информацию о своих услугах, а клиенту, в свою очередь, изучить все особенности функционирования сервисов.

Проведя исследование информации и опрос, в котором приняли участие 121 студент ОГБПОУ «ТТИТ» в возрасте от 15 до 23 лет вы выявили, что обучающие используют сложные пароли, постоянно меняют их, используют двухфакторную аутентификацию, также тщательно следят за своими действиями в интернете, следят за тем, на какие сайты они заходят. Из этого можно сделать вывод, что данные способы защиты работают, использование каждого из них по отдельности или даже лучше всех их вместе повышает защиту ваших персональных данных. (Рис.1)

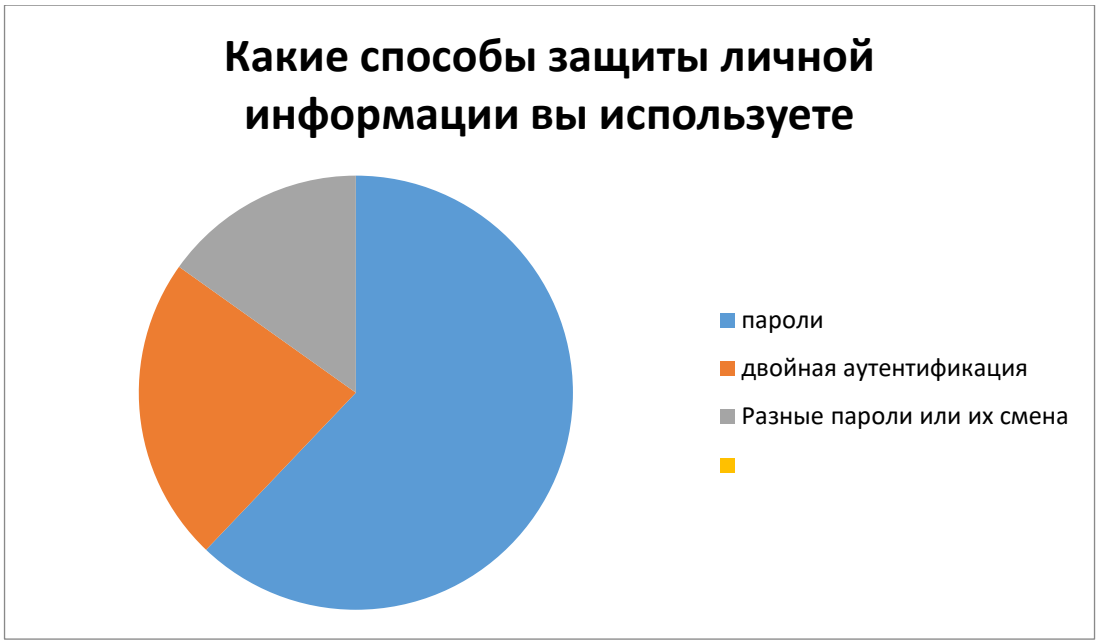


Рис. 1. Опрос студентов ТТИТ

Как минимизировать риски?

1) Использовать надежное облачное хранилище.
2) Использовать трудные пароли
3) Включить везде двухфакторную аутентификацию.
4) Не хранить личную (конфиденциальную) информацию в облачном хранилище.

Заключение

Передавать что-то в чужие руки противоречит человеческой природе, передавая что-то кому-либо, мы чувствуем себя менее защищенными. Сегодня

десятки тысяч компаний знают, что безопасность IT-инфраструктуры не всегда зависит от того, в чьих руках она находится. В мире растет количество киберугроз, которые одинаково опасны для данных и в облаке, и в локальной инфраструктуре.

