Танцура Анжелика Евгеньевна
студентка кафедры Экономической Безопасности
Санкт-Петербургского государственного
архитектурно-строительного университета, г. Санкт-Петербург

ПЕРСОНАЛЬНЫЕ ДАННЫЕ КАК ИНСТРУМЕНТ МОШЕННИЧЕСТВА: АНАЛИЗ УГРОЗ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Аннотация: Статья посвящена исследованию рисков, связанных с использованием персональных данных в мошеннических целях и их влияние на безопасность личности. Предметом исследования являются современные методы получения и использования личных данных, статистические сведения о преступлениях за 2022-2024 гг., а также существующие меры противодействия им, включая технические и правовые решения. Особое внимание уделено уязвимостям различных информационных систем, приводящим к утечкам и методам их минимизации.

Ключевые слова: персональные данные, мошенничество с данными, фишинг, утечка данных, экономическая безопасность.

Tantsura Anzhelika Evgenievna
student of the Department of Economic Security St. Petersburg State
University of Architecture and Civil Engineering St. Petersburg

PERSONAL DATA AS A TOOL OF FRAUD: ANALYSIS OF THREATS TO INDIVIDUAL ECONOMIC SECURITY

Abstract: The article investigates the risks associated with the use of personal data for fraudulent purposes and their impact on personal security. The study focuses on modern methods of obtaining and using personal data, crime statistics for 2022-

2024, and existing countermeasures including technical and legal solutions. Particular attention is paid to vulnerabilities in various information systems that lead to data leaks and methods for their minimization.

Keywords: personal data, data fraud, phishing, data breach, economic security.

Введение

Применение персональных данных в финансовой сфере, государственных услугах и цифровой коммерции, повышая удобство, создает риски несанкционированного доступа. Еникеева и Дурандина отмечают, что «активное обращение персональных данных в условиях цифровой экономики является необходимым и базовым условием динамичного развития технологии больших данных (BigData)» (2018, с.105). Однако цифровизация и накопление информации увеличивают вероятность злоупотреблений, что обусловливает необходимость разработки мер защиты.

Важно отметить, что проблема мошенничества с использованием персональных данных не является принципиально новой. Однако в последнее время она приобрела особую актуальность в связи с появлением новых технологий и методов, позволяющих злоумышленникам получать доступ к личной информации граждан и использовать ее в преступных целях. Известны случаи получения злоумышленниками доступа к персональным данным под предлогом оказания банковских или государственных услуг, проведения опросов или участия в акции [3].

Компрометация персональных данных создает серьезные угрозы для экономической безопасности личности, так как может привести к финансовым потерям, ухудшению кредитной истории, краже личных данных и другие негативные последствия. Особую опасность представляют атаки на централизованные базы данных государственных и коммерческих организаций, содержащие информацию о миллионах клиентов. В связи с этим, необходимо исследование методов получения персональных данных киберпреступниками,

анализ статистики инцидентов и разработка мер противодействия данным угрозам.

Результаты исследования

Фишинг остается одним из наиболее распространенных методов получения персональных данных, основанным на социальной инженерии. Данный способ предполагает создание поддельных веб-ресурсов и рассылку сообщений, имитирующих официальные коммуникации банков, государственных сервисов и коммерческих организаций. Особую актуальность приобрели схемы, эксплуатирующие доверие к порталу «Госуслуги» - связанные с функционалом самозапрета на кредиты [3].

Типичная схема предполагает следующие этапы:

1. Инициацию контакта под видом сотрудников «Госуслуг» с сообщением об ошибке в оформленном самозапрете;
2. Перенаправление жертвы на фишинговый ресурс для «исправления данных»;
3. Кражу учетных данных и последующее их использование для финансовых операций.

Эффективность подобных схем обусловлена:

- высоким уровнем доверия к государственным сервисам;
- эксплуатацией актуальных и социально значимых тем;
- применение техник психологического давления на жертву.

В последнее время так же наблюдается рост биометрического спуфинга – метода мошенничества, при котором злоумышленники получают доступ к финансовым и государственным сервисам путем кражи цифрового образа лица и голоса жертвы [4]. В данной схеме:

1. На смартфон жертвы поступает видеозвонок через мессенджеры с подменного номера банка;
2. Лжесотрудник просит включить камеру под предлогом идентификации;

3. Во время видеозвонка происходит запись биометрических данных лица и голоса жертвы.

   Полученные биометрические данные используются для:

- Входа в личные кабинеты банков;
- Получения доступа к дистанционным платежным системам;
- Авторизации на портале «Госуслуги».

Эффективность данного метода, как и в случае с фишингом, обусловлена тремя ключевыми факторами: доверием к официальным организациям, использованием актуальных технологий аутентификации и систематическим психологическим давлением на жертву.

Помимо описанных методов, злоумышленники активно эксплуатируют уязвимости в системах хранения данных организаций. Крупномасштабные утечки из корпоративных баз (ритейл, медучреждения, госорганы) создают риски вторичного использования информации для целевых атак на граждан.

В 2022-2024 гг. масштабы утечек персональных данных достигли критических показателей, при этом наблюдается парадоксальная ситуация: при снижении количества инцидентов объемы скомпрометированных данных продолжают расти (рисунок 1).

