Критическая информационная инфраструктура и ее категорирование

Игорь ТАРВИ,
ведущий архитектор систем безопасности АСУ ТП, АО «ДиалогНаука»

Год назад, летом 2017 г., был принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ) Российской Федерации». Он определил развитие российского рынка информационной безопасности на долгие годы, поскольку жестко указал сферы деятельности компаний (субъектов КИИ), объекты КИИ которых могут быть отнесены к значимым (ЗОКИИ) и должны быть защищены в соответствии с требованиями подзаконных нормативных документов. И даже если в компании по формальным признакам посчитали, что объекты КИИ отсутствуют, все равно необходимо провести процедуру категорирования и убедить регуляторов в отсутствии у компании критических для информационной инфраструктуры объектов.

Основные положения

Закон № 187-ФЗ требует от всех компаний из двенадцати ключевых отраслей (в законе они названы как сферы деятельности) выделить объекты, нарушение деятельности которых может привести к различным видам ущерба: экономическому, социальному, экологическому, политическому и безопасности государства. Закон обязует эти компании обеспечить защиту своих объектов, чтобы не допустить инцидентов, которые могут привести к ущербу. При этом ответственность за несоблюдение требований в рамках закона уже наступила с 1 января 2018 г. для тех компаний, которые владеют соответствующими объектами. Потому, если с такими объектами случаются инциденты информационной безопасности, приводящие к существенному ущербу, их руководство может понести ответственность – вплоть до уголовной уже сейчас.

Закон также определяет два федеральных органа исполнительной власти (ФОИВ): первый отвечает за обеспечение безопасности объектов КИИ (им в соответствии с указом Президента РФ является ФСТЭК России), а второй – за функционирование государственной системы обнаружения и предотвращения компьютерных атак на объекты КИИ (эту роль выполняет ФСБ России) – эту часть принято называть ГосСОПКА. Правительство и соответствующие ФОИВ имеют полномочия формировать требования к организациям для обеспечения безопасности объектов КИИ.

Правительство РФ в рамках своих полномочий выпустило Постановление № 127-ПП, которое определяет процедуру категорирования объектов КИИ – ее должны пройти все организации из ключевых сфер деятельности. ФСТЭК России приняла ряд приказов, в рамках которых определены требования по обеспечению безопасности ЗОКИИ, в том числе должен быть сформирован реестр ЗОКИИ. ФСБ России сформировало Национальный координационный центр по компьютерным инцидентам (НКЦКИ), который является центральным узлом ГосСОПКА, он имеет и другое название – GovCERT. Также формируются требования и форматы по обмену информацией с НКЦКИ, соответствующие нормативные документы на сегодняшний день имеют статус проекта.

Категорирование

Процедура категорирования определена на уровне Постановления Правительства РФ №127-ПП. В соответствии с этим документом компании, владеющие на любом законном основании объектами КИИ, должны создать комиссию по категорированию и принять ряд локальных актов. Состав комиссии и набор документов, которые комиссия должна подготовить, определены в постановлении. При этом ФСТЭК России наделена полномочиями потребовать проведения процедуры категорирования для компаний, чьи лицензии, уставные документы или род деятельности по ЕГРЮЛ соответствуют сферам деятельности Закона № 187-ФЗ. В результате категорирования может обнаружиться, что в компании отсутствуют ЗОКИИ – тогда выполнение требований по организации защиты остается на усмотрение компании. Критерии значимости строго определены в приложении к постановлению. Комиссия по категорированию, в ходе своей работы, выявляет критические процессы, нарушение которых может привести к ущербу и, определяет объекты КИИ, обеспечивающие их выполнение.

В итоге, первым результатом деятельности комиссии по категорированию должен стать перечень объектов КИИ с указанием сроков проведения их категорирования, который либо согласуется с вышестоящей организацией, если она есть, либо сразу направляется во ФСТЭК России в уведомительном порядке. В указанный в перечне срок, комиссия должна произвести оценку значимости выявленных объектов КИИ, соотношение между ущербом и уровнем значимости объекта как раз указано в приложении к постановлению. Всего уровней значимости три, хотя если ущерба нет ни по одному критерию, то такой объект признается незначимым. Если объект подпадает под несколько критериев значимости, то уровень выбирается по наивысшему показателю.

Далее проводится моделирование угроз с оценкой уровней риска по каждому вектору атаки и выбираются меры защиты в соответствии с уровнем значимости ЗОКИИ, которые подобные риски могут снизить. Вся эта информация заносится в акт категорирования, а также в специальную форму уведомления, которая передается во ФСТЭК России, специалисты которой могут не согласиться с выводами комиссии по категорированию и в определенный срок прислать предписание по исправлению обнаруженных недочетов. Когда все документы согласованы, они вносятся в реестр ЗОКИИ, ситуация с ИБ которых будет находиться под контролем ФСТЭК России.

