kaspersky

187-ФЗ и мирЪ. Значимые изменения с 2019-го года с пояснениями и пополнениями

Дмитрий Сатанин

07.06.2022 Version 1.0

В статье рассмотрены изменения и дополнения, внесённые в нормативную базу по защите критической информационной инфраструктуры Российской Федерации (далее — КИИ) с 2019-го года, новые нормативные документы, а также соответствующие планы на ближайшую перспективу. Актуальность этого материала обусловлена не только текущими непростыми событиями, но ещё и тем фактом, что в прошлом, 2021-м, году был запущен процесс государственного инспекторского контроля ФСТЭК России состояния безопасности КИИ. В связи с этим вопросам понимания и корректного выполнения положений указанной нормативной базы, а также знанию перспектив её развития следует уделять особое внимание.

Новый майский указ

Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (далее — Указ) в настоящее время является наиболее актуальным и обсуждаемым нормативным документом, который, несомненно, повлияет на состояние дел в области защиты информации.

Первое, что необходимо отметить, это перечень организаций и мероприятий, которых указ касается напрямую (см. п. 1), а именно:

- все госорганы;
- все госкомпании;
- все госкорпорации;
- все стратегические предприятия, стратегические акционерные общества и системообразующие организации (соответствующие списки есть у каждого министерства);
- все субъекты КИИ.

Другими словами, действие Указа распространяется на весь госсектор и весь крупный бизнес (далее — организации или предприятия).

Второй очень важный момент — введение персональной ответственности за обеспечение информационной безопасности на руководителя организации или предприятия, подпавшего под действие Указа (см. пункт 2). Он, в свою очередь, должен назначить одного из своих заместителей ответственным за данное направление, в частности, возложить на него полномочия по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты (см. подпункт «а» пункта 1). Также должно быть создано структурное подразделение, обеспечивающее информационную безопасность организации или предприятия с соответствующим функционалом (см. подпункт «б» пункта 1).

Дополнительно Указ устанавливает, что теперь внешние организации, привлекаемые к работам по обеспечению информационной безопасности, в обязательном порядке должны иметь лицензии на осуществление деятельности по технической защите конфиденциальной информации (см. подпункт «в» пункта 1). А для проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты могут привлекаться исключительно организации, являющиеся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации — ГосСОПКА (см. подпункт «г» пункта 1). Данное положение

указа заработает в полную силу по истечении переходного периода, длительность которого не указана (скорее всего, в пределах 6-12 месяцев).

В соответствии с п. 3 Указа Правительство Российской Федерации в июне 2022 года должно утвердить типовые положения о заместителе руководителя и структурном подразделении, ответственных за обеспечение информационной безопасности.

ФСБ России получает право доступа и мониторинга информационных систем организации или предприятия, подключённых к сети «Интернет» (см. подпункт «д» пункта 1). Ранее данный функционал ФСБ России выполняла по взаимной договорённости. Дополнительно организации и предприятия обязаны незамедлительно реализовывать организационные и технически меры, необходимость которых установлена ФСБ и ФСТЭК России. Скорее всего, такие меры будут доводиться циркулярными письмами.

Также ФСБ России должна (см. п. 5 Указа):

- организовать аккредитацию центров ГосСОПКА;
- определить переходный период, в течение которого допускается осуществлять мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в интересах организаций и предприятий на основании заключенных с ФСБ России и Национальным координационным центром по компьютерным инцидентам (НКЦКИ) соглашений;
- определить порядок осуществления мониторинга защищенности информационных ресурсов организаций и предприятий.

Ну и п. 6 Указа с 01.01.2025 г. вводит запрет организациям и предприятиям использовать средства защиты информации, произведённые в недружественных по отношению к Российской Федерации странах.

Отметим, что с учётом необходимости многочисленных согласований, скорее всего, проект Указа появился ещё в прошлом году, что позволяет предположить, что ход работ по созданию системы ГосСОПКА шёл недостаточно активно, и рассмотренный Указ должен стать важным стимулом для их ускорения.

