УДК 336.719

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСАХ

Е. С. Шейман[1)], К. Д. Руднец[2)]

[1)] *студент, Белорусский государственный университет, г. Минск, Беларусь, sheyman.yevgeniya@bk.ru*
[2)] *студент, Белорусский государственный университет, г. Минск, Беларусь, ksusha.rudnets@gmail.ru*

Научный руководитель: **Н. И. Шандора**

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, shandoranatasha@tut.by

Статья посвящена актуальным угрозам и рискам, с которыми сталкиваются финансовые учреждения в цифровой экономике; анализируется роль человеческого фактора в уязвимости систем финансового сектора; предлагаются меры предосторожности и защиты данных, которые могут быть приняты. В статье также рассматриваются меры регулирования кибербезопасности финансового сектора в Республике Беларусь, делается вывод о важности кибербезопасности в современном мире.

Ключевые слова: кибербезопасность; киберугрозы; защита информации; информационная безопасность; финансовый сектор; фишинг; DDoS.

INFORMATION SECURITY IN FINANCE

E. S. Sheiman[1)], K. D. Rudnets[2)]

[1)] *student, Belarusian State University, Minsk, Belarus, sheyman.yevgeniya@bk.ru*
[2)] *student, Belarusian State University, Minsk, Belarus, ksusha.rudnets@gmail.ru*

Supervisor: **N. I. Shandora**

senior lecturer, Belarusian State University, Minsk, Belarus, shandoranatasha@tut.by

The article is devoted to the current threats and risks faced by financial institutions in the digital economy; analyzes the role of the human factor in the vulnerability of financial sector systems; suggests precautions and data protection measures that can be taken. The article also discusses measures to regulate the cybersecurity of the financial sector in the Republic of Belarus, and concludes that cybersecurity is important in the modern world.

Keywords: cybersecurity; cyber threats; information protection; information security; financial sector; phishing; DDoS.

В условиях цифровой эпохи финансовый сектор становится ключевой целью для киберугроз, что объясняется его экономическим значением и конфиденциальностью обрабатываемой информации. Возникновение интернет-банкинга, цифровых платежей и других инноваций в области финансовых технологий изменило восприятие удобства и доступности для клиентов по всему миру. Тем не менее, данная цифровая трансформация также привела к появлению новых уязвимостей, которые активно используют киберпреступники.

Основными киберугрозами для финансового сектора являются атаки программ-вымогателей, фишинг и социальная инженерия, DDoS-атаки, уязвимость на сетевом периметре, атаки на цепочку поставок. Атаки программ-вымогателей могут привести к шифрованию данных и требованию выкупа за их восстановление. Атаки типа «отказ в обслуживании» (DDoS) направлены на перегрузку серверов и сетевой инфраструктуры, что может привести к временной недоступности онлайн-сервисов. [1].

Кибератаки на финансовый сектор имеют серьезные последствия, которые могут затронуть как отдельные организации, так и экономическую систему в целом. Основными последствиями могут быть: утечка конфиденциальной информации, прекращение работы критически важных сервисов и бизнес-процессов, значительные финансовые потери как для организаций, так и для клиентов, потеря доверия клиентов к финансовым учреждениям, дестабилизация всей финансовой системы.

Большинство утечек включает в себя персональные данные клиентов и коммерческую информацию компаний. Кроме того, в таких утечках часто встречаются номера платежных карт и учетные данные, а также медицинская информация из страховых компаний (рис. 1).

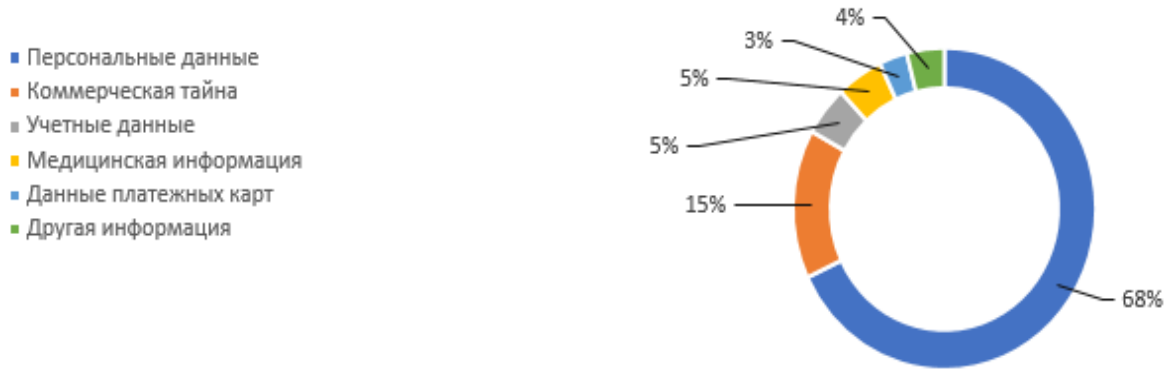

Рис. 1. Типы украденных данных в успешных атаках на финансовые организации. Источник: [2]

Треть проанализированных объявлений (36 %) не привязанных к конкретным регионам, указывает на безразличие преступников к местополо-

жению жертвы. Тем не менее, большинство объявлений о продаже или покупке товаров и услуг содержат запросы или указания на определённый регион. Россия и страны СНГ занимают ведущие позиции в этом контексте, что связано с особенно напряжённой геополитической ситуацией, находящей своё отражение и в киберпространстве (рис. 2).