Интеграция решений облачного хранения произвела революцию в области безопасности данных и возможностей правоохранительных органов, особенно в борьбе с преступной деятельностью, включая терроризм, в даркнете. Платформы облачного хранения предлагают надежные меры шифрования и безопасности, защищая конфиденциальные данные от несанкционированного доступа. Более того, эти платформы позволяют властям более эффективно отслеживать и отслеживать деятельность в темной сети, используя сотрудничество в режиме реального времени и обмен разведданными между правоохранительными органами и международными партнерами. Благодаря передовым инструментам криминалистического анализа и сбора доказательств облачное хранилище облегчает восстановление цифровых следов и сбор доказательств против преступников. Кроме того, функции мониторинга соответствия и нормативного надзора обеспечивают соблюдение законов о защите данных, предотвращая неправомерное использование данных преступными организациями и повышая общественную безопасность. Таким образом, внедрение технологии облачного хранения не только защищает данные, но и дает правоохранительным органам возможность разрушать террористические сети и задерживать лиц, участвующих в незаконной деятельности, тем самым способствуя глобальным усилиям по обеспечению безопасности.

Список литературы

1.Антонов В.Н. Современный терроризм: теория и реальность // Азиатско-Тихоокеанский регион. Экономика. Политика. Право, 2012. – № 2.

2. Беликова Ю. В. Сетевые технологии в информационных операциях НАТО и зарубежных неправительственных организаций в ходе цветных революций и военных

конфликтов : монография / Ю. В. Беликова, А. В. Крикунов, А. В. Королёв. – М.: Академия ФСО России, ЦАТУ, 2012. – 89 с.

3.Димлевич Н.А. Угроза из киберпространства // Информационно-аналитический журнал Центра анализа террористических угроз и центр прогнозирования конфликтов (ЦАТУ): Асимметричные угрозы и конфликты низкой интенсивности. 2009. № 5–6. — С. 26–28.

4.Старостина Е.В., Защита от компьютерных преступлений: вопросы и ответы / Е. В. Старостина, Д. Б. Фролов. – 2-е изд. – М.: Эксмо, 2005. – 183 с.

5. Терновсков В. Б., Вертий Е. А., Борода С. А. Использование цифровых технологий (в том числе мобильных приложений) для борьбы с терроризмом // Молодой ученый. 2020. № 45 (335). — С. 8-11.

6. Шендорова О. Б. К вопросу о понятии терроризма // Молодой ученый. — 2019, № 14, с. 208–209.

7. Информационный Терроризм [Электронный ресурс] https://slide-share.ru/informacionnij-terrorizm-32766 (дата обращения: 04.12.2023).

ПРОТИВОДЕЙСТВИЕ ПРОПАГАНДЕ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В СОЦИАЛЬНЫХ СЕТЯХ ИНТЕРНЕТА

Сергиенко Милана Артемовна, Титова София Павловна

Областное государственное бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»

Руководитель: Симонов Андрей Юрьевич

ВВЕДЕНИЕ

Актуальность: Актуальность работы заключается в том, чтобы выявить способы профилактики распространения терроризма и экстремизма за счет пропаганды в Интернет-ресурсах.

Цель: изучить профилактические методы борьбы с экстремизмом и терроризмом в молодежной среде

Задачи:

1) Изучить понятие терроризма и экстремизма и причины их действий.

2) Выделить разновидности пропаганды терроризма и экстремизма в социальных сетях.

3) Рассмотреть средства профилактики против терроризма и экстремизма.

4) Сделать выводы и рекомендации по борьбе с пропагандой терроризма и экстремизма.

Объект исследования: способы противодействия терроризму в соц. сетях

Метод работы:

— изучение интернет-источников и литературы;

— теоретический анализ

— обобщение полученных результатов.

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

1. ЧТО ТАКОЕ ТЕРРОРИЗМ И ЭКСТРЕМИЗМ?

Терроризм — это метод, который используют некоторые организованные группы или политические партии для достижения своих целей. Терроризм основан на насилии. Отличительная черта терроризма – применение насилия в отношении не противника, а мирных людей, которые часто и не подозревают о политическом противостоянии.

