CIO.RU

Настольный журнал ИТ-руководителя

№11 Ноябрь 2014

Директор

информационной службы

Загрузите в App Store

ЗАГРУЗИТЕ НА Google play

ISSN 1680-8177

МАКСИМ ПУСТОВОЙ, заместитель председателя правления «ОТП Банк», — об изменении корпоративной культуры принятия решений

Культурная революция

РИСК-МЕНЕДЖМЕНТ В ФИНАНСОВОМ СЕКТОРЕ

ПЛАНШЕТНЫЕ ПЛАТФОРМЫ В БИЗНЕСЕ

«СТРАХИ» CIO И ИХ ПРЕОДОЛЕНИЕ

Михаил Зырянов

Информационная безопасность: **равнение на регулятора или на лучший опыт?**

На что следует опираться службам ИБ — на выполнение требований регуляторов или на имеющийся в стране и в мире передовой опыт? И можно ли сбалансировать эти два подхода?

Можно выделить два фундаментальных подхода к выстраиванию информационной безопасности — с опорой на выполнение требований регуляторов либо на лучший опыт. Первый подразумевает, что организация стремится обеспечить выполнение рекомендаций и требований, зафиксированных в документах государственных и отраслевых регуляторов. Таким образом она снижает риск претензий со стороны регуляторов, однако, поскольку их документы, как правило, выходят значительно позже, чем появляются угрозы и риски, против которых они направлены, организация на какое-то время остается беззащитной против новых угроз. Другой подход характерен для компаний, которые нацелены на обеспечение разумной безопасности и черпают методы защиты от угроз из «копилки опыта», наработанного другими организациями. Таким образом достигается достаточно высокая защищенность, однако требования регуляторов выполняются не всегда, что чревато санкциями.

По мнению Петра Курило, начальника департамента информационной безопасности «Транскапиталбанка», необходимо максимально учитывать требования и рекомендации регуляторов и лучший опыт. Правда, отмечает он, для выполнения требований регуляторов, возможно, понадобится увеличение бюджета. Одно требование использовать сертифицированные средства защиты информации чего стоит...

«На мой взгляд, во всех ситуациях разумнее полагаться на лучший опыт, — советует Саид Аль-Уляфи, директор по информационной безопасности Национального банка "Траст". — Рекомендации регуляторов носят, как правило, фундаментальный характер и не учитывают особенности конкретной организации и динамично растущий технологический уровень угроз, к тому же они обычно запаздывают. Если система обеспечения ИБ в организации выстроена надлежащим образом, занимается защитой информации, то все по настоящему эффективные меры предпринимаются задолго до того, как от регуляторов поступают какие-либо рекомендации по решению возникшей проблемы».

Алексей Грачев, руководитель направления консалтинга корпорации EMC в России и СНГ, отмечает, что лучший опыт в области ИБ учитывает и внутренние требования (исходящие от бизнеса), и внешние (контрактные обязательства, требования законодателей и регуляторов): «Принятие решений в области ИБ на основе оценки рисков и их ранжирования, а также обработки всех рисков, уровень которых превысил принятый руководством порог, является универсальным ответом», — добавляет Грачев.

По наблюдениям Артема Медведева, руководителя направления Enterprise Security компании HP в России, первый подход нередко встречается там, где ресурсы и бюджеты на обеспечение ИБ сильно ограничены либо где нет серьезных рисков, связанных с ИТ. Второй — это рациональный комплексный подход к обеспечению ИБ на предприятии. «Лучший опыт позволяет сбалансированно совершенствовать все три ключевых компонента организации защиты — человеческий фактор, технологии и процессы», — отмечает Медведев.

Согласно опыту Андрея Прозорова, ведущего эксперта компании InfoWatch по информационной безопасности, многие организации стараются совмещать два подхода. Тем не менее если приходится делать выбор, то в первую очередь оцениваются сопутствующие риски.

«Бывают случаи, когда выполнение требований и лучший опыт противоречат друг другу, однако лучшие подразделения ИБ стремятся найти взвешенный баланс между этими методиками, — говорит Кирилл Керценбаум, менеджер по развитию бизнеса "Лаборатории Касперского". — Однако иногда такой выбор делать приходится».

«На извечный вопрос "Что важнее: «бумажная» безопасность или реальная?" можно ответить другим вопросом, который показывает несостоятельность первого: "Что важнее: соблюдать правила дорожного движения или иметь исправную машину?" — продолжает Павел Эйгес, генеральный директор "МакАфи Рус". — Требования регулятора вообще не обсуждаются — их нужно выполнять, чтобы легально работать. При обеспечении соответствия этим требованиям можно использо-

вать передовые средства защиты — как технические, так и организационные. Нужно уметь держать руку на пульсе: располагать устойчивой ИБ-инфраструктурой, соответствующей вашим потребностям, и постоянно работать над ее актуализацией».

Противопоставление «бумажного» подхода и реальной безопасности было актуальным несколько лет назад, вспоминает Валентин Крохин, заместитель директора центра информационной безопасности компании «Инфосистемы Джет». Сейчас эта грань все больше стирается, считает он: «Компании стараются "вписать" бумажные требования в реальную безопасность. Тем не менее до конца разграничение не исчезло».

