KASPERSKY lab

Обзор нормативной базы ФСТЭК России

Категорирование и обеспечение информационной безопасности критической информационной инфраструктуры

Дмитрий Сатанин
Юлия Дащенко

Kaspersky Lab ICS CERT

Содержание

С началом 2018-го года в силу вступил федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Закон). На протяжении первых пяти месяцев года интереса к данной тематике растет. В частности, особое внимание со стороны потенциальных субъектов критической информационной инфраструктуры (далее – КИИ), а также представителей IT/ИБ-отрасли уделяется порядку категорирования и защиты КИИ.

Наиболее распространенные вопросы:

- Каков состав и содержание подзаконной нормативной базы?
- Как использовать ее на практике?
- Какие программные и технические средства нужны для КИИ и чему они должны соответствовать?

Ниже мы попытаемся разъяснить основные положения и практическое применение новой нормативной базы ФСТЭК России. Однако нужно понимать, что наша статья заменить по содержанию сами руководящие документы не может.

Нормативная база ФСТЭК России

Напомним, что органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ, является ФСТЭК России. Это закреплено указом Президента Российской Федерации от 25.11.2017 г. № 569 «О внесении изменений в Положение о ФСТЭК России, утвержденное Указом Президента Российской Федерации от 16.08.2004 г. № 1085». Специалисты ведомства серьезно подошли к поставленной задаче и уже к концу зимы разработали и ввели нормативную базу, необходимую для категорирования потенциальных объектов КИИ и создания систем их защиты. Состав указанной нормативной базы приведен в таблице 1.

Таблица 1. Состав нормативной базы ФСТЭК России в области обеспечения информационной безопасности КИИ

Постановления Правительства	№ 127 от 08.02.2018 г. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (далее – Правила категорирования) № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
Приказы ФСТЭК России	• № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»; • № 229 от 11.12.2017 г. «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»; • № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (далее – Приказ № 235); • № 236 от 21.12.2017 г. «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»; • № 239 от 25.12.2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее – Требования по безопасности КИИ).

Ключевыми для потенциальных субъектов КИИ и представителей IT/ИБ-отрасли, которые готовы помогать субъектам КИИ в реализации положений Закона, являются Правила категорирования, Приказ № 235 и Требования по безопасности КИИ. Эти документы и определяют последовательность действий, которые должны быть выполнены потенциальным субъектом КИИ:

1. В соответствии с Правилами категорирования провести инвентаризацию, обследование и определение категорий значимости принадлежащих ему объектов КИИ;
2. В зависимости от присвоенной категории значимости на основании Требований по безопасности КИИ спроектировать систему защиты и определить состав средств для ее реализации;
3. Внедрить систему защиты и впоследствии осуществлять ее эксплуатацию в соответствии с Приказом № 235.

Далее приводится краткий обзор требований каждого из этих документов.

Правила категорирования

Категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ.

Категория значимости определяется на основе показателей критериев значимости из Правил категорирования.

Устанавливаются три категории значимости: от самой высокой – первой, к самой низкой – третьей. Объекту КИИ по результатам категорирования присваивается категория с наивысшим значением. Например, если хотя бы по одному из критериев исследуемый объект КИИ соответствует первой категории, то присваивают именно ее.

Перечень объектов для категорирования утверждается субъектом КИИ, согласуется организацией-регулятором в соответствующей области деятельности и передается во ФСТЭК России. Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом КИИ такого перечня.

Состав установленных показателей критериев значимости приведен в таблице 2.

Таблица 2. Перечень показателей критериев значимости

Критерий значимости	Показатели критерия значимости
Социальная значимость	• причинение ущерба жизни и здоровью людей • прекращение или нарушение функционирования: ▪ объектов обеспечения жизнедеятельности населения (водоснабжения и канализации и т.д.); ▪ транспортной инфраструктуры; ▪ сети связи • отсутствие доступа к государственной услуге

Политическая значимость	• прекращение или нарушение функционирования госоргана; • нарушение условий международного договора
Экономическая значимость	• возникновение ущерба субъекту КИИ • возникновение ущерба бюджетам Российской Федерации • прекращение или нарушение проведения финансовых и банковских операций субъектом КИИ
Экологическая значимость	Вредные воздействия на окружающую среду (например, ухудшение качества воды в поверхностных водоемах, повышение уровня вредных загрязняющих веществ и прочее)
Значимость для обеспечения обороны страны, безопасности государства и правопорядка	• прекращение или нарушение функционирования: ▪ пункта управления/ситуационного центра; ▪ информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка • снижение показателей государственного оборонного заказа

