ФИНТЕХ-ИНДУСТРИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Перцева С.Ю.,
к.э.н., доцент кафедры международных финансов,
МГИМО МИД России

В статье анализируются основные достижения индустрии финансовых технологий с позиции влияния на информационную безопасность. Рассматриваются источники возникновения и основные каналы распространения кибер-угроз. Исследуется рынок киберстрахования в России.
Ключевые слова: *финтех, инновационные финансовые технологии, киберриски*

S.Pertseva. Fintech industry and information society. The article analyzes the main achievements of the financial technology industry from the standpoint of the impact on information security. We consider the sources of origin and the main channels for the spread of cyber threats. The cyber insurance market in Russia is being studied.
Key words: fintech, innovative financial technologies, cyberrisk

Бурное развитие информационных технологий и цифровых решений является ярким трендом в развитии современной мировой экономики. Наиболее значительно проявляется данная тенденция в финансовой сфере. Инновационные финансовые технологии меняют традиционные подходы к реализации операций в банковском, инвестиционном, расчетно-платежном страховом сегментах и пр.

Рассмотрим основные достижения индустрии финансовых технологий (далее по тексту ФИНТЕХ) (табл. 1).

Таблица 1. Инновационные цифровые решения

Инновационный инструмент	Краткая характеристика
Облачные системы	Новационная масштабируемая эластичная технология, представляющая собой вид вычислений для предоставления услуг через Интернет
Роботизация	Технология, позволяющая организациям конфигурировать программное обеспечение (программных роботов) на исполнение механических операций на уровне пользовательского интерфейса) использует программное обеспечение для выполнения повторяющихся задач и автоматизации процессов
Визуализация	Метод инновационного использования изображений и интерактивных технологий для изучения больших наборов данных с высокой плотностью. Визуализация дополняет интеллектуальные ресурсы предприятий и деловых площадок, предоставляя удобные в использовании интерактивные материалы с богатой графикой
Расширенная аналитика	Способ совершенствования финансовой деятельности на основе прогнозного моделирования
Когнитивные вычисления	Технология, включающая в себя: машинное обучение; распознавание речи; обработку аутентичного текста; машинное зрение; искусственный интеллект.
Вычисления в оперативной памяти	Технология, предусматривающая хранение данных на портативном запоминающем устройстве для получения быстрого отклика. Данные сжимаются, требования к хранилищу снижаются. Результатом является высокая скорость совершения операции и доступ к большому количеству данных.
Технология блокчейн	Технология, представляющая собой цифровой регистр, где транзакции проверяются и надежно хранятся в сети распределенных и подключенных узлов, без управляющего центрального органа.

Источник: составлено автором на основе [1]

Как видно данных из таблицы 1, арсенал инновационных финансовых технологий, развиваясь, систематически обновляется. Полагаем, что это эволюционное развитие экономической и цивилизационной системы в целом. Являясь закономерным процессом, индустрия финтеха оказывает как положительное, так и отрицательное влияние на жизнь общества.

[1]Умные финансы: современные технологии в международных финансах: сб.докладов / под ред. В.Д.Миловидова, С.Ю. Перцевой. – Москва: МГИМО –Университет, 2018.

Принято полагать, что позитивными последствиями финтеха являются облегчение доступа к финансовым продуктам и услугам, создание конкурентной среды в банковским и корпоративном секторах, внедрение цифровых проектов, способствующих обеспечению устойчивой финансовой системы, снижению транзакционных издержек, быстрому и эффективному осуществлению расчетов, как в рамках отдельного государства, так и на международном уровне и т.д.

В тоже время внедрение достижений отрасли финансовых технологий сопряжено со значительными рисками, ключевым среди которых является киберриск.

Киберриск - это подмножество совокупных рисков, которые сочетают в себе одновременно риски информационной безопасности и информационных технологий. К ним относятся риски, которые стали последствием реализации преднамеренных злоумышленных действий, направленных на неавторизованное раскрытие, изменение или разрушение цифровых активов[2].

