УДК 338.2

ПРОБЛЕМА И ПУТИ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ «ЕДИНЫЙ ПОРТАЛ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ»

Васина Д.А.,

Студент 4 курса направления государственная и муниципальная служба

КФ РАНХиГС

Калуга, Россия

Бобырев Д.Б.,

к.э.н., доцент

КФ РАНХиГС

Калуга, Россия

Аннотация. В данной статье рассмотрены текущие проблемы и виды мошенничества при использовании информационной системы «Единый портал государственных и муниципальных услуг». Анализируются основные виды мошеннических схем, включая фишинг, вредоносное ПО и социальную инженерию. Особое внимание уделяется факторам, способствующим распространению данных угроз, таким как неосведомлённость пользователей и низкий уровень кибербезопасности. Статья предлагает комплексный подход к противодействию мошенничеству, включая усиление мер идентификации пользователей, проведение образовательных программ, внедрение современных технологий безопасности и сотрудничество с правоохранительными органами. Также рассматриваются механизмы обратной связи, позволяющие оперативно реагировать на инциденты. Заключение подчеркивает важность повышения уровня доверия к электронным государственным услугам через эффективные меры защиты и информирования пользователей, что ведёт к более безопасному и удобному использованию портала.

Ключевые слова: мошенничество, единый портал государственных и муниципальных услуг, фишинг, вредоносное ПО, информационная безопасность, пользовательская осведомлённость, защита данных, электронные услуги

THE PROBLEM AND WAYS OF COUNTERING FRAUD WHEN USING THE INFORMATION SYSTEM "UNIFIED PORTAL OF STATE AND MUNICIPAL SERVICES"

Vasina D.A.,

4th year student of the direction of state and municipal service

CF RANHiGS

Kaluga, Russia

Bobyrev D.B.

Candidate of Economics, Associate Professor

CF RANHiGS

Kaluga, Russia

Abstract. The article discusses the current problems of fraud that arise when using the information system "Unified Portal of state and Municipal services". The main types of fraudulent schemes are analyzed, including phishing, malware and social engineering. Special attention is paid to the factors contributing to the spread of these threats, such as user ignorance and low level of cybersecurity.

The article offers a comprehensive approach to countering fraud, including strengthening user identification measures, conducting educational programs, introducing modern security technologies and cooperating with law enforcement agencies. Feedback mechanisms are also being considered to allow for rapid response to incidents.

The conclusion emphasizes the importance of increasing the level of trust in electronic public services through effective measures to protect and inform users, which leads to a safer and more convenient use of the portal.

Keywords: fraud, unified portal of state and municipal services, phishing, malware, information security, user awareness, data protection, electronic services

Данная статья актуальна, так как мошенничество в современном мире распространяется все больше, особенно распространенным стало мошенничество в сфере использования электронных услуг. Каждое третье зарегистрированное преступление в стране в настоящий промежуток времени относится к преступлениям, совершенным при помощи информационных технологий.

Так, например, за весь 2023 г. ущерб от IT-преступлений в России достиг 157 млрд рублей, таким образом в 2023 году количество преступлений в данной сфере достигло 677 тыс. случаев, что означает, что количество увеличилось на 29,7%.

На деле же количество преступлений больше, чем в официальной статистике, так как, только около 40% жертв интернет-мошенничеств заявляют о них в полицию. Остальные 60% не сообщают о мошенничестве, потому что считают, что это бесполезно и их дело раскрыть не смогут.

На данный момент статистика указывает на то, что мошенничество при использовании информационных технологий имеет один из худших показателей раскрываемости – всего 11% за 2023 год, в то время как раскрываемость по другим отраслям значительно выше, например, 96% убийств, 97% случаев причинения тяжкого вреда здоровью, 42% краж, 85% угонов автомобилей.

Само мошенничество в киберпреступлениях имеет 53%, что доказывает, что большая часть преступлений с использованием современных технологий относится к мошенничеству.

Мошенничество осуществляется посредством Единого портала государственных и муниципальных услуг. В основном, пострадавшие сталкивались со следующими видами мошенничества.

1. Фишинг и подделка сайтов.

