УДК 336.71

Важнейшие элементы единой системы обеспечения кибербезопасности банковского сектора Российской Федерации

Караева Ю.А., студентка
e-mail: kar-yulka@mail.ru
Сайбель Н.Ю., к.э.н, доцент кафедры теоретической экономики
ФГБОУ ВО «Кубанский государственный университет»
e-mail:
Россия, Краснодар

Аннотация. Исследование посвящено разработке единой системы обеспечения кибербезопасности банковской сферы России. Рассмотрены причины, по которым банки претерпевают существенные потери. Предложен механизм, позволяющий в перспективе в разы снизить огромные доходы киберпреступности, наблюдающиеся в настоящий момент.

Ключевые слова: киберпреступления, информационная безопасность, киберпространство, банковский сектор, киберугрозы.

В последние годы в связи с всеобщей информатизацией и компьютеризацией банковской деятельности значение информационной безопасности банков многократно возросло. Сегодня из-за повсеместного распространения электронных платежей, пластиковых карт, компьютерных сетей объектом информационных атак стали непосредственно денежные средства как банков, так и их клиентов. Всем известно, что ежедневная работа банковских систем непосредственно сопряжена с использованием современных компьютерных технологий и находится в полной зависимости от надежной и бесперебойной защиты электронно-вычислительных систем. Международная практика говорит об абсолютной уязвимости каждой фирмы по причине того, что киберпреступления не имеют государственных границ, вследствие чего хакеры обладают возможностью в равной мере угрожать информационным системам в любой точке мира.

Необходимо отметить, что правонарушители моментально приспосабливаются к изменяющейся обстановке, непрерывно следят за слабыми местами и внедряются значительно быстрее, чем службы безопасности банка, которые устанавливают обновления. На подпольных форумах любой пользователь имеет возможность беспрепятственно получить программное обеспечение с целью проведения атаки, приобрести детальное руководство как работать, и помимо этого познакомиться с недобросовестными сотрудниками банков и омывателями денег. При правильной подготовке злоумышленник с минимальными техническими знаниями может украсть миллионы долларов, проникнув в банковскую сеть, хотя может показаться, что такие сети должны быть хорошо защищены [1].

Количество киберпреступлений в России с каждым годом растет более, чем на 100%. Атакам киберворов подвергаются кредитные организации разных размеров. Однако злоумышленники более заинтересованы именно в средних банках, которые располагают значительной долей активов, однако в то же время недостаточно инвестируют в безопасность. При этом атаки на банковских клиентов уходят на второй план в пользу выведения денежных средств из самих банков или иных финансовых организаций.

Банки претерпевают существенные потери по целому ряду причин:

– отсутствие необходимой степени защиты от киберугроз по причине незначительной доли инвестирования в безопасность. В маленьких и средних банках акцент ставится, в первую очередь, на оптимизацию издержек, при этом недостаточно внимания уделяется автоматизированным системам и приложениям, не отвечающим требованиям информационной безопасности;

– недостаток эффективности мер, предпринимаемых кредитными организациями по выполнению рекомендаций Банка России в области стандартизации и обеспечения информационной безопасности [2];

– недостаток риск-ориентированного внутреннего контроля в кредитных организациях, позволяющего своевременно реагировать на угрозы, либо вовсе их избегать [3];

– несовершенство программного и аппаратного обеспечения автоматизированных систем и приложений в области защиты, что является следствием множественных уязвимостей;

– отсутствие среди кредитно-финансового сообщества объединенных усилий по борьбе с мошенниками, которые могли бы избавить организации от кибератак, а не только минимизировать потери.

Чтобы обезопасить себя от угроз кибермошенников, кредитным организациям следует сформировать единую систему обеспечения безопасности, которая обязана содержать следующие компоненты:

1. Оценка рисков. Первое, что необходимо сделать для формирования надежной защиты от кибератак – уделять больше внимания объективной и разносторонней оценке рисков [4]. С этой целью нужно изучить вероятность угроз информационной безопасности и дать оценку возможного ущерба целенаправленных атак.

2. Поддержание ключевых основ информационной безопасности:

– контроль и анализ (реализация периодического анализа всех элементов программного обеспечения для своевременного определения наличия уязвимостей);

– многоуровневая система защиты (отдельная защита каждой ступени информационной инфраструктуры);

– стандартизация (соответствие каждого компонента программного обеспечения всем условиям внутренних стандартов безопасности);

– мониторинг и аудит (осуществление учета всех процессов на каждом уровне информационной инфраструктуры и централизованное изучение полученных данных);

– централизованное и оперативное реагирование на угрозы;

– минимальные права сотрудников на доступ к информации и выполнение определенных задач (даст возможность снизить вероятность разглашения информации либо ее некорректного применения);

– распределение ответственности за функционирование каждого бизнес-процесса;

– документирование каждой операции и ее отдельных элементов [5].

Также необходима работа с нормативно-правовой базой, а именно утверждение и реализация следующего закона:

– Банк России вносит в список требований для получения лицензии на осуществление банковской деятельности наличие комплексной системы обеспечения безопасности;

– Банк России проверяет уже существующие банки на наличие данной системы: при ее отсутствии деятельность кредитной организации прекращается до момента установки и активации системы; при выявлении недочетов в системе на кредитную организацию возлагается крупный штраф.

Таким образом, реализация данных мер позволит противостоять хакерам и в разы снизить те огромные финансы киберпреступности, которые в настоящий момент не могут не повергать в ужас. Также данная система предоставит банку необходимый фундамент для развития и увеличения доли рынка, так как поддержание информационной безопасности на должном уровне в настоящее время является критерием конкурентоспособности.

Список литературы:

1. Гафнер В.В. Информационная безопасность: Учебное пособие. – Ростов н/Д., 2016.

2. Политика ЦБ в сфере защиты информации (кибербезопасности). URL: http://dialog-e.ru/market-news (дата обращения: 15.06.2019).

3. Кутуб-Заде А.О. Внедрение кибербезопасности в банковской системе, новейшие подходы и разработки риска // Вектор экономики. 2019. № 1(31).

4. Громов, Ю.Ю. Информационная безопасность и защита информации. – Ст. Оскол: ТНТ, 2017.

5. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России 2016 г. URL: http://www.cbr.ru/FinCER.pdf (дата обращения: 16.06.2019).