УДК 336.7

ПОВЫШЕНИЕ УРОВНЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКИХ БАНКОВ ЦИФРОВЫМИ ИНСТРУМЕНТАМИ

А. Ф. Спиридонова

студентка экономического факультета, Пермский государственный национальный исследовательский университет, г. Пермь, Россия, e-mail: asya4296@yandex.ru

Научный руководитель: **А. В. Бобков**

кандидат экономических наук, доцент, кафедры предпринимательства и экономической безопасности, Пермский государственный национальный исследовательский университет, г. Пермь, Россия, e-mail: bobkovav@yandex.ru

Актуальность исследования подтверждается ростом киберпреступлений, за январь-март 2023 года мошенниками проведено 252,1 тыс. операций с общим объемом 4,5 млрд руб, что на 30 % выше, чем в 2022. В статье рассмотрены основные инструменты, структура и виды преступлений в банковском секторе с использованием информационных технологий за 2018–2022 года, проведен анализ компьютерных систем, отслеживающих отклонения и подозрительные операции, а также предложены цифровые решения, которые позволят снизить количество мошеннических операций в банковском секторе и представлен эффект от их внедрения.

Ключевые слова: кибербезопасность; банковская система; банкинг; ущерб; Банк России; социальный инжиниринг.

INCREASING THE LEVEL OF FINANCIAL SECURITY OF COMMERCIAL BANKS WITH DIGITAL TOOLS

A. F. Spiridonova

Student of the Faculty of Economics, Perm State National Research University, Perm, Russia, e-mail: asya4296@yandex.ru

Supervisor: **A. V. Bobkov**

PhD in Economics, Associate Professor, Department of Entrepreneurship and Economic Security, Perm State National Research University, Perm, Russia, e-mail: bobkovav@yandex.ru

The relevance of the study is confirmed by the growth of cybercrime, in January-March 2023, fraudsters conducted 252.1 thousand transactions with a total volume of 4.5 billion rubles, which is 30 % higher than in 2022. The article considers the main tools, structure and types of crimes in the banking sector using information technology for 2018–2022, analyzes computer systems that track deviations and suspicious transactions, and

proposes digital solutions that will reduce the number of fraudulent transactions in the banking sector and presents the effect of their implementation.

Keywords: cybersecurity; banking system; banking; damage; Bank of Russia; social engineering.

В банковской системе РФ ежегодно меняется статистика общего количества реализованных киберугроз и постоянно повышается объем потерь от киберпреступлений. За 2022 год сумма потерь от кибератак составила 14 165, 44 млн рублей, (на 30,9 % выше, чем в 2020 года) за счет роста расходов на восстановление имиджа и функционирование банковских учреждений, а также выплат убытков причиненных клиентам банков для возвращения доверия населения к банковской системы на прежний уровень. Увеличение объемов потерь объясняется атаками со стороны недружественных государств для дестабилизации банковской системы, а также за счет дискредитации топ-менеджеров крупнейших банков (табл. 1).

Таблица 1

Показатели киберугроз банковской системы РФ с 2017–2022 гг.

Показатели	2017	2018	2019	2020	2021	2022
1. Количество реализованных киберугроз на субъекты банковской системы, ед.	514	687	1723	773	1035	876
1.1 Коммерческие банки II уровня	407	488	879	580	598	528
1.2 НКФО	97	181	811	175	414	298
2. Объем потерь от реализованных киберугроз, млн руб.	961,3	1384,7	5723,5	9783,1	13582,2	14165,4
2.1 Убытки, причиненные клиентам банковских организаций	541	779	3219	6801	10032	10615
2.2 Расходы на восстановление нормального функционирования банков после атак	301	411	1 987	2 342	1 926	2 032
2.3 Непрямые убытки и потери	120	195	518	640	1 624	1518

Стоит отметить низкий удельный вес отраженных атак от киберугроз в банковском секторе и тенденцию снижения уровня возмещения потерь средств клиентов, что говорит о недостаточности мероприятий, применяемых для защиты данных и по обнаружению недостатков банковской защиты. Систематизирующие банки обладают высоким уровнем устойчивости к кибератакам в банковском секторе. Клиенты коммерческих банков наиболее подвержены атакам, за счет размещения персональных данных при открытии счетов и низкой финансовой грамотности населения. Тенденция снижения прослеживается у НКФО за счет высокого объема оборота денежных средств и использования ими дешевых операционных систем, а также низкоэффективных программ защиты, что порождает высокую привлекательность для кибермошенников (табл. 2).