Фишинг является самым распространенным видом мошенничества. Этот вид мошенничества заключается в приемах, при помощи которых мошенники получают доступ к личным данным пользователя, например, доступ к паролям и

банковским счетам.[1] Мошенники могут заполучить эти данные следующими методами:

- Создание поддельных сайтов. Часто мошенники создают сайты, которые напоминают дизайн Госуслуг. Доступ к этим сайтам жертва мошенничества может получать через рассылки, рекламу или даже в поисковике. На данных сайтах необходимо авторизоваться, так как пользователи уверены, что это официальный сайт Госуслуг, то они вводят свои данные, не опасаясь, что они попадут в руки к мошенникам. На этих сайтах необходимо ввести данные (паспорт, снилс), которые позволяют мошенникам получать доступ или даже красть учетную запись. Таким образом, правонарушители получают доступ к персональным данным, которые потом используют в своих целях.

Данный вид фишинга является одним из опаснейших для личных данных человека. Мошенники создают подобные сайты достаточно часто, так, например, только за январь 2024 году было создано более 5 тыс. подобных сайтов, что превышает количество поддельных сайтов в декабре 2023 года. Также стоит отметить и тот факт, что данные сайты появляются практически в геометрической прогрессии, так за первое полугодие 2023 года количество таких источников возросло в 11 раз по отношению к этому же периоду 2022 года.

[2]- Захват доменных имен. Часто люди не проверяют полное название ссылки, по который переходят, этим и пользуются мошенники. Правонарушители создают домены, меняя символы на похожие или же используют .net вместо .gov, чего не замечают пользователи и переходят по ссылкам, в это время данные оказываются у мошенников.

[1] Беляев, И. П. Поддельные сайты и способы их распознавания // Современные тренды в кибербезопасности. — М.: Инфра-М, 2021. — С. 123–129.

[2] Защита личных данных: практическое руководство / Под ред. А. Н. Петрова. — М.: Юрайт, 2020. — 256 с. / [электронный ресурс]. URL: https://urait.ru (дата обращения: 13.11.2024)

- Использование вирусных ссылок. Мошенники направляют пользователь уведомление, похожее на официальное письмо от Госуслуг, когда пользователь открывает данное сообщение или переходит по ссылке на его гаджет устанавливается программа, которая передает данные мошенникам. Данный вид мошенничества встречается реже остальных, но он опасен не только тем, что данные перейдут к третьим лицам, но и тем, что вирусная ссылка может нанести ущерб гаджету.

- Инсценировка процессов. Этот метод заключается в том, что мошенники сообщают о выполнении действий на Госуслугах, которые человек не совершал. Например, вход на госуслуги, оформление заявления через Госуслуги, попытку взлома Госуслуг. Для нейтрализации последствий действий пользователю предлагается сообщить личные данные, так мошенники получают доступ к личным данным. Чаще всего этот способ мошенники совершают при звонке жертве.

Зная приемы, которые применяют мошенники, можно предложить ряд методов для обеспечения безопасности при использовании Госуслуг:

- Образование пользователей. Необходимо просвещать граждан об опасности, с которой они могут столкнуться при использовании портала Госуслуг. Можно создать телеканал, который будет вещать о преступлениях в этой сфере, раздавать брошюры с информацией, создать методы для просвещения пенсионеров, так как они чаще всего страдают от мошенников.

- Проверка URL. Необходимо донести до пользователей необходимость проверять сайты, на которые они переходят, проверять название сайта необходимо целиком, ведь бывают фишинговые сайты, которые от оригинала отличает один символ. Если пользователи будут проверять все символы ссылки на Госуслуги, то вероятность, что они перейдут по неверной ссылке, снизится.

- Использование антивирусов и браузеров с защитой от фишинга. Данные методы позволяют автоматически блокировать подозрительные сайты и ссылки, а также предупреждают о возможной угрозе. При использовании данных методов риск столкновения с мошенническим сайтом существенно уменьшается.

- Двухфакторная аутентификация. Данный метод заключается в том, что, кроме доступа через логин и пароль, требуется подтверждения входа другим способом, например, введение сообщения. Данный способ существенно затрудняет мошенникам вход в учетную запись пользователя, так как получить доступ без второго фактора аутентификации очень сложно. Этот прием позволяет защитить свои данные от мошенников, однако не дает 100% защиты.

- Сообщение о мошенничестве. Необходимо сообщать о мошенничестве, это позволит блокировать сайты, похожие на Госуслуги, из-за чего меньшее количество пользователей перейдет на этот сайт.

Эти меры помогут не только защитить пользователей от мошенничества, но и укрепить доверие к использованию электронных услуг на государственном уровне, что позволит снизить количество мошенничества с использованием информационных технологий.[3]

2. Использование вредоносного ПО.

