

Обзор законодательства РФ о критической информационной инфраструктуре

Часть 1. Категорирование объектов КИИ и обязанности субъектов КИИ

Общие положения

С 01.01.2018 вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который предназначен для регулирования деятельности по обеспечению безопасности объектов информационной инфраструктуры РФ, функционирование которых критически важно для экономики государства. Такие объекты в законе называются объектами критической информационной инфраструктуры (КИИ). Согласно законодательству, к объектам КИИ могут быть отнесены информационные системы и сети, а также автоматизированные системы управления, функционирующие в сфере:

1. здравоохранения;
2. науки;
3. транспорта;
4. связи;
5. энергетики;
6. банковской и иных сферах финансового рынка;
7. топливно-энергетического комплекса;
8. атомной энергии;
9. оборонной и ракетно-космической промышленности;
10. горнодобывающей, металлургической и химической промышленности.

Объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия между ними, составляют понятие критической информационной инфраструктуры.

Главной целью обеспечения безопасности КИИ является устойчивое функционирование КИИ, в том числе при проведении в отношении нее компьютерных атак. Главным принципом обеспечения безопасности является предотвращение компьютерных атак.

Требования 187-ФЗ затрагивают те организации (государственные органы и учреждения, юридические лица и индивидуальные предприниматели), которым принадлежат (на праве собственности, аренды или ином законном основании) объекты КИИ или которые обеспечивают их взаимодействие. Такие организации называются субъектами КИИ. Согласно законодательству, субъекты КИИ должны провести категорирование объектов КИИ.

Список терминов и определений в области КИИ

Ниже приведен список терминов и их определений, используемых в области регулирования и обеспечения безопасности КИИ:

Автоматизированная обработка информации - Обработка информации с помощью средств вычислительной техники.

Безопасность КИИ - Состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Значимый объект КИИ - Объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры

Информационная система - Совокупность содержащейся в БД информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии - Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Конфиденциальность информации - Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Компьютерная атака - Целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации

Компьютерный инцидент - Факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Критическая информационная инфраструктура (КИИ) Объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Материальный носитель информации - Материальный объект, используемый для закрепления и хранения на нем речевой, звуковой или изобразительной информации, в т.ч. в преобразованном виде.

Обработка информации - Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Объект КИИ (ОКИИ) - Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Оператор ИС - Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации ИС, в т.ч. по обработке информации, содержащихся в ее БД. Если иное не установлено федеральными законами, оператором ИС является собственник технических средств, используемых для обработки содержащихся в БД информации, который правомерно пользуется такими БД, или лицо, с которым этот собственник заключил договор об эксплуатации ИС.

Передача информации - Распространение, предоставление или доступ к информации.

Субъект КИИ - Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Техническое средство - Изделие, оборудование, аппаратура или их составные части, функционирование которых основано на законах электротехники, радиотехники и (или) электроники, содержащие электронные компоненты и (или) схемы, которые выполняют одну или несколько следующих функций: усиление, генерирование, преобразование, переключение и запоминание.

Критические процессы - Управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

Категорирование объектов КИИ

Категорирование объектов КИИ осуществляется исходя из:

1. социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;
2. политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;
3. экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;
4. экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;
5. значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

В соответствии с п.3 ч.2 ст.7 187-ФЗ устанавливаются три категории значимости объектов КИИ – первая (самая высокая), вторая и третья (самая низкая).

В соответствии с ч.4 п.2 ст.7 187-ФЗ субъект КИИ в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования (127-П) присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам КИИ. Если объект КИИ не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

В соответствии с п.3 127-П категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта в КИИ.

Определение категорий значимости объектов КИИ осуществляется на основании показателей критериев значимости объектов КИИ и их значений, предусмотренных в перечне показателей критериев значимости объектов КИИ РФ и их значений в 127-П.

В соответствии с п.11 127-П для проведения категорирования решением руководителя субъекта критической информационной инфраструктуры создается комиссия по категорированию.

Комиссия по категорированию в ходе своей работы:

1. определяет процессы, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ;
2. выявляет наличие критических процессов у субъекта КИИ;
3. выявляет объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов;
4. рассматривает возможные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации;
5. анализирует угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;
6. оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;
7. устанавливает каждому из объектов КИИ одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости.

Решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте КИИ, результаты анализа угроз безопасности информации объекта КИИ, реализованные меры по обеспечению безопасности объекта КИИ, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ. Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта КИИ.

Сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий субъект КИИ в письменном виде в десятидневный срок со дня принятия ими соответствующего решения направляют во ФСТЭК России.

ФСТЭК России в тридцатидневный срок со дня получения сведений о результатах присвоения объекту КИИ одной из категорий значимости, проверяет соблюдение порядка осуществления категорирования и правильность присвоения объекту КИИ одной из категорий значимости либо не присвоения ему ни одной из таких категорий.

В случае, если субъектом КИИ соблюден порядок осуществления категорирования и принадлежащему ему на праве собственности, аренды или ином законном основании объектам КИИ правильно присвоена одна из категорий значимости, ФСТЭК России вносит сведения о таких объектах КИИ в реестр значимых объектов КИИ, о чем в десятидневный срок уведомляется субъект КИИ.

В случае, если ФСТЭК России выявлены нарушения порядка осуществления категорирования и (или) объекту КИИ, принадлежащему на праве собственности, аренды или ином законном основании субъекту КИИ, неправильно присвоена одна из категорий значимости и (или) необоснованно не присвоена ни одна из таких категорий и (или) субъектом КИИ представлены неполные и (или) недостоверные сведения о результатах присвоения такому объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, ФСТЭК России, в десятидневный срок со дня поступления представленных сведений возвращает их в письменном виде субъекту КИИ с мотивированным обоснованием причин возврата.

Субъект КИИ после получения мотивированного обоснования причин возврата сведений, не более чем в десятидневный срок устраняет отмеченные недостатки и повторно направляет такие сведения во ФСТЭК России.

Субъект КИИ не реже чем один раз в 5 лет осуществляет пересмотр установленной категории значимости в соответствии с требованиями 127-П. В случае изменения категории значимости сведения о результатах пересмотра категории значимости направляются во ФСТЭК России.

Обязанности субъектов КИИ

4.2 ст.9 187-ФЗ предусматривает следующие обязанности субъектов КИИ:

1. незамедлительно информировать о компьютерных инцидентах ФСБ России, а также ЦБ РФ в установленном ими порядке;
2. оказывать содействие должностным лицам ФСБ России в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;
3. в случае установки на объектах КИИ средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

4.3 ст.9 187-ФЗ предусматривает следующие дополнительные обязанности для субъектов, которым принадлежат значимые объекты КИИ:

1. соблюдать требования по обеспечению безопасности значимых объектов КИИ, установленные ФСТЭК России;
2. выполнять предписания должностных лиц ФСТЭК России об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта КИИ, выданные этими лицами в соответствии со своей компетенцией;
3. реагировать на компьютерные инциденты в порядке, утвержденном ФСБ России, принимать меры по ликвидации последствий

- компьютерных атак, проведенных в отношении значимых объектов КИИ;
4. обеспечивать беспрепятственный доступ должностным лицам ФСТЭК России, к значимым объектам критической информационной инфраструктуры при реализации этими лицами полномочий по государственному контролю в области обеспечения безопасности значимых объектов КИИ.

Часть 2. Система безопасности значимых объектов КИИ

Общие положения

ФСТЭК России является Федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры (КИИ) РФ. ФСБ России является Федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

ФСТЭК России осуществляет плановые и внеплановые проверки субъектов КИИ в части обеспечения ими безопасности значимых объектов КИИ. ФСТЭК России ведет Реестр значимых объектов критической информационной инфраструктуры.

В соответствии с п. 31 П-239¹⁾ в значимом объекте не допускаются:

1. наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в том числе СЗИ для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ;
2. наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в том числе СЗИ, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ;
3. передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе СЗИ, или иным лицам без контроля со стороны субъекта КИИ.

Система безопасности значимых объектов КИИ

В соответствии с требованиями ст.10 187-ФЗ²⁾ субъект КИИ (Заказчик) создает систему безопасности значимых объектов КИИ и обеспечивает её функционирование в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными ФСТЭК России (П-235³⁾ и П-239).

