Ю. С. Вигриянова,
Уральский федеральный университет, Екатеринбург, Россия

КИБЕРУГРОЗЫ В ЭКОЛОГИЧЕСКИХ ПРОЕКТАХ КОММЕРЧЕСКОГО БАНКА

The spread of environmental innovations in the financial sector is associated with the new types of fraud. The paper discusses the features of cyber risks in innovative «green» projects. «Green» initiatives are subject to the risks of increased cyber security, as they affect the area of significant financial flows.

Мировой рынок киберпреступлений активно развивается. Ключевой целью кибермошенников по-прежнему остаются инновационные, в том числе «зеленые» проекты кредитно-финансовых организаций.

Банковский сектор мирового сообщества наращивает позиции в «зеленом» финансировании. Для масштабирования объемов природоохранных «зеленых» инвестиций задействованы разнообразные финансовые инструменты – государственные кредиты и гарантии, гранты, долговые обязательства, «зеленые тарифы на подключение» (продажа возобновляемой энергии), кредитные линии, акционерный и венчурный капитал. В связи с повсеместным ростом интереса к проблемам экологии, финансовые институты, способные структурировать и направлять инвестиции на обеспечение охраны окружающей среды, становятся все более и более востребованными. Мировые инвестиции в возобновляемые источники энергии в 2018 г. составляли 332,1 млрд долл. [1]. В России финансовые институты только начинают кредитовать «зеленую» экономику, но не вкладывают средства на длительное время (более 10–20 лет).

Экологические новации привлекают новый круг эмитентов и держателей промышленного и гражданского сектора, влияют на себестоимость продуктов. поскольку, как правило, государство поддерживает природоохранные проекты через субсидирование. Интерес инвесторов к «зеленой» проблематике, независимо от исторических и культурных факторов, особенностей системы регулирования, увеличивается. К данным сферам относятся проекты ресурсоэффективности, адаптации к изменению климата.

Однако распространение данных экологических инноваций в финансовой сфере сопряжено с появлением новых видов мошенничества, которые всегда активизируется в новых областях экономической деятельности. «Зеленые» инициативы подвержены рискам повышенной киберопасности, т. к. затрагивают область значительных финансовых потоков на проекты возобновляемой энергетики, энергоэффективности, сферы управления отходами и переработки отходов, очистки сточных вод.

Так, ПАО «Сбербанк» совместно с Минприроды инициировал шестилетний проект «Чистый воздух» стоимостью 480 млрд рублей, входящий в нацпроект «Экология» [2]. Ситибанк в номинации «Самый зеленый банк в мире» по результатам 2018 г. занял первое место среди компаний, вкладывающихся в энергоэффективные проекты. Ситибанк завершает десятилетний проект финансирования $ 50 млрд. в течение 10 лет на программы по борьбе с глобальными изменениями климата [3].

В 2017 г. (год экологии) рабочая группа по экологии Экспертного совета при правительстве РФ предложила создать в России «зеленый банк». Предполагаемые источники фондирования – средства федерального бюджета, кредиты международных институтов развития и эмиссия зеленых облигаций. Кредитный портфель банка, сформированный из проектов по внедрению наилучших доступных технологий, возобновляемых источников энергии, переработки мусора, зеленого строительства, экологических программ компаний, составит 600–730 млрд руб. [4].

Газпромбанк занимается возобновляемой энергетикой уже более пяти лет. Совместно с группой компаний «Хевел» реализуется проект в сфере солнечной и ветроэнергетики. На развитие данных технологий в общей сложности выделены кредиты в размере 80 млрд руб. сроком свыше 10 лет [4].

Банковскому риску подвержены все типы проектов, включая экологические, как вероятность (угроза) потери банком части своих ресурсов, недополучения доходов или произведения дополнительных расходов в результате осуществления определенных банковских операций [5].