Вредоносные программы (вирусы, шпионские программы, трояны и прочее) представляют собой серьёзную угрозу для пользователей Единого портала государственных и муниципальных услуг. Такие программы могут использоваться для кражи личной информации и доступа к учётным записям, что создаёт условия для мошенничества. Основные аспекты этой угрозы включают:

- Шпионские программы: они могут устанавливать на устройствах пользователей, собирая информацию о вводимых паролях, логинах и другой конфиденциальной информации. Без ведома пользователя шпионские программы могут отслеживать действия, что делает их особенно опасными.

- Трояны: Некоторые вредоносные программы могут делать устройства частью бот-сетей для дальнейших атак на другие системы или шифровать данные на компьютере пользователя и требовать выкуп за их восстановление. В случае

[3] Громова, Е. В., Дьяконова, Л. В. Электронные услуги и мошенничество: современное состояние и пути решения проблемы // Вестник государственного управления. — 2022. — Т. 10. — № 1. — С. 135–142.

взаимодействия с государственными услугами это может привести к утечке данных.

- Эксплуатация уязвимостей: Мошенники могут использовать уязвимости в программном обеспечении или браузерах для внедрения вредоносных программ. Такой подход требует от пользователей постоянного обновления своих систем и программ.

- Поддельные установки: Вредоносное ПО может маскироваться под полезные приложения, обещающие улучшение функциональности, но на самом деле оно предназначено для кражи данных. Пользователи могут загружать такие программы, думая, что они безопасны.

Для минимизации рисков, связанных с использованием вредоносного ПО, можно предпринять следующие меры:

- Антивирусное программное обеспечение: Установка и регулярное обновление антивирусных программ помогут защитить устройства от множества угроз, включая шпионские программы и вирусы.

- Осторожность при загрузке: Пользователи должны избегать установки программ из ненадёжных источников и проверять легитимность загружаемого ПО.

- Обновление программного обеспечения: Регулярное обновление операционных систем и приложений помогает устранить известные уязвимости, что защищает устройства от атак злоумышленников.

- Брандмауэр и настройки безопасности: Включение брандмауэра и настройка параметров безопасности в браузерах может существенно снизить риск попадания под атаку вредоносных программ.

- Обучение пользователей: Повышение осведомлённости о вредоносном ПО и методах его распространения, а также обучение принципам безопасного поведения в интернете помогут пользователям избежать потенциальных угроз.

Благодаря указанным рекомендациям, каждый пользователь может существенно снизить риски и повысить уровень безопасности своего профиля на Едином портале государственных и муниципальных услуг.[4]

