Как монетизировать ИТ-безопасность

ВАЛЕРИЙ ВАСИЛЬЕВ

ОБЗОРЫ

Российские организации и компании очень неохотно публикуют сведения об ИБ-инцидентах. Стремление не выносить сор из избы усложняет организацию консолидированного (в отраслевых и национальных масштабах) противодействия киберпреступности и реалистичную оценку последствий кибератак.

В таком отношении к инцидентам ИБ наша страна не является особенной. Так, Агентство ЕС по сетевой и информационной безопасности (European Union Agency for Network and Information Security, ENISA) отмечает, что в публиковавшихся до сего времени отчетах по Европе о потерях из-за кибератак данные редко бывают сопоставимы между собой ввиду сильного различия используемых для расчетов подходов и методов, часто имеющих значение только в конкретном контексте.

В ENISA считают, что нужны унифицированные и стандартизированные подходы, а некоторые эксперты предлагают определить единый метод измерений, чтобы исследование потерь от киберпреступлений в разных странах и отраслях стало более простым и эффективным. Предполагается, что одобренное Европарламентом новое законодательство, обязывающее компании сообщать о кибератаках, упростит решение этой задачи. Публичность данных об ущербах от ИБ-инцидентов поможет строить реалистичные модели угроз, даст возможность коллективными усилиями сообщества специалистов разработать методики оценки таких ущербов, а сами эти методики станут мощным инструментом в руках бизнес-руководителей и руководства корпоративных ИБ-служб для адекватного определения места информационной безопасности в каждой конкретной структуре, в планировании и обосновании бюджетов на ИБ.

В нашем обзоре мы обсудим, насколько расходы российских компаний и организаций на обеспечение ИБ адекватны реальным угрозам в этом отношении, что следует предпринять в плане формулирования нормативных требований, создания методик расчета расходов на ИБ, разработки современных ИБ-инструментов, организации ИБ внутри компаний, подготовки ИБ-специалистов, чтобы сделать эти расходы более соответствующими современному ландшафту ИБ-угроз и эффективными с точки зрения их окупаемости.

Расходы на ИБ: много, мало или достаточно?

Сбербанк оценил общий ущерб российской экономики от кибератак в 2015 г. в 600 млрд. руб., а Фонд развития интернет-инициатив — примерно в 200 млрд. Как видим, данные заметно разнятся. Одной из главных причин столь сильных расхождений в оценках эксперты считают сокрытие российскими компаниями сведений об инцидентах ИБ. Мотивация для этого очевидна: никто не хочет нести репутационные потери, которые в высококонкурентных рыночных сегментах (например, в кредитно-финансовом) весьма ощутимы.

Изменить ситуацию в лучшую сторону помогло бы закрепление в законодательстве норм, обязывающих публично объявлять о кибератаках и нанесенных ими ущербах. Именно по таким правилам уже не один год живут компании в США, а совсем недавно начали жить и в Евросоюзе.

Нужно сказать, что и в России ведущие игроки зрелых рынков (в качестве примера можно упомянуть ту же кредитно-финансовую отрасль) уже ощутили преимущества обмена информацией об инцидентах ИБ. Сначала это было неформальное общение между специалистами, а затем при ЦБ РФ был создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере — ФинCERT, ставший центром обмена информацией о кибератаках и о реагировании на них в кредитно-финансовой сфере.

И тем не менее, по данным исследовательской компании J`son & Partners, российский рынок ИБ в 2014 г. вырос на 13% и достиг 51 млрд. руб., что намного меньше приведенных выше оценок ущерба, причиненного кибератаками отечественным организациям и фирмам. В 2015-м расходы на ИБ, скорее всего, подросли, однако с учетом общей экономической ситуации они все равно не сравнятся с суммарным объемом нанесенного ущерба, даже если учесть высказываемые аналитиками соображения о том, что вложения в ИБ трудно выделить как независимые в отдельную статью расходов, поскольку чем дальше, тем четче реализуется на практике концепция встраивания функционала ИБ во все ИКТ-средства. В наиболее зрелых современных продуктах это реализуется начиная со стадии разработки, а в тех, которые имеют свою историю присутствия на рынке, — путём добавления такого функционала в готовое решение.

