УДК 004.056: 004.491

Тенденции развития вредоносного ПО и безопасность персональных данных: анализ угроз и уровень осведомленности пользователей

А.В. Каширин
студент 3 курса бакалавриата НИЯУ МИФИ, Москва
Email: andreykashirin04@mail.ru
И.Д. Кузьмин
студент 3 курса бакалавриата НИЯУ МИФИ, Москва
Email: kuzminivan2004@gmail.com
А.В. Орлов
студент 3 курса бакалавриата НИЯУ МИФИ, Москва
Email: temkartemka2@gmail.com
В.А. Рычков
старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва
Email: varychkov@mephi.ru
В.И. Рычкова
старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва
Email: virychkova@mephi.ru

Аннотация: *В данной статье освещается проблема развития вредоносного программного обеспечения и проблема осведомленности людей в области информационной безопасности на фоне актуальных угроз.*
Ключевые слова: *вредоносные программы, информационная безопасность, персональные данные, киберугрозы, утечки данных*

Development trends of malicious attacks and personal data security: threat analysis and user awareness

A.V. Kashirin
3rd year student at NRNU MEPhI, Moscow
Email: andreykashirin04@mail.ru
I.D. Kuzmin
3rd year student at NRNU MEPhI, Moscow
Email: kuzminivan2004@gmail.com
A.V. Orlov
3rd year student at NRNU MEPhI, Moscow
Email: temkartemka2@gmail.com

V.A. Rychkov
Senior lecturer, department of financial monitoring NRNU MEPhI, Moscow
Email: varychkov@mephi.ru
V.I. Rychkova
Senior Lecturer of financial monitoring NRNU MEPhI, Moscow
Email: virychkova@mephi.ru

Abstract: *This article highlights the problem of the development of malicious software and the problem of people's awareness of information security against the context of threats specific to our day and age*.
Keywords: *malware, cyber security, personal data, cyber threats, data leaks*

В настоящее время происходит цифровизация всех процессов начиная от документооборота и финансовых операций крупных компаний до записи к врачам и оплаты жилищных коммунальных услуг. Цифровизация не обошла стороной и производства, ведь современные станки могут быть запрограммированы и подключены к общей сети. При этом, развитие информационных технологий и появление новых информационный сервисов происходит значительно быстрее, чем люди успевают научиться безопасно ими пользоваться, прогресс происходит значительно быстрее, чем изменения в сознании людей. Поэтому с развитием информационных технологий вопрос информационной безопасности и осведомленности пользователей ещё будет актуален в ближайшие десятилетия.

Цель данной статьи заключается в рамках контекста развития вредоносного программного обеспечения и новых методов кибератак, оценить уровень осведомленности пользователей в области информационной безопасности, и используя практические проверить гипотезу, что несмотря на значительный технологический прогресс в последние годы, осведомленность пользователей о защищенности своих данных не всегда соответствует действительности.

Для достижения поставленной цели, в нашем исследовании были определены следующие задачи

- Анализ статистики, собранной крупными отечественными IT компаниями, работающих в области информационной безопасности
- Анализ частоты атак с использованием уже известным ВПО и известными методами их распространения.
- Описание новых видов угроз, вызванных развитием различных технологий, и методов использование их.
- Проведение опроса среди случайной выборки людей и последующий анализ их осведомленности, а также с разрешения полученного от опрошенных людей поиск их персональных данных с помощью средств разведки по открытым источникам (проведение OSINT).

Влияние вредоносного ПО на персональные данные

Злоумышленники, используя ВПО, могут получить доступ к персональным данным пользователей, к логинам и паролям, а также к платежным реквизитам. Основные методы, применяемые злоумышленниками, для распространения ВПО, получения доступа к устройству и краже нужной информации:

Фишинг (phishing, искаженное написание англ. fishing — рыбалка) — разновидность интернет-мошенничества, нацеленная на кражу конфиденциальной информации, такой как учетные данные от аккаунтов в интернет-сервисах или данные банковских карт, при помощи методов социальной инженерии. С помощью этих методов пользователь, сам того не понимая, передает злоумышленнику все нужные данные.

