**Индекс УДК/ББК**

**Форгунова А.Ю.**

**Щелканов А.А.**

**Применение мер по обеспечению информационной безопасности банковского сектора в области добывающей промышленности**

**Аннотация**. *Для обеспечения экономической безопасности, банки противостоят кибератакам, что актуально и для предприятий реального сектора экономики. В статье рассматриваются виды кибератак и подверженные им объекты, проведен анализ динамики несанкционированных операций и способы противостояния.*

**Ключевые слова:** *информационная безопасность,**кибербезопасность, банковский сектор, добывающая и перерабатывающая промышленность, киберриски.*

**Введение**. Концентрация участников рынка диктует условия конкурентной борьбы за потенциальных клиентов и контрагентов. Ведение деятельности подразумевает наличие коммерческой тайны и неразглашения технологий, разработок в интересах бизнеса. Внедрение новых продуктов и бизнес-процессов все больше зависит от информационных технологий. Нарушение работоспособности систем, внедрение вредоносных программ, компрометация информации и получение несанкционированного доступа имеет значительные последствия как для прибыльности бизнеса, его репутации, доверия контрагентов[1].

Использование программных сервисов в сети Интернет и коммуникационных технологий, а также действий пользователей формирует единую виртуальную среду – киберпространство. Киберпространство наполнено электронными средствами платежа, облаками, виртуальными посольствами, развлечениями, деньгами и преступлениями. Понятие кибербезопасности неразрывно связано с информационной безопасностью, безопасностью сети Интернет и информационной инфраструктурой и кибератаками. Информационные и программные средства и процессы, участвующие в обеспечении функционирования приложений определяют уровень его безопасности [2]. Неразрешенная, преднамеренная попытка и эксплуатация компьютерных систем, технологических предприятий и сетей и представляет собой кибератаку.

Регулярное отслеживание и изучение новых видов кибератак и инструментов, применяемых злоумышленниками, позволяет более эффективно противостоять угрозам.

По показателям трех кварталов 2019 года, на финансовые организации была совершена 61 атака, в 2018 году – 92. В локальную сеть финансовых организаций злоумышленники проникали с использованием фишинга (74%) и вредоносного программного обеспечения (80%) [3].

Общее количество транзакций, совершенных без согласия клиентов физических и юридических лиц с применением электронных средств платежа, в 2019 году составило порядка 576 тысяч единиц на сумму 6,4 млрд. рублей. 69% от общего объема несанкционированных операций были совершены с использованием методов социальной инженерии, то есть клиентов побуждали самостоятельно проводить транзакции обманывая их и злоупотребляя доверием. Возмещение по таким транзакциям, банками составило 935 млн. руб. или 14,55% от общей суммы.

Мошеннические действия в отношении операций физических лиц с использованием электронных средств платежа можно разделить на совершенные через: банкоматные и терминальные сети банков, импринтеры; CNP-транзакции или операции по оплате товаров и услуг в сети Интернет; системы дистанционного банковского обслуживания.

В отношении банковских карт, все чаше наблюдается тенденция к хищению и продаже текстовых данных, этому способствует распространение JS-снифферов, которым в свою очередь уступают даже банковские трояны. Для стран, в которых не распространена система 3D Secure, данная угроза будет актуальна [4].

Наибольшая доля применения методов социальной инженерии в целях хищения средств физических лиц, относится к операциям систем дистанционного банковского обслуживания – около 88,9%. Для мошенников наибольший интерес к получению доступа к системам ДБО объясняется возможностью завладеть большим объемов средств на счетах клиента. Объем ущерба клиентов составил 2227 млн. руб., возмещение банками составило порядка 7% или 162,3 млн. руб.

Большая часть мошеннических операций в отношении физических лиц территориально относится к Центральному федеральному округу (рис. 1). Эта особенность объясняется развитием инфраструктуры регионов, а соответственно и уровнем обеспечения населения финансовыми услугами.

Рисунок 1. Количество и объем переводов денежных средств без согласия клиента физического лица по месту совершения операции (без учета Московского округа) за 2019 год, тыс. руб., ед. [5].

По операциям клиентов юридических лиц в 2019 году было сообщено о 4609 транзакций без согласия клиента. Общая сумма хищения составила 701 млн. руб., банками было возмещено клиентам корпоративного сектора около 10% или 65 млн. руб. Лишь 16% от общего объема мошеннических операций было совершено с применением социальной инженерии. Остальная часть относится к операциям по получению доступа к системам дистанционного банковского обслуживания клиентов, с применением вирусного программного обеспечения.