Основные задачи Системы безопасности значимых объектов КИИ (ч.2 ст.10 187-ФЗ и п.6 П-235):

1. предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
2. недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;
3. восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;
4. непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

В соответствии с п.3 П-235 создание и функционирование систем безопасности значимых объектов КИИ должно быть направлено на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак.

Также в соответствии с п. 15 П-239 целью обеспечения безопасности значимого объекта является обеспечение его устойчивого функционирования в проектных режимах работы в условиях реализации в отношении значимого объекта угроз безопасности информации. Исходя из вышеописанного, можно сделать вывод, что основными характеристиками безопасности для значимых объектов КИИ в первую очередь являются доступность и целостность и уже потом конфиденциальность.

Системы безопасности создаются в отношении всех значимых объектов КИИ субъектов КИИ. По решению субъекта КИИ для одного или группы значимых объектов КИИ могут создаваться отдельные системы безопасности.

В соответствии с п.7 П-239 обеспечение безопасности значимых объектов КИИ является составной частью работ по созданию (модернизации), эксплуатации и вывода из эксплуатации значимых объектов. Меры по обеспечению безопасности значимых объектов принимаются на всех стадиях (этапах) их жизненного цикла.

На стадиях (этапах) жизненного цикла в ходе создания (модернизации), эксплуатации и вывода из эксплуатации значимого объекта проводятся:

1. установление требований к обеспечению безопасности значимого объекта;
2. разработка организационных и технических мер по обеспечению безопасности значимого объекта;
3. внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие;

4. обеспечение безопасности значимого объекта в ходе его эксплуатации;
5. обеспечение безопасности значимого объекта при выводе его из эксплуатации.

Требования к обеспечению безопасности включаются в ТЗ на создание значимого объекта и (или) ТЗ (частное техническое задание) на создание подсистемы безопасности значимого объекта, которые должны содержать:

1. цель и задачи обеспечения безопасности значимого объекта или подсистемы безопасности значимого объекта;
2. категорию значимости значимого объекта;
3. перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект;
4. перечень типов объектов защиты значимого объекта;
5. организационные и технические меры, применяемые для обеспечения безопасности значимого объекта;
6. стадии (этапы работ) создания подсистемы безопасности значимого объекта;
7. требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;
8. требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре);
9. требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

В соответствии с п.11.2 П-239 проектирование подсистемы безопасности значимого объекта должно осуществляться в соответствии с ТЗ на создание значимого объекта и (или) ТЗ (частным техническим заданием) на создание подсистемы безопасности значимого объекта с учетом модели угроз безопасности информации и категории значимости значимого объекта.

При проектировании подсистемы безопасности значимого объекта:

1. определяются субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа;
2. определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);
3. обосновываются организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности значимого объекта;
4. определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;
5. осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
6. разрабатывается архитектура подсистемы безопасности значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации;
7. определяются требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;
8. определяются меры по обеспечению безопасности при взаимодействии значимого объекта с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

В соответствии с п. 11.3 П-239 разработка рабочей (эксплуатационной) документации на значимый объект осуществляется в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта на основе проектной документации.

Рабочая (эксплуатационная) документация на значимый объект должна содержать:

1. описание архитектуры подсистемы безопасности значимого объекта;
2. порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;
3. правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации).

В соответствии с п.22 П-239 в значимых объектах в зависимости от их категории значимости и угроз безопасности информации должны быть реализованы следующие организационные и технические меры:

1. идентификация и аутентификация (ИАФ);
2. управление доступом (УПД);
3. ограничение программной среды (ОПС);
4. защита машинных носителей информации (ЗНИ);
5. аудит безопасности (АУД);
6. антивирусная защита (АВЗ);
7. предотвращение вторжений (компьютерных атак) (СОВ);
8. обеспечение целостности (ОЦЛ);
9. обеспечение доступности (ОДТ);
10. защита технических средств и систем (ЗТС);
11. защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
12. планирование мероприятий по обеспечению безопасности (ПЛН);
13. управление конфигурацией (УКФ);
14. управление обновлениями программного обеспечения (ОПО);

15. реагирование на инциденты информационной безопасности (ИНЦ);
16. обеспечение действий в нештатных ситуациях (ДНС);
17. информирование и обучение персонала (ИПО).