Таблица 2

Показатели банковской безопасности с 2016 по 2022 года

Показатели	2016	2017	2018	2019	2020	2021	2022
1 Удельный вес отраженных атак, в % к итогу	39,5	42,4	44,7	49,5	52,7	49,4	47,3
2 Уровень возмещения потерь средств клиентов	18,3	17,2	16,2	15,0	11,3	6,8	5,7
Индекс киберустойчивости банковского сектора:							
1 Банк России	-	1,0	2,0	4,0	-	…	…..
2 Системообразующие банки	7,9	7,2	6,8	8,0	7,7	6,4	5,8
3 Коммерческие банки II уровня	5,5	4,7	4,9	4,5	3,4	3,9	3,5
4 НКФО	6,2	5,8	5,5	4,9	4,1	3,5	3,2

Объекты инфраструктуры банковского сектора на протяжении 5 лет выступают привлекательным объектом внимания хакеров (составляя 70 % в 2022 году). Вторым по доле в общей структуре объектов, подвергающихся кибератакам выступают Web-ресурсы банков, в том числе интернет банкинг (показатель увеличился на 15 % с 2019 года), в котором хранятся данные и финансовые инструменты банковских клиентов. Популярными инструментами совершения кибератак выступают хакинг (рост с 2019 составил 18 %), использование уязвимостей инфраструктуры и ПО (рост с 2020 года составил 11 %), сохраняется высокая доля использования социальной инженерии (с 2018 года на 9 % составив 20 %). Также стоит отметить постоянную модернизацию форм мошенничества (в том числе телефонное мошенничество, спам рассылки), которая не позволяет своевременно реагировать на атаки. (рис. 1, 2).

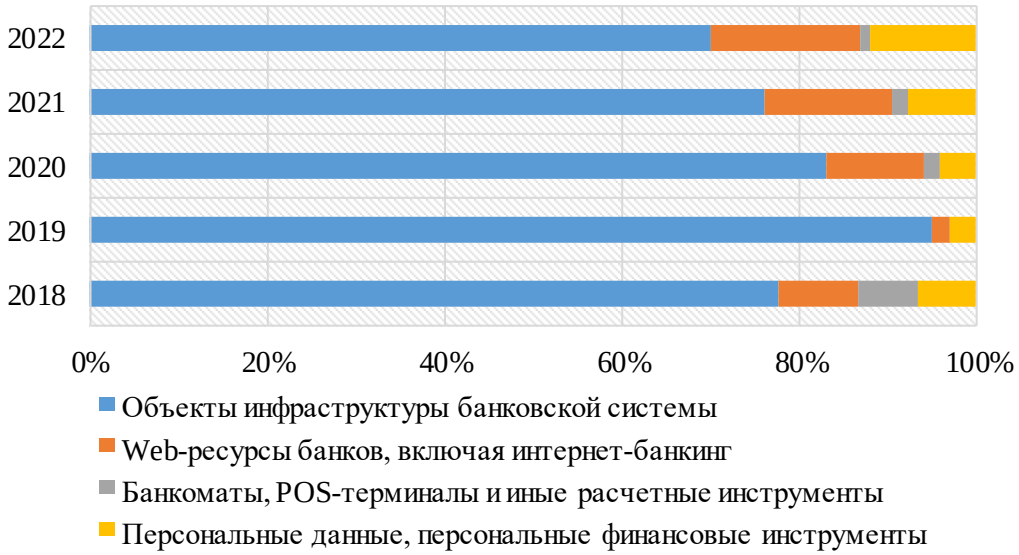

Рис. 1. Инфраструктурные объекты банковской системы, повергающиеся атакам кибермошенников в 2018–2022 гг., в %

