Артем Шейкин (Совет Федерации): Киберриски страхуют единицы

Сенатор Артем Шейкин в интервью «Б.О» пояснил, как принцип безопасности должен быть реализован в Законе о критической информационной инфраструктуре (КИИ), почему PCI DSS несет угрозу стране, а также поделился инициативами в области подготовки IT- и ИБ-кадров


Фото: Совет Федерации

Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ «Б.О»

— Артем Геннадьевич, каково отношение сенаторов к развитию института страхования киберрисков?

— Страхование киберрисков является одним из самых молодых видов страхования в мире. На российском рынке оно представлено чуть более десяти лет. Мировая статистика показывает, что расходы предприятий на страхование киберрисков значительно меньше расходов на собственные усилия по информационной безопасности, а также на киберзащиту. Рынок страховых покрытий от киберугроз достаточно узок во многом потому, что страховые компании не готовы предоставлять условия по новым видам рисков, которые эволюционируют из года в год.

В России количество предприятий, особенно крупного бизнеса, которые страхуют свои киберриски, измеряется единицами.

В рамках киберстрахования сейчас представлен достаточно узкий спектр услуг, связанных в основном с тем, чтобы компенсировать штрафы, которые накладывают регуляторы в случаях утечки персональных данных. То есть получается, что это страхование востребовано скорее для того, чтобы обезопасить себя от законодательства, нежели для защиты своих активов.

С учетом обсуждения вопроса страхования киберрисков на секции Совета по развитию цифровой экономики при Совете Федерации можно сделать вывод: данное направление нужно развивать. Рынок страхования киберрисков должен основываться на защите собственных активов предприятия, так как соблюдение всех требований по кибербезопасности, вероятно, не сможет на 100% гарантировать отсутствие киберинцидентов. Страховые выплаты в случае инцидентов нужно использовать для восстановления информационных систем, для финансирования расследования кибератак, для устранения уязвимостей, которые были скрыты, а также для компенсации расходов предприятия, если оно вынуждено было остановиться на какой-то период после инцидента.

Компании, допустившие утечку информации, должны нести ответственность, и этому будет способствовать принятие Закона об оборотном штрафе для компаний за утечку персональных данных. Полагаю, в связи с его принятием направление страхования от киберугроз будет развиваться.

Банкиров и страховщиков я бы призвал к активному содействию развитию данной сферы. Страховым компаниям необходимо расширять перечень как услуг, так и назначений страховых выплат. Принятие Закона об оборотном штрафе за утечку персональных данных позволит более четко спрогнозировать риски компаний и застраховать их.

— На что нацелены поправки в Федеральный закон № 187-ФЗ?

— Промышленные предприятия играют ключевую роль в жизни общества и экономики нашей страны, именно они производят основные товары и услуги, обеспечивая ключевые потребности государства и граждан. С учетом важности работы промпредприятий, а также в связи с потенциальными угрозами и последствиями, связанными с технологическими сбоями, хакерскими атаками, обеспечение кибербезопасности на этих предприятиях является приоритетной задачей.

Принцип инновационности должен быть закреплен в Законе о промышленной политике как принцип использования в промышленности передовых научных и технологических достиже-

ний, создания единых действенных механизмов оценки эффективности государственных вложений.

Принцип безопасности должен быть реализован в Законе о КИИ — необходимо законодательно закрепить то, что государство должно самостоятельно определять объекты, относимые к КИИ, и контролировать обеспечение их безопасности. Сейчас Минцифры инициирует данные поправки в Федеральный закон от 26.07.2017 № 187-ФЗ.

Финансовая сфера также является стратегически важным направлением в обществе и попадает под определение КИИ. Обладая большими данными, финансовая система уязвима, если она не защищена должным образом.

Особых различий в подходах к закреплению инновационности и безопасности в финансовом секторе нет. Необходимо соблюдать баланс между внедрением инновационных цифровых технологий и тем, чтобы не создать новых рисков для системы. Цифровизация и трансформация экономики должны происходить одновременно с внедрением стандартов и требований по безопасности.

— Какие еще направления совершенствования законодательной базы по кибербезопасности актуальны сегодня?

— Новшествам, проявляющимся в формах и способах мошенничества, кибератак, должны противостоять технологии защиты, выявления и подавления таких угроз. Их нужно брать на вооружение как правоохранительным органам, так и эксплуатантам объектов КИИ и иных важных предприятий, учреждений.

Вопрос интеграции этих систем и требований к их эксплуатации лишь частично касается законодательного регулирования. О законодательном же совершенствовании речь идет, когда решаются, например, такие вопросы: в какие сроки и в каком порядке заменять иностранное ПО и программно-аппаратные комплексы (ПАК) отечественными, есть ли необходимый объем радиоэлектронной продукции и ПО для такой замены, что препятствует росту промышленности в этом направлении?

Задача законодателя — создать комфортные условия для разработчиков, стимулировать льготами и преференциями важные и значимые проекты, что, например, сейчас реализуется посредством индустриальных центров компетенций (ИЦК) и стало возможно благодаря поправкам в Налоговый кодекс.

