

УДК 336.71.078.3

О.И. Русакова*Иркутский государственный университет путей сообщения,
г. Иркутск, Российская Федерация***С.А. Головань***Иркутский государственный университет путей сообщения,
г. Иркутск, Российская Федерация*

ВЛИЯНИЕ КИБЕРПРЕСТУПЛЕНИЙ НА БАНКОВСКУЮ СИСТЕМУ РОССИИ*

АННОТАЦИЯ. С экономической точки зрения киберпреступления - это особый вид деятельности человека, который ищет белые пятна в правилах и традициях экономического поведения, в объектах и методах хозяйственной деятельности, в способах контроля экономической деятельности, в уголовном праве и в практике правоохранительных органов юстиции. Финансовое мошенничество с использованием электронных технологий имеет характеристики, которые отличают его от других видов преступлений. Прежде всего, это то, что данный вид преступлений совершается в кредитно-финансовой сфере, что наносит значительный ущерб экономике. Использование компьютерных технологий с современными версиями программного обеспечения присуще совершению мошенничества в финансовом секторе и требует соответствующих решений.

КЛЮЧЕВЫЕ СЛОВА. Банковская сфера, киберпреступность, цифровая теневая экономика, электронное мошенничество.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 30 октября 2020 г.; дата принятия к печати 22 марта 2021 г.; дата онлайн-размещения 8 апреля 2021 г.

O.I. Rusakova*Irkutsk State Transport University,
Irkutsk, Russian Federation***S.A. Golovan***Irkutsk State Transport University,
Irkutsk, Russian Federation*

THE IMPACT OF CYBERCRIMES ON THE BANKING SYSTEM OF RUSSIA**

ABSTRACT. The article provides analysis of cybercrimes and their impact on banking system of Russia. From an economic point of view, cybercrime is a special type of human activity aimed at finding blank spots in the rules and traditions of economic behavior, in the methods of economic activity, in the methods of controlling economic activity, as well as in criminal law, in the practice of law enforcement agencies and organs of justice. The research stated that electronic financial fraud has characteristics that differentiate it from other types of crime. One of the most relevant issues is the fact that this type of crime is committed in the credit and financial sphere, which causes significant damage to the economy. The article concluded that the use of computer technology with modern versions of software is inherent in committing fraud in the financial sector and requires appropriate solutions.

KEYWORDS. Banking sector, cybercrime, digital shadow economy, electronic fraud.

ARTICLE INFO. Received October 30, 2020; accepted March 22, 2021; available online April 8, 2021.

* Материалы обсуждены на XI Международной научно-практической конференции «Транспортная инфраструктура Сибирского региона», посвященной 45-летию ИргУПС и 90-летию БГУ, г. Иркутск, 11–13 ноября 2020 г.

** The paper was discussed at the 11th International Scientific and Practical Conference «Transport Infrastructure of Siberian Region» dedicated to the 45th anniversary of Irkutsk State Transport University and the 90th anniversary of Baikal State University, Irkutsk, November 11–13, 2020.

© Русакова О.И., Головань С.А., 2021

Обеспечение экономической безопасности Российской Федерации становится глобальной проблемой не только по масштабам распространения, но и по глубине и сложности подрывающих ее угроз. На сегодняшний день большинство людей значительную часть своего рабочего и свободного времени проводят в сети Интернет. Этот мир безграничных возможностей во многом похож на мир реальный: преступность, которая является, к сожалению, своеобразной частью социума, существует и там.

Хотя достижения в области информационных технологий и Интернета расширили способы ведения бизнеса, они также создали среду для широкого спектра незаконных действий. Одна из самых больших проблем последнего десятилетия — это сложность в определении масштабов экономической деятельности, объектов и субъектов в киберпространстве. Через киберпространства, например, социальные сетевые платформы, электронную коммерцию, системы электронного бизнеса или компьютерные игры, в обращении находятся реальные деньги, но в большинстве случаев эти операции не учитываются и не приносят налогов в государственный бюджет. Хотя реальные масштабы теневой цифровой экономики трудно определить, недавняя оценка глобальных корпоративных потерь составляет около 750 млрд евро в год¹. По этой причине во многих странах встает актуальный вопрос о том, как объемы цифровой теневой экономики могут быть сокращены без нарушения конфиденциальности и мобильности как частных лиц, так и предприятий.

С точки зрения экономических и инновационных результатов использования цифровых технологий, Российская Федерация занимает 38-е место с большим отставанием от стран-лидеров, таких, как Финляндия, Швейцария, Швеция, Израиль, Сингапур, Нидерланды, Соединенные Штаты Америки, Норвегия, Люксембург и Германия. Такое значительное отставание в развитии цифровой экономики от мировых лидеров объясняется пробелами нормативной базы для цифровой экономики и недостаточно благоприятной средой для ведения бизнеса и инноваций и, как следствие, низким уровнем применения цифровых технологий бизнес-структурами².