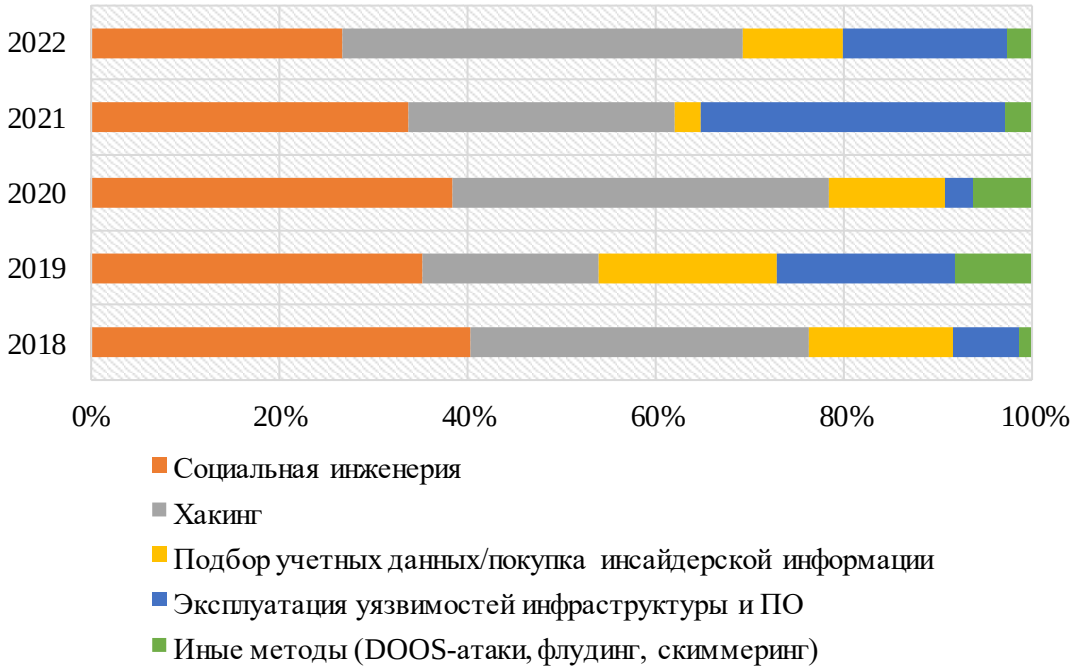

Рис. 2. Структура механизмов атак в банковском секторе в 2018–2022 гг., %

Банк России проводит действенную политику в области информационной безопасности и кибербезопасности – проводит мониторинг показателей финансовых потерь. Указом Президента от 07.05.2018 принят ряд мероприятий, направленных на повышение уровня кибербезопасности банковских учреждений:

1) обязанность банков предоставлять финансовый ущерб после совершенных кибератак (за первый квартал 2023 года банковские учреждения отразили 2,7 млн прецедентов мошенничества на сумму размером 712 млрд. руб, направленных на данные клиентов);

2) введен ГОСТ по информационной безопасности для ужесточения контроля над процессами и событиями в банках для раннего обнаружения нарушений;

3) создана специфическая характеристика кредитных организаций «риск профиль», по оценке уровня возможных информационных угроз, включающая в себя показатель вероятности возникновения проблем у банков из-за несоблюдения норм;

4) Банк России проводит мониторинг подозрительных и опасных операций (за 2022 год заблокировано 750 тыс. телефонных номеров мошенников (360 тыс. план), 23 приложения (12 план), 1,9 тыс. страниц в социальных сетях (2,3 тыс. план). 10716 доменов направлено в Генеральную Прокуратуру для ограничения доступа (11,9 тыс. план);

5) используется система SIEM при анализе расчётов клиента обнаруживает несогласованность и предупреждает сообщением о необходи-

мости блокировки карты, которая не способна бороться с угрозами, она анализирует и выявляет отклонения от норм;

6) с 2003 года игроком на рынке киберпреступлений выступает Group-IB, которая расследует хищение средств с помощью вирусов для мобильных телефонов, а также DDoS-атак. (за 2022 год системой выявлено 18000 фишинговых сайтов, что на 15% выше, чем в 2021).

Тем не менее, далеко не все показатели достигли плановых значений. Примененные мероприятия позволяют отслеживать точное количество совершенных атак и их объем, а также принимать быстрые решения и реагировать на новые виды мошенничества. Для повышения уровня киберустойчивости банковской системы целесообразно осуществить следующие мероприятия:

1) разработать Банку России и систематизирующим банкам национальную линию информационной безопасности, которая позволит создать единообразную систему защиты от киберпреступников и снизить затраты на подключение частных систем безопасности;

2) разработать Банку России, ГК «Ростеху» инфраструктурное решения для испытания финансовых продуктов, обнаружения неточностей и новых методов борьбы с кибератаками, мера поможет отработать план действий при вариативности способов совершения киберпреступлений;

3) создать межбанковский реестр счетов мошенников для сокращения вариативности вывода денежных средств за рубеж и повышения прозрачности и обнаружения сомнительных транзакций, что позволит системам блокировать транзакции незамедлительно;

4) внедрять в банковский сектор системы отслеживания кибератак: AntiFraudSuite, Nice Actimize и RSA, данная мера способствует обнаружению хакерских атак на ранних стадиях входа в систему.

Предложенные мероприятия имеют практическую значимость и применимость в целях уменьшения количества кибератак в банковском секторе и объемов потерь денежных средств при полномерном использовании новых информационных систем для повышения экономической безопасности банковского сектора.

Библиографические ссылки

1. Инциденты информационной безопасности: итоги I квартала 2023 года [Электронный ресурс]. URL: cbr.ru (дата обращения: 15.09.2023).

2. Ежегодный аналитический отчет Банка России. [Электронный ресурс] // URL: https://cbr.ru/Collection/Collection/File/43872/ar_2022.pdf (дата обращения: 15.09.2023).

3. *Лужнова Л. А.* Защита прав и законных интересов потребителей банковских услуг как фактор повышения их финансовой безопасности [Электронный ресурс] // Банковские услуги. 2022. № 9. С. 22–27. URL: https://doi.org/10.36992/2075-1915_2022_9_22 (дата обращения: 15.09.2023).