В части нормотворчества дополнительно к сказанному выше в течение ближайших примерно полугода — года можно ожидать появления:

- документа, регламентирующего доступ к информационным системам организации или предприятия, подключённым к сети «Интернет», и их мониторинг ФСБ России;

- описания процедуры аккредитации центров ГосСОПКА — в частности, методические рекомендации по созданию таких центров, скорее всего, будут доработаны и получат статус требований;
- документа, определяющего порядок осуществления мониторинга защищенности информационных ресурсов организаций и предприятий.

Разработка всех перечисленных документов находится в зоне ответственности ФСБ России (или НКЦКИ).

Изменения в нормативной базе по обеспечению безопасности КИИ

Начиная с 2019-го года, были скорректированы все основные нормативные документы ФСТЭК России по защите КИИ, а именно:

- Постановление Правительства Российской Федерации № 127 от 08 февраля 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»: **новая редакция** — Постановление Правительства № 452 от 13 апреля 2019 г. «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127» (далее — Правила категорирования);
- Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»: **новая редакция** — Приказ ФСТЭК России от 27 марта 2019 г. № 64 . «Об утверждении Требований к созданию…» (далее — Требования по созданию СБ);
- Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «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»: **новая редакция** — Приказ ФСТЭК России от 21 марта 2019 г. № 59 «О внесении изменений в форму…» (далее — Форма сведений о категорировании);
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 . «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»: **новая редакция** — Приказ ФСТЭК России от 26 марта

2019 г. № 60 «О внесении изменений в Требования по обеспечению…»; и **самая новая редакция** — Приказ ФСТЭК России от 20 февраля 2020 г. № 35 "О внесении изменений в Требования по обеспечению…» (далее — Требования по безопасности).

Также был введён в действие новый нормативный документ — Приказ ФСТЭК России от 28 мая 2020 г. № 75 «Об утверждении Порядка согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования» (далее — Порядок подключения к ССОП).

Правила категорирования

В новой редакции Правил категорирования, введённой в действие Постановлением Правительства № 452 от 13 апреля 2019 г., уточняется процедура проведения категорирования (периодичность, формирование, состав, процесс работы комиссии, сроки и т.д.) и скорректированы показатели критериев значимости.

Ключевые дополнения изложены в пунктах 14.1-14.3, а именно:

- при оценке нарушителя и анализе угроз безопасности информации должны быть рассмотрены наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты КИИ, результатом которых являются прекращение или нарушение выполнения критических процессов и нанесение максимально возможного ущерба;
- теперь необходимо учитывать следующие факторы:
    1. в случае зависимости функционирования объекта КИИ-1 от объекта КИИ-2 оценка масштаба возможных последствий для объекта КИИ-1 проводится исходя из предположения о прекращении или нарушении функционирования вследствие компьютерной атаки объекта КИИ-2;
    2. если критический процесс зависит от иных критических процессов, то оценка проводится исходя из совокупного масштаба возможных последствий от нарушения или прекращения функционирования всех выполняемых критических процессов.

Также был уточнен порядок создания/расформирования и кадрового состава комиссий по категорированию (см. пункты 11.1-11.3). В частности, в

состав комиссии могут быть включены работники фактически любого подразделения субъекта КИИ (в частности, финансово-экономического блока), а также при наличии у предприятия-субъекта КИИ филиалов и/или представительств в них могут создаваться собственные комиссии по категорированию.

Что касается показателей критериев значимости, то были снижены практически все нижние количественные значения для значимых объектов КИИ III-й категории значимости:

- с 50 до 2 человек (в случае услуг связи — до 3) — для показателей критериев, касающихся жизнеобеспечения людей;
- с 3-5% до 0-1% — для показателей экономических критериев значимости.

Такое изменение приведёт к существенному росту числа субъектов КИИ, у которых теперь могут оказаться значимые объекты III-й категории значимости.