Информация о несанкционированных операциях, территориально, приводится в зависимости от места ведения расчетного счета, то есть места обращения клиента юридического лица в обслуживающий банк (рис.2).

Рисунок 2. Количество и объем переводов денежных средств без согласия клиента юридического лица по месту совершения операции (без учета Московского округа) за 2019 год, тыс. руб., ед. [6]

Наибольшее количество операций по счетам юридических лиц, без их согласия, сосредоточенно в Центральном федеральном округе. Данная тенденция объясняется повышенным интересов злоумышленников к хищению с использованием систем ДБО корпоративных клиентов, их территориальной концентрацией.

**Выводы**

По-прежнему использование вредоносного программного обеспечения, фишинига и социальной инженерии является основными способами получения несанкционированного доступа к информации пользователей. Проблема невозможности обеспечения собственной информационной безопасности все еще актуальна среди пользователей. Большинство интернет-сервисов используют двойную аутентификацию при предоставлении доступа пользователей к их аккаунтам, что позволяет сокращать количество атак.

В 3 квартале 2019 года, 64% составили атаки с целью получения данных клиентов физических лиц, из них 47% преследовали кражу данных интернет-сервисов, 23% - данные карт, 12% - персональные данные пользователей, остальные – доступ к личной переписке [7].

Согласно исследованию экспертов Positive Technologies, 92% веб-приложений не защищены от проведения атак на пользователей. Из-за недостатков безопасности сайтов, злоумышленники получают не только возможность контролировать веб-приложение, но и сервер, что позволяет распространять вредоносное программное обеспечение, использовать JavaScript-снифферы с целью доступа к конфиденциальным данным. Тенденция к увеличению интернет-трафика говорит о важности данной проблемы и необходимости ее решения.

Применение двухфазной аутентификации плательщика будет способствовать повышению безопасности банковских систем, карточных платежей и бесконтактной оплаты. Двухфазная аутентификация предполагает проверку двух из трех элементов (ПИН-код, отпечаток пальца, лицо и т.п.), например, после проведения нескольких бесконтактных платежей, необходимо вставить карту в считыватель чипа, а ввести ПИН или авторизоваться по отпечатку пальца.

Также для снижения количества мошеннических операций, необходимо повышать уровень квалификации сотрудников в области информационной безопасности, с целью обеспечения противодействия попыткам хищения информации, а также и электронных денежных средств.

В целях повышения эффективности производства, предприятия добывающей и перерабатывающей промышленности используют новейшие технологии. При разработке месторождений необходимо пристально следить за соблюдением экологических требований [15]. Отрасль энергетики не является исключением и также занимается разработками в области производства энергии без ущерба экологии. На сегодняшний день проблемы экологии и производства тесно взаимосвязаны и недостаточно изучены. Помимо соблюдения конфиденциальности производственных процессов, также тщательно необходимо относится и к любого рода разработкам. Новые технологии и разработки ведущих исследований являются объектом повышенной опасности с точки зрения хищения информации со стороны конкурентов. Источником доступа может стать как программное обеспечение, зараженное вирусными программами, так и хищение данных доступа к учетной записи, ПК, электронной почте. Не редко проблемой информационной безопасности становится человеческий фактор. В целях защиты коммерческой тайны предприятий целесообразно перенять опыт банковской сферы, поскольку он сопряжен с повышенным рисков из-за своей специфики.

**Библиографический список**

1. Цаплев, Д. Н. Особенности транзакционного подхода в анализе межбанковской конкуренции / Д. Н. Цаплев // Проблемы экономики и менеджмента. – 2016. – № 4 (8). – С. 80–90.

2. Бакулина А.А., Попова В.В. Влияние финтеха на безопасность банковского сектора // Экономика. Налоги. Право. 2018. №2. URL: [https://cyberleninka.ru/article/n/vliyanie-finteha-na-bezopasnost-bankovskogo sektora](https://cyberleninka.ru/article/n/vliyanie-finteha-na-bezopasnost-bankovskogo%20sektora) (дата обращения: 15.05.2020).

3. Учебник «Финансовая грамотность и массовая информация». Для деловой и общественно-политической журналистики. Предназначен для высших учебных заведений. – Москва, 2017. – 520 с. – С. 81.