Экстремизм — это приверженность человека к крайним взглядам и методам действий, радикально отрицающим существующие в обществе нормы и правила. Это возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию. Экстремизм

создает угрозу, прежде всего основам конституционного строя, ведет к попиранию конституционных прав и свобод человека и гражданина, подрывает общественнуюбезопасность и государственную целостность**.**

Из-за отсутствия четкого определения явления «экстремизм» существует большое количество видов экстремизма, такие как: Религиозный, национальный, политический и молодежный.

1.2 УСЛОВИЯ ВОЗНИКНОВЕНИЯ ТЕРРОРИЗМА

Терроризм, как правило, порождается:

- Наличием социальных, национальных и религиозных проблем.
- войной и военными конфликтами.
- наличием социальных групп, отличающихся от своих ближних и дальнихсоседей высоким уровнем материального благосостояния и культуры.
- существованием тайных или полутайных обществ и организаций
- нерешенностью важных экономических и финансовых вопросов, в томчисле на законодательном уровне.

2. ПРОПАГАНДА ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В СОЦИАЛЬНЫХ СЕТЯХ.

2.1 Причины пропаганды терроризма в социальных сетях.

Одной из основных причин столь массового распространения экстремистских и террористических идей была названа общедоступность и незащищенность источников СМИ и социальных сетей. Глобальный характер интернет-террора уже давно является не выдумкой писателей-фантастов, а действительно актуальной и серьезной проблемой.[2]

Признаки глобальной паутины:

- В интернете пользователи имеют право на анонимность;
- Практически неограниченный доступ к любым данным;
- Быстрое распространение большого объема информации среди масс; Каждый день мы заходим в социальные сети на подобие Instagram, ВК,

Telegram, делимся своими личными данными, рассказываем миру практически всего своей частной жизни. Многим из нас даже в голову не приходит, что эта информация может быть использована против нас. Ведь многие информационные площадки фактически не имеют защиты и поэтому являются просто идеальными источниками для распространения разнообразных идей экстремистских группировок. Террористы все чаще обращаются к средствам массовой информации, чтобы получить определенные данные или используют их в качествеоружия воздействия на широкие массы, особенно на детей и молодых людей. Эти социальные группы в силу своего возраста и, как следствие, отсутствия жизненного опыта, более открыты к любому виду общения в интернете и, по статистике, даже чаще доверяют незнакомцам в интернете, чем близким людям.

2.2 Как проявляется пропаганда терроризма и экстремизма в социальных сетях и приемы, которыми пользуются экстремисты/террористы

На сегодняшний день глобальная сеть «Интернет» стала одним из главных источников получения информации. Но не всякая информация полезна. Имеющиешироку аудиторию «социальныесети» стали популярны и у адептов экстремизма как трибуны для пропаганды своих взглядов.

Пропагандируется комплекс целей и ценностей, которые исповедуют экстремисты, доказывается их «прогрессивность» и «неизбежность», обличаются противники и несогласные. Если организация исповедует некую субкультуру – то там могут даваться советы по стилю поведения, одежды, внешнего вида и тому подобному. Даются «советы» и «консультации» и насчет повседневной жизни – что следует делать, а чего не следует, и как «правильное» делать правильно. Далеесследует призыв «присоединяться» и участвовать в «борьбе» -в той или иной форме.

Так же можно выделить виды терроризма в интернете которые имеют несколько различных проявлений. А именно:

- Активизм — это «легитимное» использование сети Интернет для пропаганды своих идей и увеличения последователей;
- Хакерская деятельность — это хакерские атаки, которые проводятся с целью выведения из строя отдельных компьютерных сетей, баз данных либо сайтов, для получения доступа к секретной или государственной информации;
- Кибертерроризм — это компьютерные атаки, спланированные с целью нанесения максимального ущерба жизненно важным объектам информационной инфраструктуры;

Основные признаки того, что молодой человек\девушка начинают подпадать под влияние экстремистской идеологии, можно свести к следующим:

1. его\ее манера поведения становится значительно более резкой и грубой, прогрессирует ненормативная либо жаргонная лексика;
2. резко изменяется стиль одежды и внешнего вида, соответствуя правилам определенной субкультуры;
3. на компьютере оказывается много сохраненных ссылок или файлов с текстами, роликами или изображениями экстремистско-политического или социально-экстремального содержания;
4. в доме появляется непонятная и нетипичная символика или атрибутика (как вариант – нацистская символика), предметы, которые могут быть использованы как оружие;
5. он\она проводит много времени за компьютером и\или самообразованием по вопросам, не относящимся к школьному\вузовскому обучению, художественной литературе\фильмам, компьютерным играм;
6. повышенное увлечение вредными привычками;
7. резкое увеличение числа разговоров на политические и социальные темы, в ходе которых высказываются крайние суждения с признаками нетерпимости;
8. псевдонимы в Интернете, пароли и т.п. носят экстремально-

политический характер.[1]

2.3 Приемы, которыми пользуются экстремисты:

Один из самых используемых приемов — заведомо ложное истолкование истории своей потенциальной жертве или создание мифов. Этот метод нацелен на постепенное изменение общественного мировоззрения. Вербовщик затрагивает наиболее болезненные точки своего собеседника и перетягивает его на свою сторону. Преподносятся искаженные факты событий, происходит настраивание против своих же соотечественников и отказ от каких-либо ценностей в пользу наиболее «выгодных» условий существования.

Еще один популярный прием — создание эффекта присутствия. Он достигается экстремистами за счет размещения на веб-сайтах видеороликов якобыс «места боевых действий».

Так, на определенных сайтах размещены видеообращения боевиков к молодежи с призывами к вооруженным действиям и террористическим актам. Также часто используется гиперболизация негативных черт и ложных целей противника.

Социальные сети позволяют пользователям наиболее раскрепощенно выражать собственное мнение и отстаивать свою жизненную позицию, в отличие от общения «лицом к лицу».

В основном, жертвами террористов становятся подростки и молодые люди с еще не полностью сформировавшейся психикой и впечатлительным взглядом на мир. Для террористов они становятся идеальным и эффективным оружием, которым можно управлять. Ведь кто заподозрит школьника в желании совершить террористический акт? Специально обученные люди анализируют тысячи аккаунтов в социальных сетях, выбирая из них те, которые принадлежат молодым людям с проблемами в самореализации, умении общаться и взаимодействии с обществом. Такие ребята уходят в социальные сети, пытаясь в этой среде компенсировать нехватку общения, дружбы, внимания, участия и человеческой теплоты.

Все начинается с активного увлечения компьютерными играми, социальными сетями и различными сомнительными сайтами. Человек становится замкнутым, отдаляется от семьи и друзей, начинает интересоваться религией, деятельностью запрещенных организаций, темами оружия и насилия.[3]

3. СРЕДСТВА ПРОФИЛАКТИКИ ПРОТИВ ПРОПАГАНДЫ ТЕРРОРИЗМА

В рамках профилактики распространения идеологии экстремизма и терроризма, необходимо задействовать потенциал социальных медиа, путем размещения материалов с антитеррористическим контентом, путем категорического неприятия основ экстремизма и терроризма. Необходимо развенчать и дискредитировать романтический миф о борцах за всемирный халифат. Наладить взаимодействие с молодежью, организовать работу по сбору, обобщению и анализу результатов мониторинга социальных меди, блогосферы, форумов - для выявления наиболее острых и актуальных проблем, дискуссионных тем, оказывающих влияние на общественное мнение, провоцирующих их протестные настроения, конфликтные ситуации на этноконфессиональной и иной чуждой для российского государства идеологии. Создать с помощью специалистов агитационный пропагандистский продукт противодействия идеологии экстремизма и терроризма и размещать на информационных ресурсах исоциальных медиа.