Состав мер по обеспечению безопасности значимых объектов в зависимости от категории значимости приведен в приложении к П-239.

В соответствии с п.26 П-239 при отсутствии возможности реализации отдельных мер по обеспечению безопасности и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе вследствие их негативного влияния на функционирование значимого объекта в проектных режимах значимого объекта, должны быть разработаны и внедрены компенсирующие меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации с необходимым уровнем защищенности значимого объекта. При этом в ходе разработки организационных и технических мер по обеспечению безопасности значимого объекта должно быть обосновано применение компенсирующих мер, а при приемочных испытаниях (аттестации) оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В качестве компенсирующих мер могут быть рассмотрены меры по обеспечению промышленной, функциональной и (или) физической безопасности значимого объекта, поддерживающие необходимый уровень его защищенности.

Часть 3. Анализ угроз безопасности информации и защита объектов КИИ

Анализ угроз безопасности информации значимого объекта КИИ

В соответствии с п.11.1 П-239 целью анализа угроз безопасности информации является: определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов значимого объекта, взаимодействия с иными объектами КИИ, информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями (далее - архитектура значимого объекта), а также особенностей функционирования значимого объекта.

Анализ угроз безопасности информации должен включать:

1. выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
2. анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;
3. определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
4. оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

В качестве исходных данных для анализа угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России.

Модель угроз безопасности информации должна содержать краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта.

Описание каждой угрозы безопасности информации должно включать:

1. источник угрозы безопасности информации;
2. уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы безопасности информации;
3. возможные способы (сценарии) реализации угрозы безопасности информации;
4. возможные последствия от угрозы безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации должны применяться методические документы, разработанные и утвержденные ФСТЭК России.

В соответствии с п. 17 П-239 в значимых объектах объектами, подлежащими защите от угроз безопасности информации (объектами защиты), являются:

1. в информационных системах:
 - информация, обрабатываемая в информационной системе;
 - программно-аппаратные средства (в том числе машинные носители информации, автоматизированные рабочие места, серверы, телекоммуникационное оборудование, линии связи, средства обработки буквенно-цифровой, графической, видео- и речевой информации);
 - программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);
 - средства защиты информации;
 - архитектура и конфигурация информационной системы;
2. в информационно-телекоммуникационных сетях:

- информация, передаваемая по линиям связи;
 - телекоммуникационное оборудование (в том числе программное обеспечение, система управления);
 - средства защиты информации;
 - архитектура и конфигурация информационно-телекоммуникационной сети;
3. в автоматизированных системах управления:
- информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация);
 - программно-аппаратные средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, линии связи, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства);
 - программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);
 - средства защиты информации;
 - архитектура и конфигурация автоматизированной системы управления.

В соответствии с п.18 П-239 обеспечение безопасности значимого объекта достигается путем принятия в рамках подсистемы безопасности значимого объекта совокупности организационных и технических мер, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к прекращению или нарушению функционирования значимого объекта и обеспечивающего (управляемого, контролируемого) им процесса, а также нарушению безопасности обрабатываемой информации (нарушению доступности, целостности, конфиденциальности информации).

В соответствии с п.19 П-239 меры по обеспечению безопасности выбираются и реализуются в значимом объекте с учетом угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации.

В соответствии с п.23 П-239 при адаптации базового набора мер по обеспечению безопасности значимого объекта для каждой угрозы безопасности информации, включенной в модель угроз, сопоставляется мера или группа мер, обеспечивающие блокирование одной или нескольких угроз безопасности или снижающие возможность ее реализации исходя из условий функционирования значимого объекта. В случае если базовый набор мер не позволяет обеспечить блокирование (нейтрализацию) всех угроз безопасности информации, в него дополнительно включаются меры, приведенные в приложении к П-239.

В соответствии с п.25 П-239 если принятые в значимом объекте меры по обеспечению промышленной, функциональной безопасности и (или) физической безопасности достаточны для блокирования (нейтрализации) отдельных угроз безопасности информации, дополнительные меры, выбранные в соответствии с пунктами 22 и 23 П-239, могут не применяться. При этом в ходе разработки организационных и технических мер по обеспечению безопасности значимого объекта должна быть обоснована достаточность применения мер по обеспечению промышленной безопасности или физической безопасности для блокирования (нейтрализации) соответствующих угроз безопасности информации. Исходя из вышеописанного, можно сделать вывод, что Модель угроз является ключевым документом для определения состава мер защиты значимых объектов КИИ в соответствии с требованиями П-239.