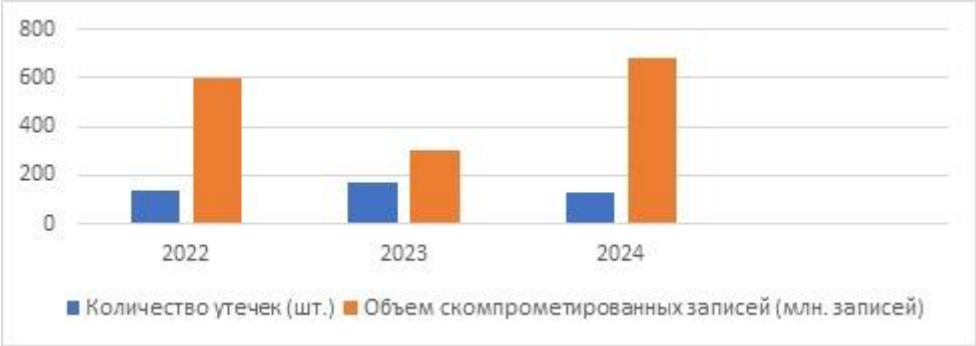

Рисунок 1. Динамика утечек персональных данных (2022-2024 гг.)

Согласно данным Роскомнадзора и ТАСС, в 2022 году зафиксировано 140 утечек (600 млн. записей), в 2023 – 168 (300 млн. записей) [6]. За 11 месяцев 2024 года выявлено 127 инцидентов с рекордными 680 млн.

скомпрометированных записей [7]. Особую тревогу вызывает увеличение среднего объема данных при каждой утечке. В ноябре 2024 года принят закон, ужесточающий ответственность за подобные нарушения [1].

Для минимизации рисков утечек и мошенничества с персональными данными требуется комплекс мер:

- **Технические решения** включают внедрение многофакторной аутентификации в банковских сервисах, использование биометрических технологий распознавания «живого» лица для предотвращения подмены, а также автоматический мониторинг и блокировку фишинговых ресурсов.
- **Правовое регулирование** предполагает ужесточение ответственности за утечки данных, введение обязательных стандартов защиты для организаций и усиление надзора за обработкой персональных данных.
- **Образовательные инициативы** должны охватывать программы повышения цифровой грамотности, в том числе специализированные уроки безопасности для школьников и информационные компании для уязвимых групп населения.

В целях реализации указанных мер Роскомнадзором принимаются активные действия. В частности, в нормативно-правовой сфере введены оборотные штрафы за повторные случаи утечек персональных данных [1] (Федеральный закон № 420-ФЗ, вступает в силу с 30.05.2025). В образовательной области организованы и проведены обучающие мероприятия, охватившие в первом квартале 2024 года более 400 тысяч школьников [5].

Заключение

Исследование выявило устойчивый рост мошенничества с использованием персональных данных, преимущественно через фишинговые схемы и биометрический спуфинг. Статистические данные за 2022-2024 годы демонстрируют увеличение объемов компрометируемой информации, что подчеркивает необходимость совершенствования защитных механизмов. Наиболее перспективными направлениями противодействия следует считать

техническую модернизацию систем защиты, законодательные инициативы и массовое обучение киберграмотности.

Литература

1. Федеральный закон от 30.11.2024 № 420-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях" // Собрание законодательства РФ. 2024. № 48. Ст. 7411.
2. Еникеева Л.А., Дурандина А.П. Организация защиты персональных данных в банковских информационных системах Российской Федерации // Петербургский экономический журнал. 2018. № 4. С. 102-119. EDN YRYDAD.
3. Ильина Н., Грачев Е., Каледина А. Не дать взять: мошенники используют самозапрет на кредиты для обмана [Электронный ресурс] // Известия. 2025. URL: https://iz.ru/1852436/natala-ilina-evgenii-gracev-anna-kaledina/ne-dat-vzat-mosenniki-ispolzuut-samozapret-na-kredity-dla-obmana (дата обращения: 14.05.2025).
4. Калугин Д. Мошенники научились красть биометрию: в опасности каждый, у кого есть смартфон [Электронный ресурс] // Выберу.ру. 2024. URL: https://www.vbr.ru/banki/novosti/2024/03/20/opasnie-videozvonki-mosenniki/ (дата обращения: 14.05.2025).
5. Более 400 тысяч школьников прошли обучающие мероприятия Роскомнадзора по защите персональных данных в I квартале 2024 года [Электронный ресурс] // Роскомнадзор. 2024. URL: https://rkn.gov.ru/press/news/news74829.htm (дата обращения: 14.05.2025).
6. В 2023 году в сеть утекло более 300 млн записей о россиянах [Электронный ресурс] // Информационное агентство ТАСС. 2024. URL: https://tass.ru/obschestvo/19693845 (дата обращения: 14.05.2025).

7. Общественный совет подвел итоги работы в 2024 году [Электронный ресурс] // Роскомнадзор. 2025. URL: https://rkn.gov.ru/press/news/news74894.htm (дата обращения: 14.05.2025).