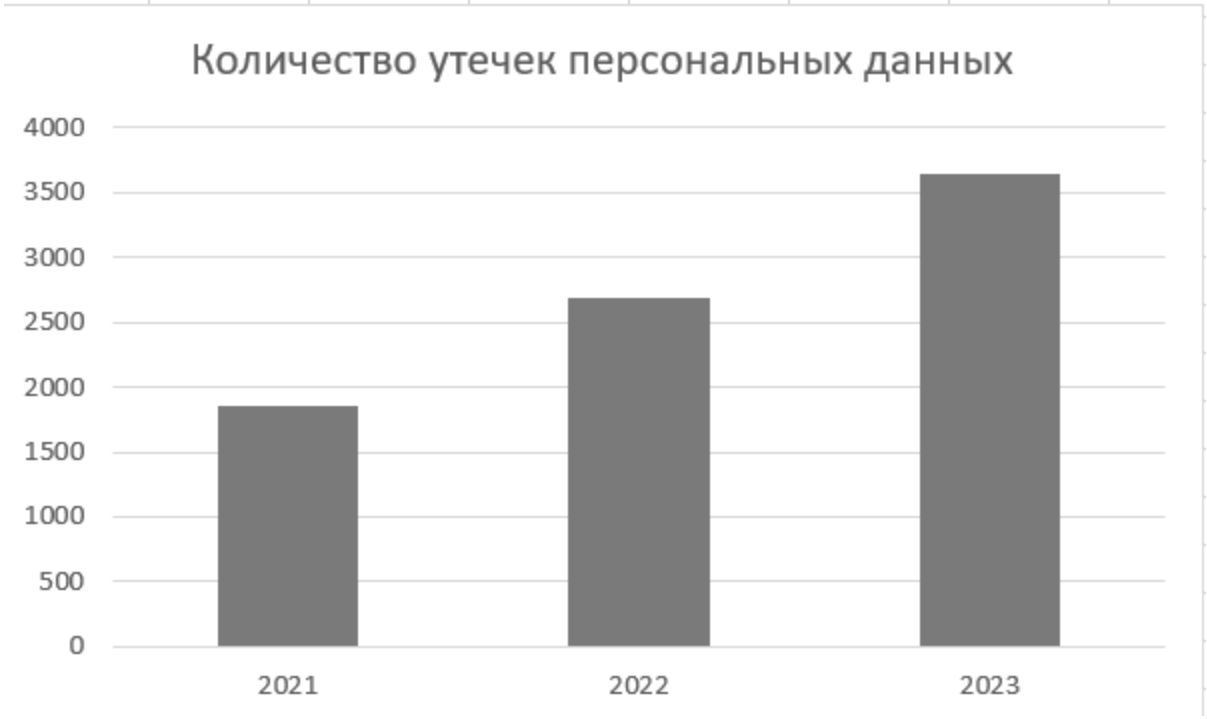

Рисунок – 1 (количество утечек персональных данных за период 2021-2023 год) [3]

Рассмотрим количество утечек персональных данных за период 2021 – 2023 год. По диаграмме видно, что за 2021 год было совершенно 1800 утечек. И далее этот показатель растет, так в 2022 году было совершенно уже 2681 утечки, что на 44% больше, чем за предыдущий год. А за 2023 на 36% больше, чем за 2022 год. Такая статистика подчеркивает важность ответственного подхода к защите своих персональных данных.

3. Социальная инженерия.

Социальная инженерия является наукой, изучающей методы манипуляций, которые используют мошенники при получении личной информации, при этом минуя техническую защиту пользователя. Этот подход исходит из понимания человеческой психологии и основывается на доверии, страхе или любопытстве. Статистика показывает, что доля мошенничества при помощи социальной

[4] Тихомиров, В. С. Защита информационных ресурсов: от теории к практике. — СПб.: Питер, 2023. — 312 с.

инженерии растет с каждым годом для частных лиц, а для организаций остается неизменной. Основные каналы мошенничества при помощи социальной инженерии[5]:

- Фишинг через звонки, сообщения, социальные сети. Данный метод заключается в том, что злоумышленники связываются с пользователем через предложенные каналы и представляются представителями банка, госуслуг и других, вызывающих доверие, организаций, после чего, под предлогом проверки данных или же оказания помощи заполучают личные данные пользователя. Стандартной является схема, при которой злоумышленник сообщает, что кто-то получил доступ от госуслуг и необходимо срочно принять меры для органичения противоправных действий, тем самым заполучает необходимые данные. Данные схемы осуществляются за счет знания человеческой психологии, мошенник заставляет пользователя испытывать страх, что не позволяет оценить ситуацию и принять меры, выгодные злоумышленнику.

- Личные встречи и поддельные представительства. Этот метод встречается редко, но имеет место быть. Смысл метода приблизительно такой же, как и в предыдущем пункте, но сбор информации происходит при личной встрече.

Способы защиты от социальной инженерии:

- Осведомлённость и обучение. Данный способ заключается в разработке источника информации о методах социальной инженерии, чтобы граждане умели распознавать мошенничество.

- Проверка источников. Данный способ заключается в том, что пользователи должны проверять кто и через какие ресурсы с ними связывается. Например, если связывается лицо, представляющее банк, и это лицо сообщает о необходимости продиктовать личные данные, то стоит найти официальный номер банка и проверить с какого номера осуществляется звонок, если звонок осуществляется не

[5] Багин, И. А. Социальная инженерия: как защитить свои данные // Безопасность информации. — 2021. — № 2. — С. 45-50.

с официального номера банка, то стоит прекратить разговор, не сообщая никаких данных.

- Использование надежных паролей и двухфакторной аутентификации. Данный метод является универсальным, он позволяет предотвратить негативные последствия, даже в случае заполучения мошенником личных данных.

4. Несоблюдение мер безопасности пользователями.

Многие пользователи недооценивают необходимость базовых правил безопасности, из-за чего их данные нередко оказываются у третьих лиц.

Примеры несоблюдения правил безопасности в информационной среде:

- Слабые пароли. Пользователи, чтобы не забывать пароли, создают варианты, которые могут легко запомнить, например, дата рождения, 12345 и тп. Данные пароли легко угадать, чем пользуются мошенники.

