УДК 336.717

ОЦЕНКА ПОТЕРЬ ОРГАНИЗАЦИЙ КРЕДИТНО-ФИНАНСОВОЙ СИСТЕМЫ ОТ КИБЕРПРЕСТУПНОСТИ

Мингалева А.Д.

Магистр, программа Международный менеджмент,

Высшая школа экономики и менеджмента,

ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина»

г.Екатеринбург, Россия

Аннотация. Целью исследования является изучение влияния процессов цифровизации на экономическую и финансовую безопасность организаций кредитно-финансового сектора, а также выявление наиболее опасных с точки зрения потенциального и реально нанесенного ущерба кибератак. Показано, что потенциальный ущерб от приостановки деятельности финансовой организации, включая упущенную выгоду и затраты на восстановление сайтов после кибератак в настоящее время все больше возрастает. Увеличивается как число таких кибератак, так и единовременный ущерб от каждой из них. На основе эмпирического исследования сделан вывод, что значительное возрастание количества преступлений, совершаемых с помощью цифровых устройств и многократное увеличение суммы ущерба от них превращает кибератаки в главную угрозу российскому кредитно-финансовому сектору и обществу в целом.

Ключевые слова. Цифровизация кредитно-банковского сектора, кибератаки, экономический ущерб от компьютерных преступлений

ASSESSMENT OF LOSSES OF ORGANIZATIONS OF THE CREDIT AND FINANCIAL SYSTEM FROM CYBERCRIME

Mingaleva A.D.
Master, International Management
Graduate School of Economics and Management,
Ural Federal University named after the first President of Russia Boris Yeltsin
Yekaterinburg, Russia

Annotation. The purpose of the study is to analyze the impact of digitalization processes on the economic and financial security of credit and financial sector organizations, as well as to identify the most dangerous cyber attacks in terms of potential and actual damage. The article shows that the potential damage from the suspension of a financial institution, including lost profits and the cost of restoring sites after cyber attacks, is currently increasing. Both the number of such cyber attacks and the one-time damage from each of them are increasing. Based on an empirical study, it was concluded that a significant increase in the number of crimes committed using digital devices and a multiple increase in the amount of damage caused by them makes cyber attacks the main threat to the Russian credit and financial sector and society as a whole.

Keywords. Digitization of the credit and banking sector, cyber attacks, economic damage from computer crimes

Введение

Расширение области применения цифровых технологий в кредитно-банковском секторе создает широкие предпосылки для повышения скорости банковских операций, улучшению обслуживания клиентов, прозрачности финансовых сделок. Однако, по признанию экспертов, применение все более и более сложных цифровых технологий в финансовом секторе сопровождается и возрастающими рисками криминального характера [8]. Рост числа и

интенсивности кибератак по всем мире ведет и к росту стоимости затрат компаний и общества в целом на обеспечение защиты от кибератак и предотвращения потерь от них. Особенно сильно страдает финансовая сфера экономики. При этом число кибератак и компьютерных преступлений против финансовой системы нашей страны возрастает колоссальными темпами.

Структура кибератак в кредитно-финансовой сфере

Исследование различного типа компьютерных преступлений в кредитно-финансовом секторе позволило выявить основные направления кибератак, которые, по мнению специалистов, представляют наибольшую угрозу в будущем и серьезное увеличение числа которых прогнозируется в ближайшее время. Так, согласно оценкам респондентов, полученным в ходе подготовки Global Risks Report [10] для Всемирного экономического форума в Давосе в 2019 году, наиболее значимыми и опасными среди кибератак являются следующие:

- «Кибератаки: кража данных / денег» - 82% ответивших (4 место в рейтинге по степени опасности);

- «Кибератаки: нарушение работы и инфраструктуры» - 80% ответивших (5 место в рейтинге);

- «Кибератаки: кража личных данных» - 64% ответивших (10 место в рейтинге);

- «Кибератаки: потеря конфиденциальности (для компаний)» - 63% ответивших (13 место в рейтинге) [10].

Согласно сведениям Национального координационного центра по компьютерным инцидентам (НКЦКИ), в 2018 году было совершено более 4,3 млрд кибератак на критическую информационную инфраструктуру, 17 тыс. из которых признаны наиболее опасными, что почти в два раза выше аналогичных показателей 2017 года – 2,4 млрд и 12 тыс. соответственно [4-6].