Клавиатурные шпионские программы (кейлоггеры) - программы, которые, записывая нажатия клавиш на клавиатуре, позволяют злоумышленникам получить доступ к введенным логинам и паролям.

Эксплойт фрагмент кода или данных, которые предназначены для использования ошибки или уязвимости в приложении или операционной системе. Воспользовавшись эксплойтом, злоумышленник получает несанкционированный доступ к приложению или операционной системе и возможность их эксплуатации.

Кража данных может привести к несанкционированному доступу к аккаунтам пользователей, что в свою очередь может вызвать финансовые потери и утрату конфиденциальной информации.

Шантаж, утечки и использование шифровальщиков

Вредоносное ПО также может использоваться для шантажа и манипуляции над пользователем. На протяжении 2024 года было зафиксирована различными компаниями, работающих в области информационной безопасности, более 500 атак с использованием шифровальщиков в России — рост почти в полтора раза по сравнению с 2023 годом. Злоумышленники могут применять следующие методы:

Шифровальщики (Ransomware): Программы, шифруют файлы на устройстве пользователя и требуют выкуп за их расшифровку. Это может привести к потере доступа к важной информации и значительным финансовым потерям.

Утечки данных: Вредоносное ПО может собирать конфиденциальную информацию (например, фотографии, документы, пароли и их хэши) и распространять ее без согласия владельца.

Социальная инженерия: Злоумышленники могут манипулировать пользователями для получения доступа к их данным или заставлять их выполнять определенные действия, которые могут нарушать закон, под угрозой раскрытия какой-либо информации, блокировки устройства, кражи денежных средств.

Последствия для пользователей

Последствия воздействия вредоносного ПО на персональные данные могут быть следующие:

Финансовые потери: утрата денег из-за несанкционированных транзакций или выплаты выкупа за восстановление доступа к данным или к системе.

Потеря репутации: для пользователей и компаний утечка данных может привести к потере доверия со стороны клиентов и партнеров.

Правовые последствия: в некоторых случаях пользователи могут столкнуться с юридическими последствиями из-за утечки конфиденциальной информации.

Таким образом, вредоносное ПО представляет собой серьезную угрозу для персональных данных пользователей, что требует повышенного внимания к вопросам безопасности и защиты информации.

Анализ текущих угроз (данные за 2020–2025 гг.)

Статистика по кибератакам на компании в России.

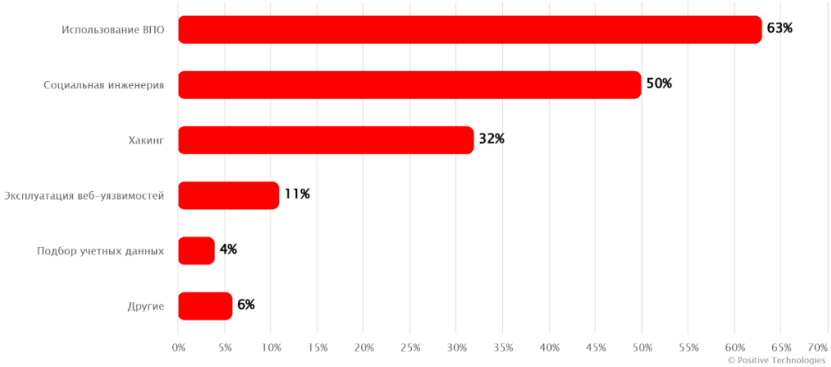


Рисунок 1 – Методы атак за 2021 год (доля успешных атак)

