Kaspersky ICS CERT

kaspersky

Обеспечение безопасности КИИ

Что год текущий нам готовит...

Дмитрий Сатанин

03.02.2021 Version 1.0

Оглавление

В наступившем 2021-м году стартуют несколько важных новаций в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации. Причём речь идёт не только об изменениях и дополнениях в нормативных документах, регламентирующих соответствующую деятельность, но и про, так сказать, вполне реальную жизнь.

Перечень новаций 2021 выглядит следующим образом:

- субъекты КИИ должны создать силы обеспечения безопасности значимых объектов КИИ (далее — ЗО КИИ);
- вносятся изменения в Кодекс Российской Федерации об административных правонарушениях (КоАП) за нарушения в области обеспечения безопасности КИИ;
- начинает работать государственный (инспекторский) контроль обеспечения безопасности КИИ со стороны ФСТЭК России.

О силах обеспечения безопасности значимых объектов КИИ

Создание сил обеспечения безопасности ЗО КИИ и требования к ним прописаны в Приказе 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» (далее — **Требования**) и уточнены в Приказе ФСТЭК России от 27 марта 2019 г. № 64 о внесении изменений в Требования.

Состав сил безопасности КИИ

Согласно Требованиям, **к силам обеспечения безопасности ЗО КИИ относятся**:

- подразделения (работники) субъекта КИИ, ответственные за обеспечение безопасности ЗО КИИ;
- подразделения (работники), эксплуатирующие и обеспечивающие функционирование (сопровождение, обслуживание, ремонт) ЗО КИИ;
- иные подразделения (работники), участвующие в обеспечении безопасности ЗО КИИ.

Ответственным за организацию и работу сил обеспечения безопасности ЗО КИИ является руководитель субъекта КИИ (или лицо, им уполномоченное). Он определяет состав, структуру и функциональные обязанности таких сил, в частности, создаёт или определяет структурное подразделение, ответственное за обеспечение безопасности ЗО КИИ или назначает отдельных работников для решения соответствующих задач.

Задачи подразделения

Структурное подразделение по безопасности, специалисты по безопасности должны:

- обеспечивать безопасность ЗО КИИ в соответствии с предъявленными к данному объекту требованиями[1]: реализовывать соответствующие организационные меры, применять средства защиты информации;
- анализировать угрозы безопасности информации и выявлять уязвимости в ЗО КИИ;

[1] См. Приказы ФСТЭК России 239-2017/60-2019/35-2020 об утверждении и внесении изменений в Требования по обеспечению безопасности КИИ.

- осуществлять реагирование на компьютерные инциденты в ЗО КИИ;
- организовывать проведение оценки соответствия ЗО КИИ требованиям по безопасности;
- готовить предложения по повышению уровня безопасности ЗО КИИ, совершенствованию функционирования соответствующих систем безопасности и организационно-распорядительных документов.

Для выполнения перечисленных функций субъектами КИИ могут привлекаться организации-лицензиаты ФСТЭК России.

Возложение на силы обеспечения безопасности ЗО КИИ функций и задач, не связанных с их непосредственной деятельностью, не допускается.

При необходимости по решению руководителя субъекта КИИ (уполномоченного лица) силы обеспечения безопасности ЗО КИИ могут быть созданы в обособленных подразделениях (филиалах, представительствах, дочерних организациях) субъекта КИИ, в которых эксплуатируются соответствующие объекты.

Требования к работникам

Работники сил обеспечения безопасности ЗО КИИ должны соответствовать следующим требованиям:

- у руководителя: высшее профессиональное образование по специальности в области информационной безопасности или иное высшее профессиональное образование в совокупности с документом о профессиональной переподготовке по направлению «Информационная безопасность» (со сроком обучения не менее 360 часов), наличие стажа работы в сфере информационной безопасности не менее 3 лет;
- у штатных работников: высшее профессиональное образование по специальности в области информационной безопасности или иное высшее профессиональное образование в совокупности с документом о повышении квалификации по направлению «Информационная безопасность» (со сроком обучения не менее 72 часов);
- прохождение не реже одного раза в 5 лет обучения по программам повышения квалификации по направлению «Информационная безопасность».

Субъект КИИ не реже одного раза в год должен проводить организационные мероприятия по повышению уровня знаний работников по вопросам обеспечения безопасности КИИ и о возможных угрозах безопасности информации.

Внесение изменений в КоАП

Начнём с главного: данные изменения были одобрены Государственной Думой Российской Федерации 27.01.2021 г., второе чтение пока не назначено, поправки принимаются до 25.02.2021 г.

В КоАП добавлены новые статьи:

1. Статья 13.12.1: нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
2. Статья 19.7.15: непредоставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Статья 13.12.1

Статья 13.12.1 состоит из пяти пунктов:

1. Нарушение порядка категорирования объектов КИИ (за исключением случаев, предусмотренных частью 1 статьи 19.7.15): административный штраф для должностных лиц — 10-50 тыс. руб.; для юридических лиц — 50-100 тыс. руб., уполномоченное ведомство — ФСТЭК России.
2. Нарушение требований к созданию и обеспечению функционирования систем безопасности ЗО КИИ (если нет признаков уголовно наказуемого деяния): административный штраф для должностных лиц — 10-40 тыс. руб.; для юридических лиц — 50-100 тыс. руб., уполномоченное ведомство — ФСТЭК России.
3. Нарушение требований по обеспечению безопасности ЗО КИИ (если нет признаков уголовно наказуемого деяния): административный штраф для должностных лиц — 10-50 тыс. руб.; для юридических лиц — 50-100 тыс. руб., уполномоченное ведомство — ФСТЭК России.
4. Нарушение порядка информирования и реагирования на компьютерные инциденты, принятия мер по ликвидации последствий компьютерных атак на ЗО КИИ: административный штраф для должностных лиц — 10-50 тыс. руб.; для юридических лиц — 150-200 тыс. руб., уполномоченное ведомство — ФСБ России.

5. Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ (в том числе — с иностранными и международными организациями): административный штраф для должностных лиц — 20-50 тыс. руб.; для юридических лиц — 150-200 тыс. руб., уполномоченное ведомство — ФСБ России.

Статья 19.7.15

Статья 19.7.15 состоит из двух пунктов:

1. Непредоставление или нарушение сроков представления во ФСТЭК России сведений о результатах категорирования: административный штраф для должностных лиц - 10-50 тыс. руб.; для юридических лиц — 50-100 тыс. руб., уполномоченное ведомство — ФСТЭК России;
2. непредставление или нарушение порядка либо сроков представления в систему ГосСОПКА: административный штраф для должностных лиц - 10-50 тыс. руб.; для юридических лиц — 100-500 тыс. руб., уполномоченное ведомство — ФСБ России.

Предлагаемые размеры штрафов позволяют сделать вывод, что утаивание информации об инцидентах и попытки сделать вид, что «ничего не было!» регуляторы считают более тяжкими административными правонарушениями, чем ошибки при реализации требований нормативных документов по обеспечению безопасности КИИ.

Предполагаемый срок введения в действие нового КоАП — конец I-го — начало II-го полугодия 2021 года.

Государственный контроль обеспечения безопасности КИИ

Нормативный документ, регламентирующий соответствующую деятельность, — Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее — **Правила государственного контроля**).

Ключевые моменты Правил государственного контроля

Уполномоченным федеральным органом, осуществляющим государственный контроль обеспечения безопасности КИИ, является ФСТЭК России и её территориальные органы.

Цель государственного контроля — проверка соблюдения субъектами КИИ положений нормативных документов по обеспечению безопасности КИИ.

Государственный контроль осуществляется путем проведения плановых и внеплановых выездных проверок, осуществляемых комиссиями в составе не менее двух сотрудников ФСТЭК России в случае плановых проверок и одним сотрудником данной службы в случае внеплановой проверки.

Плановые проверки

ФСТЭК России формирует ежегодный план, который должен быть утверждён до 20 декабря года, предшествующего году проведения плановых проверок. Основаниями для осуществления плановой проверки являются истечение 3 лет со дня:

- внесения сведений об объекте КИИ в реестр ЗО КИИ;
- окончания осуществления последней плановой проверки в отношении ЗО КИИ.

Таким образом, в 2021-м году плановые проверки могут быть проведены на ЗО КИИ, информация о присвоении категории значимости которым была внесена в реестр ЗО КИИ в 2018-м году.

Субъект КИИ уведомляется о проведении плановой проверки не менее, чем за 3 рабочих дня до начала ее проведения, любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления.

Внеплановые проверки

Основаниями для осуществления внеплановой проверки являются:

- истечение срока выполнения субъектом КИИ предписания ФСТЭК России об устранении выявленного нарушения требований по обеспечению безопасности;
- возникновение компьютерного инцидента на ЗО КИИ, повлекшего негативные последствия;
- поручение Президента или Правительства Российской Федерации, требование прокурора.

Субъект КИИ уведомляется о проведении внеплановой проверки не менее, чем за 24 часа до начала ее проведения любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления. В случае если поводом для внеплановой проверки стал компьютерный инцидент на ЗО КИИ, ФСТЭК России вправе приступить к ней незамедлительно.

Оформление результатов проверки

По результатам проверки составляется соответствующий акт, на основании которого в случае выявления нарушения требований по обеспечению безопасности проверяемому субъекту КИИ выдаётся предписание об устранении выявленного нарушения с указанием срока его устранения. К акту проверки прилагаются протоколы или заключения по результатам контрольных мероприятий, проведенных с использованием программных и аппаратно-программных средств контроля, а также предписания об устранении выявленных нарушений и иные связанные с результатами проверки документы или их копии.

В случае проведения внеплановой проверки на основании требования прокурора копия акта проверки с копиями приложений высылается в соответствующий орган прокуратуры.

В случае грубых нарушений Правил государственного контроля результаты соответствующей проверки не могут являться доказательствами нарушения субъектом КИИ требований по обеспечению безопасности и подлежат отмене на основании заявления данного субъекта КИИ. К таким грубым нарушениям относятся:

- отсутствие оснований для проведения проверки;
- нарушение срока уведомления о проведении проверки;
- нарушение срока проведения проверки;
- проведение проверки без приказа ФСТЭК России;
- невручение руководителю субъекта КИИ или уполномоченному им должностному лицу акта проверки;
- проведение **плановой проверки**, не включенной в ежегодный **план** проведения **плановых проверок**.

Заключение

С учётом изложенного можно смело говорить о том, что деятельность ФСТЭК России по обеспечению безопасности КИИ перестаёт носить чисто бюрократический, «бумажный» характер (сопровождение нормативной базы, рассмотрение и согласование документов, подготовленных субъектами КИИ, ведение реестра ЗО КИИ и т.д.) и переходит в практическую плоскость, включая инструменты давления в виде нового КоАП. В связи с этим субъектам КИИ, у которых имеются ЗО КИИ, следует оценить, насколько точно и корректно ими выполняются положения соответствующей нормативной базы. Особенно это актуально для тех субъектов КИИ, которые провели категорирование в 2018-м году.

В заключение позволим себе небольшой анонс: мы готовим ещё один материал с анализом изменений и нововведений в нормативной базе ФСТЭК России по обеспечению безопасности КИИ, который будет опубликован в ближайшее время.

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