Очень важны в этом процессе изменения в Федеральный закон от 26.07.2017 № 187-ФЗ — государство получит полномочия самостоятельно определять, что относится к объектам КИИ, а что нет, полномочия для проведения анализа и формирования государственного заказа на нужный объем как в радиоэлектронной промышленности, так и в области программного обеспечения, необходимого для замены устаревшего.

Если говорить в более узком ключе (например, о системе антифрод и регулировании работы операторов сотовой связи), то здесь много делается в рамках ИС «Антифрод», которая, по данным Роскомнадзора, в настоящее время охватывает 70% участников рынка. Полный ввод ее в эксплуатацию планируется до марта 2024 года. Система позволит операторам связи обмениваться данными и не пропускать звонки с подменными номерами.

Также надо отметить работу Центрального банка в рамках законодательного совершенствования. Например, 21 октября 2023 года вступит в силу Закон «Об информационном взаимодействии Банка России и МВД», который создаст условия для автоматизированного обмена данными между ведомствами. Закон способствует повышению скорости расследования дел по фактам мошенничества при денежных переводах.

— Имеет ли смысл продолжать выполнять требования иностранных стандартов в области ИБ, например PCI DSS?

— С учетом Положений Банка России № 672-П, 683-П и 719-П области применения отечественных требований к информационной безопасности практически сравнялись с PCI DSS, а возможно, в чем-то их уже превосходят. На основе выполнения требований Банка России можно построить надежную систему, также одновременно соответствующую требованиям PCI DSS.

В основе стандарта PCI DSS лежат фундаментальные технические и операционные требования, которые разработаны для защиты данных держателей пластиковых карт. Для того чтобы им соответствовать, необходимо передавать чувствительные данные об организации безопасности нашей платежной инфраструктуры организациям, подконтрольным правительствам недружественных стран. Следовательно, выполняя требования стандарта PCI DSS и ежегодной оценки соответствия этим требованиям, мы передаем чувствительные данные о характеристиках и уровне защищенности объектов КИИ компетентным органам другого государства.

Напротив, сотрудничество с дружественными государствами важно развивать в следующих направлениях:

- обмен информацией об угрозах ИБ; обмен информацией о новых угрозах и методах защиты может повысить эффективность борьбы;
- совместное обучение и обмен опытом;
- создание единой базы данных; совместный сбор и анализ информации о киберпреступности может помочь быстро и точно реагировать на угрозы ИБ;
- разработка общих стандартов безопасности, которые могут улучшить и обеспечить совместное расследование киберпреступлений;
- сотрудничество в области правовой защиты, в рамках которого можно устанавливать процедуры экстрадиции киберпреступников и обмена доказательствами между правоохранительными органами.

— Какие меры в области подготовки IT- и ИБ-кадров приняты и что следует изменить в существующем процессе?

— Для иностранных граждан, являющихся специалистами в сфере информационных технологий, уже упрощена процедура трудоустройства и получения вида на жительство в Российской Федерации. Специалисты из других стран могут заключать трудо-

вой договор с аккредитованными IT-компаниями без оформления разрешения или патента. Это может дать приток таких специалистов в страну.

В сфере ИБ в связи с созданием полноценных систем безопасности на предприятиях необходимы квалифицированные специалисты, которые будут их обслуживать, модернизировать и совершенствовать. Для эффективного реагирования на многие атаки сегодняшнего дня требуются специалисты с довольно редкими специальностями: реверс-инженеры, вирусные аналитики, компьютерные криминалисты. Необходимо стимулировать создание кафедр для подготовки таких специалистов и вводить программы переподготовки специалистов по данным направлениям.

Необходимо модернизировать профстандарты. В области ИБ они создавались в 2016-2017 годах и уже устарели. Кроме того, данные профстандарты предполагают, что такие специалисты должны обладать всеми возможными компетенциями в этой области, чего на практике достичь невозможно.

— Каковы ваши впечатления от участия в Уральском форуме в Екатеринбурге?

— На Форуме много говорили о необходимости обучения правилам информационной безопасности, и это правильно! Обсуждая вопросы киберграмотности, важно добиться того, чтобы каждый гражданин обладал хотя бы минимумом знаний о безопасном предоставлении личной информации, о безопасности при работе, например, с платежными сервисами и банковскими приложениями.

Поэтому считаю необходимым в образовательной программе популяризировать курс, который касается информационной безопасности. Сама программа этого курса должна включать в себя знания по трем основным векторам:

- технические знания (как защитить свои устройства, как работать с программным оборудованием, понимать функционал интернет-сайтов, настройки конфиденциальности);
- знания и навыки в области финансов, которые позволяют правильно оценивать ситуацию на рынке и принимать разумные решения (аспекты прибыльности сделки, трезвой оценки своих финансовых возможностей, планирования бюджета);
- юридические знания (понимание договорных отношений, своих прав и обязанностей).

Конечно, каждый гражданин не может быть высококвалифицированным специалистом во всех этих областях, но современные реалии жизни требуют от любого минимального уровня знаний, который позволит не стать жертвой мошенников, не влезть в долги, иметь четкое представление о своих правах и обязанностях (при нарушении условий договора, например, с банком).

Пожалуй, это был самый важный посыл форума, и, как заметила председатель Банка России **Эльвира Набиуллина:** «Человек более беззащитен перед мошенниками, чем финансовая организация. Это не только вопрос знаний, это еще и проблема психологической натуры». Б.О