Исходными данными для категорирования являются:

- сведения об объекте КИИ (назначение, архитектура объекта, применяемые программные и аппаратные средства, взаимодействие с другими объектами КИИ, наличие и характеристики доступа к сетям связи);
- выполняемые процессы (управленческие, технологические, производственные, финансово-экономические, иные) и состав обрабатываемой информации;
- декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект КИИ;
- сведения о взаимодействии и/или зависимости от других объектов КИИ;
- угрозы безопасности информации в отношении объекта КИИ, а также имеющиеся данные о компьютерных инцидентах, произошедших ранее на объектах КИИ соответствующего типа.

Для проведения категорирования решением руководителя субъекта КИИ создается комиссия по категорированию, в которую включаются:

- сам руководитель или уполномоченное им лицо – в качестве председателя комиссии;
- работники субъекта КИИ, ответственные за:
  - выполнение основных видов деятельности,
  - IT и связь,
  - технологическую (промышленную) безопасность, гражданскую оборону и защиту от чрезвычайных ситуаций, контроль за опасными веществами и материалами, учет опасных веществ и материалов,
  - информационную безопасность,
  - обеспечение режима защиты государственной тайны.

В состав комиссии также могут включаться представители организаций-регуляторов в соответствующей области по согласованию с ними.

Комиссия по категорированию в ходе работы:

- определяет основные производственные процессы в рамках осуществления видов деятельности субъекта КИИ;
- выявляет наличие критических процессов и задействованные при этом объекты КИИ (формирует перечень объектов КИИ);
- рассматривает и анализирует возможные действия нарушителей, потенциальные источники угроз безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов;
- оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;
- устанавливает каждому из них одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости;
- оформляет свое решение актом, содержащим основные результаты работ по перечисленным выше пунктам, и направляет его на проверку ФСТЭК России, где с ним могут согласиться или не согласиться. Во втором случае комиссии потребуется исправить замечания регулятора.

Субъект КИИ не реже чем один раз в пять лет осуществляет пересмотр установленной категории значимости в соответствии с настоящими Правилами. В случае изменения категории значимости сведения о результатах пересмотра направляются в федеральный орган, уполномоченный в области обеспечения безопасности КИИ.

Требования по безопасности КИИ

Первое, на что следует обратить внимание, это возможность применения данного документа к объектам КИИ, которым категория значимости присвоена не была. Решение, делать это или нет, находится в компетенции владельца КИИ. Для значимых объектов КИИ реализация положений Требований является обязательной.

Второй важный момент – это корреляционные связи с другими руководящими документами ФСТЭК России. При проектировании защиты значимых объектов КИИ, являющихся информационными системами персональных данных, необходимо учитывать Требования к защите персональных данных при их обработке в информационных системах персональных данных (постановление Правительства Российской Федерации от 01.11.2012 г. № 1119). В случае с государственными информационными системами (ГИС) – Требования о защите информации, которая содержится в ГИС и не составляет государственную тайну (приказ ФСТЭК России от 11.02.2013 г. № 17), соответственно. Причем меры защиты принимаются в соответствии с более высокой категорией значимости, классом защищенности ГИС или уровнем защищенности персональных данных.

Третье и, пожалуй, самое важное – в Требованиях закреплено, что меры по обеспечению безопасности значимого объекта КИИ принимаются субъектом КИИ на всех стадиях его жизненного цикла, включая создание, модернизацию, использование и вывод из эксплуатации, и должны содержать (см. рисунок 1):

- установление требований к обеспечению безопасности объекта;
- разработку соответствующих организационных и технических мер и их внедрение (для эксплуатируемого объекта КИИ – при его модернизации);
- обеспечение безопасности объекта КИИ в ходе его эксплуатации и при выводе его из эксплуатации.

