Обилие стандартов, требований, средств и технологий защиты не уменьшает риски

написано Александр Астахов | 10 июня, 2023

Оценка рисков сама по себе – сложная аналитическая работа. Для управления рисками, помимо всего прочего, требуется должным образом выстроенная система управления организацией, обеспечивающая обмен информацией между руководством, сотрудниками организации и консультантами, а также эффективная система принятия решений. Для того чтобы упростить эту задачу, во многих организациях используется так называемый *смешанный подход*, предполагающий проведение оценки и обработки рисков только для наиболее критичных информационных активов и систем. Во всех остальных случаях используется существующий передовой опыт и распространенные подходы к защите информации, описанные в стандартах и нормативных документах. Такой подход позволяет обеспечить некоторый *базовый уровень защиты* для большинства активов и систем организации, за исключением тех, которые являются особенно критичными и посему требующими повышенного внимания.

Использование базового уровня, на первый взгляд, выглядит наиболее рациональным, т.к. это позволяет сконцентрироваться на наиболее важных областях, сэкономив тем самым значительные ресурсы путем существенного упрощения одной из наиболее трудоемких управленческих задач. Такой подход, в частности, реализован в одной из наиболее известных методологий управления рисками CRAMM. В этой методологии для определения степени критичности систем и требуемой глубины последующего анализа используется простейший базовый опросник (см. Приложение № 4), в котором перечисляются различные виды

возможного ущерба, такие как прямой или косвенный финансовый ущерб, ущерб репутации, дезорганизация бизнес-процессов, нарушение контрактных обязательств и т.п. Система признается критичной, если нарушение ее безопасности, по мнению владельцев или пользователей этой системы, может привести к сколь-нибудь значительному ущербу хотя бы в одной из этих областей. Далее для критичных систем проводится оценка и обработка рисков, а для некритичных систем формулируются базовые требования безопасности на основе британского стандарта BS 7799.

Введение понятия «базового уровня» защиты для наименее критичных систем (также как и «повышенного уровня» защиты для критичных систем или «максимального уровня» – для особенно критичных систем), особенно если соответствующие этим уровням механизмы защиты описаны с достаточной степенью подробности и закреплены внутренними стандартами организации, предусматривающими детализацию вплоть до определения значений параметров настройки конкретных систем, является удобным способом для первоначальной расстановки приоритетов и дифференциации подходов к защите различных категорий информационных активов. Однако это нисколько не упрощает задачи оценки рисков, поскольку и в отношении «некритичных» активов остаются те же самые вопросы определения разумного баланса между рисками и расходами на защиту, выбора экономически целесообразных и эффективных мер по защите «некритичных» активов, а также вопросы интерпретации требований «базового уровня» с целью их применения к конкретным системам организации. Не говоря уже о том, что сама задача определения «базового уровня» защиты может быть решена только в рамках конкретной организации и только на основании оценки и обработки рисков этой организации, т.к. никакого универсального «базового уровня», применимого к любой организации, не существует и не может существовать. Вместо этого в мире существует более 500 стандартов и нормативных документов по информационной безопасности, с разной степенью детализации описывающих требования безопасности, технологии и

механизмы защиты для различных сфер деятельности, типов информационных систем, областей контроля и т.п. Эти документы сложно даже перечислить, не говоря уже о том, чтобы с ними ознакомиться и осмысленно применять. Одних международных стандартов в сфере информационной безопасности в настоящее время насчитывается более 100. Кроме этого в России действует более 40 ГОСТов и около 70 нормативных документов в сфере ИБ и еще примерно столько же находится в разработке.

Даже разработчики ISO 27002 – одного из наиболее востребованных международных стандартов ИБ, содержащего наиболее полное высокоуровневое описание всех областей контроля информационной безопасности, – никогда не претендовали на то, чтобы их стандарт определял некий «базовый уровень» защиты для организаций. ISO 27002 скорее рассматривается его разработчиками как сборник лучших практик, описывающий типовые механизмы контроля, применяемые в большинстве организаций для защиты своих информационных активов. Однако решение о целесообразности применения любого из описанных в этом стандарте механизмов контроля, а также о способах его применения и требуемом уровне защиты отдается на откуп пользователям стандарта и принимается только на основе оценки рисков конкретной организации.

Требования законодательной и нормативной базы в области ИБ отличаются от требований и механизмов, описанных в стандартах, прежде всего тем, что они носят обязательный характер для определенной категории организаций и граждан. Здесь стоит вопрос не о целесообразности, а об обязательности применения тех или иных требований. Однако и обязательные требования не могут заменить оценки рисков, т.к. формулируются они в еще более общем виде, нежели требования стандартов, и определить, каким образом эти требования должны быть реализованы в конкретной организации, обычно также не представляется возможным без оценки рисков.

Оценка рисков позволяет не только уточнить и конретизировать требования нормативной базы применительно к конкретной

организации, но также определить экономически обоснованные механизмы их реализации и дополнительные требования безопасности, специфичные для организации и не нашедшие отражения в нормативных документах.

Стандарты и нормативная база информационной безопасности:

- *ISO 2700x, 290xx, 13335, 15408, 18044, 18028, 15947, 15443, … всего более 100;*
- *X.800-816, X.830-835, X.736, X.740, X.1121, X.1051, … всего более 40;*
- *COBIT, ISM3, BSI-ITBPM, MITS, ISF-SoGP, SAS 70, TruSecure, SysTrust, WebTrust, BBBOnline, TRUSTe, … более40;*
- *NIST SP 800-x, FIPS 140-201, … всего более 100;*
- *ГОСТ Р 51188, 51583, 51624, 52448, 52447, 51901, 51275, … всего более 40;*
- *РД ФСТЭК, РД ФСБ, СТР-К, Указы Президента, Федеральные законы, Постановления правительства, … всего более 70.*

Нет никакого недостатка в требованиях информационной безопасности, а также в стандартах или в технологиях защиты. За последние пару десятков лет создано уже достаточно большое количество инструментов для решения проблемы защиты информации. Являясь лишь инструментами, они сами по себе не уменьшают риски. Основная задача заключается в том, чтобы выбрать нужные инструменты и разобраться с тем, как их правильно применять в конкретных условиях с учетом существующих рисков и нашего отношения к этим рискам.

Стандарты безопасности одной организации могут быть не применимы либо недостаточны для другой организации. Требования одной организации могут быть слишком жесткими либо, наоборот,

слишком мягкими для другой. Одним и тем же рискам и связанным с ними аспектам защиты в разных организациях может уделяться совершенно разное внимание в зависимости от отношения к риску руководителей и собственников этих организаций, специфики бизнеса и конкретных обстоятельств. Поэтому без оценки рисков невозможно сформировать какого-либо осмысленного набора требований либо механизмов защиты, пригодного для конкретной организации, а именно этим в основном и занимаются как в государственных, так и в частных компаниях. Такая ситуация, как будет показано далее, создает определенную неразбериху с нормативными требованиями в области информационной безопасности и с их выполнением.