Киберустойчивость финансовой сферы: что это такое?

Необходимо уметь предвидеть кибератаки, эффективно защищаться от них и быстро восстанавливать полноценную работу

В чём заключается актуальность проблемы киберустойчивости для информационной безопасности финансовой сферы, не только в России, но и во всём мире? Пример – серьёзное обсуждение этого предмета, которое ведут руководители центральных банков стран «большой двадцатки». Разработан документ рамочного характера, посвящённый подходам к обеспечению киберустойчивости. Согласно обязательствам международного сотрудничества, принятым Российской Федерацией, предстоит выработать и аргументированно сформулировать своё отношение к этому вопросу.

РАДИ УСТОЙЧИВОСТИ БИЗНЕСА

Понятие киберустойчивости в финансовой сфере подразумевает, прежде всего, способность предвидеть кибератаки, защищаться от них и потом быстро восстанавливать полноценную работу. В нашей отрасли кибератаки относятся к операционным рискам, косвенно влияя на другие риски ликвидности и кредитные. Согласно принципу окончательности, ликвидность финансовых институтов и их клиентов зависит от достоверности предположений о завершённости транзакций. Критериями оценки киберустойчивости в финансовой сфере служат возможности, во-первых, обеспечить проведение расчётов в сроки, отведённые на погашение обязательств, во-вторых – возобновить операции в течение двух часов после инцидента.

Следует помнить, что наша основная задача остаётся прежней: прежде всего, обеспечение устойчивости бизнеса, с учётом влияния различных факторов, в том числе технического характера. Киберустойчивость является подзадачей, в частности, противодействие кибератакам, минимизация и скорейшее преодоление их последствий. Для решения этой частной задачи осуществляются обнаружение и идентификация атак, защита от них и последующее восстановление штатного функционирования системы. К основополагающим компонентам обеспечения киберустойчивости относятся тестирование, ситуационная осведомлённость, накопление знаний и развитие.

Вместе с тем обеспечение киберустойчивости обладает и новыми аспектами. Киберустойчивость является системным понятием, оно охватывает в целом информационную инфраструктуру финансового рынка, её значимых институтов, находящихся в юрисдикции Российской Федерации. Это Банк России, Национальная система платёжных карт как системно-значимая на рынке платежных услуг, ряд ключевых банков, бирж.

Согласно классическому принципу информационной безопасности, общий уровень защиты информации зависит от слабого звена. Слабым звеном в единой цепочке могут оказаться организации, которые не уделяют должного внимания киберустойчивости, но непосредственно взаимодействуют с информационными инфраструктурами ключевых участников отрасли. Такими «слабыми звеньями» могут оказаться кредитные организации, а

также производители продукции и поставщики услуг для них. В поле зрения, таким образом, оказывается практически весь финансовый рынок страны, а также провайдеры телекоммуникационных услуг, некоторые производители программного обеспечения и другие его участники.

Особое внимание к киберустойчивости программного обеспечения начало уделяться в ходе общения с его производителем с прошлого 2016 года. Перенос электронной подписи документов непосредственно в автоматизированную банковскую систему, криптографии требовал обсуждения с разработчиками программного обеспечения, формулирования им мотивированного «технического задания».

Что и было сделано на рабочей встрече с двумя десятками разработчиков программного обеспечения, проведенной несколькими подразделениями центрального аппарата Банка России. На встрече была представлена позиция государственного регулятора в вопросе реализации переноса электронной подписи на сторону банка, план действий с просьбой сделать замечания, дать встречные предложения. Однако таковых, к нашему удивлению, не последовало. По всей видимости потому, что предложенные им сроки организации переноса подписей возражений не вызвали.

РЕНОВАЦИЯ НОРМАТИВНОЙ БАЗЫ

Для обеспечения киберустойчивости важно решение не только технических вопросов, но и создание организационно-правовых условий, наделение субъектов необходимыми полномочиями. На уровне федерального законодательства такая работа ведётся: соответствующий законопроект получил положительное заключение Правительства России и готовится к внесению на рассмотрение Государственной Думы РФ. Развитие законодательства позволит участникам отрасли не ограничиваться защитой только платёжных механизмов, но и полноценно заниматься обеспечением безопасности всей информационной инфраструктуры кредитных организаций.

Нужно правильно оценивать важность этих новых реалий. Можно привести простой пример, один из недавних инцидентов ? хищение денег у кредитной организации. Её сотрудник получил мошенническое электронное «письмо счастья» с вредоносным программным обеспечением. Заранее разосланное предупреждение о возможности такого типа атак было проигнорировано.

