

информационные технологии

Безопасность отформатировали

«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.

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



Андрей Редя

За неисполнение Федерального закона №187 предусмотрена уголовная ответственность

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, от-

носятся 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 ин-

формационной 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, отнесенных 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 необходимо 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 всплывает
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.

Лидирует

Review



«Мы будем работать в симбиозе»

— тренды —

Закон «О безопасности критической информационной инфраструктуры РФ» (187-ФЗ) вступил в силу 1 января 2018 года, но пока единицы компаний и предприятий активно занимаются вопросами по его исполнению. Эксперт по информационной безопасности, директор компании «ИТ Энигма Уфа» Александр Оводов рассказал о первых шагах по выполнению требования закона и о том, как предприятие может выработать план действий.

— Александр, 187-ФЗ (федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации») расширяет перечень информационных систем, к которым предъявляются обязательные требования по безопасности со стороны государства и владельцы которых теперь несут ответственность, в том числе уголовную?

— Да, действительно, несоблюдение закона приведет не к традиционным штрафам, а к уголовному наказанию. Регулятор — Федеральная служба по техническому и экспортному контролю (ФСТЭК) — предлагает предприятиям самостоятельно пройти процедуру категорирования, чтобы определить, относятся ли их информационная инфраструктура к значимым объектам КИИ (критической информационной инфраструктуры), а это не только информационные системы, но и автоматизированные системы управления и информационно-телекоммуникационные сети. Весь крупный бизнес, касающийся добычи и переработки, энергетика, медицины, связи, химической промышленности и прочего (всего 13 сфер деятельности), безусловно, относится к предприятиям, которым придется соблюдать этот закон. Но и средний бизнес, и малый — им тоже нужно будет заниматься информационной безопасностью значительно серьезнее, чем раньше.

— Какие мероприятия необходимо провести компаниям и организациям в связи с вступлением в силу этого закона? Как ваша компания может способствовать упрощению процесса?

— Это целый комплекс действий, которые нужно совершать последовательно. Сначала в компании проводится



аудит информационной безопасности — он нужен, чтобы оценить работу систем информационной безопасности, понять, существуют ли риски реализации компьютерных атак, где скрыты уязвимости, которые могут привести к нарушению работоспособности информационных систем, автоматизированных систем управления. Нужно устранить уязвимости и снизить риски успешной реализации хакерских атак и нарушений в работе из-за халатности персонала и отрегулировать работу всех систем, отвечающих за информационную безопасность. Далее — категорирование, процесс, который проводим мы, но его результаты проверяет и подтверждает уже ФСТЭК. Если субъект КИИ не предоставит данные о категорировании, ФСТЭК вправе потребовать эту информацию.

Мы можем взять на себя почти все работы, связанные с реализацией 187-ФЗ: аудит, проектирование системы защиты, установка и настройка средств защиты информации, взаимодействие с регулятором, в некоторых случаях — помощь в поддержании работоспособности системы защиты на аутсорсинге. Важно понимать, что защита автоматизированных систем управления требует привлечения специалистов, которые смогут найти общий язык с IT-департаментом, специалистами АСУ, метрологами, специалистами по информационной безопасности, объяснить принципы работы создаваемой системы защиты всем участникам

процесса, выработать корректные проектные решения. Как правило, единства внутри компаний между этими подразделениями нет.

— Насколько увеличатся, на ваш взгляд, вложения в безопасность?

— Траты будут ощутимыми, но не критичными, на мой взгляд. Максимальный срок категорирования объектов КИИ — 1 год, уже сейчас среди наших клиентов есть представители крупного и среднего бизнеса. Сроки исполнения, как правило, бывают связаны с бюджетом, выделенным на безопасность. За один год можно успеть и запустить процесс, и внедрить систему защиты. На выстраивание же процесса непрерывного обеспечения информационной безопасности внутри компании может уйти от двух до пяти лет, в зависимости от масштабов бизнеса. С конца 2021 года уже начнутся проверки исполнения 187 закона, так что времени на раскочку практически не осталось.

— Можно ли утверждать, что реализация закона позитивно скажется на деятельности организаций, которые сегодня часто несут прямые потери от своего невнимания к проблемам безопасности?

— Да. Закон создан для того, чтобы предотвратить проблемы, которые, как показывает опыт, бывают масштабными, вплоть до прекращения работы крупных заводов. Чтобы подобного не случилось, наша компания и наши клиенты — мы будем работать в симбиозе.

Пока все ждут Цифру, мы уже вещаем

С января 2019 года федеральные каналы переходят с устаревшего аналогового на цифровое телевизионное вещание в рамках ЦЦП «Развитие телерадиовещания на 2009–2018 гг. № 985 от 3 декабря 2009 года. Для телезрителей это означает улучшение качества трансляции каналов, отсутствие помех и четкий звук.

Однако Интернет-провайдер «Зеленая точка» уже сегодня вещает цифровое ТВ через сеть Интернет. Благодаря стабильной скорости 100 Мбит/с вещание цифрового телевидения от «Зеленой точки» обеспечивает высокое качество картинки в HD-формате, чистый звук без искажений. Пока все ждут переход на цифровое телевидение, «Зеленая точка» уже подключает интерактивное ТВ в 17 городах России.

Современное телевидение представляет собой комбинацию аналогового и цифрового вещания посредством выделенного кабеля от оператора связи. Для подключения моделей телевизоров, которые не поддерживают цифровое ТВ, необходимо приобретение ТВ-приставки. Но будущее за цифровым интерактивным ТВ, которое подключается через Интернет.

Абоненты «Зеленой точки» пользуются новым телевидением уже сегодня, и его достоинство заключается не только в качестве трансляции каналов, но в интерактивном управлении. Интеллектуальный поиск программ позволяет просматривать любимые фильмы и передачи в любое время. Архивная база телевизионных программ рассчитана на 14 дней — так что абонент не пропустит свое любимое шоу и больше не опоздает к началу запланированного просмотра. Абоненты «Зеле-

ной точки» сами решают, когда смотреть «Вечернего Урганта»! Полное управление эфиром позволит ставить фильм на паузу, перематывать рекламу и прокручивать любимые моменты снова и снова.

Интерактивное ТВ от «Зеленой точки» включает в себя 263 самых интересных и популярных каналов в HD-качестве. Это настоящая сокровищница для любителей кино и телепередач. Здорово, когда есть и чего выбрать, но как быть, когда в доме есть маленькие дети? «Зеленая точка» предоставляет возможность настройки персональных профилей для каждого члена семьи. Абонент может настроить столько профилей, сколько нужно. И в каждый профиль дает рекомендации по интересам члена семьи. Это новое интерактивное ТВ от «Зеленой точки», которое доступно уже сегодня!

Смотри. Слушай. Говори.

ИНТЕРАКТИВНОЕ ТВ

зелёнаяточка

226-55-55
zelenaya.net