Анализируя развитие инвестиций в ИБ в нашей стране за последние полтора десятилетия, а также размышляя, с какими статьями корпоративных бюджетов чаще всего соотносятся затраты на ИБ, руководитель центра технологий безопасности компании IBS Дмитрий Романченко отмечает, что во многих российских компаниях процесс обособления ИБ-бюджета от бюджета на ИТ только начинается, и значительная часть (возможно, более 50%) фактических ИБ-бюджетов, скорее всего, пока еще растворена в ИТ-затратах.

В крупном и среднем бизнесе, по мнению г-на Романченко, действуют как минимум три значимых драйвера увеличения ИБ-бюджетов: недофинансирование сферы ИБ в прошлом, необходимость провести заново адекватную оценку ИБ-рисков с целью функционирования бизнеса сегодня и стремление соответствовать требованиям регуляторов.

В компаниях, зрелых в отношении ИБ (как правило, это представители крупного бизнеса), на взгляд г-на Романченко, меняется структура затрат на эту сферу: от базовых задач антивирусной защиты и защиты периметра они переходят к выстраиванию эшелонированной защиты ИТ-инфраструктуры и информационных систем, а также к построению комплексных систем управления доступом к информационным ресурсам. В целом же затраты на ИБ в крупном бизнесе если и не являются сегодня достаточными, то активно наращиваются.

В среднем бизнесе, по его мнению, ИБ-затраты жестко лимитируются и выделяются по остаточному принципу. Проекты ИБ здесь запускаются скорее как ответ на проверки и требования регуляторов, оценка реальных угроз в таких компаниях ограничена, что приводит к существенному недофинансированию ИБ.

Главный инженер ИБ-проектов ГК "Компьюлинк" Николай Зенин считает, что руководство российских компаний не стремится сокращать огромный разрыв между традиционно учитываемыми при планировании расходов на ИБ угрозами и теми рисками, с которыми сталкиваются ИБ-специалисты уже в ходе повседневной работы, поскольку учет актуальных угроз чреват кратным увеличением расходов на ИБ, в то время как финансовая отдача при этом не кажется очевидной. Зачем же тогда платить?

Тем не менее в некоторых сегментах в нашей стране в силу специфики перехода России к рыночной экономике концентрировались денежные средства и вырастали крупные корпорации, которые могли (а некоторые должны были из-за конкуренции) позволить себе внедрение передовых технологий и наем лучших специалистов. Это государственные монополии, банки, энергетические и добывающие компании, сети розничной торговли. Но и там, как указывает начальник отдела консалтинга НИП "Информзащита" Андрей Тимошенко, из-за их масштабов и территориальной распределенности ИБ-риски адекватно обрабатываются в основном в головных компаниях, а в филиалах и дочерних фирмах бюджетов на это может не хватать.

В целом в российских государственных организациях и органах власти защита информации, по мнению г-на Тимошенко, сводится к выполнению требований законодательства, которое развивается не так быстро, как технологии. Поэтому и бюджеты на ИБ выделяются с запозданием и в урезанном виде. Не хватает в госструктурах и квалифицированных кадров — большая часть специалистов, способных выполнить проект по созданию комплексной централизованной системы защиты информации для распределенной компании, приходится на долю крупных ИТ- и ИБ-интеграторов. В результате не все госорганизации успевают реагировать на актуальные угрозы ИБ.

Как бы то ни было, несмотря на кризисные явления в экономике страны, эксперты отмечают сегодня заметный рост ИБ-бюджетов в российских компаниях, что соответствует общемировым тенденциям. При этом, считает менеджер по развитию бизнеса "Лаборатории Касперского" Олег Глебов, предприятия все чаще сталкиваются с проблемой, когда даже самая передовая технология не дает необходимого уровня защищенности и требуется не столько наращивать инвестиции в ИБ, сколько перенаправлять их в нужные области.