Отметим, что самые свежие изменения в Правилах категорирования могут появиться уже в 2022-м году. В марте проводилось публичное обсуждение проекта постановления Правительства Российской Федерации «О внесении изменения в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации», инициированного ФСТЭК России. В пояснительной записке к проекту постановления отмечается, что ФСТЭК России планирует нормативно закрепить возможность привлечения сторонних организаций для проверки «актуальности и достоверности сведений об объектах критической информационной инфраструктуры». Такие проверки предполагается проводить в рамках отраслевого мониторинга, предусмотренного пунктом 19.2 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127. Для проведения проверок отраслевые ведомства (отраслевые регуляторы) получают право привлекать по согласованию с ФСТЭК России специализированные подведомственные организации, имеющие компетенции в соответствующих сферах (областях), а также в области безопасности критической информационной инфраструктуры.

Требования по созданию СБ

В данные требования внесены следующие ключевые изменения:

- уточнён порядок создания систем безопасности в филиалах (представительствах) и подчиненных организациях интегрированных структур: они должны создаваться для защиты всех значимых объектов КИИ во всех обособленных подразделениях (филиалах, представительствах) субъекта КИИ, включая формирование сил обеспечения безопасности значимых объектов КИИ (далее — Силы ОБ ЗОКИИ);
- установлены требования к образованию специалистов в составе сил обеспечения безопасности значимых объектов КИИ:
    1. наличие у руководителя Сил ОБ ЗОКИИ высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по направлению «Информационная безопасность» (со сроком обучения не менее 360 часов), наличие стажа работы в сфере информационной безопасности не менее 3 лет;
    2. наличие у штатных работников Сил ОБ ЗОКИИ высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе повышения квалификации по направлению «Информационная безопасность» (со сроком обучения не менее 72 часов);
    3. прохождение не реже одного раза в 5 лет обучения по программам повышения квалификации по направлению «Информационная безопасность».

Форма сведений о категорировании

Приказ ФСТЭК России от 21 марта 2019 г. № 59 уточняет и детализирует требования по описанию объектов КИИ, которые необходимо указывать в Форме сведений о категорировании, а именно:

- наименования используемых на соответствующем объекте КИИ программно-аппаратных средств (пользовательских компьютеров,

серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество;
- применяемые средства защиты информации (СЗИ), в том числе встроенные в общесистемное и прикладное программное обеспечение (наименования, наличие и реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия СЗИ или сведения о «непроведении» (это прямая цитата из текста документа, см. пункт 5, точнее, новую формулировку п. 5.4) такой оценки, или сведения об их отсутствии.

Также в новой Форме сведений о категорировании необходимо приводить обоснование выбора показателя того или иного критерия значимости, их применимости или неприменимости и т.д.

Требования по безопасности ЗО КИИ

В указанный нормативный документ с момента его принятия изменения вносились уже дважды, в 2019-м и 2020-м годах

Изменения 2019-го года во многом обусловлены принятием нормативного документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденных приказом ФСТЭК России от 30 июля 2018 г. № 131 (далее — Требования доверия), которые стали одним из базовых в системе нормативных документов ФСТЭК России. В соответствии с указанными изменениями в составе значимых объектов КИИ становится обязательным использование СЗИ, сертифицированных ФСТЭК России на соответствие Требованиям доверия (введено в действие с 01.01.2020 г.):

- для I категории значимости — не ниже 4-го уровня доверия;
- для II категории — не ниже 5-го уровня доверия;
- для III категории — не ниже 6-го уровней доверия.

Дополнительно к этому для значимых объектов КИИ I категории:

- граничный маршрутизатор доступа в сеть Интернет должен соответствовать требованиям по безопасности информации и быть сертифицирован по Требованиям доверия по 4-му уровню и выше (фактически, такой маршрутизатор объявляется средством защиты информации);
- хранение и обработка информации должны осуществляться на территории страны (блокируется возможность использования

зарубежных «облачных инфраструктур», хостинг- и Интернет-провайдеров).

Кроме того, были значительно усилены меры по обеспечению безопасности для значимых объектов КИИ, в частности, для III категории введено более двадцати дополнительных мер защиты (если быть точным, то 21 такая мера).

В изменениях и дополнениях 2020-го года к Требованиям по безопасности ЗО КИИ определён ключевой признак модернизации значимых объектов (что автоматически влечёт за собой повторное категорирование). Это — изменение архитектуры, в том числе подсистемы его безопасности, закреплённое в отдельном техническом задании (частном техническом задании).

