АНАСТАСИЯ ХАРЫБИНА, AKTIV.CONSULTING: НУЖНО ЛИ БИЗНЕСУ ОЦЕНИВАТЬ РИСКИ ИБ?

Фрагменты прямого эфира

Екатерина ЯРЦЕВА (MediaMetrics), Анастасия ХАРЫБИНА (AKTIV.CONSULTING)

В гостях у спецпроекта NBJ и радио MediaMetrics побывала Анастасия ХАРЫБИНА – директор по развитию бизнеса AKTIV.CONSULTING и председатель АБИСС. Почему работа с рисками ИБ сегодня приобретает особую важность? Как непрерывность бизнеса связана с ИБ? Насколько эффективен классический подход к оценке рисков в ИБ и в надзорной деятельности? Об этом и многом другом она поговорила в эфире программы «Деловой гамбит» с её ведущей Екатериной ЯРЦЕВОЙ.

Е. ЯРЦЕВА: Почему важно говорить о рисках информационной безопасности?

А. ХАРЫБИНА: Нужно подчеркнуть, что сегодня мы говорим про информационную безопасность на уровне коммерческой организации. И здесь у нас есть два действующих лица: сам бизнес и функция ИБ. Справедливо будет сказать о серьёзном недопонимании между руководителями бизнеса и службами информационной безопасности. Они разное защищают: бизнес сам себя, а ИБ – информационные системы, саму информацию. Но только в отрыве от бизнес-процессов. «Безопасники» зачастую не понимают, что вообще бизнес считает риском, в том числе поэтому они не могут найти общий язык. Говоря о рисках ИБ, мы не только уменьшаем разрыв между ними, но и способствуем встраиванию рисков информационной безопасности в общую модель рисков для бизнеса в целом.

Когда коллегам задаёшь вопрос: как вы выстраиваете стратегию развития информационной безопасности? От чего отталкиваетесь? Чаще всего следует ответ – исходя из требований регуляторов. Уточняешь: а сам бизнес перед вами какие-то цели ставит, погружает в достижение своих бизнес-задач? Большинство разводят руками.

И управленцы приходят к мысли, что с бизнес-функцией информационной безопасности что-то не так, тратятся серьёзные ресурсы, но непонятно, на что. Будет правильным, если руководители служб ИБ перестанут быть просто высококлассными специалистами по информационной безопасности и научатся разговаривать на языке бизнеса, интегрировать себя в него и уметь оценивать собственную эффективность.

Е. ЯРЦЕВА: Работа с рисками информационной безопасности фундаментально чем-то отличается от работы с другими рисками?

А. ХАРЫБИНА: Фундаментально – нет. Неважно, какой это риск – информационной безопасности или другой. В первую очередь надо решить, что является объектом, для чего вы анализируете риски. Определившись с объектом и его ценностью, далее моделируете угрозы, их актуальность, вероятность наступления, ущерб, который может наступить, если реализация угрозы произойдет. Когда вы всё расписали, то принимаете решение, что с конкретным риском делать. И у вас есть четыре основных сценария.

Первый – вы прекращаете заведомо рисковую деятельность, и тогда риск точно не наступит. Второй – проводите профилактические мероприятия, которые либо убирают угрозу вообще, либо ее минимизируют. Третий – передаёте кому-то риски, например, страхуете их. И четвертая модель – вы принимаете риски и резервируете ресурсы, для того, чтобы компенсировать ущерб от наступления этих рисков. Я объяснила на пальцах, очень примитивно, но именно так это работает.

Е. ЯРЦЕВА: Что касается кредитных организаций, то они у нас впереди планеты всей по части информационной безопасности из-за требований регуляторов. Как это работает в финансовом секторе?

А. ХАРЫБИНА: Абсолютно справедливо, что финансовый сектор можно назвать локомотивом в вопросах технологий и связанных с ними вопросах информационной безопасности. Конечно, не только из-за требований регуляторов, хотя во многом требования определяют вектор.

Регулятор – Банк России – последние несколько лет осуществляет серьёзные преобразования в сфере информационной безопасности, появляются новые стандарты, нормативно-правовые акты, и это ещё далеко не конец.

Ведь если не будет доверия к банковской системе с точки зрения безопасности использования, люди просто откажутся от неё. И Банк России в этом случае – основной держатель этого риска. Поэтому и ведётся такая активная регуляторная деятельность и надзор. Банк России требует от кредитных организаций внимательно относиться к вопросу информационной безопасности. Во главу угла встаёт не просто выживаемость конкретной финансовой структуры, но и безопасность всей банковской системы.

Е. ЯРЦЕВА: На недавней конференции «РусКрипто 2021» вы рассказали о том, какие новшества в сфере ИБ озвучил Банк России. Их много?

А. ХАРЫБИНА: Всё крутится вокруг анализа и управления рисками. Банк России уже несколько лет говорит о том, что основной вектор их действий – это переход от проверок технической составляющей информационной безопасности кредитных организаций к проверкам управленческой части ИБ. Поэтому меняются принципы надзорной деятельности.

