УДК 336

СОВРЕМЕННЫЕ КИБЕРРИСКИ ФИНАНСОВОЙ СИСТЕМЫ

А.С. Карульская, Е.Д. Кучинская, 3 курс
Научный консультант – **О.А. Кукса**, к.э.н., доцент
Полесский государственный университет

Финансовая система сталкивается с различными рисками, которые могут оказать существенное воздействие на финансовые институты, рынки и экономику в целом.

Сердюкова Д.Е. отмечала, что риск в финансовой сфере – это риск потери или получения доходов, обусловленные действием как макроэкономических (экзогенных), так и внутрифирменных (эндогенных) факторов и условий [1]. В свою очередь Балабанов И.Т., Лобанова Л.Н. подразуме-

вали под риском вероятность наступления ущерба в результате проведения операций в финансово-кредитной и биржевой сферах, т.е. риска, вытекающего из самой природы этих рисков [2].

Бурное развитие информационных и цифровых технологий отразилось на всех отраслях экономики, но особенно сильное влияние оно оказало на сектор кредитно-финансовых услуг. Инновационные финансовые технологии коренным образом меняют традиционные бизнес-модели, спектр финансовых услуг и продуктов, способ взаимодействия финансовых посредников с клиентами, механизмы осуществления платёжных и других операций и т.д.

Риски подразделяются на классические и альтернативные. Классические риски в финансовой системе включают такие аспекты как:

- кредитный риск;
- рыночный риск;
- операционный риск;
- риск ликвидности;
- фондовый риск;
- валютный риск и др.

Альтернативные риски могут включать в себя: управленческий риск; транспортный риск; имущественный риск; экологический риск; ряд других нестандартных рисков, которые могут оказать влияние на финансовую систему.

Оба вида рисков играют важную роль в финансовой системе и требуют внимательного управления со стороны финансовых институтов и регуляторов.

Однако в настоящее время на первый план выходят киберриски. В рейтинге глобальных рисков Всемирного экономического форума проблема киберпреступности входит в первую пятёрку. Киберугрозы постоянно развиваются, по мере того как киберпреступность приобретает всё более сложный и транснациональный характер.

Количество успешных кибератак в финансовом секторе год от года растет. Среди киберугроз, которым подвергается финансовый сектор, основными являются кража учётных данных и личных данных учреждений и их клиентов; манипулирование похищенными из финансовых учреждений данными для получения финансовой или политической выгоды, что дестабилизирует финансовые системы и рынки; деструктивные вредоносные программы, то есть программное обеспечение, разработанное с целью нанесения урона отдельному компьютеру или целой сети, серверу; совершенствование методов кибертерроризма по мере развития новых технологий; дезинформация, которая широко применяется в ходе целевых многоэтапных атак на финансовые учреждения и рынки.

Подавляющее большинство утечек содержат персональные данные клиентов и коммерческую информацию организаций. Кроме того, среди утечек нередко можно обнаружить номера платежных карт и учетные данные, в утечках страховых компаний присутствует медицинская информация (Рисунок).

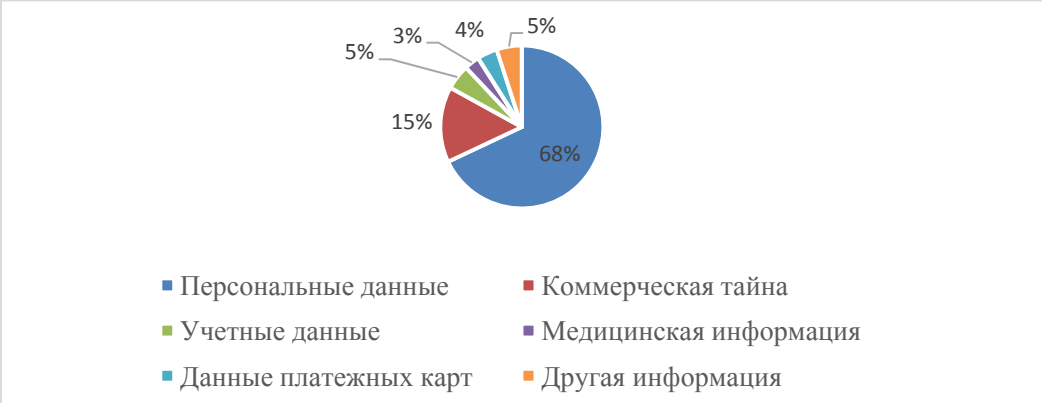

Рисунок – Типы украденных данных в успешных атаках на финансовые организации за 2023 год