Основные правила безопасности в интернете, которые нужно соблюдать,чтобы обезопасить себя и своих родных:

- Не размещайте на своей страничке
- информацию о том, где Вы живёте, где работают Ваши родители.
- Не отвечайте на вопросы незнакомых людей.
- Ограничьте доступ к своим фотографиям, записям и другим материалам исключением могут быть только кругом друзья, которых хорошо знаете или родные.

- Не откровенничайте в общедоступных группах и на форумах. Агитаторы привлекают внимание людей темами, вызывающими споры. Потом выходят на связь с теми, кто принял участие в обсуждении, и призывают в свои ряды.
- Будьте внимательны, когда к Вам кто-то проявляет настойчивыйповышенный интерес.
- Не принимайте в друзья всех подряд. Выясняйте, кто желает общатьсяс Вами и откуда Вы можете быть знакомы.
- Если Вам пришло сообщение непонятного содержания с незнакомогономера, не отвечайте на него.
- Опция «Черный список» позволяет заблокировать любого человека,который досаждает какими-то вопросами.
- Используйте возможность пожаловаться модератору или администратору сайта.

В основном недоброжелательные персоны ищут своих жертв на интернет- сайтах, в социальных сетях, на сайтах знакомств. Знакомство в интернете протекает легче, потому что легче притвориться и скрыть настоящую информацию о себе.

Первичный отбор «кандидатов» осуществляется по исследованию информации, которую вы выкладываете на своих личных страничках в соц. сетях, чаще всего подростки 13-15 лет.[4]

ЗАКЛЮЧЕНИЕ

Общие выводы: терроризм и экстремизм в социальных сетях представляют собой серьёзную угрозу обществу. Платформы социальных медиа становятся ареной для распространения радикальных идеологий, вербовки новых последователей и организации террористических действий. Эффективная борьба с этой проблемой требует комплексного подхода, включая сотрудничество между государственными структурами, частным сектором и международным обществом. Важно также развивать медиа-грамотность населения и повышать осведомленность о рисках, связанных с

экстремистским контентом в интернете. Только совместными усилиями можно создать безопасное цифровое пространство, чтобы предотвратить распространение насилия и ненависти в интернете. И поэтому подросткам нужно быть более внимательным и осторожнеев интернете. Нужно помнить, что не всё, что мы видим в онлайн, является правдой. Нужно проверять информацию, не делится личными данными и быть бдительным к незнакомцам. Использовать интернет нужно с умом, и заботиться о своей безопасности и безопасности своих близких. Наша внимательность поможет избежать неприятностей и сделать наше онлайн-пространство более безопасным.

Решены ли исследовательские задачи: в ходе выполнения проектной работы достигнута цель ознакомиться с профилактическими методами борьбы с терроризмом и экстремизмом в среде интернет.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1) Памятка для подростков: Экстремизм в сети Интернет - мвд.рф [электронный ресурс]: URL: https://264.56.xn--b1aew.xn--p1ai/news/item/40346968

2) Терроризм в интернете - угроза обществу - Пикабу инфо-портал [электронный ресурс]: URL: https://pikabu.ru/story/terrorizm_v_internete_ugroza_obshchestvu_7803009?ysclid=m3ekh4as9s328182897

3) Памятка (рекомендации) по организации профилактической работы в сети Интернет- БСПМП2 [электронный ресурс]: URL: https://bsmp2-omsk.ru/about/informatsiya-dlya-posititelej/pamyatka-rekomendatsii-po-organizatsii-profilakticheskoj-raboty-v-seti-internet/

4) Как не попасться в ловушку экстремистов в сети Интернет? - Официальный портал администрации города Тольятти [электронный ресурс]: URL: https://tgl.ru/structure/department/mku-oop-press-relizy/13201/.