Ещё недавно надзор носил только инспекционный характер. Но подобные проверки себя изживают, потому что в случае с ИБ – это история процессная. Нельзя прийти раз в три года, посмотреть, уйти и сделать вывод, что всё хорошо. Потому что через секунду в банке может что-то произойти.

Банк России планирует внедрять второе направление надзора – дистанционный надзор. Замысел заключается в том, чтобы в динамике анализировать процессы, которые происходят в кредитной организации в промежутке между инспекционными проверками.

Ещё одним элементом надзора для банков в дополнение к существующим станут киберучения. В конце 2020-го года 22 организации прошли через эти испытания. В этом году их количество хотят увеличить. Порядка 70–80 финансовых организаций должны в этом году принять участие в киберучениях.

Е. ЯРЦЕВА: Возвращаясь к вопросу о рисках ИБ в кредитной организации… Не первый год говорят о риск-профиле. Есть какая-то новая информация по этой теме?

А. ХАРЫБИНА: Коллеги из Департамента информационной безопасности Банка России рассказали, что методология оценки риск-профиля уже написана, но пока они не готовы ей поделиться, так как она проходит апробацию внутри Банка России. Думаю, что в этом году вряд ли она станет общедоступной для публичного обсуждения, скорее уже в следующем. Конечно, всем важно, что же попало в методологию, какие метрики там используются.

Мы понимаем, что там точно будет история, связанная с несанкционированными транзакциями, туда попадут все переводы без ведома клиентов, там точно будет история с инцидентами информационной безопасности, внешняя оценка аудиторов в разрезе комплаенса. Подозреваем, что войдут и киберучения, и дистанционный надзор. Вводится понятие «киберустойчивость» – свойство финансовой организации, которое будет оцениваться в динамике. Всё вышеупомянутое каким-то образом войдёт в риск-профиль.

Подчеркну два раза красной ручкой: киберриски стали частью операционных рисков и будут влиять на резервирование средств. Коллеги из Банка России на секции АБИСС на «РусКрипто 2021» во время дискуссии сказали, что если не хочет кредитная организация какие-то требования из ГОСТа выполнять, тогда ей нужно показать, что есть достаточный резерв средств, и что они готовы покрыть убытки в случае наступления инцидента. Наверное, это справедливо.

Это к разговору о новых подходах к надзору. Если раньше от банков требовали показать, как настроены доступы и средства защиты информации, каковы парольные политики, что на сервере происходит – то есть техническую сторону вопроса, то сейчас у ДИБ Банка России уже нет интереса стоять и смотреть, как работают все эти настройки, им интересна киберустойчивость кредитной организации в целом, то, как банк умеет управлять рисками.

Е. ЯРЦЕВА: На ваш взгляд, чиновники меняются? Это уже не тот стереотипный собирательный образ, который совершенно оторван от реалий и потребностей бизнеса?

А. ХАРЫБИНА: Мы видим, что в Банк России приходят работать люди из коммерческих структур, они привносят туда свой опыт. Их с удовольствием приглашают из финтеха, информационной безопасности, для того чтобы держать руку на пульсе.

В ДИБ идет приток свежей крови, молодых специалистов, которые по-другому смотрят на вещи, и с ними можно разговаривать и договариваться.

И мы в АБИСС (Ассоциация пользователей стандартов по информационной безопасности – прим. Ред.) сделали площадку для того, чтобы обсуждение важных вопросов было разносторонним. В дискуссии принимают участие представители регулятора, финансовых организаций, консалтинга, аудиторов по информационной безопасности.

Все мы варимся в одном котле, нам нужно нормально коммуницировать. А не как лебедь, рак и щука, когда каждый в свою сторону тащит. Так мы мир лучше не сделаем!

Е. ЯРЦЕВА: Я бы хотела узнать ваше мнение о ближайшем будущем. Каковы тенденции, как будет дальше развиваться информационная безопасность в финансовом секторе?

А. ХАРЫБИНА: Если говорить в разрезе сегодняшней темы, то появление риск-профиля сильно изменит общий ландшафт: финансовые организации будут вынуждены пересмотреть своё отношение к информационной безопасности, рискам ИБ, встроенности ИБ в общие процессы. Какой-то конкретный банк может отказаться от работы в этом направлении и, возможно, прекратит свое существование. Такое происходит и будет происходить. Это рынок, это нормально.

Важный момент в работе с рисками – это выбор, а что, собственно, с этим риском делать. Я уже говорила, что риск можно передать. И сейчас всё больше начинают смотреть в сторону страхования киберрисков. Это направление находится в нашей стране в зачаточном состоянии, и, по некоторым оценкам, мы в десятки, сотни раз отстаём от западных стран.

В начале прошлого года рынок киберстрахования в России оценивался в пять миллионов долларов, тогда как во всём мире – это 5 миллиардов долларов. Сами страховые компании, даже те, в которых уже есть продукты по страхованию киберрисков, оценивают этот рынок пока как очень слабый. Потому что бизнес ещё только приходит к пониманию, что страховать риски ИБ можно и нужно при определённых условиях.

Впрочем, вероятность того, что рынок киберстрахования будет набирать обороты, очень велика. Для финансовых организаций это станет возможным ответом на введение риск-профиля и новый подход Банка России к надзорной деятельности. NBJ