Развитию цифровой экономики России сегодня препятствуют новые вызовы и угрозы, прежде всего:

- проблема обеспечения прав человека в цифровом мире, в том числе при идентификации (соотнесении человека с его цифровым образом), сохранности цифровых данных пользователя, а также проблема обеспечения доверия граждан к цифровой среде;
- угрозы личности, бизнесу и государству, связанные с тенденциями к построению сложных иерархических информационно — телекоммуникационных систем, широко использующих виртуализацию, удаленные (облачные) хранилища данных, а также разнородные технологии связи и оконечные устройства;
- наращивание возможностей внешнего информационно-технического воздействия на информационную инфраструктуру, в том числе на критическую информационную инфраструктуру;
- рост масштабов компьютерной преступности, в том числе международной;
- отставание от ведущих иностранных государств в развитии конкурентоспособных информационных технологий;
- зависимость социально-экономического развития от экспортной политики иностранных государств;

¹ Cybercrime as a Business: The Digital Underground Economy // Europol. 2011. URL: <https://www.europol.europa.eu/content/press/cybercrime-business-digital-underground-economy-517>.

² Цифровая экономика Российской Федерации : Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-п. URL: <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvrR7M0.pdf>.

– недостаточная эффективность научных исследований, связанных с созданием перспективных информационных технологий, низкий уровень внедрения отечественных разработок, а также недостаточный уровень кадрового обеспечения в области информационной безопасности.

В научной литературе уже начинает формироваться определенный подход к понятию «цифровой теневой экономики», которое тесно связано с понятиями «киберпреступность» и «электронное мошенничество». Рассмотрим подходы более подробно (табл. 1).

Таблица 1

*Авторские определения в зарубежной научной литературе**

Авторский подход	Авторы
<i>Цифровая теневая экономика</i>	
– правонарушения, совершенные с использованием сетевых технологий для выполнения невероятно сложных и далеко идущих задач, которые можно повторять бесчисленное количество раз во всем мире;	Yip M., Shadbolt N., Tiropanis N. & Webber C. (2012) [1];
– преступление в Интернете, которое направлено на получение прибыли, и характер этой деятельности превышает возможности закрытой группы.	Herley C. & Florencio D. (2010) [2];
<i>Киберпреступность</i>	
– прочная теневая экономика, индустриализованная за счет создания и предоставления инструментов для преступного поведения;	Mello J.P. (2013) [3];
– высокотехнологичная преступная деятельность, включая использование ботов, целевых атак или нестандартных вредоносных программ, которые создают серьезные угрозы для потребителей, организаций и предприятий, а также для государственного сектора;	Vlachos V., Minou M., Assimakopoulos V. & Toska A. (2011) [4];
– преступления в Интернете, совершаемые удаленно с целью незаконного получения богатства или ресурсов от других. Украденные ресурсы могут включать доступ в Интернет, место на жестком диске компьютера, финансовые ресурсы, интеллектуальный капитал и другие данные;	Smith G.S. (2015) [5];
<i>Электронное мошенничество</i>	
– потребление нелегальных копий услуг цифровых продуктов;	Ho J. & Weinberg C.B. (2011) [6]; Taylor S.A. (2012) [7];
– нарушение условного контракта, установленного онлайн.	Hjort K. & Lantz B. (2012) [8].

* Составлено авторами по данным [9].

Россия, согласно международным рейтингам, в последние годы традиционно входит в тройку самых опасных, с точки зрения киберпреступности, стран. Киберпреступность является одной из самых актуальных проблем в мире и в России в частности, так как по итогам 12-месячного периода, конец которого пришелся на июнь 2019 г., ущерб российских банков от кибератак составил 510 млн р., что на 85 % относительно аналогичного отрезка времени годом ранее. Кроме того, все чаще встречаются хищение и продажи текстовых данных карт — номер, CVV, срок действия. Цена на них стала расти, при этом снижалась стоимость дампов.

Самыми дешевыми на рынке являются данные американских банков, самыми дорогими — данные карт европейских банков [10].

В табл. 2 представлены данные относительно стремительного роста числа пользователей сети Интернет за последние годы.

Таблица 2

*Рост мировой популяции и числа пользователей сети Интернет**

Год	Ежегодный прирост числа пользователей сети Интернет, %	Ежегодный прирост мирового населения, %	Охват мирового населения доступом к мировой сети Интернет, %
1994	79,74	1,47	0,4
1998	55,7	1,3	3,1
2002	32,37	1,24	10,6
2005	13,15	1,22	14,1
2009	12,18	1,2	25,6
2011	11,71	1,18	32,5
2014	7,85	1,14	40,4

* Составлено авторами по данным [11].

