информационные технологии

Безопасность отформатировали

с9

«Тактические решения формируются непосредственно на местах — в регионах и организациях. В Башкирии действует указ главы республики «Об укреплении основ по защите информации», функционирует совет по защите информации при главе республики, действует концепция об управлении инфраструктурой и определены головные подразделения — это госкомитет по информатизации и управление делами главы. Государственная доверенная инфокоммуникационная инфраструктура Республики Башкортостан (единая инфраструктура, реализующая пространство электронного взаимодействия и обеспечивающая инфокоммуникационные сервисы на основе доверенных сетей связи, — прим. «ИТ») включает три компонента: это государственная сервисная сеть для защищенного обмена информацией между госорганами и организациями, республиканский центр обработки данных для защищенного хранения и обработки государственных информационных ресурсов и система защиты, которая отвечает за безопасность как на серверах, так и на рабочих местах госорганов и организаций. В феврале 2018 года было завершено введение системы защиты информации инфраструктуры, в настоящее время продолжается процесс структуризации, в первую очередь, уделяется внимание системам социального и финансового сектора, где соответствие уровня защиты особенно важно. Это системы в сфере оказания муниципальных услуг, например, запись к врачу. В перспективе двух лет все информационные системы будут сосредоточены на единой площадке», — рассказал заслуженный системный инженер Cisco Systems Михаил Кадер.

ДМИТРИЙ ЛЕКАЙ

За неисполнение Федерального закона №187 предусмотрена уголовная ответственность

Критическая безопасность

Игроки рынка признают, что в целом новый ФЗ поможет повысить уровень информационной безопасности в регионе. Опрошенные «ИТ» эксперты не оставили без внимания и сдерживающие факторы. В их число вошли дополнительные финансовые и ресурсные затраты и тот факт, что большинство субъектов КИИ будут стараться занижать свою категорию и пользоваться типовыми решениями — то есть формально.

По мнению Александра Оводова, к преимуществам выполнения данного закона относится исключительно повышение уровня информационной безопасности, но при этом существенный недостаток заключается в том, что от участников рынка требуются дополнительные усилия и финансовые затраты. Он также выразил опасение, что среди подводных камней кроется тот факт, что для обеспечения уровня информационной безопасности выше среднего нужно иметь в штате высококвалифицированные кадры, которых пока в Башкирии единицы. «Для многих организаций, которые ранее всерьез не занимались построением системы информационной безопасности, это все станет проблемой. Если же по результатам категорирования у субъекта КИИ окажутся объекты одной из категории значимости, то ему придется выполнить еще ряд требований, определенных в Приказах ФСТЭК 235, 239 и установить на объектах КИИ технические средства ГосСОПКА. Все это потребует, как минимум, увеличения штата специалистов по информационной безопасности. Что, собственно, мы уже наблюдаем у флагманов экономики региона — в нефтяном секторе, химической промышленности и энергетике», — подчеркнул он.

Директор по развитию продуктов компании Attack Killer Михаил Бубнов обратил внимание на следующий момент: несмотря на то, что владельцы информационной инфраструктуры должны сами определить, относятся ли они к субъектам КИИ, есть риск того, что ФСБ посчитает инфраструктуру критической, а ее владельца — надлежащим субъектом КИИ, при этом мнение владельца при этом учитываться не будет. Он также выразил опасение, что реализация с достаточно высокой долей вероятности не пройдет гладко, так как предполагаемый объем запросов на выполнение работ для реализации требований может не соответствовать способностям участников местного рынка — возможны инциденты, связанные с попыткой использования типовых решений, которые далеко не всегда могут быть применимы. По его мнению, есть вероятность «формального» решения задачи, ошибки в категорировании, и в целом вероятны попытки субъектов занижать категорию собственных ИИ, чтобы снизить и расходы, и ответственность.

Многие эксперты выразили озабоченность тем фактом, что в рамках нового закона предусмотрена уголовная ответственность по статье за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ст. 274.1 УК РФ, — прим. «ИТ»). Основанием для возбуждения дела является любое нарушение правил и инструкций по эксплуатации средств хранения или информационных систем на объектах, отнесённых к КИИ. Такие правила могут содержаться в руководствах, инструкциях, положениях, приказах ФСТЭК и ФСБ, ГОСТах и т.д. В частности, ведущий аналитик «СёрчИнформ» Алексей Парфентьев отмечает, что у него есть опасение за сотрудников, обеспечивающих выполнение закона «на местах», так как в первую очередь это коснется рядовых сотрудников, к примеру, системных администраторов.

«Для реализации таких проектов необходим серьезный опыт проведения аудита, построения комплексных систем информационной безопасности, построения центров мониторинга ИБ, оказания эксплуатационных услуг, выстраивания процессов мониторинга и реагирования на инциденты ИБ — и это не весь список. Подчеркну, что компетенций компаний, занимающихся только комплаенс (от англ. Compliance — это система контроля и управления рисками, — прим. «ИТ») и «бумажной безопасностью», для данных целей недостаточно. Сложность выполнения требований закона во многом зависит от текущего состояния информационной безопасности и процессов субъекта КИИ», — рассказала руководитель направления сервиса и аутсорсинга ИБ Центра информационной безопасности компании «Инфосистемы Джет» Екатерина Сюртукова.

Рынок всплывет

В целом эксперты сходятся во мнении, что 187-ФЗ сильно повлияет на рынок информационной безопасности. Представитель онлайн-сервиса DocShell Сергей Борисов отметил, что уже сейчас появилось большое количество компаний, предлагающих услуги по категорированию объектов КИИ, а также сервисы по автоматизации этой деятельности, хотя новые требования только в начале года вступили в силу. По мнению Александра Оводова, выполнение 187-ФЗ дает возможность для региональных интеграторов в области информационной безопасности расширить спектр оказываемых услуг и внедрения решений информационной безопасности. «Уже сейчас несколько компаний, и мы в их числе, оказывают данные услуги на рынке Башкортостана. На рынке информационной безопасности в части решений для крупного бизнеса первую скрипку играют инсорсеры и московские интеграторы, тот же Сибинтек, которые в рамках группы компаний реализуют функции по обеспечению информационной безопасности или вписаны в стандарты. Что касается среднего бизнеса и органов власти, то здесь действительно есть конкуренция среди региональных игроков», — рассказал Александр Оводов.

«Все потенциальные субъекты КИИ поставлены в очень жесткие временные рамки, и количество запросов на такие работы сейчас экспоненциально растет, как следствие — растет и сам рынок. Учитывая, что для оказания услуг в сфере защиты информации необходимы соответствующие разрешительные документы, потенциальное количество исполнителей работ в этой области ограничено. Одновременно стоит отметить, что объем запросов может существенно превысить возможности данного сегмента рынка, особенно в Башкирии, где количество потенциальных исполнителей ограничено», — отметил Михаил Бубнов. По мнению руководителя направления информационной безопасности компании «Системный софт», так как местных игроков, которые будут работать в этой нише, немного, большая часть проектов уйдет к известным системным интеграторам с большим опытом выполнения проектов в части ИБ-комплаенса.

Лида Богатырева