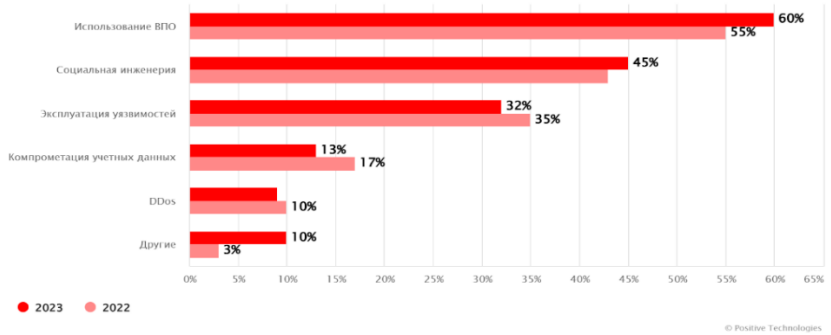


Рисунок 2 – Методы атак за 2022 и 2023 год (доля успешных атак)

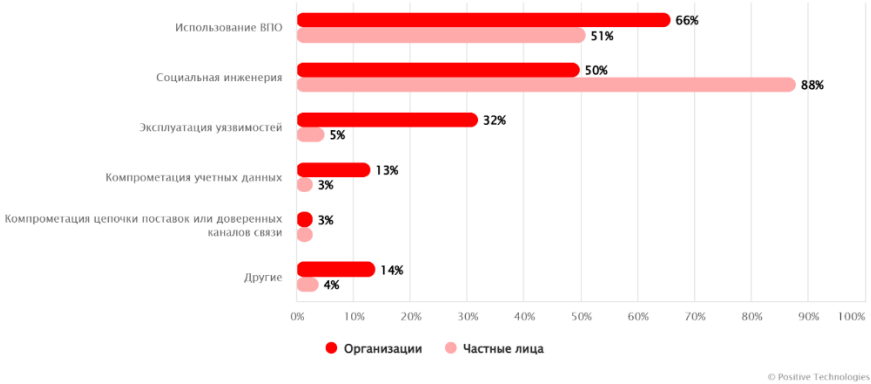


Рисунок 3 – Методы атак за 2024 и начало 2025 года (доля успешных атак)

Как видно из графиков, основанных и построенных на данных Positive Technologies, в кибератаках преобладают следующие методы: использование вредоносного программного обеспечения и социальная инженерия. Причем атаки на компании опираются в основном на программное обеспечение и на эксплуатацию уязвимостей, а атаки на пользователей опираются в основном на социальную инженерию. Причем доля успешных атак с использованием социальной инженерии на пользователей составляет почти 90%. Из этого, можно сделать несколько выводов. Первый, у злоумышленников есть персональные данные пользователей, что позволяет им манипулировать пользователями и заполучить доверие представляясь сотрудниками различных служб. Второй, цифровая грамотность населения отстает от современных методов обмана и манипуляций в интернете, так как цель социальной инженерии - обманом заставить человека сделать то или иное действие, при этом почти 9 из 10 успешных атак на пользователей использовали социальную инженерию.

Проблема кибербезопасности также остро стоит и в странах Европейского Союза. Во Франции в 2024 году Французское агентство информационной безопасности (ANSSI) обработало 4386 «событий безопасности» в компьютерных системах во Франции, что на «15%» больше, чем в предыдущем году, согласно данным, предоставленным France Inter агентством ANSSI. Эти «события безопасности» — это «события, доведенные до сведения Anssi и послужившие основанием для обработки оперативными группами».

Согласно представленным данным Total Security 360, в Италии прошлом году было зафиксировано 3541 кибератак, что на 27% больше, чем в 2023 году. Не только количество атак растет, но и их серьезность остается высокой: 79% инцидентов классифицируются как серьезные или критические. Новые тенденции свидетельствуют о значительном росте

киберпреступности, возрождении цифрового активизма и тревожном росте атак в Европе, которая сокращает разрыв с Америкой и становится все более уязвимой целью. В Британии 43% предприятий (приблизительно 612 000) и 30% благотворительных организаций (приблизительно 61 000) сообщили, что столкнулись с любым видом кибератаки в течение последних 12 месяцев.