Банковский сектор подвергается кибератакам, которые отнимают значительную долю финансового и интеллектуального потенциала для обеспечения системы защиты. Однако сегодня моделированию кибер-рисков в эко-проектировании банковского сектора уделяется недостаточно внимания из-за трудностей анализа и оценки данного вида рисков.

Понятие «кибер-риска» как вероятность нанесения экономического, технического или информационного ущерба вследствие угроз, совершаемых с помощью программно-технических средств, а также в результате ежедневной работы с информационными сетевыми технологиями расценивается как столкновение с информационными хищениями, онлайн-мошенничество, вирусная или спам-атака, внедрение шпионским программам.

Экологическая составляющая финансовых проектов в современной экономике рассматривается как дополнительное конкурентное преимущество рыночных контрагентов, поэтому именно эко-информация в последнее время стала объектом повышенного внимания кибер-шпионов.

Особенности кибер-рисков [6] связаны с вероятностным и непредсказуемым характером их проявления, трансграничностью. В процессе финансово-хозяйственной деятельности предприятий и банковских учреждений вероятность того, что произойдет кибератака, определяется действием объективных и субъективных факторов, сложно прогнозируемо и сопровождается преимуществами со стороны киберпреступников, которые применяют различные механизмы шифрования и анонимности.

Риск в финансово-хозяйственной деятельности соотносится с уровнем возможных отрицательных последствий. Он всегда сопряжен с неблагоприятными результатами: потеря прибыли, капитала предприятия (банка), дестабилизация экологического равновесия.

В итоговых документах конвенции Совета Европы [7] виды киберпреступлений объединены в пять групп. С учетом экологических последствий, классификация кибер-рисков представлена в таблице.

Таблица

Классификация кибер-рисков при реализации экологических проектов

Группа	Содержание
1	Преступления, направленные против компьютерных данных экологического проекта
2	Противоправные деяния, связанные с использованием технологий
3	Правонарушения, связанные с контентом экологического проекта
4	Нарушение авторских и смежных прав
5	Деяния, посягающие на экологическую безопасность

Составлено автором

Первая группа включает все компьютерные преступления, направленные против компьютерных данных и систем (например, незаконный доступ, вмешательство в данные или системы в целом).

Вторую группу составляют противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, получение экономической выгоды иными способами).

Правонарушения третьей группы связаны с содержанием данных или контентом.

Нарушение авторских и смежных прав относится к четвертой группе, выделение определенных видов преступлений в которой отнесено к законодательству конкретных государств.

Кибертерроризм, связанный с дестабилизацией экологической обстановки включается в пятую группу киберпреступлений.

По статистике ООН ежегодный экономический ущерб от хищения онлайн-данных в банковском секторе составляет в среднем $ 100 млрд. [8]. Рост количества киберпреступлений в России продолжается, а банковский сектор является одним из наиболее пострадавших от деяний кибермошенников. Для кредитных организаций очень важно эффективное управление кибер-рисками, которое поможет свести к минимуму величину потерь от данных угроз.

Под оценкой банковских рисков в экологических проектах понимается процесс выявления факторов риска, а также качественное (на основе экспертных

мнений) и количественное определение затрат, которые имеют взаимосвязь с рисками во время осуществления банковских операций [9].

Управление кибер-риском в экологическом проектировании включает в себя:

– разработку политики в области управления кибер-риском;

– анализ рисковой ситуации – выявление факторов риска и оценка его возможного уровня, предугадывание поведения хозяйствующих субъектов в этой ситуации;

– разработку альтернативных вариантов решения и выбор наиболее приемлемого и правомерного из них;

– определение доступных путей и средств минимизации кибер-риска;

– подготовку мер по нейтрализации, компенсации ожидаемых негативных последствий риск-решений.

Кибербезопасность финансирования экологических проектов – это совокупность условий, при которых все составляющие киберпространства защищены от любой угрозы и нежелательного воздействия. Киберпространство – среда, образованная совокупностью коммуникационных каналов Интернета и других сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства), а информационное пространство – совокупность всей информационной деятельности человечества [10].