Интернет-банкинг создал альтернативу традиционному посещению банка и использованию этого канала распространения продуктов. В 1993 г. Интернетом не пользовались даже 15 млн чел. (0,3 % от населения мира), тогда как в 2014 г. это число увеличилось до 3 млрд пользователей (40,4 % населения мира). Значительное отставание в развитии цифровой экономики от мировых лидеров объясняется пробелами нормативной базы для цифровой экономики и недостаточно благоприятной средой для ведения бизнеса и инноваций и, как следствие, низким уровнем применения цифровых технологий бизнес-структурами. Компания RSA Security, входящая в состав американской корпорации EMC Corporation, одна из крупнейших в мире корпораций на рынке продуктов, услуг и решений для хранения информации и управления ею, представила в январе 2016 г. результаты исследования, посвященного расценкам данных интернет-пользователей на рынке киберпреступности. По данным специалистов компании, активный рост пользователей социальных сетей и общая информатизация общества привели к тому, что стоимость пользовательских данных снизилась, однако они по-прежнему остаются объектом повышенного интереса злоумышленников. Так, стоимость аккаунта в популярных социальных сетях с количеством подписчиков выше 500 чел. оценивается в 7,5 дол., аккаунты с меньшим числом подписчиков обходятся киберпреступникам примерно в 5 дол. В последнее время повышенный интерес со стороны злоумышленников стал наблюдаться к учетным записям пользователей интернет-магазинов и торговых онлайн-площадок, которые, как правило, содержат много конфиденциальной информации: почтовые, домашние и электронные адреса, номера телефонов, истории покупок, номера пластиковых карт, списки транзакций, и оцениваются преступниками всего в 2–2,5 дол.³

Киберпреступления можно разделить на четыре основные группы (рис. 1).

Первым шагом большинства киберпреступлений является доставка и установка вредоносной программы. Сегодня основными способами распространения таких программ являются заражение веб-страниц и спам-рассылки. После того

³ Отдел «К» предупреждает: будьте осторожны и внимательны! // Управление МВД России по Тульской обл. URL: https://71.xn--b1aew.xn--plai/Dejatelnost/Borba_s_kiberprestupnostju/otdel-k.

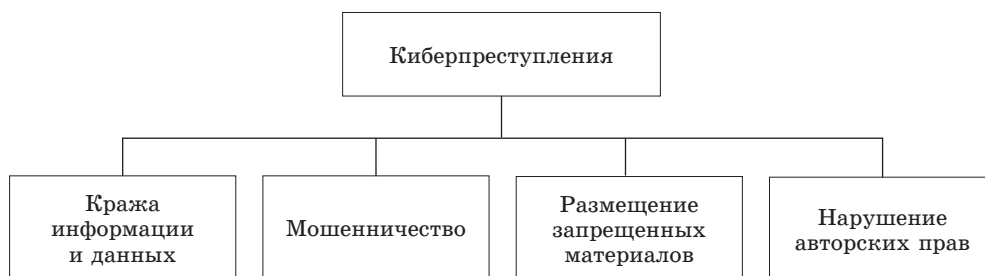


Рис. 1. Основные группы киберпреступлений

как вредоносная программа попала на незащищенный компьютер, преступники стараются как можно дольше сохранять ее необнаруженной. Наиболее тревожные тенденции настоящего времени:

- рост популярности программ-вымогателей, которые являются чрезвычайно прибыльной сферой деятельности киберпреступников благодаря тому, что «держат в заложниках» данные пользователей до тех пор, пока не будет заплачен «выкуп»;
- развитие высокоэффективных эксплойт-наборов, компрометирующих системы через использование уязвимости в программном обеспечении [12].

По данным ООН, самым распространенным преступлением в мире является кража информации при проведении финансовых операций через Интернет: данные кредитных карт или банковских счетов.

По результатам исследования компании Symantec, чаще всего жертвами кибермошенников в сети Интернет становятся компании с численностью сотрудников, не превышающей 250 чел.

В число самых привлекательных для кибермошенников отраслей вошли производственная сфера, гостиничные, рекреационные услуги, услуги ремонта, финансовый сектор, страхование и недвижимость. По некоторым данным, индивидуальные киберпреступники могут зарабатывать в год до полумиллиона долларов США просто торгуя украденными данными (рис. 2).