Подходы к оценке необходимых затрат на ИБ

Совершенно очевидно, что проблема адекватной оценки необходимых затрат на ИБ стоит и перед российскими компаниями. При этом г-н Романченко выразил сомнение в том, что для достоверного количественного расчета таких затрат можно найти какие-либо инструменты. Он полагает, что такие средства могут существовать лишь для частных задач — защиты простых объектов при ограниченном наборе актуальных угроз ИБ. "На корпоративном же уровне, — заключает он, — задача обеспечения ИБ включает множество организационных и технических мероприятий, которые, в свою очередь, могут быть многовариантными в зависимости от вида бизнеса, состава актуальных угроз, ИТ-архитектуры и т. д., поэтому делать универсальный калькулятор или сложно, или бессмысленно". В то же время он указывает на то, что нормативные документы ФСТЭК, по сути, содержат пошаговую инструкцию по обеспечению ИБ и методику реализации системы защиты. ИБ-экспертам известны также примеры бюджетов реализованных ИБ-проектов, которые позволили обеспечить разные уровни ИБ в зависимости от многих факторов и выбора вендорских продуктов для объектов различного масштаба.

Выделяя систему управления информационной безопасностью в структуре обеспечения ИБ, начальник отдела продвижения и поддержки продаж компании RedSys Владимир Перминов как наиболее эффективный инструмент для расчетов затрат на ее построение признает международный стандарт ISO 27001. "Чтобы в процесс управления ИБ вовлечь руководство компании, ИБ-служба проводит оценку рисков, выявляя наиболее критичные процессы и активы предприятия, оценивая потенциальный ущерб от реализации ИБ-угроз, предлагая приемлемые для бизнеса варианты минимизации рисков. Такой подход позволяет ранжировать задачи ИБ по степени важности и адекватно оценивать необходимые для их решения ресурсы", — говорит он.

"Мы применяем различные способы расчета средств на ИБ, — говорит главный инженер проектов ИБ ГК "Компьюлинк" Николай Зенин. — Для одних руководителей убедительны расчеты сравнительных затрат, которые несет компания при передаче задач ИБ на аутсорсинг и при организации ИБ собственными подразделениями. Для других важны требования законодательства в области ИБ или обоснованность мер защиты на базе моделирования ИБ-угроз (исходными данными для этого может быть информация об анализе уязвимостей). Важно, чтобы основная мысль обоснования была простой и умещалась на одной странице".

