

Петр Ефимов: «Риски – это обыденность»

Издание: BIS Journal, 20 февраля 2018 г.

Спикер: Петр Ефимов, президент компании «Информзащита»

В гостях у BIS Journal президент и сооснователь компании «Информзащита» Петр Ефимов



— Петр Валентинович, в июле Премьер-министр России утвердил программу «Цифровая экономика Российской Федерации». Какую роль, на ваш взгляд, это событие играет в истории отечественной ИБ?

— В программе предусмотрено много шагов: от гармонизации законодательства и создания инфраструктурных предпосылок к развитию страны в области информационных технологий до планов по становлению России как мирового лидера в области информационной безопасности. Замечательно здесь то, что впервые в таком программном документе информационной безопасности посвящен отдельный раздел. Это значимая веха в развитии национальной информационной безопасности, обусловленная ростом понимания ответственности государства за безопасность общества и личности в новом цифровом мире, неотвратимости возрастания угроз и уязвимостей.

Информационная безопасность из обязательной, но второстепенной дисциплины, становится одной из составляющей будущего цифровой экономики. Лёд тронулся!

— Программа «Цифровая экономика» — это революция или эволюция?

— Новая программа — далеко не первый документ такого рода. Можно вспомнить программы ФЦП «Электронная Россия» (2003–2010 гг.), «Информационное общество» (2011–2020 гг.), Доктрину информационной безопасности, а также совсем свежую «Стратегию развития информационного общества в Российской Федерации на 2017–2030 годы». Существуют и более общие концептуальные и программные документы, также затрагивающие проблему перехода российского общества к цифровым технологиям. С этой точки зрения программа «Цифровая экономика» — документ эволюционный.

По сути эта программа — попытка консолидации уже имеющегося задела. Она нацелена на эволюцию правового и технического регулирования, обеспечивающего рост отечественного интеллектуального и технологического потенциала. Впоследствии это приведет к серьезным изменениям для каждого из нас: от регистрации при рождении до электронного сопровождения в течение всей нашей жизни. Примеров много уже сейчас: госуслуги, платежные и банковские документы, документы, удостоверяющие личность и права собственности, медицинские, пенсионные и социальные права. Всего и не перечислишь. Программа способствует последовательному накоплению больших объемов информации в цифровом виде, росту потребности в ее оперативном поиске и использовании. Поэтому, я считаю, что «Цифровая экономика» — это эволюция с революционными результатами.

— Реальны ли, на Ваш взгляд, сроки (реализация до 2025 г.), обозначенные в программе «Цифровая экономика»?

— Я бы оценил их как амбициозные. В первую очередь, потому, что для выполнения программы требуется гармонизация законодательства, которое пока ориентировано на традиционную модель взаимодействия хозяйствующих субъектов.

Вспомните заявление Google, которое в 2004 году прозвучало как вызов. Компания объявила, что к 2020 году она оцифрует все изданные на тот момент в мире книги. Этого не случилось, и помехой стала правовая ситуация в области авторских прав.

Я уверен, что добиться высоких показателей к указанному сроку — задача вполне реальная. При условии, что на «раскачку» уйдет минимум времени, и реализацию программы начать прямо сейчас.

— Какие, на Ваш взгляд, серьезные изменения ждут сферу ИБ в течение этого срока?

— Давать прогнозы на такой долгий срок — дело неблагодарное, но некоторые тренды не вызывают особых сомнений, поскольку безопасность всегда следует за меняющимся миром. В парадигме развития цифровой экономики будут стираться границы между видами безопасности, поскольку методы и средства работы, скажем, экономической и информационной безопасности будут смешиваться, взаимно дополняя друг друга.

Использование технологий «облачных вычислений» и растущая пропускная способность каналов связи потребует повышения функциональности и быстродействия средств защиты. Будет происходить переход к сервисной модели обеспечения безопасности. Существенно повысится роль информационного обмена об уязвимостях в тех или иных системах, о событиях безопасности и другой специфической информации. Безопасность должна стать максимально проактивной.

