УДК 336.719 **Экономические науки**

Ахметзянова Зульфия Ринатовна, *магистр 2 курса МФП, з/о,*
Институт права, Кафедра финансового и экологического права, БашГУ
Недорезков Вячеслав Викторович, *научный руководитель к.ю.н., доцент,*
Институт права, Кафедра финансового и экологического права, БашГУ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВО-КРЕДИТНОЙ СФЕРЫ

Аннотация: Актуальность данной темы обусловлена тем, что утечка как финансовых, так и персональных данных при их передаче в рамках финансово-кредитной сферы может привести к неизбежным последствиям, будь то банкротство физических лиц или компаний до финансового кризиса. В этой связи важно выбрать и реализовать правильные технологические и правовые решения, чтобы избежать потенциальных проблем с информационной безопасностью в финансово-кредитной сфере. Автор заключает, что бурное развитие информационных технологий приводит к необходимости дополнения и уточнения перечня структур, имеющих доступ к банковской тайне. В этом контексте заключение соглашения об электронном информационном взаимодействии между Банком России и МВД России позволит правоохранительным органам незамедлительно реагировать на мошеннические действия в финансово-кредитной сфере и пресекать их. По мнению автора, во избежание утечек информации о персональных данных клиентов финансово-кредитных организаций видится целесообразным создать единые (общие) нормы, регламентирующие защиту персональной информации в финансово-кредитной сфере с учетом трансформации этих отношений под влиянием цифровой экономики.

Ключевые слова: информационная безопасность, финансово-кредитная сфера, финансово-кредитные организации, киберугрозы, кибербезопасность,

банковская тайна.

Abstract: The relevance of this topic is due to the fact that the leakage of both financial and personal data during their transfer within the financial and credit sphere can lead to inevitable consequences, whether it is the bankruptcy of individuals or companies before the financial crisis. In this regard, it is important to choose and implement the right technological and legal solutions to avoid potential problems with information security in the financial and credit sphere. The author concludes that the rapid development of information technologies leads to the need to supplement and clarify the list of structures that have access to bank secrecy. In this context, the conclusion of an agreement on electronic information interaction between the Bank of Russia and the Ministry of Internal Affairs of Russia will allow law enforcement agencies to immediately respond to fraudulent actions in the financial and credit sphere and suppress them. According to the author, in order to avoid leaks of information about the personal data of customers of financial and credit organizations, it seems expedient to create uniform (general) norms governing the protection of personal information in the financial and credit sphere, taking into account the transformation of these relations under the influence of the digital economy.

Key words: information security, financial and credit sphere, financial and credit organizations, cyber threats, cybersecurity, banking secrecy.

С возрастающей ролью цифровизации растет и угроза информационной безопасности в финансово-кредитной сфере. Методы, применяемые для защиты информации, приобретают решающее значение для обеспечения информационной безопасности в финансово-кредитных организациях.

Доступность электронных платежных сервисов, создание и развитие цифровых банков, а также мобильных приложений, позволяющих клиентам самостоятельно осуществлять переводы и платежи, рост числа банковских счетов, а также операций по ним, безусловно, определяют развитие финансово-кредитной сферы [5, с. 164]. Однако новые технологии влекут за собой новые

киберугрозы.

Финансово-кредитные учреждения сталкиваются со значительными и разнообразными киберугрозами, с которыми можно справиться с помощью эффективных стратегий кибербезопасности. Необходимо подробно остановиться на рассмотрении угроз информационной безопасности в кредитно-банковской системе передачи данных.

Подробный анализ кибератак в финансово-кредитной сфере был освещен в обзоре Центра мониторинга и реагирования на компьютерные атаки в финансово-кредитной сфере (ФинЦЕРТ) [8], специальной структурной единицей Центрального банка РФ. Более подробную механику осуществления подобных посягательств на инфраструктуру кредитно-финансовых организаций, в конечном счете преследующих корыстную экономическую выгоду, рассматривают специалисты международной компании, специализирующейся на разработке инновационных решений в сфере информационной безопасности «Positive Technologies».

Изучив исследования компании «Positive Technologies», можно выделить два основных типа информационных атак. Безусловно, их больше, разумеется, и оснований для более детальной классификации достаточно много [8].

К основным относятся:

– Dos-атаки (Denial of Service) – дословно это отказ в обслуживании, атака, которая создает нагрузку на сервер и приводит к отказу всей или какой-либо части системы.

– APT (Advanced persistent threat) – дословно это развитая устойчивая угроза, т.е. целевая атака. Чаще всего используется при внедрении в банковскую инфраструктуру. Характеризуется незаметным проникновением в банковскую среду для дальнейшего изучения и хищения необходимой информации.

ФинЦЕРТ выделяет следующие категории атак: компьютерные атаки и атаки с использованием социальных мессенджеров.

Первую категорию составляют атаки:

– на инфраструктуру финансово-кредитных организаций;

– на инфраструктуру клиентов финансово-кредитных организаций;

– атаки с использованием программ-шифровальщиков;

– атаки типа «отказ в обслуживании»;

– атаки на банкоматы [9, с. 202].

