Антон СВИНЦИЦКИЙ
директор по консалтингу
АО «ДиалогНаука»

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

БанКИИ

ВСЕ БАНКИ ЯВЛЯЮТСЯ СУБЪЕКТАМИ КИИ И ПОДПАДАЮТ ПОД ДЕЙСТВИЕ ФЕДЕРАЛЬНОГО ЗАКОНА №187-ФЗ

Летом прошлого года Государственная Дума приняла федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры» (КИИ), который вступил в действие первого января текущего года. В нем установлены требования по обеспечению безопасности значимых объектов КИИ (ЗОКИИ). Причем в определениях закона указывается двенадцать сфер деятельности, объекты которых могут быть отнесены к ЗОКИИ. Следует отметить, что финансовая сфера полностью и банки в частности подпадают под действие этого закона и являются субъектами КИИ.

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА

Закон № 187-ФЗ причисляет к критической информационной инфраструктуре все предприятия из указанных сфер деятельности. Относится или нет конкретное предприятие к одной из сфер определяется по ОКВЭД, который заполняется при регистрации предприятия, по полученным компанией лицензиям, а также по уставным документам. Однако обязательные требования к защите информации предъявляются только к ЗОКИИ, хотя владельцы незначимых объектов также должны исполнить ряд требований закона, например, в части подготовки перечня объектов КИИ и выполнения процедуры их категорирования.

Также в законе устанавливаются два Федеральных органа исполнительной власти (ФОИВ): один отвечает за безопасность объектов КИИ, в том числе за определение требований по защите информации для объектов КИИ, а второй — за поддержание работоспособности государственной системы обнаружения и предотвращения компьютерных атак (ГосСОПКА) на объекты КИИ. В соответствии с подписанными в конце прошлого года указами первым ФОИВ стала ФСТЭК России, которая в результате получила полномочия устанавливать требования по информационной безопасности для объектов КИИ и осуществлять контроль, а вторым — ФСБ России.

Таким образом, в законе есть две ветки требований: обеспечения безопасности объектов КИИ, контролировать которую будет ФСТЭК России в рамках своих полномочий, и взаимодействия с ГосСОПКА с соблюдением всех регламентов. С точки зрения взаимодействия с ГосСОПКА для кредитно-финансовых организаций предполагается, что оно будет осуществляться через ФинЦЕРТ, который по факту будет являться ведомственным центром ГосСОПКА.

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА № 127-ПП

В начале 2018 года было принято Постановление Правительства № 127-ПП, которое определяет процедуру проведения категорирования объектов КИИ. То есть описанные в нем правила позволяют определить, относится ли объект КИИ к ЗОКИИ или нет. Постановление описывает три категории значимости — от первой до третьей (первая наивысшая) — на основании которой и определяется базовый состав мер обеспечения информационной безопасности, необходимый к реализации субъектами КИИ. Категория значимости определяется по степени ущерба в пяти критериях значимости: социальной, политической, экономической, экологической и значимость для обеспечения обороны страны, безопасности государства и правопорядка. Таблица соотнесения показателей критериев значимости объектов КИИ и категории значимости находится в приложениях к постановлению.

Для проведения процедуры категорирования объектов КИИ нужно создать специальную комиссию, сформировать перечень объектов КИИ, определить процессы, происходящие на объектах, выявить информационные системы, которые поддерживают эти процессы и оценить ущерб, который может быть нанесен в случае нарушения и (или) прекращения функционирования информационной системы. На процедуру категорирования отводится ровно год со дня формирования и утверждения субъектом перечня объектов КИИ. Результатами этой деятельности должны стать документы о присвоении категорий значимости объектам КИИ, которые необходимо направить во ФСТЭК для регистрации в реестре ЗОКИИ. Первая плановая государственная проверка соблюдения требований по информационной безопасности может быть проведена через 3 года после регистрации объекта в реестре. Впрочем, возможны внеплановые проверки после зафиксированных инцидентов.