Анализ способов совершаемых в кредитно-финансовой сфере преступлений показал, что преступники, наряду с применением высокотехнологичных хакерских схем для получения доступа к банковским системам, продолжают широко использовать методы социальной инженерии. Наиболее распространенной формой такой подготовительной противоправной деятельности является претекстинг, то есть предварительное вступление в контакт с потенциальными потерпевшими посредством телефонной связи, в мессенджерах (Skype, WhatsApp, Viber, Telegram и др.) или в социальных сетях («ВКонтакте», «Фейсбук» и др.) с целью получения сведений, необходимых для доступа к распоряжению их денежными средствами [1].

Согласно позиции Главного управления безопасности и защиты информации Банка России, повышенная опасность подобных преступных действий определяется доверчивостью и невысоким уровнем финансовой грамотности населения, вследствие чего в ближайшее время снижение распространенности претекстинга как подготовительной деятельности к совершению хищений денежных средств с банковских счетов и электронных денежных средств представляется маловероятным.

Экономический ущерб от кибератак

Закономерно с ростом числа компьютерных преступлений и расширением областей их применения, возрастает и прямой экономический ущерб от их совершения, который несут организации кредитно-финансовой и банковской сферы.

Исследования последних лет показали огромный ущерб для кредитно-финансовой сферы из-за приостановки хотя бы на 1 день работы банка или другого финансового учреждения. Так, в ходе проведенного компанией *Positive Technologies* в 2017 году исследования «Сколько стоит безопасность» было установлено, что стоимость атаки на веб-ресурсы в течение часа в даркенете оценивается приблизительно в $5, а в течение суток — $300 [7, 16].

Еще более значимыми выглядят цифры ежедневных потерь учреждений кредитно-финансовой сферы от уже перечисленных ранее кибератак. Приведем результаты оценки потенциального ущерба от приостановки деятельности финансовой организации, включая упущенную выгоду, а также затраты на восстановление сайтов, представленные самими учреждениями кредитно-финансовой и банковской сферы[1]. Структура и размер финансовых потерь по отдельным видам кибератак и размеру потенциального ущерба приведена на рисунках 1-4 (источник: составлено автором по [7, 14-16: 7, 18]). Рисунки 1-2 отражают прямые потери от отказа корпоративной инфраструктуры (рисунок 1) и дополнительные затраты на ее восстановление (рисунок 2). Таким образом, ущерб от таких кибератак значительно больше, чем при простой оценке. Ответы сгруппированы в процентах от ответивших. Так, из рисунка 1 видно, что 25% респондентов оценили свои потери от отказа всей корпоративной банковской инфраструктуры в течение одного дня в размере 2-10 млн.руб., а для 30% респондентов такие однодневные потении составили уже более 50 млн.руб. И т.д.

[1] Помимо учреждений кредитно-финансовой и банковской сферы в опросе приняли участие государственные учреждения, учреждения транспорта, учреждения системы образования, промышленные компании, ИТ компании, СМИ. Их ответы в данной статье не анализируются.

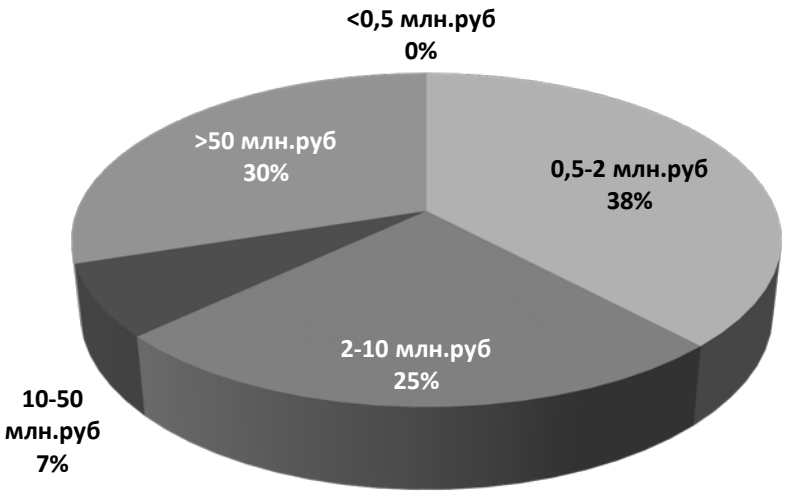

Рисунок 1. Потери от отказа всей корпоративной банковской инфраструктуры в течение одного дня

