Форум
Актуальные вопросы информационной безопасности

Опыт проверок, выявляемые нарушения и рекомендации в области соблюдения законодательства о критической информационной инфраструктуре

Владивосток
16.06.2021

начальник управления правовой статистики, информационных технологий и защиты информации прокуратуры Приморского края Соколова Екатерина Александровна

Генеральная прокуратура → Органы прокуратуры субъектов Российской Федерации

- Исполнение обязанностей, предусмотренных ст. 9, 187-ФЗ;
- Категорирование объектов КИИ;
- Создание системы безопасности значимых объектов КИИ;
- Соблюдение требований по безопасности значимых объектов КИИ.

Пункт КоАП 13.12.1 и 19.7.15	Должностное	Юр. лицо
Нарушение требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов	10-50 тыс.	50-100 тыс.
Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ	10-50 тыс.	100-500 тыс.
Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации	20-50 тыс.	100-500 тыс.
Непредставление или нарушение сроков представления сведений о результатах присвоения объекту КИИ одной из категорий значимости	10-50 тыс.	50-100 тыс.
Непредставление или нарушение порядка либо сроков представления в ГосСОПКА информации, предусмотренной законодательством в области обеспечения безопасности КИИ РФ	10-50 тыс.	100-500 тыс.

Ч.8 ст. 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»:

Сфера деятельности:

- здравоохранение;
- наука;
- транспорт;
- связь;
- энергетика;
- банковская сфера и иные сферы финансового рынка;
- топливно-энергетический комплекс;
- атомная энергия;
- оборонная отрасль;
- ракетно-космическая отрасль;

также промышленность:

- горнодобывающая;
- металлургическая ;
- химическая.

Наличие:

На праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления

Вид организации:

государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели

Для потенциальных субъектов КИИ в целях оценки применимости законодательства в сфере КИИ к организации

9 статья 187-ФЗ, для любых субъектов КИИ:

1) незамедлительно информировать о компьютерных инцидентах НКЦКИ, а также Центральный банк Российской Федерации (для банковской сферы и в иных сферах финансового рынка) в установленном порядке;

2) оказывать содействие должностным лицам НКЦКИ в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

3) в случае установки на объектах критической информационной инфраструктуры 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.

Приказ Федеральной службы безопасности Российской Федерации от 19 июня 2019 года № 282

1. Приказ о назначение ответственного за реагирование на компьютерные инциденты.
2. Приказ о назначении ответственного за взаимодействие с НКЦКИ и содействие ФСБ (в этом же документе – порядок передачи сведений в НКЦКИ в соответствии с вариантами, предусмотренными 282 приказом ФСБ и информацией с официального портала).
3. Журнал учета компьютерных инцидентов.
4. Журнал регистрации обращений НКЦКИ.

При наличии ГосСОПКА:

+Приказ Федеральной службы безопасности Российской Федерации от 19 июня 2019 года № 281

Если компоненты ГосСОПКА развернуты в Вашей организации, то у Вас должны быть:

1. Письмо от ФСБ с согласованием установки средств ГосСОПКА
2. Исходящее письмо в НКЦКИ с уведомлением о начале эксплуатации в организации средств ГосСОПКА
3. Организационно-распорядительная документация по эксплуатации средств ГосСОПКА.

Либо

В случае привлечения ведомственного или корпоративного (коммерческого) центра ГосСОПКА, то вышеуказанная документация заменяется договором или соглашением с соответствующим центром мониторинга, реализующего функции центра ГосСОПКА.

9 статья 187-ФЗ, ч.3, для субъектов со значимыми объектами КИИ:

1) соблюдать требования по обеспечению безопасности значимых объектов КИИ, установленных приказом ФСТЭК № 239;
2) выполнять предписания должностных лиц ФСТЭК, 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 федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры;
4) обеспечивать беспрепятственный доступ должностным лицам ФСТЭК, к значимым объектам критической информационной инфраструктуры при реализации этими лицами полномочий, предусмотренных статьей 13 187-ФЗ.

Для подтверждения исполнения обязанностей:

1. Подтверждение исполнений требования по обеспечению безопасности значимых объектов КИИ, установленных ФСТЭК России в 239 приказе: акт или аттестат с положительным заключением о соответствии значимого объекта установленным требованиям по обеспечению безопасности.
2. При наличии предписания: вы прилагаете документы, подтверждающие ответ об устранении нарушения, либо ответ с приложением плана по устранению выявленного нарушения.
3. Реагирование на компьютерные инциденты (пункты 6-10 приказа ФСБ № 282):

- План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий
- План проведения учений по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак.

4. Обеспечение беспрепятственного доступа сотрудников ФСТЭК к Вашему объекту КИИ, не препятствуем

Контролю подлежит исполнение субъектом КИИ мероприятий по категорированию своих объектов, предусмотренных Постановлением Правительства Российской Федерации от 8 февраля 2018 года № 127 «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». Для подтверждения исполнения этих обязательств организация должна предъявить:

- Приказ о создании комиссии по категорированию объектов КИИ.
- Утвержденный перечень объектов КИИ.
- Акт категорирования Объектов КИИ.

Создание системы безопасности значимых объектов КИИ, подтверждается следующими документами, в соответствии с Приказом ФСТЭК № 235:

1. Приказ о назначении специалиста безопасности, либо создания структурного подразделения по безопасности.
2. Документы, подтверждающие квалификацию работников структурного подразделения по безопасности, специалистов по безопасности (п. 12).
3. Приказ об утверждении состава и структуры системы безопасности организации, а также функций ее участников при обеспечении безопасности ЗОКИИ. Либо, договор с лицензиатом ФСТЭК на выполнение функций структурного подразделения безопасности.
4. План мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры.
5. Соглашение с НКЦКИ/договор с ведомственным (корпоративным) центром ГосСОПКА. Этот вопрос уже затрагивали ранее.

Спасибо за внимание!