ПРОТИВОДЕЙСТВИЕ ПРОПАГАНДЕ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА, ПРОФИЛАКТИКА ЭТИХ СОЦИАЛЬНЫХ ЯВЛЕНИЙ В МОЛОДЁЖНОЙ СРЕДЕ

Асадова Амина Эльшадовна, Мокрецкая Татьяна Дмитриевна
Областное государственное бюджетное профессиональное образовательное учреждение «Томский индустриальный техникум»
Руководитель: Симонов Андрей Юрьевич

Актуальность: после появления интернета информация стала доступнее для обычных граждан. В социальных сетях и мессенджерах экстремистам и террористам проще агитировать за свои идеологические взгляды, вовлекая людей в свою деятельность. Профилактика этих явлений в молодёжной среде важна, так как молодое поколение является психологически уязвимым и легко поддаётся влиянию. Создание безопасной среды в интернете является приоритетным в борьбе с пропагандой экстремистских движений.

Цель: изучить, как экстремисты могут влиять на сознание людей и вовлекать их в различные движения.

Рассмотреть: методы государства по противодействию терроризму в интернете.

Задачи:

1. Познакомиться с методом психологического влияния экстремистов и террористов на сознание людей.
2. Изучить меры государства по борьбе с терроризмом в интернете.
3. Подумать, как мы можем обезопасить себя от опасного влияния.

Объект исследования: Экстремизм и терроризм, как форма влияния на сознание людей.

Метод работы:

1. Анализ приёмов и манипуляций, которые используются экстремистами и террористами.
2. Изучение методов борьбы государства с терроризмом в интернете.

3. Изучение методов, как обезопасить себя и близких от влияния радикальных идеологий.

1. ИНДИВИДУАЛЬНЫЙ МЕТОД ПСИХОЛОГИЧЕСКОГО ВЛИЯНИЯ

1.1. Как люди попадают в террористические организации [3]

На начальном этапе исследования нас интересовало, как террористы психологически влияют на сознание граждан, которые присоединяются к террористическим группировкам. Помимо традиционных подходов, таких как запугивание или обещания различных благ, мы изучили один из способов психологического влияния на жертву. В первую очередь он основан на завоевании доверия и прививании идеологических взглядов. Стоит отметить, что этот метод действителен как в реальной жизни, так и в интернет-сетях. Рассмотрим поэтапно.

1) Знакомство. В начале вы просто познакомитесь с приятным человеком, с которым у вас совпадут общие интересы или увлечения. Знакомство может произойти как в реальности, так и в интернете, причём в интернете даже проще, так как там легче притвориться другой личностью. Этот новый знакомый будет настолько хорошо вас понимать, что вполне способен стать вашим близким другом.

2) Обещания. Рычаги воздействия на жертву могут быть разными. В зависимости от её желаний террорист может давать разные обещания. Новый знакомый пообещает человеку предоставить то, в чем тот нуждается. Террорист собирает информацию о человеке, с которым он общается, анализирует ее и в последующем использует для вербовки.

3) «Круг избранных». Вербуя, террорист постепенно будет углублять представление о несправедливости жизни и неправильном поведении окружающих, подчеркивать и усиливать границу между вербуемым и реальным миром. Он подведет к мысли, что из затруднительного положения есть выход, где-то может быть по-другому, что ты где-то нужен, сможешь себя

реализовать, внести личный вклад и изменить мир в сторону справедливости и сделать что-то важное. Далее, когда вербуемый «готов», наступает следующий шаг – приглашение на встречу. Это может быть встреча с «кругом избранных», знакомство с «важным человеком» и т.п. На этой встрече человеку дадут понять, что его заметили, выбрали. Причем, одного из немногих и для важного дела. Они помогут создать положительный эмоциональный настрой по отношению к вербовщику, ослабят критическое мышление и способность здраво мыслить. За это время эмоциональные связи вербовщика с жертвой становятся теснее.

4) Отъезд. Для того, чтобы не спугнуть жертву, террорист позовет его уехать в страну, где он проживает. Может предложить поехать на встречу с каким-то авторитетным лидером, на курсы изучения иностранного языка или на работу. Предлогов может быть много. Отъезд обычно бывает внезапным и срочным, билет покупают за день-другой до поездки, не давая времени на раздумье. Террорист убеждает завербованного в том, что такой шанс выпадает раз в жизни и его легко упустить.

