Идентификация требований безопасности

написано Александр Астахов | 10 июня, 2023

После идентификации активов должны быть определены требования безопасности для этих активов. Ранее мы уже определили основные требования для бизнес-процессов. Теперь наша задача заключается в том, чтобы трансформировать требования, сформулированные на уровне бизнес-процессов, в требования, предъявляемые к безопасности конкретных информационных активов, участвующих в процессах, т.е. выразить их в терминах конфиденциальности, целостности и доступности.

В любой организации *требования безопасности происходят из трех основных источников:*

1. уникальный для данной организации набор угроз и уязвимостей, которые могут привести к значительным потерям, в случае их реализации;
2. применимые к организации, ее коммерческим партнерам, подрядчикам и сервис-провайдерам требования законодательства, нормативной базы и договоров;
3. уникальный набор принципов, целей и требований к обработке информации, который организация разработала для поддержки своих деловых операций и процессов и который применяется к информационным системам организации.

Первая категория требований формируется на основе оценки рисков. В этом и заключается основная идея риск-ориентированного подхода, выраженного в ISO 27001. Большинство механизмов контроля, описанных в этом стандарте, носят опциональный характер и должны выбираться на основе оценки рисков. Эти требования мы сможем сформулировать позднее по результатам оценки рисков.

Вторая категория требований безопасности «спускается сверху» государственными регулирующими органами и носит обязательный характер, независимо от результатов оценки рисков. В отношении этой категории требований наблюдается устойчивая тенденция к постоянному разрастанию и ужесточению. Как было показано ранее, эти требования могут и не уменьшать риски, но зато всегда создают дополнительные юридические риски для организации. Организация обязана обеспечить соответствие этим требованиям по закону, однако сделать это порой бывает не просто и не только потому, что требует дополнительных затрат, не всегда оправданных с точки зрения бизнеса и экономически обоснованных. Законодательство, как и все созданное человеком, — вещь несовершенная и непрерывно развивающаяся. Новые нормативные документы не всегда соответствуют реалиям сегодняшнего дня и могут вступать в противоречие с другими нормативными документами, выпущенными ранее. Подробнее об этом можно почитать в статье «Что мешает развитию ИБ в России» (см. Библиографический список в конце книги).

Не все требования данной категории можно выразить в терминах конфиденциальности, целостности или доступности. К ней относятся также требования, не имеющие прямого отношения к свойствам безопасности информации, такие как требования по лицензированию, сертификации и аттестации, регистрации в качестве оператора персональных данных и т.п. Несоответствие этим требованиям порождает юридические риски для организации, которые также требуется оценить и обработать.

Таким образом, если первая группа требований формируется по результатам оценки рисков, то вторая группа требований порождает дополнительные риски и связанную с ним необходимость в оценке и обработке этих рисков.

Эти группы требований могут взаимно пересекаться. В идеале же они должны совпадать. Для этого всего лишь требуется, чтобы все требования законодательства и нормативной базы были обоснованы с точки зрения существующих рисков. Однако на практике это недостижимо хотя бы потому, что у каждой

организации существуют свои специфические риски и свое отношение к ним.

Помимо требований законодательства и нормативной базы, на данном этапе необходимо также определиться с требованиями безопасности, вытекающими из контрактных обязательств организации. Невыполнение данных требований порождает риски, связанные со штрафными санкциями, прописанными в договорах, потерей деловой репутации, разрывом отношений с партнерами или клиентами и потерей важных контрактов.

Третья категория требований – требования бизнеса – обусловлена внутренними факторами, такими как стремление организации соответствовать высоким стандартам обслуживания клиентов, оперативности реагирования на их запросы, предоставления максимально точной и полной информации. Эти требования организация определяет для себя самостоятельно, исходя из своей миссии, целей бизнеса, своего положения на рынке и текущей рыночной ситуации. Эти требования уже были идентифицированы ранее на этапе описания бизнес-процессов и могут быть трансформированы в конкретные требования к конфиденциальности, целостности и доступности тех или иных информационных активов, участвующих в этих процессах.