Для оценки банковских рисков, в частности кредитного риска, применяется модели, каждая из которых является уникальной в своем роде. Однако, для оценки кибер-рисков крайне необходима модель, которая будет учитывать все нюансы данного вида риска и поможет банку избежать потерь.

Мировой рынок киберпреступлений активно развивается. Ключевой целью кибермошенников по-прежнему остаются инновационные, в том числе «зеленые», проекты кредитно-финансовых организаций.

Киберпреступники значительно расширили свой спектр проникновения в финансовое проектирование путем проникновения в инфраструктуру банков, систему электронных денег, криптовалютные биржи, фонды управления капиталом и даже казино, последствиями чего стали выводы крупных сумм денежных средств. Количество и качество кибератак на финансовые организации продолжает расти.

В 2018-м г. на форуме Давосе были даны оценки ежегодных потерь от кибератак: от 1,5 до 3 трлн долларов [11]. Лидерами среди стран, пострадавших от киберпреступности, являются США, Китай и Бразилия.

Развитие информационных технологий, происходящее в современном мире, несет за собой негативные последствия в виде развития киберпреступности, которая постоянно порождается новыми видами атак, инструментов и методов, которые позволяют мошенникам проникать в наиболее сложные и контролируемые среды, наносить большой урон и зачастую оставаться незамеченными.

ЛИТЕРАТУРА

1. Информационно-отраслевой ресурс Energy Media. [Электронный ресурс]. – Режим доступа: https://eenergy.media//mirovye-investitsii-v-vie-v-2018-godu-upali-na-8-protsentov/ 2019.01.17. (дата обращения 12.04.2019).

2. Второе дыхание: Зачем Сбербанк участвует в проекте чистый воздух // Агентство РБК. [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/business/06/12/2018/5c078eeb9a794777c783bbea (дата обращения 12.04.2019).

3. Citi targets $50 dillion over 10 years to adress global climate change. [Электронный ресурс]. – Режим доступа: http://www.citibank.com/slovakia/homepage/english/docs/20070508_ts.pdf (дата обращения 12.04.2019).

4. Зеленые кредиты и облигации предлагает Минприроды // Агентство Banki.ru [Электронный ресурс]. – Режим доступа:

https://www.banki.ru/news/bankpress/?id=9788926 07.06.2017. (дата обращения 12.04.2019).

5. Тарасов, В. И. Деньги, кредит, банки: учебное пособие / В. И. Тарасов. – Москва: Мисанта, 2003. – 512 с.

6. Вигриянова, Ю. С. Современные тенденции развития киберпреступности в банковском секторе. / Ю. С. Вигриянова, Г. С. Чеботарува // Весенние дни науки ВШЭМ: сборник докладов международной конференции студентов, аспирантов, молодых ученых. – 2017. – С. 113–116.

7. Конвенция Совета Европы о киберпреступности *ETS* № 185.

8. Доклад ООН [Электронный ресурс]. – Режим доступа: // unodc.org – URL: http://www.unodc.org/documents/congress//Documentation/IN_SESSION/ACONF222_L3ADD1_e_V1502497.pdf (дата обращения 12.04.2019).

9. Риски – понятие и виды. Классификация рисков. Основные характеристики рисков [Электронный ресурс] – Режим доступа: grandars.ru – URL: http://www.grandars.ru/student/fin-m/vidy-riskov.html (дата обращения 12.04.2019).

10. Проект концепции стратегии кибербезопасности в России. [Электронный ресурс] – Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения 12.04.2019).

11. РИА Федерал-Пресс [Электронный ресурс] – Режим доступа: https://news.rambler.ru/other/41739414/?utm_content=rnews&utm_medium=read_more&utm_source=copylink. (дата обращения 12.04.2019).