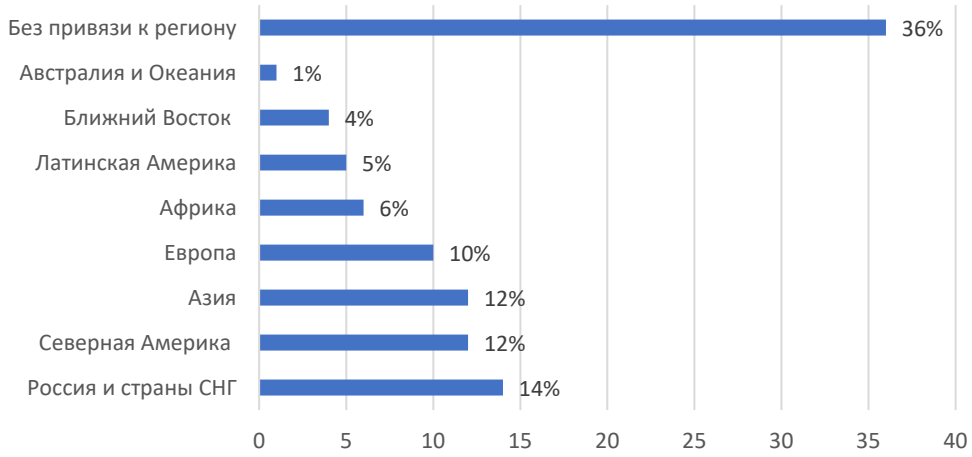

Рис. 2. Распределение сообщений на теневых площадках по географии скомпрометированных организаций.
Источник: [2]

В Республике Беларусь Концепция информационной безопасности воспринимается как национальный приоритет и важная задача для всего государства. Актуальность данной Концепции обусловлена возрастающей ролью информационного общества в социально-экономическом развитии, необходимостью защиты национальных интересов в сфере информации, потребностью информирования граждан о подходах Республики Беларусь к вопросам информационной безопасности и приоритетах ее обеспечения, а также интеграцией Беларуси в международную систему информационной безопасности [3].

В Беларуси кибербезопасность финансового сектора регулируется рядом законодательных актов, среди которых ключевую роль играет Указ № 40 «О кибербезопасности (14.02.2023). В Указе детализируются задачи и функции, направленные на обеспечение кибербезопасности государственных органов и организаций, включая финансовые учреждения, а также подчеркивается значимость защиты критически важных объектов информатизации. Этот документ является частью Концепции национальной безопасности и направлен на реализацию её положений в сфере киберзащиты [4].

Кроме Указа № 40, важную роль в регулировании кибербезопасности в финансовом секторе играют следующие документы: Банковский кодекс

Республики Беларусь (25.10.2000); Концепция обеспечения кибербезопасности в банковской сфере (20.11.2019), Концепция информационной безопасности Республики Беларусь (18.03.2019).

Государство установило ряд задач и мероприятий, направленных на обеспечение информационной безопасности. На уровне государства осуществляется мониторинг, анализ и оценка состояния информационной безопасности. Гарантируется конституционное право граждан на защиту персональных данных. С целью повышения устойчивости государственного сектора к информационным рискам внедряются современные технологии [5].

С появлением новых технологий наблюдается прогресс, но также появляется все больше угроз. Финансовый сектор одна из самых уязвимых целей киберпреступников. Информационная безопасность финансовой сферы может привести к огромному ущербу экономики страны. Поэтому важно выстроить эффективные стратегии защиты данного сектора.

Библиографические ссылки

1. Кибербезопасность в финансовом секторе [Электронный ресурс] // Smartgopro : сайт. URL: https://smartgopro.com/novosti2/cybersecurity_financial_sector/ (дата обращения: 25.09.2024).

2. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года [Электронный ресурс] // Positive technologies: сайт. URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (дата обращения: 25.09.2024).

3. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь: сайт. URL: https://pravo.by/document/?guid=3871&p0=P219s0001 (дата обращения: 25.09.2024).

4. Указ № 40 от 14 февраля 2023 г. О кибербезопасности [Электронный ресурс] // Официальный Интернет-портал Президента Республики Беларусь: сайт. URL: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g (дата обращения: 25.09.2024).

5. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь: сайт. URL: https://pravo.by/document/?guid=3871&p0=P219s0001 (дата обращения: 25.09.2024).