Также в указанных изменениях и дополнениях:

- уточнена процедура оценки СЗИ по форме испытаний или приемки, они также должны соответствовать Требованиям доверия по 6-му или более высокому уровню, что должно быть установлено в ходе указанных испытании или приёмки;
- закреплена необходимость разработки и реализации компенсирующих мер при внедрении новых информационных технологий и выявлении дополнительных угроз в отношении значимого объекта КИИ;
- детализирована процедура удалённого доступа (в частности, разрешён для сотрудников дочерних и зависимых организаций);
- вводятся требования к «новому» прикладному ПО, реализующему функции назначения значимого объекта КИИ и внедряемому в ходе модернизации (с 1 января 2023 года), а именно:

    1. необходимость выполнения процедуры безопасной разработки (наличие руководства по ней, анализ угроз, для значимых объектов КИИ I категории — описание структуры ПО на уровне подсистем с сопоставлением функций и интерфейсов данного ПО с его подсистемами);
    2. проведение испытаний по выявлению уязвимостей (статический анализ исходного кода, фаззинг-тестирование, для значимых объектов КИИ I категории — динамический анализ);
    3. поддержка безопасности ПО (поиск и исправление ошибок/уязвимостей, информирование пользователей, для значимых объектов КИИ I категории — информирование об окончании производства/поддержки ПО).

Порядок подключения к ССОП

Данный нормативный документ устанавливает процедуру согласования субъектом КИИ со ФСТЭК России подключения значимого объекта КИИ к сети связи общего пользования (читай, сети Интернет, далее — ССОП).

Важно: если значимый объект КИИ на момент его включения в реестр значимых объектов уже имел подключение к ССОП, согласование со ФСТЭК России в соответствии с рассматриваемым Порядком не требуется. Такое согласование необходимо для значимого объекта **до ввода его в действие** на этапе, определяемом субъектом критической информационной инфраструктуры и **до заключения договора с оператором связи** для действующего значимого объекта. Данный договор должен определять обязанности сторон, в частности, оператора связи по обеспечению функционирования оборудования связи, которое обеспечивает взаимодействие со значимым объектом КИИ (см. п. 6 Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры, утвержденных постановлением Правительства Российской Федерации от 8 июня 2019 г. № 743).

Следует иметь в виду, что ФСТЭК России может отказать в подключении значимого объекта КИИ к ССОП. Основания для такого отказа являются:

- представление неполных сведений и документов;
- несоответствие имеющихся СЗИ заявленным;
- несоответствие имеющихся СЗИ требованиям по защите ЗОКИИ.

Заключение

Описанные выше изменения, внесённые в нормативную базу по защите КИИ за прошедшие три года, позволяют с достаточной долей уверенности утверждать, что по мере накопления практического опыта ФСТЭК России выявляет лакуны и узкие места в нормативных документах в зоне своей ответственности и постепенно устраняет их. Также данные изменения указывают на явную тенденцию, направленную на повышение уровня безопасности КИИ, ужесточение требований к используемому для этого программно-аппаратному обеспечению и к обслуживающему персоналу. А планируемое привлечение к процедуре категорирования специализированных организаций, подведомственных отраслевым регуляторам, в перспективе позволит существенно повысить её объективность и помешать попыткам занижения категорий значимости объектов КИИ или вовсе не присвоения (ошибочного или намеренного) категорий значимости.

В целом, указанная тенденция будет главенствующей в среднесрочной перспективе, что также подтверждается предложением о создании государственной системы защиты информации, которое президент России Путин В.В. озвучил на заседании Совета Безопасности 20 мая 2022 года. Поэтому в течение года следует ожидать соответствующего указа по аналогии с указом от 15.01.2013 г. № 31с о системе ГосСОПКА, где будут прописаны основные задачи, которые будет решать государственная система защиты информации, а также госорганы, ответственные за её создание, и их соответствующие полномочия (скорее всего, основными акторами данного процесса будут ФСБ, ФСТЭК и Минцифры России).

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com