Наши эксперты


ИВАН БОЙЦОВ, *ведущий менеджер по продукту, "Код безопасности"*


ОЛЕГ ГЛЕБОВ, *менеджер по развитию бизнеса, "Лаборатория Касперского"*


НИКОЛАЙ ЗЕНИН, *главный инженер проектов ИБ, ГК "Компьюлинк"*


МИХАИЛ КАДЕР, *заслуженный инженер, Cisco*


ВЛАДИМИР ПЕРМИНОВ, *начальник отдела продвижения и поддержки продаж, RedSys*


ВЛАДИМИР ПИСКУНОВ, *вице-президент по коммерческой деятельности, "Аквариус"*


ДМИТРИЙ РОМАНЧЕНКО, *руководитель центра технологий безопасности, IBS*


АНДРЕЙ ТИМОШЕНКО, *начальник отдела консалтинга, "Информзащита"*


ОЛЕГ ШАБУРОВ, *руководитель департамента ИБ, ГК Softline*


АНДРЕЙ ЯНКИН, *руководитель отдела консалтинга Центра ИБ, "Инфосистемы Джет"*

Обычно расходы на ИБ начинаются с решения применить тот или иной конкретный ИБ-продукт, а это зависит от потребностей, которые, как утверждает вице-президент по коммерческой деятельности компании "Аквариус" Владимир Пискунов, определяются моделями угроз, моделями нарушителя и моделями защиты. Он предлагает такой алгоритм действий. Для разработки упомянутых моделей следует провести аудит и вникнуть в бизнес- и технологические процессы предприятия. Это требует существенных затрат, которые прибавляются к затратам на ИБ. Для разработанных моделей нужно использовать готовые методики расчета и анализа ИБ-рисков — в разных отраслях есть уже устоявшиеся такие методики. На основании проведённого анализа формируются требования к ИБ-продукту, к услугам или инфраструктуре в целом, затем изучается рынок или объявляется тендер на выполнение этих требований, запрашиваются коммерческие предложения, определяется цена. Обязательно нужно учитывать амортизацию оборудования, стоимость обслуживания и перспективное развитие технологий, чтобы не купить откровенно неперспективный продукт.

Руководитель отдела консалтинга Центра ИБ компании "Инфосистемы Джет" Андрей Янкин рекомендует освоить методики расчета ROI и применять их к ИБ-проектам хотя бы частично (на основе оценки денег, сохраненных от нереализованных рисков), ввести систему метрик и KPI, которые позволят измерять эффективность ИБ в целом, а также отдельных проектов и сотрудников в частности. "Это даст возможность наладить контакт с бизнесом, а самим ИБ-специалистам сосредоточиться на главном. Такие расчеты делать непросто, — констатирует г-н Янкин, — как, впрочем, и для любых других направлений деятельности".

К инструментам расчета затрат на ИБ верхнего уровня следует отнести рекомендуемые г-ном Тимошенко системы относительно нового класса — "Управление предприятием, рисками и соблюдением нормативных требований" (Governance, Risk management and Compliance, GRC). В их основе лежит комплексный подход, позволяющий структурировать бизнес-процессы и автоматизировать их, интегрировать процессы управления ИБ-рисками в единую систему корпоративного риск-управления, внедрять контрольные процедуры и оценивать их эффективность, централизованно управлять планами по обработке рисков. Системы GRC позволяют агрегировать информацию о рисках, требованиях и контрольных процедурах и предоставляют возможность менеджменту принимать обоснованные и своевременные управленческие решения.

Самоокупаемость корпоративной ИБ — миф или реальность?

Как утверждает г-н Перминов, не более десятка российских компаний может похвастаться самоокупаемостью своих ИБ-служб: работая по сервисной модели, они предоставляют ИБ-услуги внутри компании на основе договорных ставок и SLA.

Судя по малому количеству таких компаний, ситуацию с самоокупаемостью корпоративной ИБ в нашей стране типичной не назовешь. Но и негативной, если судить по комментариям экспертов, она тоже не выглядит. И хотя мнения наших экспертов распределились по всей шкале от "да" до "нет", концентрируются они все же возле "да".

Андрей Тимошенко, относящийся к экспертам-скептикам, полагает, что самоокупаемость ИБ маловероятна, поскольку в структуре компаний это затратное подразделение и говорить здесь можно только о минимизации рисков и потерь. Однако и он считает, что в телеком-сегменте зарабатывать на ИБ можно. Зарубежная практика уже имеет реализованные кейсы по монетизации ИБ в телекоме, и российские компании, перенимая лучшие иностранные практики, тоже начинают формировать соответствующие пакеты ИБ-услуг.

"ИБ — поддерживающий сервис и не может быть самоокупаемым подобно тому, как не могут быть самоокупаемыми прокуратура, суды, законодательные органы, которые тем не менее способствуют организации жизни общества", — заявляет г-н Романченко. Вместе со своим коллегой Тимошенко он говорит только об оптимизации затрат на ИБ в корпоративном секторе за счет оптимального разделения ИБ-функций между собственной службой и профессиональными ИБ-компаниями, привлекаемыми на контрактной основе, или частичной замены инвестиций в собственную ИБ-инфраструктуру на эквивалентный сервис. Но к сожалению, предложений ИБ-сервисов должного уровня, которые гарантировали бы требуемый уровень SLA и возврат потерянных средств в случае ИБ-инцидентов, он в России не видит.

