94 → **ЗАКОННОЕ ОТСТАВАНИЕ** Главная сложность киберпреступлений заключается в том, что преступник физически может находиться в одной точке земного шара, а жертва совсем в другой. И выйти на преступника порой просто невозможно — поэтому нет прямой зависимости от глубины проработки законодательства в этой области и количеством киберпреступлений, полагают специалисты в сфере ИБ.

Юрист коллегии адвокатов Москвы «Барщевский и партнеры» Антон Куликов перечисляет сразу несколько серьезных проблем для раскрытия и предотвращения киберпреступлений с правовой точки зрения. «Во-первых, возникает проблема определения места совершения такого преступления в рамках одного государства. Правоохранительные органы могут неоднократно передавать материал проверки по территориальности, тем самым затягивая возбуждение уголовного дела и, как итог, усложняя последующее расследование. Целесообразно возбуждать уголовное дело по месту обращения потерпевшего, а после следственных действий и установления места, где было совершено компьютерное преступление, все материалы уголовного дела могут передаваться по месту совершения преступления.

Во-вторых, много сложностей, когда преступник и жертва киберпреступления находятся в разных странах: это требует взаимодействия органов юстиции нескольких государств и, соответственно, упорядочивания их отношений на уровне актов международного права. Россия при этом, например, как и Китай, отказалась от участия в конвенции Совета Европы „О преступности в сфере компьютерной информации“.

В третьих, и в России, и за рубежом, несопоставим уровень возможностей правонарушителей и правоохранителей. Проблема заключается в сложности работы с электронными доказательствами, недостаточном уровне знаний компьютерных технологий. Сегодня ни одно государство не защищено на 100% от кибератак. Отдельные сотрудники спецслужб в частных разговорах упоминают о том, что закупаемая на службу техника изначально считается устаревшей, а на создание модификаций уходит минимум несколько месяцев. А в это время злоумышленники всегда действуют на опережение, что обеспечивает им успешность и внезапность атак», — рассказывает господин Куликов.

Увы, сейчас мы наблюдаем ситуацию, когда законодатели не успевают реагировать на стремительно меняющиеся реалии, констатирует председатель совета директоров «Серч Информ» Лев Матвеев. «Зачастую политика отдельно взятой компании или сервиса в плане безопасности более эффективна, чем принятые законом нормы. В РФ основным актом для этой отрасли является закон о персональных данных, который исполняется только на бумаге. В действительности же у большинства операторов персональных данных нет инструментов, которыми они смогли бы обеспечить защиту и контроль конфиденциальной информации. Наиболее защищены у нас в стране кредитно-финансовые учреждения и частный бизнес, которые в случае атаки или инсайдерства потеряют „живые деньги“. А вот львиная доля госучреждений — министерства, больницы, школы и вузы — остаются без защиты. Как изменить ситуацию? Внести в законодательство четкое требование по средствам защиты информации: так же как есть, например, требования к противопожарной безопасности в зданиях», — призывает господин Матвеев.

Законодательство всегда будет отставать от реальных угроз, уверен руководитель направления информационной безопасности компании «Системный софт» Яков Гродзенский. С одной стороны, потому что после появления угрозы требуется время на прохождение сложных законотворческих процедур, с другой — из-за инертности регуляторов. «Но отрадно видеть, что сдвиги с точки зрения внимания государства к проблемам информационной безопасности есть. Это появление Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере при Банке России (Fincert) и государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак при ФСБ (ГосСОПКА), создание Доктрины информационной безопасности РФ. Важен и проект закона о критической инфраструктуре, устанавливающий требования к компаниям, оказывающим услуги в сфере кибербезопасности и нововведения, требующие согласовывать модели угроз с регуляторами при использовании государственных информационных систем», — рассказывает господин Гродзенский.

ЗАДАЧА ГОСУДАРСТВЕННОЙ ВАЖНОСТИ Для информационной безопасности государство должно делать то же самое, что и для всех остальных сфер жизни: создавать понятные правила игры и следить за их соблюдением, уверен генеральный директор компании «Атак Киллер» Рустэм Хайретдинов. «Бизнес давно объединился для борьбы с киберпреступлениями — не только IT-компании, но и финансовые организации, и телекоммуникационные операторы. Совместно они успешно борются с такими киберугрозами, как хищение денег со счетов банков, в том числе и через атаку на клиентов, мошенничество с авторизацией через SMS. Накопив опыт, такие альянсы обращаются к государству в лице Банка России и Минкомсвязи РФ с инициативами, в том числе и законодательными. Кибербезопасность страны определяется защищенностью каждого звена ее инфраструктуры. Пока мы только в самом начале пути — есть отдельные успехи в защите отдельных объектов, но для эффективности защиты надо создавать новую архитектуру самих защищаемых объектов. Старые подходы вроде „вот сейчас сделаем систему, потом отдадим ее защищать“ уже не работают, а большинство ныне работающих систем именно такие. Проектировать не безопасность систем, а защищенные на уровне архитектуры системы — вот единственный работающий путь. К сожалению, большинство ныне работающих систем как в бизнесе, так и государственных, создавались в старой парадигме и будут защищаться „навесными“ решениями, малоэффективными в сегодняшнем быстро меняющемся мире», — рассуждает господин Хайретдинов. По его прогнозам, замена на изначально защищенные системы займет годы: они будут появляться только по мере амортизации и вывода старых систем из эксплуатации.