Новые методы атак (например, с использованием deepfake)

Дипфейк (deepfake, от *deep learning* — «глубокое обучение» и *fake* — «подделка») — синтез правдоподобных поддельных изображений, видео и звука при помощи искусственного интеллекта. Также дипфейками называют контент, полученный в результате этого синтеза. Чаще всего дипфейки изображают известных людей в вымышленных ситуациях. В некоторых случаях к дипфейкам относят также письменные тексты, созданные при помощи искусственного интеллекта в целях имитации речи конкретного человека.

С развитием нейросетей, развиваются дипфейки. Эти технологии предоставляют каждому человеку легко изменить видео, где человек заснятый на видео будет изменен на какого-либо другого человека, причем уже сейчас подделку очень сложно отличить от оригинала. В настоящее время атаки с применением дипфейков используются в основном для пропаганды или для нанесения ущерба репутации различным знаменитым личностям. Как пример, созданный ИИ дипфейк Тейлор Свифт сексуального характера стал быстро распространяться в «X» 22.01.2024 и один из постов набрал свыше 45 млн. просмотров и более 24 тыс. репостов, прежде чем был удален**.** Однако встречались и случаи мошенничества с использованием дипфейков. Так, например, злоумышленник может преобразовать себя в генерального директора какой-либо компании и использовать видеозвонки для общения с кем-либо от лица компании, а это уже дает пространство для действий, способных нанести ущерб компании. Также с помощью дипфейков злоумышленники могут представиться родственником жертвы, что может вынудить жертву перечислить средства “пострадавшему родственнику”. Дипфейки расширяют методологию атак с использованием социальной инженерии, что вынудит людей меньше доверять звонкам и видеозвонкам, а также все деловые встречи проводить офлайн, дабы избежать различных потерь.

Уровень осведомленности пользователей

Учитывая вышеприведенный теоретический контекст роста угрозы от кибератак по всему миру, мы решили провести собственный анализ текущей осведомленности пользователей (как и в России, так и заграницей) и сделать выводы насчет данного вопроса исходя из первичных, свежих данных.

Были созданы три опроса, которые впоследствии были объедены для представления полноценной картины. В итоге были опрошены 40 человек, половина из которых заполняли опрос очно на бумаге, с которой ходили

авторы статьи по разным улицам и паркам Москвы - как и в центре (Никольская ул, Красная Площадь, Парк Зарядье), так и вдали от центра (Сокольники, скамейки около м. Каширская, Царицыно). Прежде всего, такие локации были выбраны для получения разнообразного контингента участников опроса (не только какую-то одну социальную категорию) для получения общей картины об осведомленности людей насчет защищенности их персональных данных. Вторая половина результатов опроса была собрана через дистанционный опрос - одна версия была на русском, одна на английском с полностью дублирующими вопросами (все вопросы на обоих языках, также, как и анонимизированные результаты, расположены в приложении к статье). Эти опросы были распространены через знакомых, бывших одноклассников и группы в соц. сетях.

При этом, для более широкого покрытия опроса, мы использовали нестандартный метод поиска международных участников опроса. В условиях ограниченного бюджета, платить людям за прохождение опроса не было возможным, поэтому решили значительно увеличить количество пользователей, на которых был нацелен опрос, и даже при низкой конверсии в ~0,1% набрался набор людей из восьми разных стран, не включая Россию. Были использованы специальные возможности поиска Google (известны как Google Dorks), для нахождения свежих (публикация не позже чем месяц назад) документов в формате pdf с ссылкой на сайт chat.whatsapp.com, который используется исключи в приглашениях на открытые группы в WhatsApp. Несмотря на то, что мы были дважды в последствии заблокированы администраторами приложения за спам, каждый раз блокировку получилось отменить, и за это время получилось набрать достаточно ответов с разных стран мира, начиная с Норвегии и Франции, заканчивая Пакистаном и Мозамбиком.