4. Банки вернули обманутым мошенниками клиентам только седьмую часть денег  
URL: <https://www.newsru.com/finance/19feb2020/only_7th.html> (дата обращения: 15.05.2020)

5. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год // Центр мониторинга и реагирования на компьютерные атаки в финансово-кредитной сфере (ФинЦЕРТ). 2020. URL: https://www.cbr.ru/Content/Document/File/103609/Review\_of\_transactions\_2019.pdf (дата обращения: 16.05.2020)

6. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год // Центр мониторинга и реагирования на компьютерные атаки в финансово-кредитной сфере (ФинЦЕРТ). 2020. URL: https://www.cbr.ru/Content/Document/File/103609/Review\_of\_transactions\_2019.pdf (дата обращения: 16.05.2020).

7. Закон о персональных данных №152-ФЗ URL: <http://www.tadviser.ru/a/66813> (дата обращения: 16.05.2020).

[8. ГОДОВОЙ ОТЧЕТ ПАО «Сургутнефтегаз» ЗА 2018 ГОД](https://www.surgutneftegas.ru/file.php?id=4570) URL: https://www.surgutneftegas.ru/file.php?id=4570 (дата обращения: 16.05.2020).

**Информация об авторах**

Форгунова Анна Юрьевна (Россия, г. Санкт-Петербург) – аспирант, АНО ВО «Международный банковский институт имени Анатолия Собчака», Россия, 191023, г. Санкт-Петербург, Невский пр., д. 60, anna.forgunova@mail.ru

Щелканов Александр Александрович (Россия, г. Санкт-Петербург) - к.э.н., доцент Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный экономический университет», Россия, 191023, г. Санкт-Петербург, ул. Садовая, д. 21, aa.shchelkanov@mail.ru

**Forgunova A.Y.**

**Shchelkanov A.A.**

**Application of measures to ensure information security of the banking sector in the field of mining industry**

**Abstract.** *To ensure economic security, banks must resist cyber attacks, which is also relevant for enterprises in the real sector of the economy. The article discusses the types of cyber attacks and objects subject to them, analyzes the dynamics of unauthorized operations and methods of confrontation.*

**Keywords:** *information security, cybersecurity, banking sector, mining and processing industry, cyber risks*

**About authors**

Forgunova Anna Yuryevna (Russia, Saint Petersburg) - postgraduate, International Banking Institute, Russia, 191023, Saint Petersburg, Nevsky Ave. 60, [anna.forgunova@mail.ru](mailto:anna.forgunova@mail.ru)

Shchelkanov Alexander Alexandrovich (Russia, Saint Petersburg) - Ph. D., associate professor St. Petersburg State University of Economics, Russia, 191023, Saint Petersburg, Sadovaya street, 21, aa.shchelkanov@mail.ru

**Bibliographical list**

1. Caplev, D. N. Osobennosti tranzakcionnogo podhoda v analize mezhbankovskoj konkurencii / D. N. Caplev // Problemy ekonomiki i menedzhmenta. – 2016. – № 4 (8). – S. 80–90.

2. Bakulina A.A., Popova V.V. Vliyanie fintekha na bezopasnost' bankovskogo sektora // Ekonomika. Nalogi. Pravo. 2018. №2. URL: https://cyberleninka.ru/article/n/vliyanie-finteha-na-bezopasnost-bankovskogo sektora (data obrashcheniya: 15.05.2020).

3. Kiberbezopasnost' 2019—2020: tendencii i prognozy URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2019-2020-rus.pdf (data obrashcheniya: 15.05.2020)

4. Banki vernuli obmanutym moshennikami klientam tol'ko sed'muyu chast' deneg URL: https://www.newsru.com/finance/19feb2020/only\_7th.html (data obrashcheniya: 15.05.2020)

5. Obzor operacij, sovershennyh bez soglasiya klientov finansovyh organizacij za 2019 god // Centr monitoringa i reagirovaniya na komp'yuternye ataki v finansovo-kreditnoj sfere (FinCERT). 2020. URL: https://www.cbr.ru/Content/Document/File/103609/Review\_of\_transactions\_2019.pdf (data obrashcheniya: 16.05.2020)

6. Obzor operacij, sovershennyh bez soglasiya klientov finansovyh organizacij za 2019 god // Centr monitoringa i reagirovaniya na komp'yuternye ataki v finansovo-kreditnoj sfere (FinCERT). 2020. URL: https://www.cbr.ru/Content/Document/File/103609/Review\_of\_transactions\_2019.pdf (data obrashcheniya: 16.05.2020).

7. Zakon o personal'nyh dannyh №152-FZ URL: http://www.tadviser.ru/a/66813 (data obrashcheniya: 16.05.2020).

8. GODOVOJ OTCHET PAO «Surgutneftegaz» ZA 2018 GOD URL: https://www.surgutneftegas.ru/file.php?id=4570 (data obrashcheniya: 16.05.2020).