Публичность данных об ущербах от ИБ-инцидентов поможет строить реалистичные модели угроз, даст возможность коллективными усилиями сообщества специалистов разработать методики оценки таких ущербов, а сами эти методики станут мощным инструментом в руках бизнес-руководителей и руководства корпоративных ИБ-служб для адекватного определения места информационной безопасности в каждой конкретной структуре, в планировании и обосновании бюджетов на ИБ.

Оппонируя г-ну Романченко, г-н Пискунов приводит другую аналогию — с окупаемостью страховки на автомобиль. Решение, страховать или не страховать машину, принимает владелец, оценивая возможные риски и добиваясь в результате самоокупаемости страховки.

Не только телеком-операторы успешно монетизируют ИБ, считает заслуженный инженер компании Cisco Михаил Кадер. Все динамично развивающиеся компании смотрят на ИБ как на средство снижения расходов, добавления новых сервисов, повышения эффективности труда. В этом случае экономический эффект рассчитать можно, и такие компании говорят не о "самоокупаемости", а о получении прибыли за счет внедрения ИБ-решений.

Самоокупаемость ИБ становится реальностью, полагает г-н Зенин, если она интегрирована в основную деятельность компании. Для этого необходимо, чтобы обоснование ИБ-бюджетов содержало убедительные данные, в основе которых лежит, как правило, модель угроз по отношению к ИБ, а в концепции защиты компании должны быть прописаны аргументированные меры предотвращения актуальных угроз. Для того чтобы угроза была признана актуальной, рассматриваются характеристики вероятности ее реализации в инфраструктуре компании и уровень ее опасности — всё это индивидуально для каждой компании.

Реальностью, причем не отдаленной, считает самоокупаемость ИБ г-н Перминов. Основным препятствием для этого, по его мнению, является недостаточная квалификация ИБ-служб и отсутствие взаимопонимания с руководством. "Через два-три года сервисная модель отношений между бизнесом и департаментами ИТ и ИБ, которая доказала свою состоятельность на Западе, будет массово применяться и у нас", — полагает он.

Как повысить эффективность расходов на ИБ?

Чтобы бизнес начал заниматься эффективностью ИБ, ему необходим серьезный мотив. Сейчас, по мнению г-на Зенина, этому препятствуют три фактора:

— ИБ-риски не находятся в числе главных бизнес-рисков российских компаний;

— ИБ рассматривается руководством только как затратная статья;

— бюджеты ИБ не настолько велики, чтобы руководство заостряло на них внимание.

Для изменения ситуации необходимо ИБ представить бизнесу как самоокупающееся направление деятельности.

В поисках ответа на вопрос о повышении эффективности ИБ г-н Романченко рекомендует руководствоваться двумя критериями: во-первых, ИБ-инвестиции должны быть адекватны значимости актуальных для бизнеса угроз, а во-вторых, нужно просчитать фактически предотвращенный ущерб из-за случившихся инцидентов.

Наши эксперты выделили ряд направлений, в которых следует действовать для повышения эффективности ИБ.

Регулирование ИБ. Дополняя сказанное выше об отраслевом регулировании ИБ Центробанком РФ, г-н Тимошенко упоминает разрабатываемые этой организацией отраслевые документы, направленные на обеспечение ИБ в банковской сфере России. Такие документы создают системную основу для оценки и повышения эффективности расходов на ИБ в организациях банковской системы (несмотря даже на то, что, как показывают аудиторские проверки, ими пользуются далеко не все банки).

Наши эксперты высоко оценивают деятельность ФСТЭК РФ. Эта федеральная служба сегодня наибольшее внимание обращает на оперативное информирование профессионалов и устранение уязвимостей. "Новых нормативных актов от ФСТЭК специалистам ждать приходится несколько дольше, чем хотелось бы, зато документы получаются высокого качества и доступными для практического применения при определении ИБ-угроз и планировании мер защиты", — отмечает г-н Зенин, особо выделяя банк данных угроз безопасности ФСТЭК.