Выполнение требований регуляторов не ведет напрямую ни к реальной защите, ни к увеличению зрелости ИБ, хотя и является обязательным, отмечает Михаил Башлыков, руководитель направления информационной безопасности компании «Крок»: «Если нужна эффективная система управления ИБ, то ограничиваться только выполнением требований регуляторов нельзя».

Александр Ульянов, ведущий инженер департамента телекоммуникационных решений компании «ЛанКей», уверен, что подход, основанный на рекомендациях и опыте реальных внедрений, эффективнее и надежнее.

«Окончательный выбор подхода всегда остается за владельцами бизнеса, — уверен Алексей Сабанов, заместитель генерального директора компании "Аладдин Р.Д.". — Многое обусловлено профилем организации, численностью сотрудников, степенью автоматизации и, конечно же, характером обрабатываемой и хранимой информации. Большая часть крупных организаций комбинирует подходы». В ряде организаций управление ИБ является частью риск-менеджмента всего предприятия. В этом случае оба подхода гармонично учитываются в части управления рисками.

ОТ ВЫБОРА ПОДХОДОВ — К БАЛАНСУ МЕЖДУ НИМИ

По наблюдениям Медведева, сегодня в России едва ли удастся встретить только один из подходов в чистом виде: «Организации понимают, что не изолированы и живут в экосистеме ИТ. Им нужны новые возможности ИТ, чтобы дальше вести бизнес успешно в современной конкурентной среде».

Если говорить об организациях финансового сектора, то они, по словам Курило, в первую очередь стараются выполнить все требования регулятора отрасли. «Оставшиеся время и деньги идут на то, чтобы дополнить систему защиты информации решениями, выстраиваемыми на основе лучшего опыта, — поясняет Курило. — Такой подход отражается на перегруженности специалистов ИБ и бюджета. Впрочем, влияние регуляторов не следует рассматривать как негативный фактор — нередко выполнение их требований идет на пользу службам ИБ банков».

«Требования регуляторов мы обязаны выполнять, поэтому именно на их концептуальной основе разрабатывается верхнеуровневая регламентирующая база ИБ (то есть политики), — добавляет Аль-Уляфи. — Требования эти, как правило, избыточны. Специфика реальной деятельности банка в части организации процессов и реализации технической защиты отражена в документах, непосредственно их описывающих (порядки, процедуры, инструкции и т.д.)».

По опыту Прозорова, выбор подхода очень сильно влияет на выстраивание всей системы информационной безопасности: «В первом случае организация, как правило, нанимает консультантов, которые помогают ей выстроить инфраструктуру ИБ, отвечающую требованиям регуляторов. Потом готовятся политики безопасности, но они чаще всего остаются на бумаге. Разумеется, информация защищается плохо — впрочем, лишь до первого громкого инцидента».

«"Бумажный" подход часто превращается в преобладание "бумажных" требований над реальными инструментами защиты, запретительных мер над контрольными, — делится своими наблюдениями Керценбаум. — Часто вместо разработки собственной адаптированной модели угроз за основу берется стандартная, рекомендуемая. В бизнес-процессы вносятся подчас совершенно противоречащие здравому смыслу ограничения или надстройки. С другой стороны, если использовать чисто практический подход, не коррелирующий с нормативными требованиями, могут возникать юридические и репутационные риски».

«Законопослушность не отменяет заботу о реальной защищенности», — добавляет Сабанов.

ИЩЕМ ЗОЛОТУЮ СЕРЕДИНУ

Эксперты единодушны: между двумя ключевыми подходами к ИБ можно и нужно искать баланс. «Безопасность не бывает стопроцентной, это многие знают и потому решают задачи, наиболее критичные для их организации в данный момент, пользуясь лучшими практиками и одновременно соблюдая требования регуляторов, если последствия от их неисполнения обойдутся дороже, чем их исполнение», — комментирует Медведев.

«Регуляторные требования должны исполняться в минимально необходимом объеме, — делится опытом Аль-Уляфи. — Выполнять их все без исключения очень накладно. Приоритет, безусловно, следует отдавать опыту — и мировому, и отечественному, и накопленному внутри организации, закрывая регуляторные риски различными компенсирующими мерами».

«Реальная безопасность не должна противоречить требованиям законодательства, но и законодательство не должно вынуждать компании строить неэффективные или бессмысленные инструменты и политики ИБ, — поясняет Керценбаум. — Скорее, инструменты должны максимально подстраиваться под эти требования, но не полностью меняться под их давлением».

Как отмечает Крохин, золотая середина возможна только в том случае, когда требования регуляторов вписываются в существующую ИБ-инфраструктуру. «До недавнего времени требования регуляторов и реальная безопасность иногда были "перпендикулярны" друг другу, — сетует Крохин. — К счастью, ситуация меняется».

Принципиально важно при создании решения ИБ, считает Ульянов, помнить о цели и задаче его внедрения: «Если решение не выполняет возложенных на него задач, оно бесполезно».

Итак, следует искать разумный баланс между «бумажной» и реальной безопасностью. И скорее всего, перевес будет за реальным опытом, поскольку соблюдение требований регуляторов, как правило, не самоцель. Вместе с тем очень полезно, внедряя новые решения ИБ, сопоставлять, насколько они соответствуют тенденциям развития регуляторной базы, — чтобы потом не пришлось серьезно перестраивать «цитадель» защиты информации. CIO.RU