Кроме того, влиять будут и новые методы атак, предсказать появление которых сложно. Скажем, на конференции Black Hat Europe 2017 был продемонстрирован метод Process Doppelganging — бесфайловых атак. За счет умелого обращения с файловой системой NTFS они могут обманывать существующие антивирусные решения. Это вызов, на который придется реагировать. А сколько их еще предстоит — неизвестно.

— Окажут ли все эти изменения влияние на работу «Информзащиты»?

— Изменения в компании уже идут и достаточно активно. С одной стороны, мы стараемся развивать свои компетенции в различных направлениях безопасности, создавая специализированные центры, например, по противодействию мошенничеству (фроду), по защите АСУТП. Постоянно ищем способы совершенствования этих направлений, занимаемся изучением тех возможностей, которые может дать искусственный интеллект в совокупности с машинным обучением, смотрим на существующие и развиваем собственные сервисы в киберразведке (Threat Intelligence). Сегодняшняя жизнь нам не дает возможности быть в роли наблюдателя и просто следовать за ситуацией, мы обязаны быть готовы к решению любого вызова, вне зависимости от его сложности.



— Как Вы считаете, какое место занимает «Информзащита» в цифровой экономике в части ИБ?

— Давайте будем осторожнее с терминами. Поисковые системы трактуют «цифровую экономику» как экономическую деятельность, основанную на цифровых технологиях. Причем речь идёт не столько о разработке и продаже, например, программного обеспечения, сколько об электронных товарах и сервисах, а также их доступности в рамках цифрового пространства. Мы же должны обеспечить безопасность в цифровом пространстве. При этом не стоит путать обеспечение безопасности и предоставление безопасных сервисов.

ИБ в «Цифровой экономике» — это инструмент, который делает цифровую экономику безопасной. «Информзащита» участвует в обеспечении безопасности этой экономики, а не только лишь предоставляет безопасные сервисы. Если рассуждать в рамках этих терминов, то «Информзащита» движется в направлении вывода части своих услуг в цифровое пространство, оставаясь компанией реального сектора экономики, которая производит осязаемые услуги — от создания организационно-распорядительной и проектной документации до защиты бизнеса наших заказчиков.

— По сути Вы — непосредственный участник формирования отрасли информационной безопасности в России. Как, на ваш взгляд, меняется ее ландшафт?

— Изменений множество. Особо хочется отметить полное и окончательное размытие «периметра» информационных систем, аутсорсинг практически любых функций ИБ, включая администрирование средств защиты. Изменения продолжаются постоянно. Например, те же персональные данные. Сегодня это не только адрес и номер паспорта, но и тот массив информации, который можно собрать о каждом человеке по его поисковым запросам, активности в социальных сетях, выбранным новостным лентам и т.п. Что делать и как защищать эти данные — пока еще предстоит разобраться. Но с другой стороны, подходы к защите глобально не меняются, хотя и начинают базироваться на все более совершенных технологиях. Главное, сегодня ни у кого нет сомнений, что ИБ — неразрывная часть современного ИТ-ландшафта. В том числе, важность этого вопроса для государства подтверждается принятой в декабре 2016 года Доктриной информационной безопасности РФ.

— Можете дать прогноз ситуации в Вашей компании и отрасли на ближайшие 5–10 лет?

— Наиболее значимые изменения, на мой взгляд, могут произойти в области правового регулирования. Сейчас вышли в свет требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры (КИИ), строится ГосСОПКА, ужесточаются требования по защите персональных данных (GDPR), усиливается контроль за действиями пользователей в сети Интернет. Сейчас, пожалуй, мы являемся участниками чрезвычайно интересного процесса.

Сегодня нам недостаточно быть просто высококвалифицированными специалистами в области информационной безопасности. Нам необходимо хорошо разбираться в специфике бизнеса наших клиентов, т.к. безопасность информационных систем и бизнес-процессов неразделимы.