Наши эксперты полагают, что повышение штрафов за нарушение закона "О персональных данных" может существенно улучшить ситуацию с защитой ПДн, поскольку неадекватная ответственность в этой области по сути порождает "защиту от регулятора" и вовсе не способствует эффективной защите персональных данных.

"В то же время возможности повышать эффективность ИБ через регулирование, — отмечает ведущий менеджер по продукту компании "Код безопасности" Иван Бойцов, — ограничены тем, что при составлении своих требований регуляторы диктуют меры и способы обеспечения защиты, описывают возможные угрозы, не учитывая рыночной конкретики, не руководствуясь стоимостью ИБ-средств и экономической эффективностью их эксплуатации". Как раз сейчас страна пытается как-то приспособиться к одной из таких законотворческих новаций — так называемому закону Яровой.

Обучение и информированность. "Нет ничего легче, — утверждает руководитель департамента ИБ группы компаний Softline Олег Шабуров, — чем воспользоваться невежеством человека, его нежеланием выполнять разработанные правила или стремлением узнать что-то изначально закрытое от него. Поэтому простейшим способом повышения эффективности ИБ является работа с самым слабым в сфере ИБ звеном (по возможности исключая его из процесса обеспечения информбезопасности, т. е. полагаясь на технику)".

Бывает, что пользователям достаточно объяснить, какие бывают риски, к чему они могут привести и как правильно реагировать на те или иные ситуации. Заниматься этим нужно регулярно, что, кстати, соответствует мировому тренду: расходы компаний на обучение сотрудников и уровень их осведомленности в области ИБ в последние годы существенно растут.

Нелестно оценивают наши эксперты подготовку ИБ-специалистов в учебных заведениях. По наблюдениям г-на Тимошенко, почти каждому молодому специалисту требуется как минимум год дополнительной практической подготовки, прежде чем он начнёт выполнять свои обязанности самостоятельно. Эксперт считает, что вузы должны чаще привлекать к обучению опытных ИБ-практиков, а студентов отправлять на дипломные работы в высокотехнологичные компании, которые способны предложить им действительно интересные и полезные темы для исследований.

Требования к технологиям. Напомнив о том, что среднее время обнаружения взлома сейчас составляет около двухсот дней, г-н Кадер заявляет, что улучшать ситуацию неизбежно следует через развитие технической области, иначе отставание от злоумышленников приведет к дальнейшему росту "незаметных" вторжений.

Наши эксперты надеются, что разработчики ИБ-средств и ИКТ-оборудования будут развивать набирающую обороты практику сквозной ИБ, т. е. реализацию ИБ в условиях цифровизации жизни как одного из главных функционалов пользовательских продуктов.

Важнейшее значение для повышения эффективности ИБ приобретает возможность интегрировать между собой отдельные ИБ-средства и решения, с тем чтобы специалисты могли строить из них единые комплексы ИБ с централизованными управлением и обработкой данных. Это означает, что ИБ-вендоры "обречены" на совместные действия для создания таких комплексов.

На изменения в стратегии организации ИБ указывает г-н Глебов, отмечающий, что сегодня предприятия переключают своё внимание с превентивной защиты на построение процессов реагирования на ИБ-инциденты, а это требует дополнительных технологий и изменений, связанных с централизацией управления ИБ, обработкой больших данных, интеллектуализацией и автоматизацией в области ИБ.

Потребность в централизации управления ИБ, в консолидации ИБ-данных, в централизованной их обработке должна изменить положение службы ИБ в структуре компаний. По мнению г-на Пискунова, корпоративные службы ИБ и ИТ должны наконец-то стать единым целым, а глубокая интеграция информационной безопасности в ИТ позволит строить современную комплексную защиту.

Возможность унификации и консолидации ИБ-решений, где каждый элемент становится частью единой интегрированной экосистемы, не только выполняя свои задачи, но и качественно влияя на общую эффективность ИБ, является, по мнению г-на Глебова, одним из весомых показателей экономической обоснованности их внедрения. Такой подход позволяет как повысить ИБ, так и снизить общую стоимость владения решениями корпоративной информбезопасности.