Безопасность объектов КИИ в госсекторе

Екатерина СЮРТУКОВА,
руководитель группы, дирекция по интеграции, компания «Ростелеком-Солар

К госсектору относятся десятки тысяч компаний из различных отраслей существенно различающихся по масштабу, структуре, форме управления. При этом зачастую в отношении госорганов осуществляется более жесткое нормативное регулирование. Так, в рамках нормативных актов Закона № 187-ФЗ «О безопасности КИИ» именно для госорганов и госучреждений были установлены строгие сроки категорирования, для всех остальных субъектов КИИ они носили лишь рекомендательный характер. Все госорганы должны были в обязательном порядке провести категорирование до 1 сентября 2020 г.

Категорирование

В рамках освещения темы КИИ в госсекторе условно можно разделить на два блока. Первый – это крупные госкорпорации, функционирующие в сфере транспорта, энергетики, производства и других ключевых отраслях экономики, которые со всей серьезностью относятся к вопросам непрерывности бизнеса, в том числе и к информационной безопасности. Поэтому требования регуляторов, в частности в области защиты КИИ, реализуются максимально полно с учетом всех возможных угроз для инфраструктуры. Успешные кибератаки на такие предприятия могут привести к катастрофическим последствиям, поэтому во главу угла ставится реальная безопасность. Второй блок – госорганы и государственные учреждения, где ситуация сложнее из-за различных объективных факторов, таких как дефицит кадров, что иногда приводит к более формальному подходу к обеспечению информационной безопасности.

Несмотря на то что сроки истекли, некоторые организации до сих пор не завершили этот процесс, столкнувшись с объективными трудностями. Например, не всегда очевидно, является ли госорган (например, местная администрация) собственником или арендатором информационных систем, функционирующих в сферах, определенных в Законе № 187-ФЗ: здравоохранения, науки, транспорта, связи и пр. Госорганы не могут определить свою принадлежность к КИИ по ОКВЭД, где прописано «деятельность органов государственной власти» без детализации и отнесения к сферам КИИ. Необходимо анализировать более глубоко, смотреть дополнительный классификатор – Общероссийский классификатор органов государственной власти и управления (ОКОГУ), учредительные документы и положения организаций, в которых может быть прописан вид деятельности, указывающий на принадлежность к критичным отраслям.

На последних профильных конференциях представители ФСТЭК рассказали, что с сентября 2020 г. начинают совместные с прокуратурой проверки потенциальных субъектов КИИ. Это должно стать дополнительным драйвером процесса категорирования. Поэтому, если самостоятельно не получается однозначно установить принадлежность к КИИ, лучше своевременно обратиться за помощью во ФСТЭК.

Обеспечение безопасности ЗОКИИ

Следующим шагом после категорирования, если в структуру организации входят значимые объекты КИИ, является создание системы обеспечения информационной безопасности значимых объектов КИИ (СОИБ ЗОКИИ). Меры по обеспечению безопасности значимого объекта определяются на основе установленной категории значимости, с учетом угроз безопасности, применяемых информационных технологий и особенностей функционирования ЗОКИИ. Кроме того, важно определить, какие еще требования регуляторов распространяются на защищаемые информационные системы. Если значимый объект КИИ является ИСПДн, необходимо учесть требования приказа № 21 ФСТЭК России, если государственной информационной системой (ГИС) – требования приказа № 17 ФСТЭК России. Последний случай особенно актуален для госорганизаций, так как в госсекторе государственные информационные системы встречаются часто, что добавляет свою специфику.

Во-первых, требования приказов № 17 (ГИС) и № 239 (ЗОКИИ) ФСТЭК России во многом пересекаются. Во-вторых, начиная с 1 июля 2020 г. эксплуатация ГИС без наличия аттестата соответствия запрещена, поэтому все операторы ГИС уже реализовали комплекс необходимых мер по информационной безопасности и прошли оценку соответствия в форме аттестации.

Таким образом сейчас немалая часть объектов КИИ в государственных организациях – аттестованные ГИС, для которых существенная часть мер информационной безопасности уже реализована: внедрены системы межсетевого экранирования, системы криптографической защиты, системы обнаружения вторжений, реализованы защита от несанкционированного доступа, антивирусная защита и др. Для таких ИС обеспечить выполнение требований НПА в области КИИ будет значительно проще. Нужно оценить достаточность реализованных мер безопасности и при необходимости внедрить недостающие – в соответствии с категорией КИИ.