В этой связи особую важность приобретает проблема обеспечения кибербезопасности. Рассмотрим основные киберинциденты в мировой практике финансовых организаций и корпораций (табл. 2).

Таблица 2. Мировые кибератаки

№	Год	Киберинцидент	Описание	Финансовый ущерб
1.	1988г.	Червь Морриса	Один из первых сетевых червей, распространяемых через интернет, написанный аспирантом Корнеллского университета Р. Т. Моррисом. Запущен в Массачусетском технологическом институте.	96,5 млн. долл.
2.	1998г.	«Чернобыль»	Первая вредоносная программа, способная повредить аппаратную часть компьютера – микросхему Flash BIOS.	100 млн. долл.
3.	1999г.	Melissa	Первый вредоносный код, распространяющийся по электронной почте, нарушая работу почтовых серверов нескольких крупных компаний во многих странах.	80 млн. долл.

2 Управления рисками ИТ и ИБ в условиях современных вызовов [Электронный ресурс]. Режим доступа: http://profitday.kz/Content/files/2015/interbank/2-1.pdf

4.	2000г.	Mafiaboy	Одна из первых полномасштабных DDoS-атак (распределенный отказ в обслуживании) через интернет-серверы крупных компаний. Атаку на несколько известных сайтов, включая Yahoo, Fifa.com, Amazon, Dell, eBay и CNN, начал ученик канадской средней школы.	1,2 млрд. долл.
5.	2004г.	Cabir	Первый мобильный вирус – полноценный компьютерный червь, заражавший мобильные телефоны.	Более 1 млрд. долл.
6.	2007г.	ZeuS	Троянская программа, первый в истории случай распространения вредоносного софта через социальные сети. Программа внедрялась в систему, перехватывала регистрационные данные пользователя, что позволяло похищать средства со счетов клиентов ведущих европейских банков. Вирусная атака затронула Испанию, Италию, Германию и Нидерланды. Атакам подверглись не только персональный компьютер жертвы, но и мобильные устройства.	Более 1 млрд. долл.
7.	2010г.	StuxNet	Первый вирус военного назначения и первое реально использованное кибероружие. Вывел из строя ядерные объекты Ирана, физически разрушив инфраструктуру: тогда могло пострадать до 20% ядерных центрифуг Ирана.	Не уточняется

8.	2014г.	Lazarus	Вирус привел к масштабной утечке личных данных сотрудников Sony Pictures, электронной почты и неизданных фильмов киностудии.	100 млн.долл.
9.	2016г.	Industroyer	Специально разработанный для атак на энергетические компании вирус. Использует четыре легитимных протокола связи, широко распространенных в энергетике, управлении транспортом, водоснабжении и др. Как следствие, он не требует от хакеров предварительного поиска уязвимостей в сетях.	Не уточняется
10.	2017г.	WannaCry	Вирус-шифровальщик атаковал 200 000 компьютеров в 150 странах мира. Вирус проникал на компьютеры с операционной системой Windows, куда не были установлены обновления, шифровал содержимое жестких дисков и требовал с пользователей $300 за расшифровку.	1 млрд. долл.

Источник: составлено автором на основе[3]

Число хакерских атак на информационные ресурсы постоянно возрастает, что приводит к значительным потерям и убыткам для компаний. По оценкам ФСБ России мировой ущерб от подобных атак может составлять 0,4-1,5% мирового ВВП[4].

Самое значительное количество хакерских атак наблюдается в банковской сфере и в сфере расчетов и платежей. Злоумышленников интересуют персональные данные владельцев счетов, платежных карт и виртуальных кошельков, PIN – коды и другая финансовая информация.