За январь — сентябрь 2018 г. правоохранительными органами РФ зарегистрировано 121 тыс. 247 преступлений, совершенных с использованием информацион-

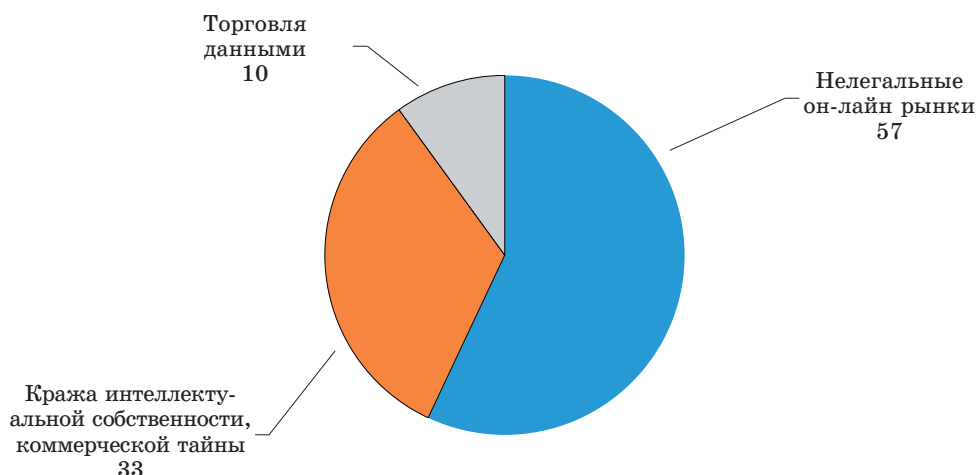


Рис. 2. Структура мирового рынка киберпреступлений, %

но-телекоммуникационных технологий или в сфере компьютерной информации. За весь 2017 г. — 90 тыс. 587. Таким образом, если в прошлом году их регистрировалось в среднем 7,5 тыс. в месяц, то в этом году уже более 13 тыс. в месяц. Их доля в общем числе преступлений выросла с 4,4 % до 8,1 %, при этом расследовано лишь 31,8 тыс. таких преступлений.

Последние шесть лет киберпреступность, согласно статистике, демонстрирует десятикратный рост (в 2013 г. подобных преступлений было 11 тыс., в 2014 г. — 44 тыс., в 2016 г. — 66 тыс.). Ранее в Генпрокуратуре сообщали, что только с 2015 по 2016 г. в шесть раз выросло число мошенничеств (с 2,2 тыс. до 13,4 тыс.) и более чем в три раза — краж (с 2,3 тыс. до 8,5 тыс.) с использованием интернета и иных коммуникационных ресурсов, в 5,5 раза (с 995 до 5,5 тыс.) выросло количество преступлений, связанных с хищением, удалением, блокировкой компьютерной информации с целью мошенничества (ст. 159.6 УК РФ).

К 2023 г. доля киберпреступлений может вырасти с 14 до 30 %, прогнозируют аналитики организации «Интернет-розыск». Это связано с низкой раскрываемостью и слабыми возможностями по идентификации онлайн-злоумышленников. Нужны новые технологии, которые позволят эффективно находить нарушителей Уголовного кодекса по электронно-цифровому следу, полагают эксперты. В МВД, однако, утверждают, что количество раскрытых IT-преступлений за 2018–2019 гг. выросло в полтора-два раза.

По данным статистики Генпрокуратуры, за январь–ноябрь 2019 г. правоохранительные органы зарегистрировали 261 208 киберпреступлений — это седьмая часть от общего количества уголовных дел. Прирост по сравнению с 2018-м достиг 67,1 %. Предварительно расследовано менее 60 тыс. Речь идет о нарушениях УК, которые совершаются с помощью интернета, мобильной связи, с использованием банковских карт (рис. 3).

По оценке специалистов компании кибербезопасности «Интернет-розыск», раскрываемость преступлений в сфере компьютерной информации снижается: с 36 % в 2016 г. до 23 % в 2019 г.

По данным экспертов, использование современных баз данных (агрегаторов, позволяющих проанализировать большие массивы информации, в том числе персональные данные) — «Палантир», «Осирис», «Шерлок», «Псков» и других — для

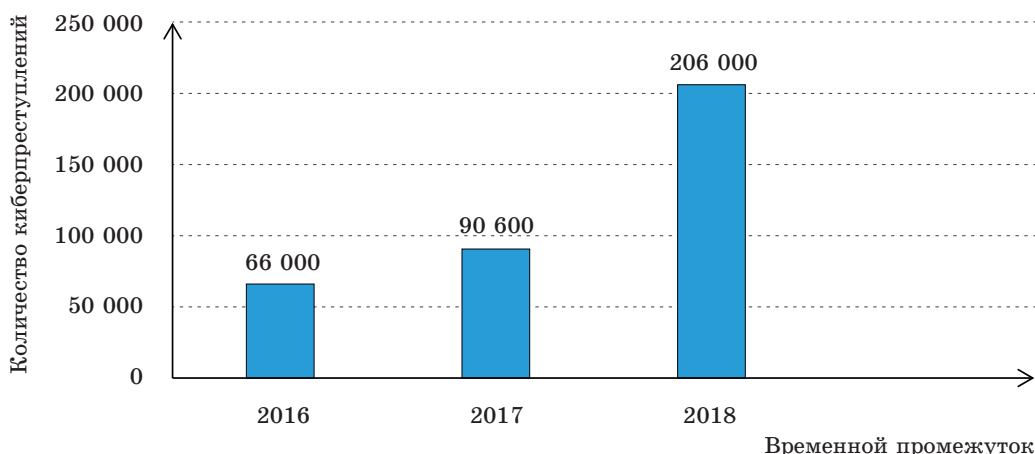


Рис. 3. Количество киберпреступлений в финансовом секторе Российской Федерации
Источник [13].