Как правило, дополнительные меры связаны с выстраиванием процессов реагирования на инциденты ИБ, обеспечения действий работников в нештатных ситуациях, информирования и обучения персонала, с доработкой организационно-распорядительной документации (положение о подразделении ИБ, регламент управления инцидентами, регламент доступа к значимым объектам, порядок действий в нештатных ситуациях и др.), а также с полным комплексом работ по обеспечению информационного взаимодействия с НКЦКИ в рамках выполнения Закона № 187-ФЗ.

При разработке мер для ЗОКИИ нужно учитывать, что согласно приказу № 239 ФСТЭК России, если ЗОКИИ является ГИС или ИСПДн, меры по обеспечению безопасности значимого объекта и меры защиты информации (по обеспечению персональных данных) принимаются в соответствии с более высокой категорией значимости, классом защищенности или уровнем защищенности персональных данных.

Если система не является ГИС или ИСПДн, то, скорее всего, в госорганизациях для нее реализованы минимальные меры по ИБ и необходимо строить СОИБ ЗОКИИ практически с нуля. И здесь помимо технической составляющей большой объем задач лежит в области выстраивания процессов ИБ.

Импортозамещение

При выборе средств защиты субъектам КИИ рекомендовано в первую очередь обращать внимание на решения отечественных производителей, так как сейчас активно обсуждается проект указа Президента и постановления Правительства об импортозамещении в КИИ. В проекте документа указано, что переход на российское (и евразийское) ПО должен произойти до 1 января 2021 г., на российское (и евразийское) оборудование – до 1 января 2022 г. В отличие от частных компаний, которых пугают отказ от иностранных решений и сжатые сроки перехода, госорганы и госкорпорации в полном объеме готовы к новым требованиям, поскольку отечественное ПО и оборудование достаточно давно являются для них стандартом. В 2015–2018 гг. разрабатывались и принимались некоторые нормативные акты, регулирующие импортозамещение в органах государственной власти и местного самоуправления, многие госкорпорации также достаточно давно ввели запрет на закупку иностранного программного обеспечения. Поэтому для них планируемые изменения – очередной понятный шаг на пути к полному импортозамещению.

Кадры

Если с техничексими средствами в целом все понятно, то с квалифицированными специалистами дела обстоят сложнее. Процессы и средства защиты не функционируют сами по себе, нужны ИБ-специалисты, которых в госорганизациях, как правило, недостаточно. Ситуация в конкретном учреждении от региона к региону может различаться и зависеть от ведомственной принадлежности, но проблемы кадров и ограниченного бюджета на ИБ являются актуальными практически для всех.

С 1 января 2021 г. (согласно уже принятым изменениям к приказу № 235 ФСТЭК России) к специалистам подразделения по безопасности субъектов КИИ будут предъявляться дополнительные требования по наличию высшего профильного образования, квалификации и стажа. Требования уже утверждены, поэтому у госкомпаний есть совсем небольшой запас времени, чтобы при необходимости повысить квалификацию своих специалистов, или организовать процессы ИБ с привлечением внешней компании (аутсорсера). В рамках реализации требований Закона № 187-ФЗ не запрещается привлечение организаций-лицензиатов для установки, настройки и эксплуатации средств защиты субъекта КИИ. Поэтому передать часть задач по выполнению требований закона на аутсорсинг – вполне целесообразное решение, которое позволит оптимизировать и финансовые, и кадровые затраты.

Бюджет или Финансирование

Если говорить о бюджетировании ИБ, то, с одной стороны, в отличие от частных компаний, которые вынуждены самостоятельно инвестировать в системы и процессы ИБ, госсектор финансируется государством. С другой стороны, обосновать достаточный бюджет, особенно на решение задач за рамками регуляторных требований, весьма сложно. Кроме того, в непростой экономической ситуации всегда есть вероятность секвестирования бюджета, что может негативно отразиться и на статьях затрат, связанных с информационной безопасностью.

Тем не менее, несмотря на все сложности, госкомпании должны шаг за шагом развивать ИБ, причем не только в рамках формального выполнения требований регуляторов. Примеры хакерских атак на госкомпании наглядно демонстрируют необходимость обеспечения реальной информационной безопасности в госсекторе и потребность в комплексном подходе к решению этой задачи. ■