Рисунок 1. Состав требований по обеспечению безопасности КИИ

Конкретные требования по защите значимого объекта КИИ определяются субъектом КИИ в соответствии с его категорией значимости и включаются в техническое задание, которое должно содержать:

- цель и задачи обеспечения безопасности данного объекта;
- категорию значимости объекта;
- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать данный объект;
- перечень типов объектов защиты (архитектура и конфигурация данного объекта КИИ, обрабатываемая (циркулирующая, передаваемая, хранимая) информация, используемые программно-аппаратные средства, в том числе, средства защиты информации);
- организационные и технические меры защиты данного объекта;
- стадии (этапы работ) создания подсистемы безопасности;
- требования к применяемым программным и аппаратным средствам, в том числе средствам защиты информации (СрЗИ);
- требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре);
- требования к информационному взаимодействию с иными информационными системами, сетями, автоматизированными системами управления, в том числе объектами КИИ (при разработке должны учитываться организационные и технические меры защиты).

Целью защиты значимого объекта КИИ является обеспечение его устойчивого функционирования в проектных режимах работы в условиях реализации угроз безопасности информации.

Разработка организационных и технических мер защиты включает:

- анализ угроз безопасности информации и разработку модели угроз;
- проектирование соответствующей подсистемы безопасности;
- разработку рабочей (эксплуатационной) документации.

При разработке мер защиты объекта КИИ должно учитываться его взаимодействие с другими системами и сетями. При этом меры защиты не должны оказывать негативного влияния на создание и функционирование объекта КИИ.

Для проведения соответствующих работ допускается привлечение внешних организаций, имеющих лицензию на деятельность по технической защите информации, составляющей государственную тайну, и/или конфиденциальной информации. Однако необходимо учитывать, что для значимого объекта КИИ не допускается:

- наличие локального бесконтрольного доступа и прямого удаленного доступа для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ;
- передача информации кому-либо без контроля со стороны субъекта КИИ.

Все работы должны документироваться в соответствии с действующими государственными стандартами.

Основные этапы создания системы защиты значимого объекта КИИ и их содержание приведено на рисунке 2.

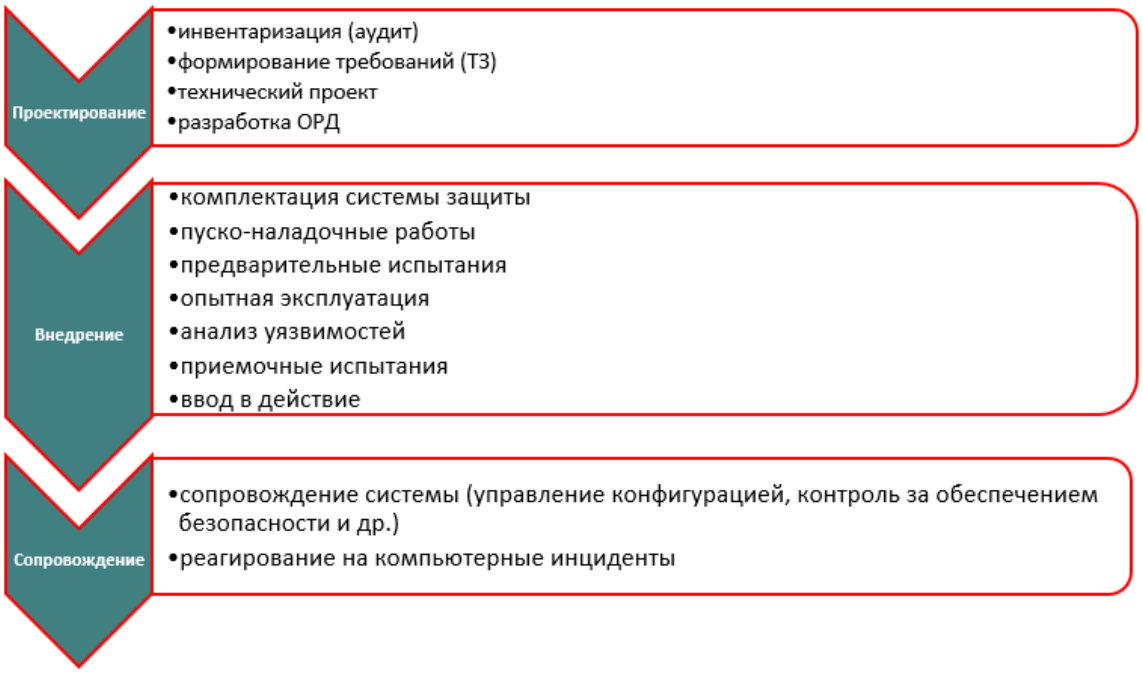

Рисунок 2. Состав и содержание этапов создания системы защиты

В значимых объектах КИИ должны быть реализованы следующие организационные и технические меры:

- идентификация и аутентификация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений;
- обеспечение целостности;
- обеспечение доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- планирование мероприятий по обеспечению безопасности;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- реагирование на инциденты информационной безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Содержание перечисленных мер конкретизируется в приложении к Требованиям и определяется в зависимости от категории значимости объекта КИИ. При этом базовый набор мер целесообразно адаптировать с учетом особенностей конкретного объекта КИИ и при необходимости дополнять (см. рисунок 3).

Рисунок 3. Порядок формирования набора мер по защите КИИ

Для реализации итогового набора мер должны применяться СрЗИ, прошедшие оценку на соответствие требованиям по безопасности в формах сертификации (обязательно – в случаях, установленных законодательством Российской Федерации), испытаний или приемки (в иных случаях), проведенных субъектами КИИ самостоятельно или с привлечением специализированных организаций. При этом классы защиты, сертифицированные СрЗИ и используемые средства вычислительной техники (СВТ) должны подбираться в соответствии с категорией значимости объектов КИИ, как показано в таблице 3.

Таблица 3. Требования к СВТ и СрЗИ, применяемым для защиты значимого объекта КИИ

Категория значимости объекта КИИ	Класс средств вычислительной техники	Уровень контроля отсутствия НДВ	Класс защиты СрЗИ
1 категория	Не ниже 5 класса	Не ниже 4 уровня	Не ниже 4 класса
2 категория	Не ниже 5 класса	Не ниже 4 уровня	Не ниже 5 класса
3 категория	Не ниже 5 класса	-	Не ниже 6 класса

Приказ № 235

Приказ № 235 содержит требования к составу и функционированию систем безопасности, а также организационно-распорядительным документам по безопасности значимых объектов КИИ.

Согласно документу, системы безопасности включают в себя силы (уполномоченные работники субъекта КИИ) и средства обеспечения безопасности значимых объектов КИИ (далее – Силы и Средства), которые должны:

- предотвращать неправомерный доступ к информации, обрабатываемой значимыми объектами КИИ, а также иные неправомерные действия с информацией;
- не допускать воздействия на технические средства, способного привести к сбоям и нарушениям в функционировании значимых объектов КИИ;
- позволять восстановление функционирования значимых объектов КИИ;
- непрерывно взаимодействовать с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (системой ГосСОПКА).

Особое внимание нужно обратить на то, что системы безопасности должны быть созданы для всех значимых объектов КИИ, имеющихся у субъекта КИИ, но по его решению отдельные системы безопасности могут создаваться как для одного, так и для группы значимых объектов. Это – важно, потому что позволит существенно сократить расходы.

Состав и структура систем безопасности значимых объектов КИИ, функции ее участников определяются руководителем соответствующего субъекта КИИ в зависимости от количества таких объектов и особенностей деятельности самого субъекта КИИ, в частности:

- создаются Силы – структурное подразделение по безопасности или отдельные работники (далее – специалисты по безопасности), на которых не допускается возложение функций, не связанных с обеспечением информационной безопасности значимого объекта и субъекта КИИ в целом;
- при необходимости осуществляется привлечение внешних организаций, имеющих соответствующие лицензии в области защиты информации;
- субъект КИИ должен проводить не реже одного раза в год организационные мероприятия по повышению уровня знаний уполномоченных работников субъекта КИИ (Сил обеспечения безопасности значимых объектов КИИ).

К Средствам относятся:

- СрЗИ от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение);
- межсетевые экраны;
- средства обнаружения (предотвращения) вторжений (компьютерных атак);
- средства антивирусной защиты;
- средства (системы) контроля (анализа) защищенности;

- средства управления событиями безопасности;
- средства защиты каналов передачи данных.

Все они должны быть сертифицированы на соответствие требованиям по безопасности или пройти оценку соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27.12.2002 г. № 184-ФЗ «О техническом регулировании».