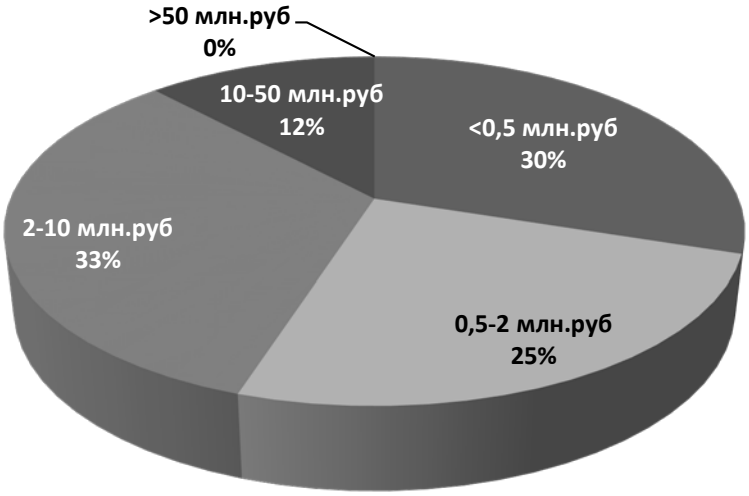

Рисунок 2. Затраты на восстановление банковской инфраструктуры после вывода из строя всех ресурсов

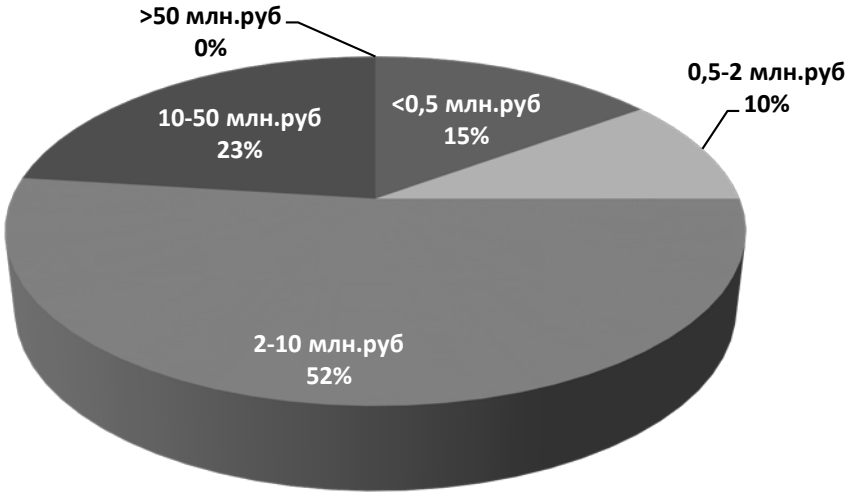

Рисунок 3. Потери от недоступности критически важных веб-приложений в течение одного дня

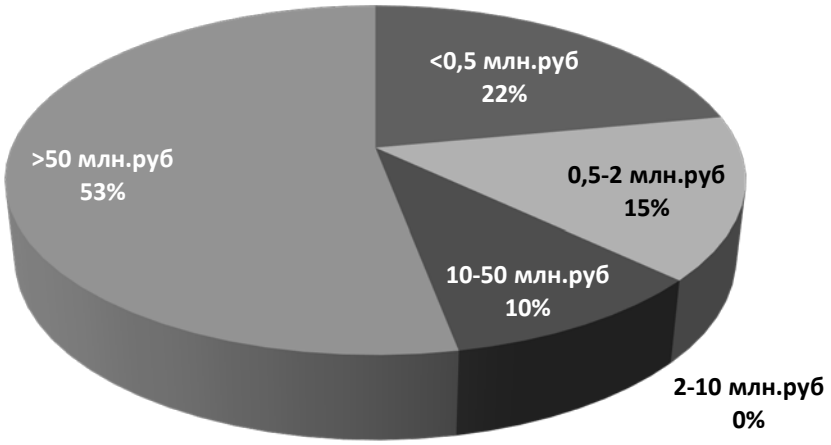

Рисунок 4. Потери от кражи баз данных клиентов конкурентом

Итак, как видно из рисунков 1-4, потери учреждений кредитно-финансовой и банковской сферы от различного рода кибреатак наиболее значимые (более 50 млн.рублей) при кражах баз данных о клиентах (у 53% респондентов) и в случае отказа всей корпоративной инфраструктуры в течение одного дня (у 30% респондентов). Потенциальный ущерб от недоступности

критически важных веб-приложений в течение одного дня большинством респондентов (52%) оценивается в пределах 2-10 млн.руб. Что касается дополнительных затрат на восстановление корпоративной инфраструктуры после вывода из строя всех ресурсов домена то они в большинстве случаев не превышают 10 млн.руб. - эту сумму и меньше назвали в совокупности 88% респондентов.