раскрытия интернет-преступлений представляется неэффективным. Для качественного функционирования агрегаторов требуются колоссальные вычислительные мощности и серьезный штат обслуживающего персонала (техников, программистов, аналитиков).

В социальных сетях 82 % атак представляли собой фальшивые предложения. В глобальном почтовом трафике 62,1 % пришлось на долю спама. Наибольшей популярностью у спамеров среди доменов верхнего уровня пользовался домен. COM.

В пятерку стран — получателей спама вошли Шри-Ланка (74,7 %), Израиль (68,8 %), Бразилия (66,9 %), Южная Африка (65,3 %) и Кувейт (64,8 %). Страна-ми — источниками спама стали Канада (7,7 %), Испания (6,8 %), Россия (6,4 %), США (5,9 %), Финляндия (5,6 %) ⁴.

Ущерб от кражи интеллектуальной собственности и конфиденциальной деловой информации является наиболее важной категорией ущерба. Интернет часто становится торговой площадкой для распространения запрещенных товаров и различных подделок. За последние годы объем контрафактной продукции, поставляемой из стран Азии, вырос почти в десять раз. Значительная доля приходится на лекарства, оборот которых в Европе составляет примерно 10 млрд дол. Как правило, подобные товары распространяются через различные интернет-сайты, а также через спам-рассылки в социальных сетях и на электронную почту. Но почему же именно банки являются частым предметом для атак киберпреступников. Для того чтобы ответить на этот вопрос необходимо проанализировать деятельность банков и их размер внутри страны. В табл. 3 приведены самые крупные банки России по размеру их активов.

Таблица 3

Топ — 5 банков России по размеру активов (в млн р.)

Номер	Банк	Сумма актива
1	Сбербанк	30 333 085
2	Банк «ВТБ»	14 831 480
3	Газпромбанк	6 600 325
4	Альфа-Банк	3 832 677
5	Россельхозбанк	3 582 842

Киберпреступники понимают, что им проще будет «работать» с физическими лицами и их банковскими картами, нежели со сложной системой защиты банка или юридического лица. Поэтому в число самых атакуемых банков входят те, которые работают с физическими лицами (табл. 4). По результатам исследований, проведенных специалистами компании Сбербанк в 2019 г., кибератаки проводятся каждые 14 с, а потери крупных мировых компаний составляют около 2,5 трлн дол. год [14].

Точной статистики о потерях, которые несет государство от киберпреступников, не существует. По официальным данным, это 120–130 млрд р. в год, по неофициальным данным — не менее 600 млрд р. Но в любом случае можно противостоять атакам преступников, совершенствуя не только правоохранительные и судебные системы, но и ИТ-инфраструктуру, модернизируя финансовые инструменты и повышая грамотность населения в борьбе с кибер-мошенничеством.

Экономические потери от киберпреступлений с каждым годом только увеличиваются (табл. 5).

⁴ Кибератаки на банковские счета: виды и способы борьбы с ними // ИПП «Гарант». URL: <http://www.garant.ru/article/1290354/>.

Таблица 4

**Ранжирг банков по объему привлеченных средств физических лиц
и индивидуальных предпринимателей**

Место на 01.04.2020	Место на 01.04.2019	Наименование банка	Остаток средств на счетах ФЛ и ИП на 01.04.2020, млн р.	Остаток средств на счетах ФЛ и ИП на 01.04.2019, млн р.	Темп при- роста при- влеченных средств ФЛ и ИП за период с 01.04.2019 по 01.04.2020, в %	Доля при- влеченных средств ФЛ и ИП в пассивах, в %
1	1	ПАО Сбербанк	13 692 154	12 584 290	8,8	46,1
2	2	Банк ВТБ (ПАО)	4 623 898	3 947 751	17,1	31,0
3	4	АО «АЛЬ- ФА-БАНК»	1 268 087	1 038 614	22,1	30,3
4	5	Банк ГПБ (АО)	1 262 228	979 588	28,9	18,1
5	3	АО «Россель- хозбанк»	1 237 612	1 068 718	15,8	34,5

Таблица 5

Экономические потери от киберпреступлений*

В млрд дол.					
Экономические потери от киберпреступлений мировой экономики					
Год	2018	2019	2020 (прогноз)	2022 (прогноз)	2030 (прогноз)
Экономические потери	1 500	2 500	3 000	8 000	90 000
Экономические потери от киберпреступлений в России					
Год	2018	2019	2020	2021 (прогноз)	2022 (прогноз)
Экономические потери	28	35	50,4	98	126

* Составлено авторами по данным: Оценены потери российской экономики от кибератак // Росбалт. 2020. 21 янв. URL: <https://www.rosbalt.ru/business/2020/01/21/1823728.html>; Сбербанк предсказал рост ущерба экономики России от кибератак до 40 %. // РБК. 2020. 21 янв. URL: <https://www.rbc.ru/finances/21/01/2020/5e26e6a79a7947798bc80db7>.

