Код ИБ| ЕКАТЕРИНБУРГ 2025

Особенности обеспечения ИБ в ходе модернизации информационной инфраструктуры предприятия

Христолюбова Анна Анатольевна

Независимый эксперт по ИБ

09 октября 2025 г.

Ожидание

- Реализовать меры, предусмотренные Указом № 250
- Создать систему безопасности объекта КИИ и обеспечивать ее функционирование (№ 187-ФЗ, Статья 10, п. 1)
- Определить состав и структуру системы безопасности объектов КИИ, а также функции ее участников, имеющихся в необходимом количестве и должной квалификации
- Координировать и осуществлять контроль выполнения требований законодательства
- Иметь выстроенный и работающий процесс реагирования на компьютерные инциденты

СИЛЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

объектов критической информационной инфраструктуры (ЗО КИИ)

Подразделения (работники) субъекта КИИ			
ответственные за обеспечение безопасности значимых объектов КИИ	**эксплуатирующие** значимые объекты КИИ	**обеспечивающие функционирование** (сопровождение, обслуживание, ремонт) значимых объектов КИИ	**участвующие** в обеспечении безопасности значимых объектов КИИ
Заместитель руководителя юридического лица (заместитель генерального директора, уполномоченный в вопросах информационной безопасности)	**Начальники департаментов (отделов) информационных технологий**	Главный механик и его специалисты	Специалисты РСП (опционально)
	Начальники служб АСУТП	Главный энергетик и его специалисты	Специалисты подрядных организаций
Заместитель руководителя филиала юридического лица (при наличии соответствующих положений в уставной документации, положений передоверия полномочий)	Операторы, пользователи	**Главный инженер**	Операторы связи
Структурное подразделение, ответственное за обеспечение безопасности значимых объектов КИИ (структурное подразделение по безопасности) или специалисты по безопасности.	Начальники отделов испытаний	Начальники цехов	Представители регуляторов, ФОИВ, органов государственного контроля

Приказ ФСТЭК России от 21.12.2017 № 235, п.4

Текущее положение: что дальше?

УЖЕ ЕСТЬ КИИ

Процедура категорирования пройдена, уже определены объекты КИИ, сведения во ФСТЭК направлены

- Использование доверенных ПАК **01.01.2030** (ПП № 1912 от 14 ноября 2023 г., п.2)
- Соблюдение правил эксплуатации (УК РФ 274.1, ч.3)
- Информирование о компьютерных инцидентах (187-ФЗ, ст.9, ч.2)
- Создание системы обеспечения ИБ (если это значимый объект) (187-ФЗ, ст.9, ч.3)
- Направление изменений в сведениях во ФСТЭК (ПП № 127, п. 19(1))

ВОЗМОЖНО БУДЕТ КИИ

Есть планы внедрить новую информационную систему, автоматизировать процесс, модернизировать существующий элемент информационной инфраструктуры

- Раздел требований в техническом задании, техническом проекте, программах и методиках испытаний (Приказ ФСТЭК № 239, п.7)
- Выявление процесса, который автоматизируется, оценка его критичности (влияния на деятельность по выпуску продукции) (ПП № 127, п. 14, «а)», «б)»)
- Оценка технических решений в рамках реализации рабочего проекта (импортонезависимость) (ПП № 1912 от 14 ноября 2023 г., п.2)
- Проведение анализа уязвимостей (Приказ ФСТЭК № 239, п.12.6)
- Документирование процесса проектирования, внедрения, приемочные испытания, эксплуатации (Приказ ФСТЭК № 239, п.12.6)

Доверенные ПАК

Доверенный ПАК (аппаратная часть, программная часть, средство защиты информации)

Уровень доверия – не ниже 4 («Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», приказом ФСТЭК России от 02 июня 2020 г. № 76), только программно-аппаратные СЗИ.

Класс МСЭ – в зависимости от модели угроз, условий эксплуатации, модели нарушителя, сценариев реализации потенциальных компьютерных атак.

Включение аппаратной части в Единый реестр российской радиоэлектронной продукции (ПП РФ 878)

(https://gisp.gov.ru/pp719v2/pub/prod/rep//)

Включение программной части в Единый реестр российских программ для ЭВМ и БД

(https://reestr.digital.gov.ru/)

Наличие сертификата ФСТЭК России, ФСБ России

(Государственный реестр сертифицированных средств защиты информации https://reestr.fstec.ru/reg3)

Организационные меры

КОНТРОЛЬ ФИЗИЧЕСКОГО ДОСТУПА	УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ	РЕАЛИЗАЦИЯ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ	РАЗГРАНИЧЕНИЕ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ	ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНАЯ ДОКУМЕНТАЦИЯ
• контроль доступа на территорию • регламентация доступа в серверные помещения, в шкафы коммутации • ограничение доступа к линиям связи • организация безопасной передачи данных по каналам связи	• управление копиями файлов настроек коммутационного оборудования • сохранение конфигурации сетевого оборудования • определение лиц, которым разрешены действия по внесению изменений • контроль действий по внесению изменений в сетевую инфраструктуру, конфигурацию	• управление учетными записями пользователей • управление средствами защиты информации • управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации • мониторинг и анализ зарегистрированных событий безопасности	• регламентация прав доступа субъектов доступа к объектам доступа • введение ограничений на действия пользователей • ограничения на право изменения условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств	• ведение эксплуатационной документации • правила эксплуатации должны быть зафиксированы в локальных нормативных актах организации • локальный нормативный акт вместе с листом ознакомления нумеруется, прошивается и скрепляется печатью и подписью должностного лица