- Использование одного пароля для нескольких аккаунтов. Пользователи могут применять один пароль к социальным сетям, банкам, госуслугам, из-за чего мошенники, заполучив пароль от чего-то одного, получают доступ ко всем данным человека.

- Невнимательность и безответственное отношение к личным данным. Некоторые пользователи входят в свою учетную запись на устройствах, к которым имеют доступ другие люди, например, работник на офисном компьютере входит в госуслуги и не выходит из своей учетной записи на постоянной основе, из-за чего другие работники, злоумышленники в том числе, могут заполучить данные и использовать их в своих целях.

Способы защиты от несоблюдений правил безопасности в информационной среде:

- Важно устанавливать сложные пароли. Сложность которых заключается в многообразии комбинаций букв, цифр и иных символов. Данный способ позволит защитить от простого подбора пароля мошенниками.

- Обновления программного обеспечения. Привлечение пользователей к регулярным обновлениям операционных систем и приложений, чтобы устранить уязвимости, это не позволит мошенникам заполучить личные данные.

Соблюдение этих мер поможет значительно снизить риски, связанные с мошенничеством, и повысить уровень безопасности личных данных пользователей Единого портала государственных и муниципальных услуг. Кроме госуслуг эти меры стоит применять и на других платформах, так как доступ к данным для входа госуслуги мошенники могут получить из других источников, принадлежащих пользователю.

[6]Выше были рассмотрены основные проблемы мошенничества при помощи «Госуслуг» и примеры предотвращения данных проблем. Систематизирую необходимые действия, которые будут являться путями противодействия мошенничеству:

1. Улучшение системы идентификации пользователей. Например, использованием двухфакторной аутентификации или использования биометрических данных.

2. Обучение пользователей. Например, создание ресурса с описанием видов мошенничества в целях предотвращения утечки личных данных.

3. Оптимизация технологической платформы. Например, постоянное обновление системы безопасности и программного обеспечения, а также постоянная смена паролей раз в определенный промежуток времени.

4. Создание механизма обратной связи. Например, создание источника, в который можно сообщать о подозрительных действиях, похожих на мошеннические схемы.

Мошенничество на Едином портале государственных и муниципальных услуг — это проблема, требующая комплексного подхода, которая требует решения в сжатые сроки. Улучшение мер безопасности, обучение граждан и эффективное

[6] Мошенничество в сети: проблемы и решения / Под ред. К. Л. Иванова. — М.: ОГИ, 2023. — 289 с.

сотрудничество с правоохранительными органами помогут сократить количество случаев мошенничества и повысить доверие к электронным услугам.

Библиографический список:

1. Апрелев, А. В., Сазонов, О. К. Мошенничество в интернете: методы и способы противодействия // Информационные технологии. — 2022. — Т. 15. — № 4. — С. 89–96.
2. Багин, И. А. Социальная инженерия: как защитить свои данные // Безопасность информации. — 2021. — № 2. — С. 45-50.
3. Беляев, И. П. Поддельные сайты и способы их распознавания // Современные тренды в кибербезопасности. — М.: Инфра-М, 2021. — С. 123–129.
4. Громова, Е. В., Дьяконова, Л. В. Электронные услуги и мошенничество: современное состояние и пути решения проблемы // Вестник государственного управления. — 2022. — Т. 10. — № 1. — С. 135–142.
5. Защита личных данных: практическое руководство / Под ред. А. Н. Петрова. — М.: Юрайт, 2020. — 256 с. // [электронный ресурс]. – Режим доступа – URL: https://urait.ru (дата обращения: 13.11.2024)
6. Квартанков, П. А., Ларин, И. Г. Актуальные проблемы в области кибербезопасности государственных порталов // Вестник информационных технологий. — 2020. — № 3. — С. 67-74.
7. Мошенничество в сети: проблемы и решения / Под ред. К. Л. Иванова. — М.: ОГИ, 2023. — 289 с.
8. Официальный сайт Единого портала государственных и муниципальных услуг. / [электронный ресурс]. – Режим доступа – URL: https://www.gosuslugi.ru (дата обращения: 5.11.2024).
9. Сайфулин, А. Р. Социальная инженерия: как защитить себя и свои данные // Cybersecurity Review. — 2022. — Т. 8. — № 3. — С. 207–215.
10. Тихомиров, В. С. Защита информационных ресурсов: от теории к практике. — СПб.: Питер, 2023. — 312 с.

Оригинальность 81%