Вторую категорию составляют: электронная почта, звонки, СМС, WhatsApp, Viber.

Утечка как финансовых, так и персональных данных при их передаче в рамках финансово-кредитной сферы может привести к неизбежным последствиям, будь то банкротство физических лиц или компаний до финансового кризиса.

Все названные выше проблемы, несомненно, должны быть взяты под контроль специалистами службы кибербезопасности. Соответственно, от уровня организации управления данным процессом напрямую зависит качество организации безопасности банковских данных. В этой связи важно выбрать и реализовать правильные технологические и правовые решения, чтобы избежать потенциальных проблем с безопасностью в финансово-кредитной сфере [7, с. 619].

Так во избежание серьезных последствий Центральный банк РФ обеспечивает мониторинг в сфере киберустойчивости финансово-кредитных организаций, предупреждает их о возможных новых типах атак и способах реагирования на них.

В 2019 году Банк России принял первый стратегический документ – «Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019-2021 годов» [6], обозначив приоритеты на ближайшую перспективу, в том числе:

– разработку требований и условий безопасности управления финансовой информацией;

– недопущение утечек персональной информации из финансово-кредитных организаций;

– развитие информационно-цифровой культуры финансово-кредитной

сферы.

Правовые проблемы имеют место при регламентации защиты банковской тайны, когда конфиденциальная информация была получена должностными лицами государственных структур (либо наоборот). При этом у каждого субъекта будет собственный регламент защиты информации [4, с. 101].

Доступ к конфиденциальной банковской информации ограничен сотрудниками соответствующих бизнес-направлений, служб безопасности, совета директоров и учредителей бизнеса.

Данная информация может быть предоставлена государственным органам и их должностным лицам только при наличии обстоятельств и в установленном порядке.

В апреле 2020 г. глава МВД России В.А. Колокольцев внес предложение в Банк России о заключении с ним соглашения об информационном взаимодействии для предоставления представителям правоохранительных органов расширенных полномочий в получении информации и материалов, относящихся к банковской тайне. Это позволило бы ускорить процесс получения необходимой информации с целью более эффективного противодействия преступлениям в финансово-кредитной сфере [2]. Следует отметить, что Банк России поддержал данное предложение, однако его рассмотрение продлилось два года до сегодняшнего дня.

Так, 16 мая 2022 г. Банк России предложил изменить федеральный закон № 161-ФЗ «О национальной платежной системе» [1] и предоставить силовым структурам доступ к базе данных ФинЦЕРТа. В настоящее время данное предложение находится на стадии межведомственного согласования. База данных ФинЦЕРТа включает в себя информацию о данных банков, провайдеров, операторов связи, системных интеграторов, разработчиков антивирусов и иных компаний в области информационной безопасности [3].

Таким образом, бурное развитие информационных технологий приводит к необходимости дополнения и уточнения перечня структур, имеющих доступ к банковской тайне. В этом контексте заключение соглашения об электронном

информационном взаимодействии между Банком России и МВД России позволит правоохранительным органам незамедлительно реагировать на мошеннические действия в финансово-кредитной сфере и пресекать их.

На наш взгляд, во избежание утечек информации о персональных данных клиентов финансово-кредитных организаций видится целесообразным создать единые (общие) нормы, регламентирующие защиту персональной информации в финансово-кредитной сфере с учетом трансформации этих отношений под влиянием цифровой экономики.

Библиографический список:

1. Федеральный закон от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе» (ред. от 02.07.2021 г. № 343).

2. «Известия»: Колокольцев предложил ЦБ облегчить доступ сотрудников МВД к банковской тайне. 29.04.2020 [Электронный ресурс]. URL: https://tass.ru/ekonomika/8359653?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 17.05.2022).

3. Банк России хочет открыть полиции доступ к кибербазе ФинЦЕРТ 16.05.2022 [Электронный ресурс]. URL: https://www.anti-malware.ru/news/2022-05-16-118537/38686 (дата обращения: 17.05.2022).

4. Казаченок О.П. Воздействие цифровых технологий на правовой режим защиты персональных данных в банковской деятельности // Legal Concept. 2021. № 1. С. 99-104.

5. Мартыненко Н.Н., Овчаренко А.В. Мошенничество в сфере дистанционного банковского обслуживания и методы борьбы с ним в условиях пандемии // Инновации и инвестиции. 2020. № 12. С. 163-168.

6. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019 - 2021 годов (утв. Банком России).

7. Резниченко С.А., Дмитриева Т.В., Подкосов С.В., Евдокимов О.Г., Семухин С.Д. Проблемы управления информационной безопасностью в

кредитно-банковской системе передачи данных // Московский экономический журнал. 2022. № 2. С. 617-625.

8. ФинЦЕРТ Банка России [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/fincert/ (дата обращения: 17.05.2022).

9. Ястребова Л.О. Квалификация информационных атак в банковской сфере: вопросы теории и практики // Закон и право. 2022. №2. С. 201-204.