Достичь этого можно только глубоким погружением в бизнес-процессы наших заказчиков с точки зрения их уязвимости. Для этого мы сегодня строим нашу компанию как некоторый набор профильных и отраслевых центров, специализирующихся в тех или иных областях.

— Вы стоите у руля компании 22 года. Расскажите, пожалуйста, о ключевых моментах ее развития? Что в тот или иной период становилось драйвером роста? Какие моменты остро запомнились?

— Мы начинали бизнес в качестве вендора — разработчика системы Secret Net. На первом этапе нам повезло с тем, что у нас было сразу несколько интересных и крупных клиентов. Тогда еще не было современных конкурсных процедур, и борьба за право реализации проекта была иной. Во главе угла стояло не предложение меньшей цены, а качество предлагаемого решения. И главным было убедить — оно лучшее. Через живое общение мы неоднократно доказывали, что наши средства лучше всего подходят для защиты той или иной конкретной системы. Большое число крупных компаний страны стало нам доверять.

Спустя какое-то время на рынке появилась потребность в системной интеграции — когда заказчики поняли, что помимо покупки средств защиты их еще нужно правильно установить и настроить. Так мы превратились в системного интегратора, и стали наращивать свои компетенции, оказывать консалтинговые услуги. А затем поняли, что быть одновременно разработчиками и консультантами с элементами интеграции — тяжело. Направления нужно было разделить. В то время было принято решение выделить разработку в отдельную компанию. Так появился «Код Безопасности».

После этого была череда и других перемен. Со временем мы также поняли, что оказание услуг по внедрению, технической поддержке и т. п. может и должно быть самостоятельным бизнесом. Подразделение, которое раньше внутри «Информзащиты» занималось сервисом, выделилось в отдельную компанию — «Информзащита-Сервис». Следующим важным этапом стало осознание перспективности сервисной модели и создание своего Security Operation Center. А это подразумевает, что заказчики стали давать нам на аутсорсинг процесс управления своей информационной безопасностью.

— Что Вы лично привнесли в развитие «Информзащиты»? Чем искренне гордитесь?

— Еще в юности мне хотелось создать и развивать свою компанию. У меня это получилось. И я горжусь, что, невзирая на многочисленные кризисы, когда многие компании уходили с рынка или сокращали штат, «Информзащита» всегда преодолевала критические ситуации и доросла до компании с историей почти в четверть века. Пожалуй, горжусь тем, что принимаю на себя ответственность за принятие сложных решений. Был ряд судьбоносных для компании ситуаций, из которых удавалось выходить достойно. И не просто преодолевать трудности, но при этом непрерывно развиваться, двигаться по восходящей. Ну и, наверное, стоит отметить, что с моей подачи в компании привита такая система ценностей, при которой дело — прежде всего. Многие компании на словах заявляют о своей клиенто-ориентированности. Мы же стараемся в первую очередь решить проблему заказчика. Очень сложно предусмотреть всё, и так нередко случается, что мы делаем в рамках проектов больше, чем было прописано в договоре.



— Можно ли утверждать, что Вы обладаете чутьём на возможные риски и можете предугадывать исход тех или иных событий на рынке ИБ, в ИТ-отрасли и экономике страны в целом?

— Хотелось бы верить, что да. В «экономике страны» — громко сказано, но если говорить о рисках для нашей компании, то их я стараюсь избегать. Перед принятием тех или иных сложных решений приходится руководствоваться известной русской пословицей «... — один раз отрежь». При планировании мы прорабатываем возможные сценарии развития ситуации и в результате можем гибко подстраиваться под любые изменения. В памяти достаточно случаев, когда приходилось отказываться от заманчивых предложений и после об этом не пожалеть.

— Существует мнение, что на рынке ИБ не хватает кадров. Согласны ли Вы с этим, и является ли это для Вас проблемой?