Консалтинговое агентство Marksworld признало Сбербанк лучшим цифровым банком для крупного бизнеса. В рамках исследования Digital Corporate Banking Rank 2020 аналитики изучили цифровые сервисы ключевых банков. В результате Сбербанк стал лидером рейтинга, набрав 73,6 балла (у ближайшего преследователя 60,5 баллов)⁵. Как видно из таблиц 3 и 4 лидирующие позиции в банковском секторе занимает Сбербанк России. Именно поэтому он является наиболее привлекательным для преступников в сети интернет.

Сбербанк отчитался, что за 2018 г. он отразил 90 DDoS-атак, 25 из которых были высокой мощности. Кроме того, на его системы пришлось 5 % от всех киб-

⁵ Годовой отчет 2019 / Сбербанк. М., 2019. URL: <https://www.sberbank.com/common/img/uploaded/files/pdf/yrep/sberbank-ar19-rus.pdf>.

ратак в России за прошлый год. Сбербанк заверил, что ни одна из этих попыток не смогла нарушить функционирование систем кредитной организации⁶. Основные направления борьбы с киберпреступностью в ПАО Сбербанк — это защита ключевых банковских систем и подходы к разработке продуктов и участию безопасности в этих процессах⁷.

К сожалению, в последние годы появился тренд на увеличение попыток атаковать клиентов кредитных учреждений с использованием методов социальной инженерии. Доля таких преступлений сейчас превышает 87 % от всего объема реализованного мошенничества.

Этому противостоит фрод-мониторинг Сбербанка, в основе которого лежит искусственный интеллект. Его показатель эффективности сегодня составляет около 97 %. Операции, которые являются мошенническими, банк умеет хеджировать и не допускать совершения преступления. Так, благодаря системе фрод-мониторинга с января по август 2019 г. Сбербанку удалось предотвратить хищение средств клиентов на 25 млрд р.

Но помимо кражи данных пользователей с помощью социальной инженерии существует способ внедрения банковского вируса, как в корпоративную программу банка, так и на гаджеты обычных пользователей. С помощью такого банковского вируса, можно без труда получать ту информацию, которая нужна мошенникам. В 2019 г. Россия осталась лидером по атакам банковских вирусов. Об этом свидетельствуют данные «Лаборатории Касперского», обнародованные 16 апреля 2020 г.

Основные направления борьбы с киберпреступностью в ПАО Сбербанк — это защита ключевых банковских систем и подходы к разработке продуктов и участию безопасности в этих процессах.

К сожалению, в последние годы появился тренд на увеличение попыток атаковать клиентов кредитных учреждений с использованием методов социальной инженерии. Доля таких преступлений сейчас превышает 87 % от всего объема реализованного мошенничества.

Комплексная программа борьбы с киберпреступностью должна включать совокупность действий, как государственных структур, так и частного сектора экономики, и состоять из следующих компонентов (рис. 4).

Результаты многочисленных мировых исследований подтвердили, что проблемы безопасности банков влияют также на удовлетворенность и лояльность клиентов [11]. Отдельные исследования также подтверждают гипотезу, что доверие к банковской системе со стороны клиентов во многом определяют их желание расширять перечень банковских услуг. Таким образом, можно сделать вывод, что безопасность электронного банкинга представляет собой вызов для нынешнего руководства банков во всем мире, что подтверждается многочисленными успешными атаками на коммерческие банки. Банковский сектор значительно развил электронное общение со своими клиентами в последние годы. Этот процесс был вызван в основном увеличением количества пользователей сети Интернет. Улучшение электронных каналов сбыта банков, с одной стороны, связано с большей доступностью продуктов и услуг для клиентов, с другой это ведет к увеличению потенциального риска. Этот риск представляет собой возможную кражу личных данных, а также доступ хакеров к счетам клиентов и, в конце концов, кражи денежных средств.

⁶ Потери компаний от кибератак в мире // Коммерсантъ. 2019. 26 апр. URL: <https://www.kommersant.ru/doc/3957187>.

⁷ Сбербанк стал первым партнером-основателем Центра кибербезопасности Всемирного экономического форума // Сбербанк. 2018. 23 авг. URL: https://www.sberbank.ru/ru/press_center/all/article?newsID=9c2d6d45-aaf8-4805-b527-df0130a89a1b&blockID=1303®ionID=77&lang=ru&type=NEWS.