ПЕРВАЯ ПЛАНОВАЯ ГОСУДАРСТВЕННАЯ ПРОВЕРКА СОБЛЮДЕНИЯ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОЖЕТ БЫТЬ ПРОВЕДЕНА ЧЕРЕЗ 3 ГОДА ПОСЛЕ РЕГИСТРАЦИИ ОБЪЕКТА В РЕЕСТРЕ

Чтобы объект был признан не значимым, нужно провести полноценную процедуру категорирования, пройти по всем типам ущерба и показать, что ни по одному из них он (объект) не может соответствовать указанным в постановлении уровням ущерба. Эти документы также нужно будет подготовить для ФСТЭК России, которая может и не согласиться с выводами комиссии. Однако именно не значимые объекты КИИ освобождаются от соблюдения требований приказов ФСТЭК России № 235 и № 239 в соответствующих закону № 187-ФЗ сферах деятельности, но могут ими руководствоваться при определении требований к системе защиты информации и при построении такой системы защиты.

Процедура категорирования может проводиться банками самостоятельно, либо для этого могут привлекаться сторонние компании, имеющие необходимые лицензии ФСТЭК России.

ПРИКАЗЫ ФСТЭК РОССИИ

В рамках реализации требования закона № 187-ФЗ ФСТЭК России разработала пять приказов, которые определяют различные аспекты обеспечения защиты значимых объектов КИИ — от формы представления результатов в Службу до правил ведения реестра ЗОКИИ.

Ключевыми являются два приказа: № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» и № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Первый относится к субъектам, а второй — к объектам. Первый определяет обязанности владельцев ЗОКИИ по построению службы информационной безопасности, которая будет обеспечивать контроль ИБ всех критических объектов. Второй же устанавливает требования к самим системам защиты, которые обеспечивают безопасность объектов критической инфраструктуры от целенаправленных атак и управляются службами ИБ.

ФСТЭК России отмечает, что строить параллельную структуру для соответствия требованиям приказа № 235 не нужно. Важно только, чтобы служба ИБ занималась именно защитой, а не техническим сопровождением ИТ и другими не свойственными ей обязанностями. Впрочем, для защиты можно привлекать и сторонние организации, которые имеют соответствующие лицензии на предоставление услуг по защите информации.

Требования приказа № 239 определяют меры, которые необходимо будет выполнить для защиты объектов КИИ. При этом сертификация средств защиты в явном виде не требуется и может быть заменена процедурой оценки соответствия. Она необходима только при условии, что ИС является государственной (в соответствии с требованиями закона № 149-ФЗ). Однако же оценка эффективности средств защиты должна быть проведена в любом случае. В частности, ее можно провести в виде приемочных испытаний. Фактически этот приказ определяет минимально необходимый уровень безопасности для всех предприятий России, и исполнение этих требований должно повысить уровень защищенности всего российского бизнеса.

ГОССОПКА И ФИНЦЕРТ

Вторая часть закона № 187-ФЗ относится к построению системы обнаружения вторжений и взаимодействию с распределенной системой ГосСОПКА. К счастью, банкам не нужно взаимодействовать с ГосСОПКА напрямую — взаимодействие может происходить через ведомственный центр, который получил наименование ФинЦЕРТ. Ранее он функционировал в рамках предписаний Центробанка, а теперь получает более высокий статус. Естественно, взаимодействие с ним будет обязательным как минимум для тех банков, которые будут признаны ЗОКИИ.

В настоящее время Центробанк ведет работу по значительному расширению возможностей по взаимодействию банков через ФинЦЕРТ как в части информирования об инцидентах, так и в части процессов расследования и реагирования на них.

* * *

На сегодняшний день важно отметить, что все банки являются субъектами КИИ и подпадают под действие Федерального закона № 187-ФЗ. В первую очередь банки должны составить перечень объектов КИИ и провести процедуру их категорирования в соответствии с требованиями Постановления Правительства № 127. Несмотря на то, что на эту процедуру формально отводится один год, с нашей точки зрения лучше уже сейчас начать планировать данные работы.