Основная цель была проверить соответствие мнения участников опроса насчет нахождения их персональных данных в открытом доступе с наличием персональных данных в открытом доступе в действительности, а также оценить общую картину насчёт доступности данных настоящих людей в открытом доступе, и оценить цифровую грамотность населения. Про методику выявления наличие утечки ПД того или иного респондента будет более подробно сказано в следующем разделе.

Результаты опроса

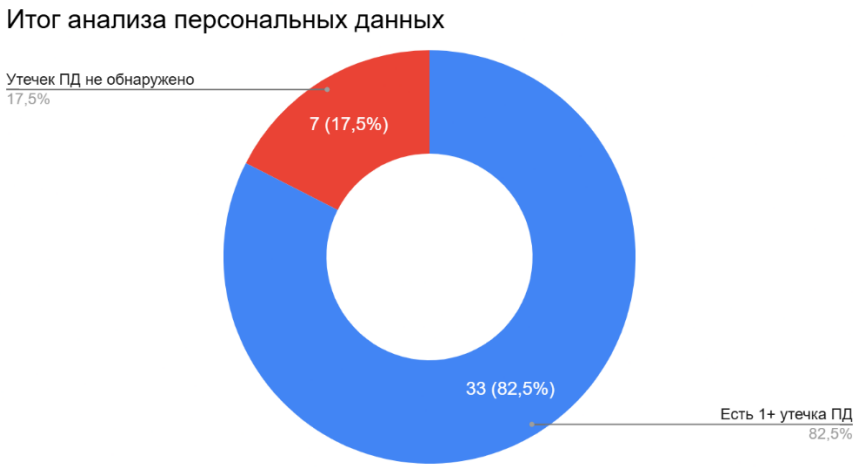


Рисунок 4 – Итоги по поиску персональных данных по предоставленным данным

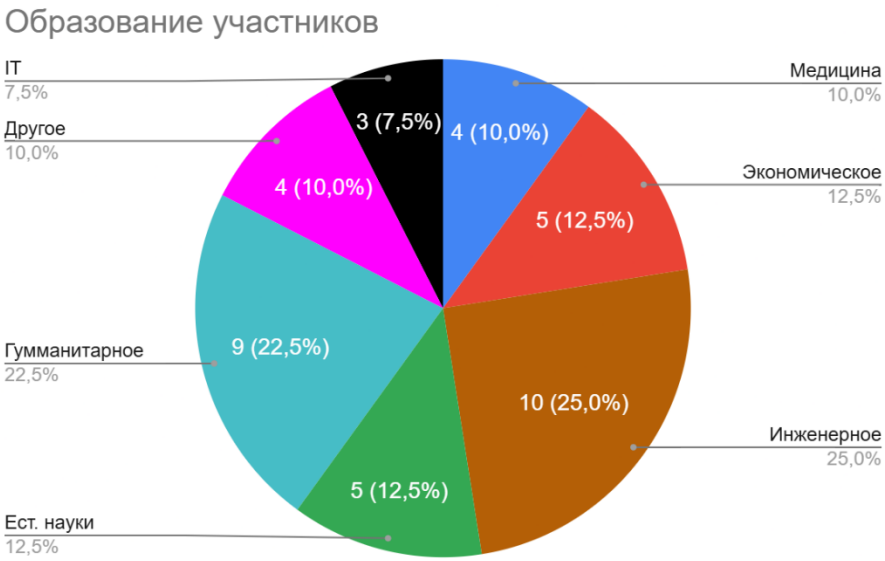


Рисунок 5 – Образование людей, предоставивших данные

Рисунок 6 – Возрастная группа людей, предоставивших данные

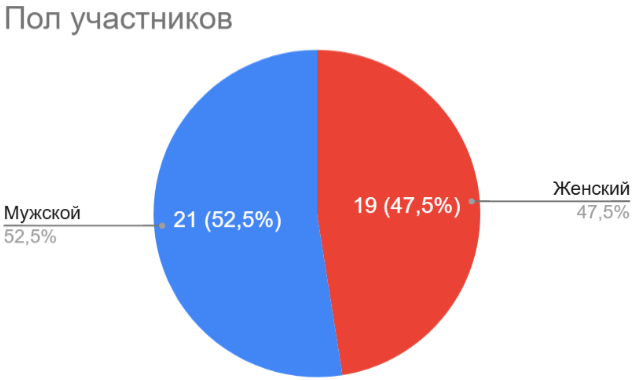


Рисунок 7 – Пол людей, предоставивших данные

Рисунок 8 – Знание людей, предоставивших данные, о существовании антивирусного

ПО

Рисунок 9 – Использование людьми, предоставивших данные, антивирусного ПО

Рисунок 10 – Подвергались ли устройства людей, предоставивших данные, заражению ВПО

Рисунок 11 – Мнение людей, предоставивших данные, о нахождение своих ПД в открытом доступе