Исходя из вышеописанного, можно сделать вывод, что Модель угроз является ключевым документом для определения состава мер защиты значимых объектов КИИ в соответствии с требованиями П-239.

В соответствии с п.32 П-236⁴⁾ при использовании в значимых объектах новых информационных технологий и выявлении дополнительных угроз безопасности информации, для которых не определены меры по обеспечению безопасности, должны разрабатываться компенсирующие меры в соответствии с требованиями П-239.

Организационные меры защиты значимых объектов КИИ

В соответствии с п.23 П-235 субъектом КИИ в рамках функционирования системы безопасности должны быть утверждены организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила функционирования системы безопасности значимых объектов, а также порядок и правила обеспечения безопасности значимых объектов КИИ.

Организационно-распорядительные документы по безопасности значимых объектов являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) субъекта КИИ. При этом положения, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, могут быть включены в общие документы по вопросам обеспечения информационной безопасности (защиты информации), а также могут являться частью документов по вопросам функционирования значимого объекта КИИ.

Организационно-распорядительные документы по безопасности значимых объектов должны определять:

1. цели и задачи обеспечения безопасности значимых объектов КИИ;
2. основные угрозы безопасности информации и категории нарушителей;
3. основные организационные и технические мероприятия по обеспечению безопасности значимых объектов КИИ, проводимые субъектом КИИ;
4. состав и структуру системы безопасности и функции ее участников;
5. порядок применения, формы оценки соответствия значимых объектов КИИ и средств защиты информации требованиям по безопасности;

6. планы мероприятий по обеспечению безопасности значимых объектов КИИ;
7. модели угроз безопасности информации в отношении значимых объектов КИИ;
8. порядок реализации отдельных мер по обеспечению безопасности значимых объектов КИИ;
9. порядок проведения испытаний или приемки средств защиты информации;
10. порядок реагирования на компьютерные инциденты;
11. порядок информирования и обучения работников;
12. порядок взаимодействия подразделений (работников) субъекта КИИ при решении задач обеспечения безопасности значимых объектов КИИ;
13. порядок взаимодействия субъекта КИИ с ГосСОПКА(ой);
14. правила безопасной работы работников субъекта КИИ на значимых объектах КИИ;
15. действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций.

В соответствии с п. 12.2 П-239 организационно-распорядительные документы по безопасности значимого объекта должны в том числе устанавливать правила безопасной работы работников, эксплуатирующих значимые объекты, и работников, обеспечивающих функционирование значимых объектов, а также действия работников при возникновении нештатных ситуаций, в том числе вызванных компьютерными инцидентами.

Организационно-распорядительные документы по безопасности значимых объектов должны быть доведены до руководства субъекта КИИ, подразделения по безопасности, специалистов по безопасности, а также до иных подразделений (работников), участвующих в обеспечении безопасности значимых объектов КИИ, в части, их касающейся.

Технические меры защиты значимых объектов КИИ

В соответствии с п.5 П-235 системы безопасности значимых объектов КИИ должны функционировать в соответствии с организационно-распорядительными документами по обеспечению безопасности значимых объектов КИИ, разрабатываемыми субъектами КИИ в соответствии с требованиями П-235.

В соответствии с п.21 П-235 применяемые СЗИ должны быть обеспечены гарантийной, технической поддержкой со стороны разработчиков (производителей).

Порядок применения СЗИ определяется субъектом КИИ в организационно-распорядительных документах по безопасности значимых объектов с учетом особенностей деятельности субъекта КИИ.

В соответствии с п. 28 П-235 для обеспечения безопасности значимых объектов КИИ должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

В случае использования в значимом объекте сертифицированных на соответствие требованиям по безопасности информации СЗИ:

1. в значимых объектах 1 категории применяются СЗИ не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса;
2. в значимых объектах 2 категории применяются СЗИ не ниже 5 класса защиты, а также средства вычислительной техники не ниже 5 класса;
3. в значимых объектах 3 категории применяются СЗИ 6 класса защиты, а также средства вычислительной техники не ниже 5 класса.