В результате атаки злоумышленники получили несанкционированный доступ к управлению инфраструктурой кредитной организации и похитили денежные средства. В данной схеме злоумышленники использовали не инфраструктуру не платежей, а исключительно финансового блока. Новые нормы федерального законодательства позволят предотвращать подобные инциденты, отражать информационные атаки такого типа.

Ещё одно направление совершенствования нашей нормативно-правовой базы – дальнейшее развитие стандартизации, государственной (ГОСТ) и корпоративной, организаций (СТО). Разрабатывается проект нормативов стандартизации аутсорсинга как защиты информации, так и информационной безопасности как таковой. Это важное направление, которое, с большой степенью вероятности, также обретёт форму ГОСТ.

Ряд технических деталей из ведомственных нормативных документов предполагается перенести в следующие стандарты:

- ГОСТ Р «Безопасность финансовых (банковских) операций. Базовый состав организационных и технических мер защиты информации» (вводится в 2017 году);
- СТО БР ИБСС / ГОСТ «Обеспечение защиты информации для цели непрерывности деятельности финансовых организаций»;
- СТО БР ИБСС / ГОСТ «Аутсорсинг защиты информации и взаимодействие с поставщиками информационных услуг» (название предварительное).

В пользу такого решения говорит мировой опыт. Информационная безопасность и защита информации в финансовой сфере волнует не только нас, но и наших коллег за рубежом. Интересный опыт есть в Сингапуре, где целенаправленно проработаны требования регулятора к аутсорсингу не только для кредитных организаций, но и для их поставщиков продуктов и услуг. По всей видимости, для повышения киберустойчивости и нам предстоит усилить взаимодействие не только с кредитными организациями, но и с теми, кто поставляет им информационные продукты и услуги.

ПРОГНОЗИРОВАТЬ, ОТСЛЕЖИВАТЬ, НЕЙТРАЛИЗОВАТЬ

К настоящему времени в отраслевом обмене данными в сфере информационной безопасности участвуют порядка 330 организаций. Наверное, на сегодняшний момент это редкий случай такого взаимодействия, в котором активно участвуют, кроме государственного регулятора в лице Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) ГУБиЗИ Банка России, также большое количество различных участников отрасли. Новые нормы будут обосновывать и развитие информационных сервисов FinCERT, и достоверный контроль государственного регулятора за подведомственными организациями.

Такое взаимовыгодное сотрудничество плодотворно, оно даёт ощутимые результаты. Удается своевременно выявлять новые типы информационных атак, получать неординарные схемы компрометации разных банков – и своевременно предупреждать о новых угрозах коллег, позволяя оградить от попыток хищений финансовые средства. Что подтверждает известный принцип: вовремя предупреждён ? значит, вооружён.

На сегодняшний момент в комплексе документов Банка России в области стандартизации информационной безопасности есть практически все, что необходимо банкам для обеспечения киберустойчивости. Пока что, возможно, не хватает дополнения ? документов, определяющих подход к обеспечению отказоустойчивости и непрерывности бизнеса. Этот пробел в обозримом будущем должен быть восполнен.

Следует отметить, что регулярное наблюдение зафиксировало увеличение количества кибератак в финансовой сфере практически вдвое за прошлый 2016 год. С каждым месяцем всё больше рассылок электронных писем, содержащих различное вредоносное программное обеспечение с элементами социальной инженерии. Характер уловок злоумышленников крайне разнообразен. Мошеннические SMS-рассылки множатся просто в геометрической прогрессии: ежедневно поступает по пять-десять заявление от сознательных граждан, а сколько получателей никуда не обращаются.

С другой стороны, есть и положительная тенденция. Хотя количество и разнообразие кибератак в финансовом секторе растут, их результативность снижается. Ряд

информационных атак, зафиксированных нами в конце прошлого и в начале этого года, не принесли существенных осложнений ни одной кредитной организации. Кроме отдельных временных неудобств, не был нарушен ни один сервиса.

Среди угроз нового типа – попытки злоумышленников использовать «умные вещи». Становятся возможными криминальные инструменты, которые прежде не было, например, создание бот-сети из смарт-телевизоров. Для своевременного отслеживания и нейтрализации таких прогнозируемых информационных угроз нужно усиление взаимодействия с Минкомсвязи РФ и Федеральным агентством связи – Россвязью.