Секция «Экономика инноваций: экономические и организационные факторы»

Реконструкция модели информационной безопасности в российских банках

Научный руководитель – Кондюкова Елена Станиславовна

Вигриянова Юлия Сергеевна
Студент (бакалавр)
Уральский федеральный университет имени первого Президента России Б.Н.Ельцина,
Высшая школа экономики и менеджмента, Екатеринбург, Россия
E-mail: vigrik1@gmail.com

В экономических системах рост киберугроз является пандемией XXI века. Чем более развит в "цифровом" аспекте рынок, тем более он подвержен "издержкам цивилизации" в виде информационных потерь.

Пресс-релиз компании Juniper Research представил оценку убытков от мошенничества с онлайн-платежами в $22 млрд по итогам 2018 года. К 2023 году прогнозные потери удвоятся и достигнут 48 млрд. долларов [6].

Рост киберпреступлений порождает и новые "вызовы", среди которых рассматриваются трудности с идентификацией вредоносных сайтов; большое количество "уязвимых" пользователей, автоматизация и отсутствие контроля массированной передачи данных; анонимность сети, уязвимость беспроводного доступа и использование прокси-серверов.

Финансовые институты самостоятельно разрабатывают собственные системы защиты информации, оптимизируя процессы обмена информацией с использованием способов идентификации, наличия прав на доступ информации, антивирусами и модулями безопасности. Угроза информационной безопасности (далее - ИБ) в банковской сфере уже давно приобрела черты транснациональности.

Несмотря на сложные системы защиты, банкам не всегда удается отклонить хакерские атаки, а затраты банка на устранение последствий колоссальны.

Необходимо переосмысливать модель реагирования на возмущающие воздействия. В чем суть смены модели? Исходя из представления, что защитить все составляющие контента невозможно, топ-менеджменту банков необходимо выработать стратегию, основанную на понимании и принятии факта о том, что ни одна самая продвинутая система не может гарантировать идеальный результат по предотвращению внешних воздействий и 100%-ную безопасность, даже в условиях привлечения значительного объема средств.

При этом в контексте мониторинга вполне реально сформировать устойчивость (выживаемость) системы в условиях кибератак. Для этого предстоит сконцентрироваться на ключевых, витальных характеристиках системы с вероятностью резервирования, дублирования, контроля жизненного цикла системы и критериях оценки возмущающих воздействий. Так, кибератаки причисляются в банковской сфере к операционным рискам, актуализирующее "рисковое поле" других элементов системы, например, ликвидности, кредитных и репутационных потерь. Банковские организации стремятся "скрыть" причиненный ущерб, т.к. он влечет за собой ухудшение конкурентных позиций.

Соответственно, речь идет о повышении устойчивости банка к воздействиям, при которых для клиентов задержки проведения операций некритичны. Банк обязан обеспечить проведение расчётов в сроки, отведённые на погашение обязательств и возобновить операции в течение двух часов после инцидента [2].

Наиболее популярными моделями обеспечения "безопасности" становятся DR (Detection & Response) - "обнаружение и реагирование", смысл которых заключается в постулатах "теории надежности", разработанной научными школами советского времени еще до 90-х

годов XX века. Под надежностью понимают "вероятность" стабильной работы от момента начала работы до первого отказа системы. Надежность характеризуется ожидаемым поведением системы в смысле ошибки ее функционирования в заданном интервале времени, потерей работоспособности, которая может быть восстановлена только путем внешней корректировки [1].

Сегодня при изменении модели реагирования на угрозы потери информационных массивов в глоссарии специалистов по инфобезопасности закрепляется дефиниция "киберустойчивость" по аналогии с другими аспектами устойчивого развития банковских организаций. Киберустойчивость - показатель реагирования на кибератаки при сохранении эффективности функционирования бизнеса [5].

Базой для формирования киберустойчивости отдельного банка являются бизнес-процессы управления инцидентами, обеспечение непрерывности бизнеса, систематическое повышение квалификации персонала по информационной безопасности, систематическая оценка эффективности ИБ.

ИБ финансовой сферы страны охватывает информационную инфраструктуру всего финансового рынка Российской Федерации, включающих Банк России, ключевые банки, фондовые биржи, национальную систему платёжных инструментов. Общий уровень безопасности инфраструктуры зависит от "слабого звена", а слабым звеном может оказаться любая организация в системе, не уделяющая должного внимания вопросам безопасности. Например, для небольших кредитно-финансовых организаций вопрос кибербезопасности все ещё занимает второстепенное место. Так, в деятельности пятидесяти девяти российских банков регулятором были выявлены нарушения, связанные, прежде всего, с человеческим фактором, беззаботным отношением менеджеров и собственников к существованию киберугроз, низкой ответственностью сотрудников, неудовлетворительной организацией внутреннего аудита [3]. В данном аспекте необходим постоянный мониторинг системы контрагентов и коммуникаций (специалистов банка, партнеров, контрагентов, поставщиков).

Эффективным экономическим инструментом выступает страхование кибер-рисков. Кроме покрытия расходов связанных с прямым ущербом и устранением последствий атаки, страховой полис может покрывать обязательства по защите данных, безопасности сети, издержки от тайм-аута в функционировании, возникающие в случае успешной хакерской атаки, а также такие угрозы, как кибер-шантаж и телефонное хакерство. Первой компанией, которая представила страхование рисков киберугроз на российском рынке, стала АО "АИГ", несущая опыт урегулирования страховых случаев в данной сфере [7].

Инструментом контрольно-надзорной деятельности регулятора в области информационной защиты является масштабирование автоматизированной системы обработки инцидентов, формирование национальных стандартов и концепции риск-ориентированного подхода в сфере защиты финансовой информации [4].

Таким образом, авторское представление о новой модели "киберустойчивости" выражено в симбиозе четырех базовых элементов:

- Изменение стратегии защиты с концентрацией внимания на ключевых, витальных характеристиках системы и пониманием неизбежности и невозможности 100%-ного устранения атак;
- Своевременное выявление "слабых звеньев" информационной инфраструктуры с помощью мониторинга внешних наблюдателей;
- Страхование рисков киберугроз;
- Государственно-правовая поддержка финансовых институтов.

Источники и литература

1) Маскатов, Г.К. Надежность адаптивных систем / Г.К. Маскатов. - М.: Советское радио, 2014. - 104 с.

2) Сычев А. Киберустойчивость финансовой сферы - что это такое? // 2017, BIS Jornal №2. IB-bank.ru. Отраслевой журнал. URL: https://journal.ib-bank.ru/post/540

3) ЦБ усилит надзор за кибербезопасностью банков // РИА-новости, 2019, 31 января. URL: https://ria.ru/20190131/1550202898.html

4) Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1 сентября 2017 – 31 августа 2018 // Банк России. URL: https://www.cbr.ru/fincert

5) Groot J. What is Cyber Resilience? // Digital guardian, 2019, 4 Feb. URL: https://digitalguardian.com/blog/what-cyber-resilience

6) Losses from Online Payment Fraud to More than Double by 2023, Reaching $48 Billion Annually // Juniper Research. URL: https://www.juniperresearch.com/press/press-releases/losses-from-online-payment-fraud?utm_source=ixbtcom

7) АО “АИГ”. Страхование кибер-рисков. URL: https://www.aig.ru/business/products/cyber-edge