Анализ данных в зависимости от определенных условий

Всевозможные комбинации демографических данных и ответов на вопросы, связанные с утечками ПД долго представить, поэтому мы представляем самые интересные данные на наш взгляд и их анализ. Наличие утечек ПД было собрано через 3 метода: проверка через базу данных в ПО Телеграм “Глаз Бога”, проверку на ресурсе HaveIBeenPwned.com, поиск точных совпадений почты и телефона в Google и Яндексе. Если как минимум в одном из этих ресурсов была найдена утечка ПД, то для респондента отмечалось значение “Есть утечка”, и наоборот.

Рисунок 12 – График наличия утечек ПД у мужчин, предоставивших данные

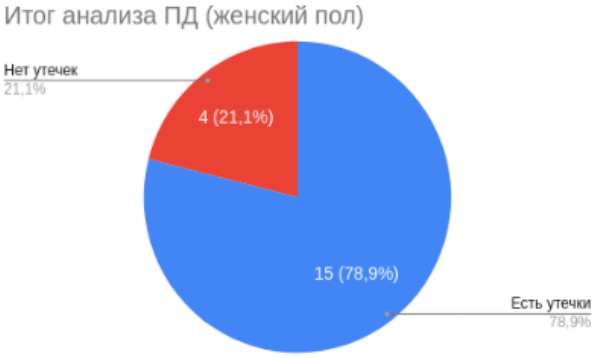


Рисунок 13 – График наличия утечек ПД у женщин, предоставивших данные

Разница по наличии утечек между участниками мужского и женского пола несущественны, но тем не менее замечена более значительная пропорция девушек, у которых утечек не было найдено. Предположительно это можно объяснить тем, что мужчины в среднем проводят больше времени

в интернете, а также пользуются большим количеством сервисов, в то время, когда женщины чаще ограничиваются парой проверенных сервисов.