При этом в значимых объектах 1 и 2 категорий значимости применяются сертифицированные СЗИ, прошедшие проверку не ниже чем по 4 уровню контроля отсутствия недеklarированных возможностей. Функции безопасности СЗИ должны обеспечивать выполнение требований П-239.

Часть 4. Меры защиты значимых объектов КИИ и иные аспекты обеспечения безопасности значимых объектов КИИ

Процессы управления безопасностью значимых объектов КИИ

В соответствии с п.28 235-П в рамках функционирования системы безопасности субъектом КИИ должны быть внедрены следующие процессы:

1. планирование и разработка мероприятий по обеспечению безопасности значимых объектов КИИ;
2. реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов КИИ;
3. контроль состояния безопасности значимых объектов КИИ;
4. совершенствование безопасности значимых объектов КИИ.

Требования к вышеупомянутым процессам определены в разделе 5 П-235.

Внедрение организационных и технических мер защиты значимых объектов КИИ

Внедрение организационных и технических мер по обеспечению безопасности значимого объекта организуется субъектом критической информационной инфраструктуры в соответствии с проектной и рабочей (эксплуатационной) документацией на значимый объект, стандартами организаций и включает:

1. установку и настройку средств защиты информации, настройку программных и программно-аппаратных средств;
2. разработку организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности значимого объекта;
3. внедрение организационных мер по обеспечению безопасности значимого объекта;
4. предварительные испытания значимого объекта и его подсистемы безопасности;
5. опытную эксплуатацию значимого объекта и его подсистемы безопасности;
6. анализ уязвимостей значимого объекта и принятие мер по их устранению;
7. приемочные испытания значимого объекта и его подсистемы безопасности.

При внедрении организационных мер по обеспечению безопасности значимого объекта осуществляются:

1. организация контроля физического доступа к программно-аппаратным средствам значимого объекта и его линиям связи;
2. реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств;
3. проверка полноты и детальности описания в организационно-распорядительных документах по безопасности значимых объектов действий пользователей и администраторов значимого объекта по реализации организационных мер;
4. определение администратора безопасности значимого объекта;
5. отработка действий пользователей и администраторов значимого объекта по реализации мер по обеспечению безопасности значимого объекта.

В соответствии с п.16.7 П-239 Анализ уязвимостей значимого объекта проводится в целях выявления недостатков (слабостей) в подсистеме безопасности значимого объекта и оценки возможности их использования для реализации угроз безопасности информации. При этом анализу подлежат уязвимости кода, конфигурации и архитектуры значимого объекта.

Анализ уязвимостей проводится для всех программных и программно-аппаратных средств, в том числе средств защиты информации, значимого объекта. При проведении анализа уязвимостей применяются следующие способы их выявления:

1. анализ проектной, рабочей (эксплуатационной) документации и организационно-распорядительных документов по безопасности значимого объекта;
2. анализ настроек программных и программно-аппаратных средств, в том числе средств защиты информации, значимого объекта;
3. выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, посредством анализа состава установленного программного обеспечения и обновлений безопасности с применением средств контроля (анализа) защищенности и (или) иных средств защиты информации;
4. выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, сетевых служб, доступных для сетевого взаимодействия, с применением средств контроля (анализа) защищенности;
5. тестирование на проникновение в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации.

Допускается проведение анализа уязвимостей на макете (в тестовой зоне) значимого объекта или макетах отдельных сегментов значимого объекта.

В случае выявления уязвимостей значимого объекта, которые могут быть использованы для реализации (способствовать возникновению) угроз безопасности информации, принимаются меры, направленные на их устранение или исключающие возможность использования (эксплуатации) нарушителем выявленных уязвимостей.

По результатам анализа уязвимостей должно быть подтверждено, что в значимом объекте, отсутствуют уязвимости, как минимум содержащиеся в банке данных угроз безопасности информации ФСТЭК России или выявленные уязвимости не приводят к возникновению угроз безопасности информации в отношении значимого объекта.