Петер Гъенгеши из Balabit видит три направления в сфере ИБ, в которых может участвовать государство. «Первое — издать четкие инструкции реагирования с опорой на передовой опыт, адаптированные под конкретную ситуацию в стране. Для высокочувствительных отраслей типа здравоохранения или промышленности они должны выходить за рамки рекомендаций и обязательно предпринимать шаги для защиты IT-инфраструктуры. Второе — найти баланс между укреплением безопасности людей и компаний и законодательным одобрением сбора информации в цифровом пространстве правоохранительными органами и разведслужбами. И, наконец, государство может использовать свою колоссальную покупательную способность для приобретения услуг и технологий, которые соответствуют определенным стандартам безопасности, стимулируя вендоров и поставщиков услуг присоединиться к ним», — считает эксперт.

Технологический инвестор Денис Черкасов называет одним из приоритетов в вопросах российской кибербезопасности импортозамещение в IT-сегменте. «Сегодня российская промышленность все еще зависит от западных технологий, но существует ряд отечественных проектов, призванных обеспечивать кибербезопасность. К примеру, Россия является лидером в разработке защитных систем класса оберон, контролирующих целостность системы и используемые параллельно с классическим антивирусным ПО. Импортозамещение в IT-сегменте нуждается в развитии, и государство может в этом смысле поддерживать бизнес», — полагает господин Черкасов.

Информационная безопасность на уровне целого государства во многом зависит от уровня грамотности конкретных пользователей, поэтому старший менеджер группы по оказанию услуг в области управления информационными рисками КПМГ в России и СНГ Илья Шаленков призывает государство направлять усилия на работу с обычными людьми. «Начинать надо с их повседневной жизни: каждый из нас — это маленькая организация со своим бюджетом, принципами управления и порядками. Если мы будем знать основные принципы безопасной работы со своим интернет-банкингом, смартфоном и прочими устройствами, а главное будем искренне понимать, зачем все это, то нам не составит труда на работе точно так же относиться и к корпоративной информации», — говорит господин Шаленков. ■

ПРЯМАЯ РЕЧЬ

93 → **ИРИНА ПАНАРИНА,**
генеральный директор компании «АстраЗенека»:
— Для привлечения частного финансирования государству необходимо внедрять разнообразные инструменты поддержки инвесторов с учетом отраслевой специфики. Среди них — специальный инвестиционный контракт (СПИК). СПИК представляет собой трехстороннее соглашение между компанией, регионом и Министерством промышленности и торговли РФ об условиях, приоритетах и льготах, получаемых инвестором при запуске важных для региона и страны проектов. При заключении СПИК компании получают гарантии стабильных условий для бизнеса, а государство — приток инвестиций.

АЛЕКСАНДР КОЛОСКОВ,
директор автономной некоммерческой организации «Независимая финансовая экспертиза»:
— Можно попытаться найти ответ, как в математике, «от противного». Требования элементарной безопасности страны говорят нам, у кого деньги брать нельзя. Это иностранные инвесторы. Им нельзя давать «на откуп» отрасли, так как иностранные инвестиции, давая деньги экономике один раз, требуют от нее взамен два вечных права. Первое — беспрепятственный и законный вывод своих инвестиций из страны тогда, когда это нужно инвестору, а не национальной экономике. Второе — беспрепятственный и законный вывод прибыли. Воспользовавшись инвестицией один раз, экономика обрекает себя на вечную дань иностранному инвестору.

У всех других источников деньги под инвестиции можно брать. Такой источник в стране всего один — население. Деньги «под подушкой», отложенные «на всякий случай». «Народные» ОФЗ — один из таких примеров.

Если же говорить более откровенно, то есть главный источник инвестиций, который правительство пока не рассматривает. Это бывшие «новые русские». В 1990-х годах прошлого века эти люди приватизировали национальное достояние всей страны. Оно отошло им просто так, без особых затрат. Можно эти активы попробовать вернуть назад, под государственное крыло, и сформировать что-то вроде «Национального инвестиционного фонда» (НИФ).

АЛЕКСАНДР ХРУСТАЛЕВ,
глава «НДВ Групп»:
— Реализация подобных проектов в текущих условиях экономики возможна только за счет собственных средств. Деньги, полученные из внешних источников, в том числе кредитных продуктов, не обеспечат рентабельности инвестиций, вложенных в развитие инфраструктуры и внедрение инноваций. Драконовские проценты делают этот вариант абсолютно неэффективным. Чтобы такие проекты успешно окупались, стоимость денег не должна превышать 10%.

ВЛАДИМИР КИЛИНКАРОВ,
руководитель практики ГЧП Maxima Legal:
— На мой взгляд, большой проблемы с финансированием проектов государственно-частного партнерства ни в одной сфере инфраструктуры в стране сейчас нет. Это касается как микропроектов, до 500 млн рублей, которые финансируются на 20–30% частным инвестором, а в остальной части банками, так и мегапроектов, к которым охотно подключаются бюджет, пенсионные и инвестиционные фонды. В такие проекты, благодаря гарантиям, которые дает законодательство в этой сфере, публичности проектов и их прозрачности, нередко приходят зарубежные операторы и инвестиционные фонды. Ввиду послаблений ЦБ банки кредитуют такие проекты под меньший процент и под залог прав на получение выручки от проекта, что обостряет интерес бизнеса к ГЧП. ■