Постановление предписывает проводить не реже чем один раз в пять лет пересмотр установленной категории значимости объектов. Предполагается также проводить не реже чем раз в три года плановую проверку объектов со стороны государственных органов. Однако возможно и проведение внеплановой проверки. По результатам проверки также могут быть выданы предписания по устранению замечаний, которые будут направлены владельцу ЗОКИИ для исправления ситуации. Предполагается, что если владелец ЗОКИИ выполнил все требования регуляторов, но инцидент все-таки произошел, то ответственность может быть разделена – ее мера для каждой стороны будет определена в процессе следствия, но в этом случае уголовная ответственность руководителя уже не предусмотрена.

Требования ФСТЭК России

В первую очередь владелец ЗОКИИ должен выполнить требования ФСТЭК России, которые сформулированы в двух приказах:

- **№ 235 «Об утверждении Требований к созданию систем безопасности ЗОКИИ РФ и обеспечению их функционирования»** – обязывает компании создавать системы безопасности на предприятии, направленные на обеспечение информационной безопасности ЗОКИИ, а также необходимые как для выявления инцидентов, так и реагирования на них;
- **№ 239 «Об утверждении Требований по обеспечению безопасности ЗОКИИ РФ»** – определяет требования к применяемым на предприятии мерам защиты ЗОКИИ.

Ответственным за обеспечение безопасности ЗОКИИ в соответствии с требованиями приказа № 235 должно быть отдельное подразделение (работники), которое должно заниматься исключительно вопросами обеспечения безопасности ЗОКИИ – совмещение ролей, не связанных с вопросами обеспечения ИБ, например эксплуатация ИТ-инфраструктуры, не допускается.

На подразделение, занимающееся защитой ЗОКИИ, в частности, возлагается обязанность взаимодействовать с ГосСОПКА как с целью информирования ФСБ России о произошедших

> Если с соответствующими объектами случаются инциденты информационной безопасности, приводящие к существенному ущербу, их руководство может понести ответственность – вплоть до уголовной.

на ЗОКИИ инцидентах, оказавших влияние на их функционирование или выполнение критических процессов, так и для реакции на предупреждения, поступающие из системы. Собственно, именно поэтому требования приказов ФСТЭК России необходимо выполнить прежде, чем организовать взаимодействие с ГосСОПКА, поскольку при отсутствии службы безопасности подобное взаимодействие не имеет особого смысла.

Приказ № 239 определяет требования к мерам и средствам, которые применяются для защиты ЗОКИИ от кибератак. Хотя сам приказ не требует применения только сертифицированных средств защиты, но обязывает проводить оценку соответствия для установленных на ЗОКИИ средств защиты. Форма такой оценки может быть в виде испытаний или приемки, которые проводятся субъектами КИИ самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации. Испытания (приемка) средств защиты информации проводятся отдельно или в составе ЗОКИИ в соответствии с программой и методиками испытаний (приемки), утверждаемыми субъектом КИИ. Однако для государственных ИС и систем обработки персональных данных сертификация все-таки требуется, на это указано в других законах (Закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ и Закон «О персональных данных» № 152-ФЗ). Следует отметить, что приказ № 239 будет в дальнейшем основным для формирования необходимых к применению мер обеспечения ИБ для российских компаний – под него будут выпущены новые версии приказов № 17 (по ГИС) и № 21 (по ИСПДн).

> Первым результатом деятельности комиссии по категорированию должен стать перечень объектов КИИ с указанием сроков проведения их категорирования, который направляется во ФСТЭК России.

ГосСОПКА

Важной составляющей системы защиты ЗОКИИ является система ГосСОПКА, которая контролируется НКЦКИ и ФСБ России. Система предполагает создание отраслевых, региональных, корпоративных и других центров реагирования на компьютерные инциденты, объединенные форматами взаимодействия, разработанными в ФСБ России. Предполагается двунаправленный обмен информацией: снизу вверх должны поступать сведения об инцидентах, обобщенные в каждом узле сети в рамках его полномочий, а сверху вниз предполагается поступление предупреждений для служб ИБ, которые должны реагировать на возможные атаки и проверять признаки компрометации собственных объектов. Таким образом, ГосСОПКА предназначена для оперативной защиты ЗОКИИ, выявления инцидентов, реагирования на них, обобщения опыта и совершенствования средств защиты.

В этом плане наиболее продвинутой сферой деятельности является финансовая, которая контролируется ЦБ РФ. Это ведомство уже достаточно давно занимается совершенствованием системы информационной защиты подотчетных организаций и имеет свой отраслевой центр реагирования, который получил название FinCERT. Есть отраслевая система стандартов, которая сейчас переносится отраслевым комитетом «Росстандарта» на уровень государственных и становится обязательной. Скорее всего, по аналогичному пути развития пойдут и другие отрасли, упомянутые в Законе № 187-ФЗ. Хотя в этом процессе существуют передовые отрасли, такие как телекоммуникационная или промышленная индустрии, но есть и аутсайдеры. Тем не менее закон одинаков для всех, и в ближайшее время все значимые для экономики России компании будут вынуждены реализовать хотя бы базовые инструменты защиты для своих информационных систем. ■

> ГосСОПКА предназначена для оперативной защиты ЗОКИИ, выявления инцидентов, реагирования на них, обобщения опыта и совершенствования средств защиты.