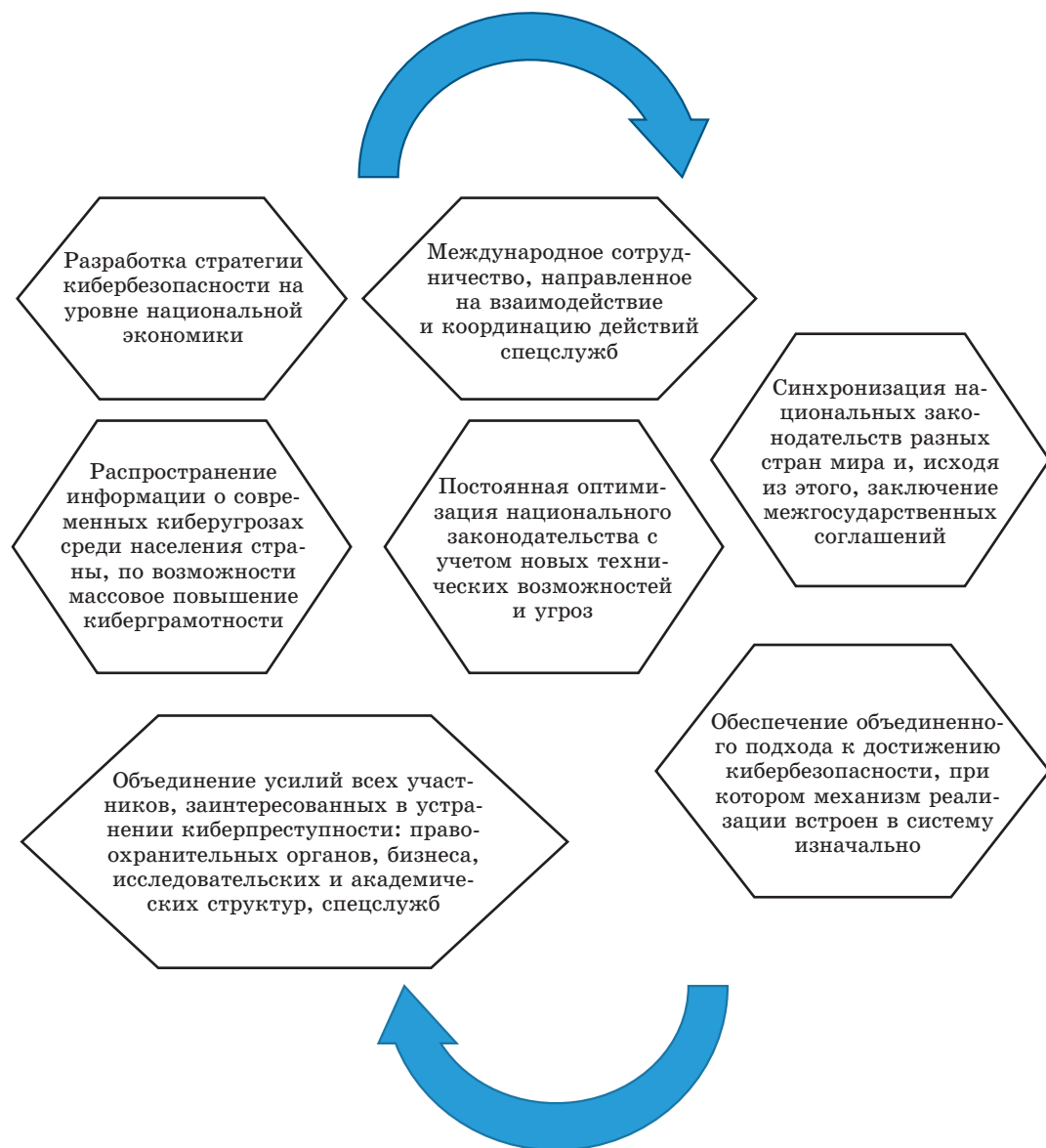


Рис. 4. Компоненты комплексной программы борьбы с киберпреступностью [15]

По результатам проведенного исследования можно предложить следующие действия, которые позволят наиболее эффективно противодействовать киберпреступникам и в целом повысят уровень кибербезопасности в банковской сфере.

Во-первых, нами выделена необходимость создания отделов по предупреждению и противодействию киберпреступности в кредитных организациях, обеспечивающих постоянное повышение квалификации сотрудников этого отдела. Во-вторых, необходимо предусмотреть постоянное обновление систем безопасности кредитно-финансовыми организациями, сотрудничество с производителями антивирусного программного обеспечения.

Помимо этого важно проводить комплексную политику на государственном уровне, учитывающую взаимодействие между государствами и международными организациями, оказывающими помощь в предотвращении угроз и борьбе с недостатками в информационных технологиях банков. Отдельно необходимо отметить важность повышения финансовой грамотности населения путем распространения среди граждан индивидуальных методов и способов защиты личной информации.