Здесь уместно обратить внимание на то, какие группы наиболее подвержены эмоциональному воздействию вербовщиков. Некоторые люди могут ошибочно предполагать, что они не относятся к группам риска; однако жертвой влияния может стать каждый из нас.

1.2. Кто подвержен вербовки в террористические организации

1. Замкнутые и малообщительные люди.
2. Кто недавно пережил горе и потерю близких.
3. Кто попал в острую или хроническую стрессовую ситуацию (конфликты, ссоры, череда неудач, развод свой или родителей).
4. Молодежь, ищущая смысл жизни, авторитета или учителя для подражания.
5. Легко внушаемые люди.

6. Люди, чувствующие себя непонятыми, непризнанными, недооцененными в обществе.

Мы можем сделать вывод, что под вышеперечисленные критерии, в большинстве своём, попадают молодые люди, особенно подростки. Во-первых, в этом возрасте формируется идентичность, и молодые люди часто ищут смысл и принадлежность, что делает их уязвимыми к манипуляциям. Во-вторых, эмоциональная нестабильность и желание быть принятыми в группе могут заставлять молодых людей принимать рискованные решения.

1.3. Как дать отпор?

Для того, чтобы не попасться на уловки террориста, стоит быть избирательным в общении с незнакомыми людьми. Родители должны внимательнее относиться к подросткам. Родственники и друзья быть внимательнее друг к другу. Только так они смогут заметить, что с их ребенком или лучшим другом происходит что-то неладное.

Общаясь с новыми людьми в интернете и не только, соблюдайте три правила:

1. Сохраняйте осознанность, понимание того, что с вами происходит в данный момент времени. Вырабатывайте навык наблюдателя, задавая вопросы: «Зачем вы мне это говорите?», «Для чего вам это нужно?».

2. Проверяйте информацию, исследуя её полностью, начиная с отзывов в интернете и заканчивая сводками МВД.

3. Найдите цель в жизни, продумайте путь к её достижению. И тогда ни один вербовщик не сможет сдвинуть вас с намеченного пути, по которому вы следуете для достижения намеченных планов и целей.

2. МАССОВЫЕ МЕТОДЫ ПСИХОЛОГИЧЕСКОГО ВЛИЯНИЯ

Собственные наблюдения в этом плане показали, что в условиях глобализации и развития технологий, особенно интернет-пространства,

террористы также применяют более массовые и эффективные стратегии. Социальные сети и онлайн-платформы становятся мощными инструментами для распространения идеологии, формирования общественного мнения и создания виртуальных сообществ, где радикальные идеи могут свободно циркулировать. Веб-сайты, идеологические мультфильмы для детей, онлайн-видеоигры, специальные пособия для будущих новобранцев, как проводить террористические атаки – это одни из немногих методов, того, как с помощью разного рода контента у людей формируются неправильное восприятие мира и толерантность к насилию.[1]

Рисунок 1. Фрагмент из террористической онлайн-игры

3. ГОСУДАРСТВЕННЫЕ МЕРЫ ПО БОРЬБЕ С ТЕРРОРИЗМОМ В ИНТЕРНЕТЕ

С развитием технологий и ростом популярности социальных сетей экстремистские группы всё чаще используют интернет для вербовки, распространения идеологий и координации действий. Имеются ряд работ, в которых полностью или частично раскрыта тема противодействия терроризму в интернете. Например, в работе Гурьяновой К.В. «Правовое регулирование противодействия терроризму и экстремизму в сети «интернет»[2] рассмотрены способы борьбы государства с распространением террористической информации:

«В настоящее время наше государство принимает различные меры для борьбы с терроризмом в интернете. К основным автор относит:

1) Формирование федерального перечня экстремистских материалов, а также символики и атрибутики нацистских и экстремистских группировок, а также осуществление мониторинга Интернет-пространства для выявления этих материалов и символов.