Заключение

Таким образом, кибератаки, нацеленные на отдельные кредитные организации, в совокупности составляют колоссальную угрозу для всей финансовой сферы экономики страны. Как было отмечено на состоявшемся в Москве 17 апреля 2018 года форуме страховых технологий InnoIns-2018, ежедневно в России 16 предприятий подвергаются кибератакам [9]. Бизнес тратит около 122,5 млрд долларов в год на защиту информационных систем.

С целью повышения уровня национальной компьютерной безопасности страны и в соответствии с частями 4 статьи 5 и пунктом 2 части 4 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" в июле 2018 годы был создан Национальный координационный центр по компьютерным инцидентам [3].

В целом же согласно экспертным оценкам ущерб мировой экономике от массовых кибератак может вырасти 2019 году до $2 трлн и в 2020 году до $3 трлн. [1]. Соответственно, возрастает и стоимость затрат компаний и общества в целом на обеспечение защиты от кибератак и предотвращения потерь от них. По прогнозам ПАО «Сбербанк России», объем мировых расходов компаний на кибербезопасность до 2021 года вырастет в 14 раз и достигнет примерно триллиона долларов [2].

Библиографический список:

1. Глобальные потери от киберпреступности в 2019 году могут достичь 2 триллионов долларов. [Электронный ресурс]. — Режим доступа — URL: https://www.banki.ru/news/lenta/?id=10404738 (Дата обращения 04.08.2019)
2. За год на Россию было совершено более четырех миллиардов кибератак. . [Электронный ресурс]. — Режим доступа — URL: https://rg.ru/2018/12/12/za-god-na-rossiiu-bylo-soversheno-bolee-chetyreh-milliardov-kiberatak.html Дата обращения 12.08.2019)
3. Приказ ФСБ России от 24 июля 2018 г. N 366 «О Национальном координационном центре по компьютерным инцидентам» [Электронный ресурс]. — Режим доступа — URL: http://base.garant.ru/ 72041506/ #ixzztv1rQY2i (Дата обращения 11.08.2019)
4. Сводная статистика по криминальному статусу в России за 2016 год // Судебный департамент при Верховном Суде Российской Федерации. [Электронный ресурс]. — Режим доступа — URL: http://www.cdep.ru/index.php?id=79 (Дата обращения 14.08.2019)
5. Сводная статистика по криминальному статусу в России в 2017 году // Судебный департамент при Верховном Суде Российской Федерации. - [Электронный ресурс]. — Режим доступа — URL: http://www.cdep.ru/index.php?id=79 (Дата обращения 14.08.2019)
6. Сводная статистика по криминальному статусу в России за 6 месяцев 2018 года // Судебный департамент при Верховном Суде Российской Федерации. [Электронный ресурс]. — Режим доступа — URL: http://www.cdep.ru/index.php?id=79 (Дата обращения 14.08.2019)
7. Сколько стоит безопасность? Анализ процессов информационной безопасности в российских компаниях. Позитивные технологии. [Электронный ресурс]. — Режим доступа — URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf (Дата обращения 04.08.2019)
8. Совершенствование мер уголовной ответственности за киберпреступления в финансовом секторе экономики. [Электронный ресурс]. — Режим доступа — URL: http://ormvd.ru/pubs/102/improvement-of-measures-of-criminal-liability-for-cyber-crimes-in-the-financial-sector-of-the-econom/ (Дата обращения 18.08.2019)
9. Форум страховых технологий InnoIns-2018 [Электронный ресурс]. — Режим доступа — URL: http://www.insur-info.ru/overviews/22/ (Дата обращения 21.08.2019)
10. The Global Risks Report 2019, 14th Edition, World Economic Forum, Geneva. 2019.

Оригинальность 83%