Список использованной литературы

1. The Digital Underground Economy: A Social Network Approach to Understanding Cybercrime / M. Yip, N. Shadbolt, N. Tiropanis, C. Webber // Digital Futures. — 2012. — 23–25 October. — URL: http://eprints.soton.ac.uk/343351/1/yip_de2012_submission.pdf.
2. Herley C. Nobody sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy / C. Herley, D. Florencio // Economics of Information Security and Privacy. — 2010. — Vol. 10. — P. 33–53.
3. Mello J.P. Cybercrime Fueled by Mature Digital Underground / J.P. Mello // CSO. — 2013. — Jun. 27. — URL: <http://www.csoonline.com/article/2133649/identity-access/cybercrime-fueled-by-mature-digital-underground.html>.
4. The Landscape of Cybercrime in Greece / V. Vlachos, M. Minou, V. Assimakopoulos, A. Totska // Information Management & Computer Security. — 2011. — Vol. 19, no. 2. — P. 113–123.
5. Smith G.S. Management Models for International Cybercrime / G.S. Smith // Journal of Financial Crime. — 2015. — Vol. 22, no. 1. — P. 104–125.
6. Ho J. Segmenting Consumers of Pirated Movies / J. Ho, C.B. Weinberg. // Journal of Consumer Marketing. — 2011. — Vol. 28, iss. 4. — P. 252–260.
7. Taylor S.A. Evaluating Digital Piracy Intentions on Behaviors / S.A. Taylor // Journal of Services Marketing. — 2012. — Vol. 26, iss. 7. — P. 472–483.
8. Hjort K. (R)e-tail Borrowing of Party Dresses: An Experimental Study / K. Hjort, B. Lantz // International Journal of Retail & Distribution Management. — 2012. — Vol. 40, iss. 12. — P. 997–1012.
9. Gaspareniene L. Digital Shadow Economy: A Critical Review of the Literature / L. Gaspareniene, R. Remeikiene // Mediterranean Journal of Social Sciences. — 2015. — Vol. 6, no. 6 S5. — P. 402–409.
10. Орешкин М.В. Теневая экономика: сущность, опасные тенденции расширения ее масштабов, организация мер безопасности : учеб. пособие / М.В. Орешкин, В.И. Богачев. — Луганск : Промпечать, 2017. — 96 с.
11. Electronic Banking Security and Customer Satisfaction in Commercial Banks / J. Belás, M. Korauš, F. Kombo, A. Korauš // Journal of Security and Sustainability Issues. — 2016. — Vol. 5, no. 3. — P. 411–422.
12. Журавленко Н.И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере / Н.И. Журавленко, Л.Е. Шведова // Общество и право. — 2015. — № 3 (53). — С. 66–70.
13. Розанова Н.М. Национальная экономика. В 2 ч. / Н.М. Розанова. — 2-е изд., перераб. и доп. — Москва : Юрайт, 2019. — Ч. 1. — 541 с.
14. Калиниченко И.А. Начиная с разборки «железа» / И.А. Калиниченко // Полиция России. — 2017. — № 8. — С. 18–21.
15. Головинов О.Н., Погорелов А.В. Киберпреступность в современной экономике: состояние и тенденции развития / О.Н. Головинов, А.В. Погорелов // Вопросы инновационной экономики. — 2016. — № 6 (1). — С. 73–88.

Информация об авторах

Русакова Оксана Игоревна — кандидат экономических наук, доцент, декан факультета экономики и управления, Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация, e-mail: rusakova.oi@yandex.ru.

Головань Софья Андреевна — кандидат экономических наук, доцент, кафедра финансов и бухгалтерского учета, Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация, e-mail: free9sonjas@gmail.com.

Authors

Oksana I. Rusakova — PhD in Economics, Associate Professor, Dean of the Faculty of Economics and Management, Irkutsk State Transport University, Irkutsk, Russian Federation, e-mail: rusakova.oi@yandex.ru.

Sofia S. Golovan — PhD in Economics, Associate Professor, Department of Finance and Accounting, Irkutsk State Transport University, Irkutsk, Russian Federation, e-mail: free-9sonjas@gmail.com.

Для цитирования

Русакова О.И. Влияние киберпреступлений на банковскую систему России / О.И. Русакова, С.А. Головань. — DOI: 10.17150/2411-6262.2021.12(1).1 // *Baikal Research Journal*. — 2021. — Т. 12, № 1.

For Citation

Rusakova O.I., Golovan S.S. The Impact of Cybercrimes on the Banking System of Russia. *Baikal Research Journal*, 2021, vol. 12, no. 1. DOI: 10.17150/2411-6262.2021.12(1).1. (In Russian).