В ходе приемочных испытаний значимого объекта и его подсистемы безопасности должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие значимого объекта и его подсистемы безопасности требованиям П-239, а также требованиям ТЗ на создание значимого объекта и (или) ТЗ (частного технического задания) на создание подсистемы безопасности значимого объекта.

Ввод в действие значимого объекта и его подсистемы безопасности осуществляется при положительном заключении (выводе) в акте приемки (или в аттестате соответствия) о соответствии значимого объекта установленным требованиям по обеспечению безопасности.

Силы обеспечения безопасности значимых объектов КИИ

В соответствии с п.8 П-235 руководитель субъекта КИИ или уполномоченное им лицо, на которое возложены функции обеспечения безопасности значимых объектов КИИ (далее - уполномоченное лицо), создает систему безопасности, организует и контролирует

ее функционирование.

Руководитель субъекта КИИ определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов КИИ в зависимости от количества значимых объектов КИИ, а также особенностей деятельности субъекта КИИ.

В соответствии с п.10 П-235 руководитель субъекта КИИ создает или определяет структурное подразделение, ответственное за обеспечение безопасности значимых объектов КИИ (далее - структурное подразделение по безопасности), или назначает отдельных работников, ответственных за обеспечение безопасности значимых объектов КИИ (далее - специалисты по безопасности).

Структурное подразделение по безопасности, специалисты по безопасности должны осуществлять следующие функции:

1. разрабатывать предложения по совершенствованию организационно-распорядительных документов по безопасности значимых объектов и представлять их руководителю субъекта КИИ (уполномоченному лицу);
2. проводить анализ угроз безопасности информации в отношении значимых объектов КИИ и выявлять уязвимости в них;
3. обеспечивать реализацию требований по обеспечению безопасности значимых объектов КИИ, установленных в соответствии со ст. 11 187-ФЗ (далее - требования по безопасности);
4. обеспечивать в соответствии с требованиями по безопасности реализацию организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации;
5. осуществлять реагирование на компьютерные инциденты в порядке, установленном в соответствии с п. 6 ч. 4 ст. 6 187-ФЗ;
6. организовывать проведение оценки соответствия значимых объектов КИИ требованиям по безопасности;
7. готовить предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов КИИ.

Структурное подразделение по безопасности, специалисты по безопасности реализуют вышеуказанные функции во взаимодействии с подразделениями (работниками), эксплуатирующими значимые объекты КИИ, и подразделениями (работниками), обеспечивающими функционирование значимых объектов КИИ.

Для выполнения вышеупомянутых функций, субъектами КИИ могут привлекаться организации, имеющие в зависимости от информации, обрабатываемой значимым объектом КИИ, лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации (далее - лицензии в области защиты информации).

Работники структурного подразделения по безопасности, специалисты по безопасности должны обладать знаниями и навыками, необходимыми для обеспечения безопасности значимых объектов КИИ в соответствии с требованиями П-235.

В соответствии с п. 13 П-235: не допускается возложение на структурное подразделение по безопасности, специалистов по безопасности функций, не связанных с обеспечением безопасности значимых объектов КИИ или обеспечением информационной безопасности субъекта КИИ в целом.

Обязанности, возлагаемые на работников структурного подразделения по безопасности, специалистов по безопасности, должны быть определены в их должностных регламентах (инструкциях).

Работники, эксплуатирующие значимые объекты КИИ (пользователи), а также работники, обеспечивающие функционирование значимых объектов КИИ, должны выполнять свои обязанности на значимых объектах КИИ в соответствии с правилами безопасности, установленными организационно-распорядительными документами по безопасности значимых объектов (инструкциями, руководствами). До работников должны быть доведены положения организационно-распорядительных документов по безопасности значимых объектов в части, их касающейся.

В соответствии с п. 15 П-235 субъект КИИ должен проводить не реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности КИИ и о возможных угрозах безопасности информации.

Представители организаций, привлекаемых субъектом КИИ для эксплуатации, обеспечения функционирования значимых объектов КИИ и (или) для обеспечения их безопасности, должны быть ознакомлены с организационно-распорядительными документами по безопасности значимых объектов.