[3] Эксперты антивирусных компаний «Доктор Веб», Eset и «Лаборатории Касперского», а также компании Digital Security (анализ уязвимостей IT-систем), www.vedomosti.ru

4 ФСБ оценила ущерб от кибератак в мире в сумму от $300 млрд до $1 трлн [Электронный ресурс] / РБК – Режим доступа: https://www.rbc.ru/technology_and_media/02/02/2017/5892f53b9a7947133199f417

Количество несанкционированных операций в российском банковском секторе является весьма существенным (табл.3).

Таблица 3.

Несанкционированные операции в российском банковском секторе за 2015-2017 гг.

Период		Несанкционированное списание со счетов физических лиц[5]		Несанкционированное списание со счетов юридических лиц	
		число операций, шт.	размер операций, млн. руб.	число операций, шт.	размер операций, млн. руб.
2015г.	1кв.	72,2	315,4	210	415,4
	2кв.	61,7	271,5	265	1036,5
	3кв.	69,1	299,7	366	1732,2
	4кв.	57,9	260,4	223	609,5
2016г.	1кв.	63,1	253,1	196	352,6
	2кв.	65,8	244,0	161	342,5
	3кв.	77,5	293,9	164	428,7
	4кв.	90,3	284,4	196	770,6
2017г.	1кв.	90,2	246,2	182	405,6
	2кв.	78,3	229,5	256	440,3
	3кв.	64,1	225,7	217	343,7
	4кв.	84,6	259,9	186	380,0

Источник: составлено автором на основе[6]

Как показывают данные таблицы 3, количество и размер операций, связанных с несанкционированным списанием средств с банковских счетов клиентов - физических и юридических лиц остается весьма значительным за представленный период. Видно, что мошенники предпочитают осуществлять атаки на компании, в основном, представителей малого и среднего бизнеса. Крупный бизнес является более защищенным в связи с использованием дорогостоящих систем диагностики и предотвращения киберугроз. Немаловажным являются новые правовые нормы, устанавливающие жесткое наказание за кибератаки на стратегически важные компании.

При этом, в сегменте операций, связанных с незаконным списанием средств со счетов физических лиц в основном преобладает социальный инженеринг и применение новых мошеннических схем. В частности, ФИНЦЕРТ - структура Банка России, занимающаяся кибербезопасностью финансовой сферы, раскрыла 1668 фишинговых доменов. Это мошеннические сайты или сайты компаний, не имеющих лицензии Центрального банка на оказание предлагаемых финансовых услуг. Кроме того, выявлены основные

[5] Списание средств производилось с платежных карт

[6] ФИНЦЕРТ, www.cbr.ru

каналы кибератак на счета клиентов посредством вредоносного программного обеспечения (табл. 4).

Таблица 4.

Разновидности вредоносного программного обеспечения

№	Вид вредоносных программ	Частота применения
1	Атаки на финансовые организации	40,2
2	Атаки на клиентов финансовых организаций	36,4
3	Программы- вымогатели	11,7
4	Прочее	11,7

Источник: составлено автором на основе[7]

Таблица 4 демонстрирует преобладание хакерских атак на финансовые организации. Целью данных киберинцидентов являются атаки на кредитные организации для получения контроля над их инфраструктурой, прежде всего, платежной. Особенность атак состоит в попытках подмена информации в процессинговом механизме банковской структуры, похищении денежных средств с помощью системы SWIFT. Человеческий фактор – одна из причин распространенности кибератак на финансовые организации: сотрудники открывают подозрительные письма, не обновляют программное обеспечение, используют простые пароли. Кроме того, в ряде банков уделяется незначительное внимание системе внутренней безопасности (нет сегментирования сети, неправильно настроена система управления событиями информационной безопасности и т.д.).

Кибератаки на клиентов финансовых организаций также являются весьма частыми. Основная причина распространенности – социальная инженерия, инструментарий которой совершенствуется вместе с внедрением достижений индустрии финтеха. По данным Сберегательного банка России каждую неделю на клиентов осуществляется свыше 5000 хакерских атак методами социальной инженерии. Число кибератак растет: в январе – мае 2018 г. Сбербанк зафиксировал в 1,5 раза больше мощных DDoS-атак, чем за аналогичный период прошлого года (за весь 2017 год их было 48)[8].