Применение сертифицированных СрЗИ или средств, прошедших испытания или приемку, регламентируются так же, как и в Требованиях по безопасности КИИ. Параметры и характеристики применяемых средств защиты информации должны обеспечивать реализацию технических мер по обеспечению безопасности значимых объектов КИИ. В приоритетном порядке подлежат применению СрЗИ, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов КИИ (при их наличии).

Важно отметить, что при выборе СрЗИ должно учитываться возможное наличие ограничений со стороны разработчиков (производителей) или иных лиц на применение этих средств. Это замечание особо существенно в условиях существующих санкций и их возможного расширения.

Система безопасности объекта КИИ должна функционировать на основе организационно-распорядительных документов, разработанных с учетом особенностей деятельности субъекта КИИ и положений нормативных правовых актов в области защиты КИИ, которые должны определять:

- цели и задачи обеспечения безопасности значимых объектов КИИ;
- модель угроз и категории нарушителей безопасности информации;
- основные организационные и технические мероприятия по обеспечению безопасности значимых объектов КИИ;
- состав и структуру системы безопасности и функции ее участников;
- порядок применения, формы оценки соответствия значимых объектов КИИ и СрЗИ требованиям по безопасности, планы мероприятий по обеспечению безопасности значимых объектов КИИ;
- деятельность Сил, включая порядок действий при возникновении компьютерных инцидентов и иных нештатных ситуаций, обучение, взаимодействие с другими подразделениями субъекта КИИ и др.;
- порядок взаимодействия субъекта КИИ с системой ГосСОПКА.

Организационно-распорядительные документы по безопасности значимых объектов утверждаются руководителем субъекта КИИ или уполномоченными на это сотрудниками и доводятся до сотрудников других подразделений субъекта КИИ в части, их касающейся.

В рамках функционирования системы безопасности субъектом КИИ должны быть внедрены следующие процессы:

- ежегодное и перспективное планирование, разработка и реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов КИИ;
- контроль состояния и совершенствование безопасности значимых объектов КИИ.

Перечисленные процессы за исключением контроля реализуются и документируются структурным подразделением по безопасности и (или) специалистами по безопасности, по результатам составляется и утверждается соответствующий отчет, а также предложения по совершенствованию системы безопасности по результатам анализа ее функционирования.

Контроль проводится ежегодно комиссией, назначаемой субъектом КИИ. Для оценки эффективности принятых организационных и технических мер по обеспечению безопасности могут применяться средства контроля (анализа) защищенности. Результаты контроля оформляются актом. В случае проведения по решению руководителя субъекта КИИ внешней оценки (аудита) внутренний контроль может не проводиться. Для внешней оценки привлекаются организации, имеющие лицензии на деятельность в области защиты информации (в части услуг по контролю защищенности информации от несанкционированного доступа и ее модификации в средствах и системах информатизации).

В итоге

С вступлением в силу Закона и подзаконной нормативной базы окончательно поставлена точка в вопросе необходимости обеспечения информационной безопасности КИИ. Защищать КИИ нужно! И делать это придется планомерно и на регулярной основе всем организациям, которые осуществляют деятельность в банковской и кредитно-финансовой сфере, в областях здравоохранения, науки, транспорта, связи, энергетики и ТЭК, а также оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленностях.

Начать необходимо с инвентаризации собственной информационной инфраструктуры, что позволит выявить потенциальные значимые объекты КИИ. После чего провести их категорирование и сформировать набор требований по обеспечению безопасности, и затем создать и обеспечить эксплуатацию соответствующей системы защиты.

Для создания системы защиты потребуются качественные СрЗИ, подтвержденные сертификатами соответствия регуляторов (ФСТЭК России и ФСБ России), а также наличие квалифицированного персонала.

Центр «Лаборатории Касперского» по реагированию на инциденты информационной безопасности промышленных инфраструктур (Kaspersky Lab ICS CERT) — глобальный проект, нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий от кибератак. Усилия Kaspersky Lab ICS CERT направлены в первую очередь на выявление потенциальных и существующих угроз для систем промышленной автоматизации и промышленного интернета вещей.

Kaspersky Lab ICS CERT
Ics-cert@kaspersky.com