Примечание –Источник [3]

Согласно глобальному индексу кибербезопасности (Global Cybersecurity Index, далее – GCI), отражающему степень готовности стран к кибератакам, среди рассматриваемых 184 стран мира по

итогам 2020 года Беларусь заняла 89 место – первая половина рейтинга, при этом возглавили данный рейтинг США. Последнее место в рейтинге занимает Йемен [4].

Республика Беларусь уделяет большое внимание вопросам безопасности в киберпространстве, в том числе в контексте противодействия террористическим угрозам. В рамках реализации мер по защите информации и кибербезопасности в Республике Беларусь в августе 2018 г. в структуре Национального банка Республики Беларусь был создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERTby) [5]. В свою очередь, представители банковских учреждений выразили готовность сотрудничать и поддерживать функционирование FinCERT в нашей стране, пожелав автоматизировать процесс обмена данными об угрозах, что позволит скоординировать обмен информацией Центра, правоохранительных органов и банков, осуществлять в реальном времени анализ данных о фактах компьютерных атак в финансовых организациях и подготовку аналитических материалов, устанавливать рекомендации (стандарты) в области обеспечения защиты информации при осуществлении банковской деятельности. От информационной безопасности банка зависят его репутация и конкурентоспособность. Высокий уровень обеспечения информационной безопасности кредитной организации позволяет минимизировать риски [6].

Беларусь поддержала инициативу Российской Федерации о создании новой Рабочей группы открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих ИКТ на 2021-2025 годы в соответствии с резолюцией ГА ООН 75/240 и принимает активное участие в ее работе. Беларусь стала соавтором принятой в мае 2021 г. по инициативе России резолюции ГА ООН 75/282 «О противодействии использованию информационных и коммуникационных технологий в преступных целях», которая определила модальности работы специального комитета для разработки под эгидой ООН универсальной международной конвенции по борьбе с использованием ИКТ в преступных целях. Белорусская сторона принимает активное участие в сессиях данного переговорного органа [8].

Таким образом, с развитием информационных технологий в мире наблюдается рост рисков, связанных с информационной безопасностью, и киберрисков. Существенные риски современных организаций возникают в киберпространстве, а их последствия могут оказывать прямое влияние на финансовую и хозяйственную деятельность. При этом наблюдается значительный рост сумм ущерба от киберинцидентов, в глобальном масштабе исчисляемых миллионами долларов. Это потребовало интеграции международного законодательства с законодательством разных стран с целью выработки единых мер по противодействию киберрискам. Требуется комплексный подход к оценке рисков, который позволяет точечно и осознанно подходить к инвестициям, связанным с вложениями в информационную безопасность, как в Республике Беларусь, так и в финансово-банковской сфере. Особое внимание следует уделять критически важным сегментам. Интеграция киберриска в систему оценки банками всех рисков, авторский подход к методологии оценки банковских рисков углубят банковскую методологию оценки рисков и позволят банкам более осознанно подходить к возникающим угрозам и оценивать киберриски не только на стадии инцидентов, но и осуществлять прогнозную оценку кибератак и управлять предстоящими финансовыми вложениями в информационную защищенность банков.

Список использованных источников

1. Ильин, В. В. Системный подход к оценке финансовых рисков / В. В. Ильин, Н. А. Сердюкова // Финансы. − 2014. − № 1. − С. 68-72.

2. Балабанов, И. Т. Риск-менеджмент. /И.Т.Балабанов - М.: Финансы и статистика, 2010. – 312с.

3. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года: [https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023].

4. Global Cybersecurity Index 2020: [https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf].

5. О ходе реализации стратегического проекта Национального банка «Создание системы мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере (FinCERT)» : [http://www.nbrb.by/bv/articles/10561.pdf].

6. Итоговый документ XV Международного форума по банковским информационным технологиям «БанкИТ’2018» : [http://www.nbrb.by/bv/articles/10585.pdf].

7. Международная информационная безопасность: [https://www.mfa.gov.by/mulateral/global_issues/inform/].