Представляется важным оценить финансовый ущерб российских банков от реализации кибератак (табл.5)

Таблица 5.

Ущерб российских банков от кибератак

Вид потерь	млрд. руб.
Украдено со счетов юридических лиц	1,57
Украдено со счетов банков	1,35
Украдено со счетов физических лиц	0,96

Источник: составлено автором на основе[9]

[7] ФИНЦЕРТ, www.cbr.ru
[8] Сбербанк, www.sberbank.ru
[9] ФИНЦЕРТ, www.cbr.ru

В настоящее время Центральным банком России предпринимаются решительные меры по выявлению, предотвращению и борьбе с кибератаками.

Одним из новационных решений в данной сфере является требование Банка России о предоставлении коммерческими банками полной и своевременной информации о кибератаках, включая данные об устройствах, с помощью которых похищали деньги.

Пристальное внимание со стороны регулятора к киберрискам обусловлено их постоянным ростом, совершенствованием механизма их реализации и растущим ущербом. Кроме того, следует понимать, что высокая частота кибератак может обусловить реализацию социальных и политических рисков. Поэтому для монетарного органа приоритетной задачей является предотвращение рисков и минимизация их последствий.

Проблема реализации киберрисков является общемировой. Среди стран –лидеров по количеству кибератак следует выделить США (57% от общего количества кибер- инцидентов), Россия, Великобритания и т.д. (рис. 1).

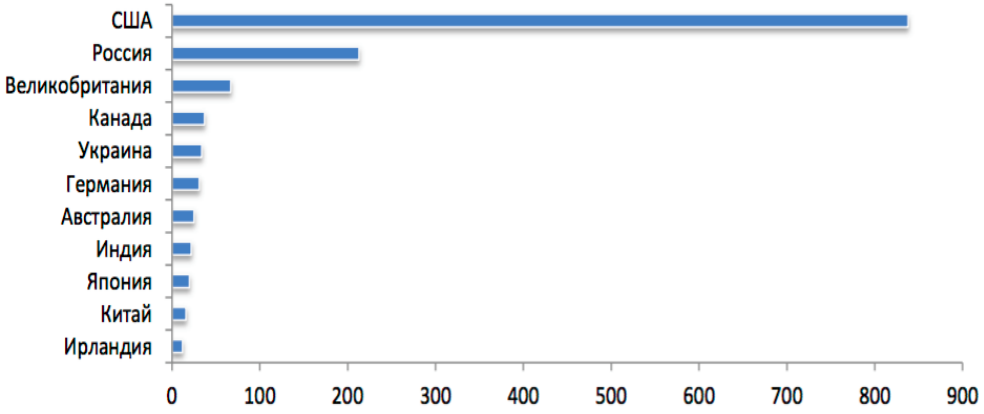

Рис 1. Число утечек информации по странам

Источник: по данным аналитического центра InfoWatch[10]

Появление особого направления в развитии страхового сегмента – киберстрахования, является объективной необходимостью в цифровой экономике.

Рынок киберстрахования более 10 лет функционирует в США. По оценкам по оценкам PwC, к 2020 году его размер достигнет 7,5 млрд. долл.[11]

Лидерами рынка являются крупнейшие мировые страховщики: Allianz, Lloyd's, AIG, Chubb и др.

В настоящее время в России назрела необходимость развития системы киберстрахования. По предварительным оценкам, расходы федерального

10 Глобальное исследование утечек конфиденциальной информации в 2016 году [Электронный ресурс] / Аналитический центр InfoWatch – Режим доступа: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2016_year.pdf

11 Там же.