Обеспечение безопасности значимых объектов КИИ в ходе их эксплуатации

В соответствии с п.13 П-239 обеспечение безопасности в ходе эксплуатации значимого объекта осуществляется субъектом КИИ в соответствии с эксплуатационной документацией и организационно-распорядительными документами по безопасности значимого объекта и должно включать реализацию следующих мероприятий:

1. планирование мероприятий по обеспечению безопасности значимого объекта;
2. анализ угроз безопасности информации в значимом объекте и последствий от их реализации;
3. управление (администрирование) подсистемой безопасности значимого объекта;
4. управление конфигурацией значимого объекта и его подсистемой безопасности;
5. реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта;
6. обеспечение действий в нештатных ситуациях в ходе эксплуатации значимого объекта;

7. информирование и обучение персонала значимого объекта;
8. контроль за обеспечением безопасности значимого объекта.

Обеспечение безопасности значимых объектов КИИ при выводе их из эксплуатации

В соответствии с п.14 П-239 обеспечение безопасности значимого объекта при выводе его из эксплуатации или после принятия решения об окончании обработки информации осуществляется субъектом критической информационной инфраструктуры в соответствии с эксплуатационной документацией на значимый объект и организационно-распорядительными документами по безопасности значимого объекта. Обеспечение безопасности значимого объекта при выводе его из эксплуатации должно предусматривать:

1. архивирование информации, содержащейся в значимом объекте;
2. уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации;
3. уничтожение данных об архитектуре и конфигурации значимого объекта;
4. архивирование или уничтожение эксплуатационной документации на значимый объект и его подсистему безопасности и организационно-распорядительных документов по безопасности значимого объекта.

Государственный контроль в области обеспечения безопасности значимых объектов КИИ

В соответствии с ч.1 ст.13 187-ФЗ Государственный контроль в области обеспечения безопасности значимых объектов КИИ проводится в целях проверки соблюдения субъектами КИИ, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, требований, установленных 187-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Указанный государственный контроль проводится путем осуществления ФСТЭК России плановых или внеплановых проверок.

Основанием для осуществления плановой проверки является истечение трех лет со дня:

1. внесения сведений об объекте КИИ в реестр значимых объектов КИИ;
2. окончания осуществления последней плановой проверки в отношении значимого объекта КИИ.

Основанием для осуществления внеплановой проверки является:

1. истечение срока выполнения субъектом КИИ выданного ФСТЭК России предписания об устранении выявленного нарушения требований по обеспечению безопасности значимых объектов КИИ;
2. возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте КИИ;
3. приказ (распоряжение) руководителя ФСТЭК России, изданный в соответствии с поручением Президента РФ или Правительства РФ либо на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

По итогам плановой или внеплановой проверки ФСТЭК России составляется акт проверки по утвержденной указанным органом форме.

На основании акта проверки в случае выявления нарушения требований 187-ФЗ и принятых в соответствии с ним нормативных правовых актов по обеспечению безопасности значимых объектов КИИ ФСТЭК России выдает субъекту КИИ предписание об устранении выявленного нарушения с указанием сроков его устранения.

Ответственность за неправомерное воздействие на КИИ

Законодательство РФ предусматривает уголовную ответственность за неправомерное воздействие на КИИ РФ.

Часть 3 ст.274.1 УК РФ – нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ РФ, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда КИИ РФ. Наказывается принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового либо лишением свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.

Часть 4 ст.274.1 УК РФ предусматривает ужесточение наказания в случае, если деяния, предусмотренные ч.3 ст.274.1 УК РФ, совершены группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения. Наказываются лишением свободы на срок от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.

Часть 5 ст.274.1 УК РФ предусматривает ужесточение наказания в случае, если деяния, предусмотренные ч.3 ст.274.1 УК РФ, повлекли тяжкие последствия. Наказываются лишением свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового.

[безопасность критической информационной инфраструктуры, аналитика](#)

¹⁾ Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 25.12.2017 № 239).

²⁾ Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

³⁾ Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 21.12.2017 № 235).

⁴⁾ Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (утв. приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 22 декабря 2017 г. № 236).

From:

<https://sps-ib.ru:80/> - Справочно-правовая система по информационной безопасности

Permanent link:

https://sps-ib.ru:80/analitika:obzor_zakonodatelstva_o_kii



Last update: **2019/03/04 21:04**