2) Регулярный анализ социальных сетей, живых журналов, блогов и других ресурсов с целью обнаружения запрещённых материалов и символики

3) Применение мер прокурорского к виновным лицам, а также их привлечение к административной и уголовной ответственности».

В данной статье автор не только освещает методы борьбы государства с терроризмом в интернете, но также предлагает, как улучшить способы борьбы с идеологическими группировками в сети.

Наши собственные наблюдения в этом плане нам показали, что помимо ограничения и блокировок недопустимого контента, необходимо также с помощью медиа материалов распространять антитеррористические взгляды, направленные на разоблачение идеологии. Например, медийные личности, могли бы помогать государству и обществу в информационном противоборстве с идеологами терроризма.

4. РЕКОМЕНДАЦИИ ДЛЯ ПЕДАГОГОВ И РОДИТЕЛЕЙ ПО ПРОФИЛАКТИКЕ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА СРЕДИ ДЕТЕЙ И ПОДРОСТКОВ[4]

Мы не можем не отметить, что профилактика терроризма и экстремизма является важной задачей для родителей и педагогов, поскольку она способствует формированию у молодежи устойчивых ценностей, критического мышления и навыков безопасного поведения в обществе. Приведённые ниже пункты являются рекомендациями по профилактике экстремизма и терроризма среди молодёжи.

4.1. Рекомендации для педагогов

1) Организовать постоянный мониторинг общественного мнения в молодежной среде в целях выявления радикальных настроений среди учащихся и студентов (проводить опросы, личные беседы с учащимися, наиболее подверженными влиянию террористических идей, осуществлять контроль за деятельностью неформальных молодежных группировок).

2) Разъяснять на постоянной основе сущность и общественную опасность терроризма, ответственность за совершение действий террористического характера (организовывать лекции, классные часы по антитеррористической тематике).

3) Активно проводить пропагандистские мероприятия, направленных на дискредитацию террористической идеологии, формирование в молодежной среде идей межнациональной и межрелигиозной толерантности.

4.2. Рекомендации для родителей

1) Как можно чаще говорите с детьми, помогайте решать их, пусть даже пустяковые, по вашему мнению, проблемы.

2) Учите ребёнка правилам безопасности, однако и сами следуйте им, показывая ему пример.

3) Создавайте доверительные отношения с детьми с самого начала: так будет легче выявить, что с вашим ребёнком что-то происходит неладное.

ЗАКЛЮЧЕНИЕ

В итоге хотелось бы подчеркнуть следующее: в первую очередь, каждый из нас должен заботиться о собственной безопасности и безопасности близких в Интернете. Важно помнить, что насильственные действия не приведут к решению проблем, а лёгкие способы получения денег, положения, славы не сулят ничего хорошего. За любые противозаконные действия будут применены меры наказания, после совершения преступлений жизнь никогда не станет прежней. Необходимо помнить, что любые проблемы: будь то психологические, финансовые – решаемы и прибегать к применению насилия не нужно.

5. СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. https://www.buzzfeednews.com/article/andrewkaczynski/8-ways-terrorists-use-the-internet-for-recruitment[Электронный ресурс] 8 Способов, которыми террористы используют Интернет для вербовки.
2. https://cyberleninka.ru/article/n/pravovoe-regulirovanie-protivodeystviya-terrorizmu-i-ekstremizmu-v-seti-internet/viewer [Электронный ресурс] Текст научной статьи Правовое регулирование противодействия терроризму и экстремизму в сети «интернет».
3. https://245.56.мвд.рф/news/item/17503954 [Электронный ресурс] Способы вербовки молодежи в террористические организации.
4. https://nsportal.ru/shkola/raznoe/library/2022/03/17/metodicheskie-rekomendatsii-dlya-pedagogicheskih-rabotnikov-po [Электронный ресурс] Методические рекомендации для педагогических работников по профилактике проявлений терроризма и экстремизма в образовательных организациях.