— Да, это действительно проблема, квалифицированных кадров на рынке не хватает. Но это больше связано с тем, что информационные технологии развиваются очень быстро, а задачи по информационной безопасности сейчас стоят очень остро. Заказчикам требуется квалифицированное построение и эксплуатация систем защиты. Если вузам сегодня дать команду увеличить наборы, то мы получим существенную прибавку специалистов только через 5–6 лет.

Тем не менее в количественном выражении число специалистов сферы ИБ возросло, чего, к сожалению, нельзя сказать об их качестве. Могу заявить определенно: настоящим специалистом становится тот, кто постоянно ищет возможности самосовершенствования в профессии, учится, понимает, чего и в какой области он хочет добиться. Ситуация сейчас такова, что остро востребованы именно практические компетенции, т.е. знания и умение делать что-то конкретное, а не разводить теорию.

— В состоянии ли, на Ваш взгляд, сложившаяся система образования и подготовки кадров обеспечить потребности отрасли в специалистах?

— Ничего нет невозможного при правильном построении учебного процесса и грамотном подборе преподавателей. Задача учебных заведений правильно и гибко подходить к учебным программам. В современных реалиях необходимо больше обсуждения практических и актуальных проблем и меньше лекций, как мы их называем, об истории предмета. Мир меняется быстро, и образование должно поспевать за этими изменениями. Хорошо зарекомендовала себя практика, когда лекторами выступают «практикующие» специалисты из профильных компаний и структур.

— Как Ваша компания вкладывается в обучение и развитие молодых неопытных специалистов?

Мы вкладываемся в обучение не только новичков: у нас на каждый год принимается план обучения для всех специалистов разных категорий. Выделяются необходимые средства, которые становятся защищенной строкой в бюджете компании. Мы отправляем сотрудников на разные курсы, развиваем систему наставничества. Хотелось бы еще отметить, что из-за высокой экспертизы наших работников у других компаний есть соблазн переманить их, и нам очень неприятно, когда наших специалистов заполучают не совсем честным путем.

— Какими инструментами Вы стараетесь удерживать сильных экспертов от ухода к конкурентам?

Прежде всего, формируем многоступенчатую мотивацию. Просто платить хорошую зарплату уже недостаточно. У нынешних молодых специалистов есть потребность в самореализации, получении признания, самоутверждения. Таким людям нужно ставить интересные, масштабные задачи. Стараемся это делать регулярно. Также всеми способами поддерживаем здоровый климат в коллективе и заботимся о сотрудниках. Например, мы были одной из первых в России ИТ-компаний, которая полностью покрывает медицинскую страховку персонала.

— Напоследок, хочется задать Вам несколько блиц-вопросов, чтобы лучше узнать вас. Считаете ли Вы себя добрым человеком?

— О моей доброте лучше спросить у других людей. Точно считаю себя человеком порядочным.

— Какие личные качества в людях для Вас неприемлемы?

— Не терплю предательства и подлость. Даже глупость могу простить, а предательство — никогда. Особенно от тех, от кого этого точно не ожидал.

— У Вас когда-нибудь были кумиры?

— Первое, что в связи с этим вспоминается, фраза «не создай себе кумира». Нет, у меня не было кумиров. Не умею настолько сильно очаровываться. Мы видим лишь внешнюю сторону известных людей, но не знаем их лично. А если бы узнали, то неизвестно, хотели бы на них быть похожими.

Многие любили Стива Джобса, его презентации. Им нравился его стиль, и они захотели его повторить. Я считаю, что лучше быть самим собой, а если хочешь выделиться, то придумай что-то свое.

— Есть ли современные технологии, которые Вам не нравятся?

— Вы удивитесь, но я не люблю Интернет. Для меня есть «хороший» Интернет, который мне помогает в работе, учебе, поиске нужной информации и тот, который лишает нас живого общения. Из-за второго у многих отпала необходимость личных встреч с друзьями. Сегодня не выходя из дома можно связаться с кем угодно. Но без живого общения наша речь становится все более непонятной и примитивной. Я не готов обменивать свои эмоции на пиктограммки.

Подробнее: <https://journal.ib-bank.ru/post/609>