бюджета на популяризацию киберстрахования составят 200 млн. руб. в ближайшие годы.[12]

Важными проблемами, препятствующими развитию киберстрахования в России являются:

- сложность выявления и идентификации киберрисков;
- неполнота и несвоевременность информации о реализации киберугроз в связи с наличием высоких репутационных рисков;
- невозможность предусмотреть в страховом договоре полного покрытия ущерба от реализации киберинцидентов;
- недостаточность капитальной базы российских страховых организаций (ни одна страховая компания не сможет принять на себя обязательства по страхованию киберрисков крупных российских банков, так как даже единичный значимый ущерб банка по этому риску станет фатальным для любого страховщика);
- существуют сложности с оценкой возможного ущерба кредитной организации при реализации киберриска, а значит, трудно рассчитать стоимость страхового полиса;
- расходы на страхование от кибератак не освобождаются от налогообложения;
- отсутствует правовая база регулирующая киберстрахование.

Несмотря на отмеченные препятствия, система киберстрахования должна стать неотъемлемой частью финансового рынка. Важную роль в этом процессе должен сыграть мегарегулятор в лице Банка России. Создание адекватного правового поля, объективных требований к капиталу, резервам, показателям финансовой устойчивости страховых компаний, позволит минимизировать потери российской финансовой системе от киберугроз.

Важное значение должно отводиться системам ранней диагностики, тестированию и оптимизации процессингового механизма, каналов связи, информационных систем и технологии. Понимая, что преступная мысль не дремлет, а достижения индустрии финтеха используются в том числе и для совершения мошеннических действий, важно осуществлять предиктивные меры. Своевременное выявление киберрисков, достоверное и в полном объеме получение информации о возможных киберинцидентах, передача сигналов контролирующим органам – факторы обеспечения информационной безопасности.

Таким образом, цифровая революция, обусловленная появлением и активным внедрением инновационных технологий, ставит перед обществом новые вызовы и угрозы. Одной из стратегически важных угроз является нарушение информационной безопасности.

---

12 Тренды развития ИТ в страховании. Киберстрахование. Страхование киберрисков. "Умное" страхование [Электронный ресурс] – (Режим доступа: http://www.tadviser.ru/index.php/Статья:Тренды_развития_ИТ_в_страховании_(киберстрахование_и_телематические_данные)

Участникам финансовых операций необходима уверенность в обеспечении безопасности данных, возможности минимизации киберрисков и защиты от киберугроз.

Возрастающий финансовый ущерб от реализации кибератак в сочетании с возрастающим объемом информационных данных, хранящихся в сетевой инфраструктуре, обусловливают необходимость разработки новых инструментов, обеспечивающих информационную безопасность.

Список литературы:

1. Глобальное исследование утечек конфиденциальной информации в 2016 году [Электронный ресурс] / Аналитический центр InfoWatch – Режим доступа: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2016_year.pdf
2. Сбербанк, www.sberbank.ru
3. Списание средств производилось с платежных карт
4. Тренды развития ИТ в страховании. Киберстрахование. Страхование киберрисков. "Умное" страхование [Электронный ресурс] – (Режим доступа: http://www.tadviser.ru/index.php/Статья:Тренды_развития_ИТ_в_страховании_(киберстрахование_и_телематические_данные)
5. Умные финансы: современные технологии в международных финансах: сб.докладов / под ред. В.Д.Миловидова, С.Ю. Перцевой. – Москва: МГИМО –Университет, 2018.
6. Управления рисками ИТ и ИБ в условиях современных вызовов [Электронный ресурс]. Режим доступа: http://profitday.kz/Content/files/2015/interbank/2-1.pdf
7. ФИНЦЕРТ, www.cbr.ru
8. ФСБ оценила ущерб от кибератак в мире в сумму от $300 млрд до $1 трлн [Электронный ресурс] / РБК – Режим доступа: https://www.rbc.ru/technology_and_media/02/02/2017/5892f53b9a7947133199f417
9. Эксперты антивирусных компаний «Доктор Веб», Eset и «Лаборатории Касперского», а также компании Digital Security (анализ уязвимостей IT-систем), www.vedomosti.ru