Андрей Выборнов
заместитель директора
Департамента информационной безопасности
Банка России

Ключевые нормакты

О нормативных новеллах в области информационной безопасности, операционной надежности некредитных финансовых организаций и создании центра компетенций импортозамещения*

** По материалам выступления на II конференции «Информационная безопасность в НФО» (организована НАУФОР и ассоциацией «Звезда» 27 октября 2022 года).*

За последний год было выпущено несколько ключевых нормативных актов по тематике информационной безопасности. Во-первых, это Положение Банка России №757-П, которое устанавливает требования к защите информации для некредитных финансовых организаций. Суть его изменений – не просто новая редакция прежнего нормативного акта 684-П, в нем появились новые субъекты, которые появились в законодательстве: маркетплейсы, операторы ЦФА, краудфандинговые платформы. Изменение субъектного состава потребовало введения специальных глав для новых категорий субъектов.

Для остальных организаций внесены небольшие корректировки с точки зрения организации взаимодействия с клиентами и использования разных видов подписей, обеспечения целостности информации при взаимодействии между клиентами и организациями. Во-вторых, были выпущены два документа, касающиеся обеспечения операционной надежности.

Небольшая предыстория этого вопроса. На международных площадках, по линии Базеля и других авторитетных международных площадках последние несколько лет активно развивалась тема киберустойчивости. Нами были изданы рекомендации по обеспечению киберустойчивости, по реагированию и восстановлению после инцидентов, связанных с кибератаками и т.д. Для центральных банков были выпущены специальные рекомендации - каким образом центральные банки должны это регулировать и контролировать тематику киберустойчивости. Вот в развитие этой темы были

внесены изменения в закон в прошлом году. Вопрос назвали в рамках нашего законодательства «операционная надежность».

Используя этот багаж знаний, наши наработки, мы приступили к реализации полномочий Банка России по установлению требований к операционной надежности и контролю за этими процессами. Вот эти два нормативных акта.

Первый – это требования к опернадежности в отношении банков, и в отношении некредитных финансовых организаций. В отношении некредитных и финансовых организаций - № 779-П. По сути, он как бы содержит классические темы операционной киберустойчивости, которые на международных площадках активно обсуждались.

В этом нормакте мы установили только рамочные вещи, базовые высокоуровневые требования.

В этих целях мы провели почти двухлетнюю работу на площадке Банка России с участниками рынка по разработке стандарта, который развивает положения нормативного акта по операционной надежности уже в конкретные меры, в конкретные требования, в конкретные рекомендации.

Такой стандарт был разработан, его активно обсуждали, правили, прошли все необходимые процедуры согласования, и сейчас документ готовится на площадке Росстандарта для утверждения как ГОСТа по обеспечению операционной надежности.

Эти документы устанавливают базовые высокоуровневые требования, каждое требование детализируется в ГОСТе по тем или иным направлениям деятельности, по тем или иным процессам обеспечения операционной надежности. Документы необходимо применять в совокупности, поэтому мы рассчитываем, что до Нового года данный ГОСТ должен быть утвержден Росстандартом и будет доступен для участников.

Сутевая вещь — что должны быть реализованы процессы, которые позволили бы в условии компьютерных атак и проблем с IT обеспечить непрерывность предоставления финансовых услуг.

Важный момент, который сейчас заиграл отдельными красками, - это вопросы, вызванные учетом критичной архитектуры, прописанные в нормативном акте, и применение процессов операционной надежности в отношении этой критичной архитектуры. Имеется в виду технологический стык под этими системами, который обеспечивает основную деятельность, основные технологические процессы в некредитных финансовых организациях, успешные атаки на который или проблемы в области информационных технологий могут привести к неполучению в нужное время потребителем финансовых услуг соответствующей услуги.

Не секрет, что с начала 2022 года кратно увеличилось количество кибератак на различные отрасли экономики. В целом, несмотря на то, что наша финансовая отрасль является, одной из основных целей кибератак, каких-то серьезных пробоев мы не отметили. То есть, в принципе, отрасль выдержала этот вал атак, и это хорошо.

Но возник другой риск – это риск применения иностранного оборудования. С учетом требований операционной надежности необходимость импортозамещения вышла сейчас, по крайней мере для нас, на первое место.

В нашем департаменте создан Центр координации обеспечения технологического суверенитета, так называемый центр компетенций импортозамещения. Сейчас туда входят крупные банки, страховые и пенсионные компании, и мы туда активно вовлекаем ассоциации, в том числе, и НАУФОР. В рамках этого центра мы работаем над тем, чтобы нивелировать риски применения иностранного оборудования и координировать деятельность наших разработчиков банковского ПО, ассоциаций, которые занимаются разработкой, для того чтобы выработать подходы к импортозамещению.

И еще один важный момент, на который я хотел бы обратить внимание.

Мы с отраслью обсуждаем, как улучшить через ФинЦЕРТ, инфообмен о компьютерных атаках и результаты этой работы скоро реализуются в виде выпуска стандарта - нового ГОСТа, который описывает процедуры и форматы обмена информацией.

И банки, и некредитные финансовые организации, согласно требованию норматива, должны будут передавать в Банк России информацию о событиях, операционных рисках, связанных с защитой информации, и о негативных событиях, связанных с инцидентами операционной надежности. Нормативно это требование зафиксировано как в Положении о защите информации, так и в Положении об операционной надежности.

Мы ожидаем, что этот стандарт обмена информации появится очень скоро.

Вся эта работа в совокупности должно повысить устойчивость финансовой системы и опернадежность в деятельности наших поднадзорных организаций. ◻