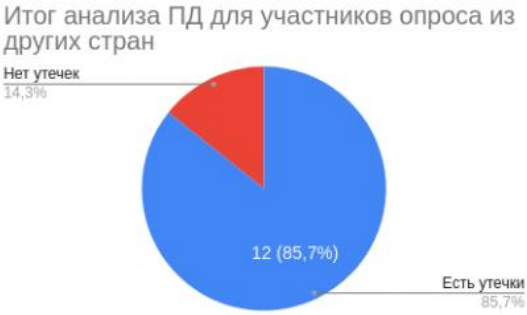


Рисунок 14 – График наличия утечек ПД у иностранцев, предоставивших данные

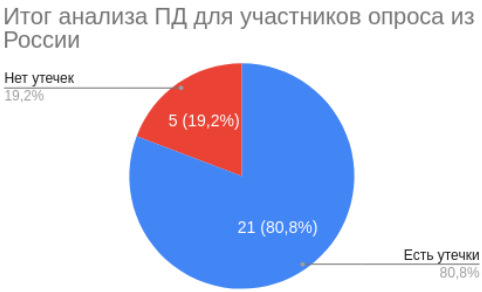


Рисунок 15 – График наличия утечек ПД у граждан РФ, предоставивших данные

Несмотря на то, что больше кибератак затрагивают Россию чем другие страны, меньше утечек замечено у участников из России чем у респондентов с других стран. Но тем не менее, в обеих случаях более 80% людей подвергались утечкам, что значительно больше ожидаемого.

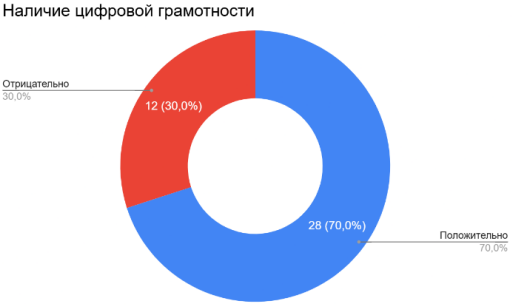


Рисунок 16 – График наличия базовой цифровой грамотности людей, предоставивших данные

Цифровая грамотность была оценена на основе открытого вопроса “Знаете ли Вы, что такое антивирус?”. Ответы, соответствующие действительности (напр. взлом аккаунтов, кража паролей, использование мощностей компьютера в целях майнинга), то было проставлено “Положительно”. В противоположном случае, (напр. ответ “печальные”), то была проставлено отсутствие цифровой грамотности для данного участника опроса.

Рисунок 17 – График наличия утечек ПД людей, предоставивших данные и считающих, что их ПД не были в утечках баз данных

Рис. 18 – График наличия утечек ПД людей, предоставивших данные и считающих, что их ПД были в утечках баз данных

Данные диаграммы иллюстрирует одно наблюдение, которое в других исследованиях не нашли - значительно более утечек найдены у тех людей, кто наоборот считают, что в открытом доступе их данных нет. Причины такого вывода уже скорее из сферы человеческой психологии, и вне рамок данной статьи.

И главный вывод статьи - для подавляющего большинства участников нашего опроса, ожидание о нахождении их персональных данных в утечке

противоположны действительностью - что свидетельствует о крайнем недостатке в знании на личном уровне какие из личных данных доступны в интернете, а какие нет - даже сама их доступность люди крайне часто оценивают неправильно. И несмотря на довольно высокий уровень общей цифровой грамотности в 70%, всего 25% грамотно оценивают наличие своих данных в открытом доступе, и именно в этом направлении дальнейшая работа по осведомленности населения должна продолжаться в приоритетном порядке, а также при возможности внедрять автоматизацию процесса обработки данных. Многие утечки происходят именно из-за неосторожности людей в работе и ошибок, которые автоматизированные процессы могли бы предотвратить. И именно через минимизации человеческого фактора мы сможем повысить надежность информационных систем.

Список использованных источников:

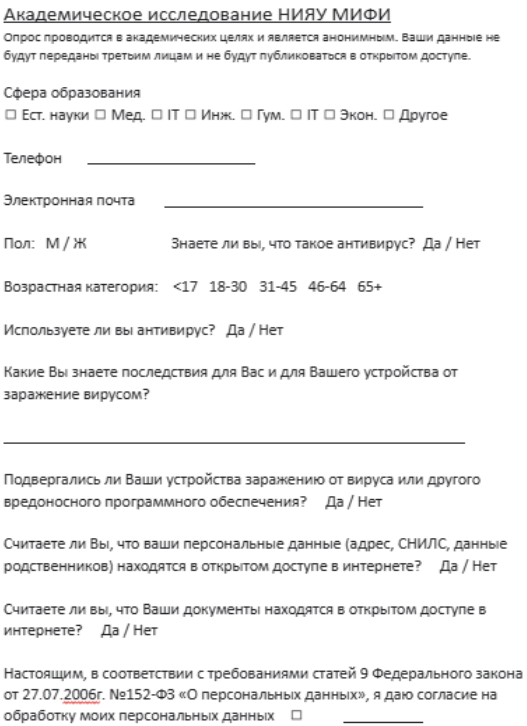
1. Определения // Энциклопедия Касперского URL: https://encyclopedia.kaspersky.ru/
2. Статистика атак за 2021-й год // Positive Technologies URL: https://ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/
3. Статистика атак за 2022-й год // Positive Technologies URL: https://ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/
4. Статистика атак за 2023-й год // Positive Technologies URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/
5. Статистика атак за 2024-й и начало 2025-го года // Positive Technologies URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id1
6. Использование технологии deepfake для совершения киберпреступлений // SumSub URL: https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/
7. Использование ИИ в кибератаках // Positive Technologies URL: https://ptsecurity.com/ru-ru/research/analytics/iskusstvennyj-intellekt-v-kiberatakah/#id6
8. Методы злоумышленников в атаках на компании // Solar URL: https://rt-solar.ru/analytics/reports/5320/#:~:text=Всего%20за%202024%20год%20мониторинг,целом%20соответствует%20показателям%202023%20года.&text=Ниже%20представлена%20статистика%20по%20наиболее%20распространенным%20типам%20инцидентов.
9. Инцидент нанесения ущерба репутации с использованием технологии deepfake // VC URL: https://vc.ru/social/1004440-dipfeik-teilor-svift-vskolyhnul-vseh-ot-polzovatelei-h-do-belogo-doma

10. Статистика и динамика киберпреступлений в Италии // Cybersecurity 360 URL: https://www.cybersecurity360.it/nuove-minacce/cybersecurity-2025-rapporto-clusit-dati-tendenze/#:~:text=Secondo%20i%20dati%20presentati%2C%20lo,mappati%20dal%202011%20ad%20oggi.

11. Статистика и динамика киберпреступлений во Франции // L'Ansii URL: https://www.francebleu.fr/infos/societe/cyberattaques-4-386-evenements-de-securite-detectes-en-france-en-2024-en-hausse-de-15-en-un-an-3076380

12. Статистика и динамика киберпреступлений в Англии // GOV.uk URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025#fn:2

Приложение 1
https://clck.ru/3M544a - объединенная таблица ответов на опрос (с анонимизированными персональными данными)
Приложение 2
Скан опросного листа, с котором было проведена очная часть анализа



Академическое исследование НИЯУ МИФИ

Опрос проводится в академических целях и является анонимным. Ваши данные не будут переданы третьим лицам и не будут публиковаться в открытом доступе.

Сфера образования
☐ Ест. науки ☐ Мед. ☐ IT ☐ Инж. ☐ Гум. ☐ IT ☐ Экон. ☐ Другое

Телефон _____

Электронная почта _____

Пол: М / Ж Знаете ли вы, что такое антивирус? Да / Нет

Возрастная категория: <17 18-30 31-45 46-64 65+

Используете ли вы антивирус? Да / Нет

Какие Вы знаете последствия для Вас и для Вашего устройства от заражение вирусом?

_____

Подвергались ли Ваши устройства заражению от вируса или другого вредоносного программного обеспечения? Да / Нет

Считаете ли Вы, что ваши персональные данные (адрес, СНИЛС, данные родственников) находятся в открытом доступе в интернете? Да / Нет

Считаете ли вы, что Ваши документы находятся в открытом доступе в интернете? Да / Нет

Настоящим, в соответствии с требованиями статей 9 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных», я даю согласие на обработку моих персональных данных ☐ _____