КОД ИБ | УФА 2024 |CyberSecurity SABANTUY 2024

Теория и практика 187-ФЗ:
как не упустить детали
и избежать неприятностей

Христолюбова Анна Анатольевна

Отраслевой центр компетенций по ИБ в промышленности
Минпромторга России

НПП "Гамма"

**ФГУП «НПП «ГАММА»
ЕКАТЕРИНБУРГСКИЙ НАУЧНО-
ТЕХНИЧЕСКИЙ ЦЕНТР
14 февраля 2024 г.**

Закон vs. Реалии

«Право собственности»	«Нельзя вот так просто взять и исключить объект из Реестра объектов КИИ..»	«Обе локальные, но разные»
«Полномочия»	«Это не то, что ты подумал»	«Всё есть объект КИИ»

Право собственности

Фабула:
Автоматизированная система управления как объект КИИ является объектом основных средств организации. Основные средства переданы по договору аренды с правом владения другой организации. Руководитель организации-арендодателя привлечен к административной ответственности за отсутствие плана реагирования на компьютерные инциденты на ЗОКИИ.

Требование:
Федеральный закон от 26 июля 2017 г. № 187-ФЗ, Статья 2, перечисление «8)»

Обратите внимание:
При определении потенциальных объектов КИИ четко и на законных основаниях идентифицируйте право владения и право распоряжения ИС, АСУ,ИТКС (и их отдельными элементами!). Объективные свидетельства этого имеются только на актуальном бухгалтерском балансе организации и в заключенных действующих договорах.

Реестр объектов КИИ

Фабула:
Бытует мнение, что направленные в адрес ФСТЭК России объекты КИИ для их включения в Реестр объектов КИИ ФСТЭК России невозможно в дальнейшем исключить из него. Однако специалисту одного из челябинских предприятий это удалось.

Требование:
Приказ ФСТЭК России
от 06 декабря 2017 г. № 227, пункт 10

Обратите внимание:
Вопрос об отсутствии критериев правоприменения положений Федерального закона от 26 июля 2017 г. № 187-ФЗ к конкретным объектам КИИ должен быть рассмотрен на очередном заседании постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры организации. Решение комиссии должно быть зафиксировано протоколом.

Политика ИБ организации

Фабула:
Требования политики информационной безопасности верхнего уровня распространили на все предприятия корпоративной структуры. Руководитель организации одной из взаимозависимых организаций получил административное наказание за отсутствие реализации парольной политики для каждого пользователя сети, не смотря на то, что АСУ ТП работала в круглосуточном режиме, а специалисты заступали на работу посменно.

Требование:
Приказ ФСТЭК России от 25 декабря 2017 г. № 239, п.12.2

Обратите внимание:
Правила и процедуры реализации отдельных организационных и (или) технических мер должны определяться политикой безопасности

Полномочия

Фабула:
В организации проведена процедура категорирования в полном соответствии с требованиями законодательства. Все документы своевременно направлены в адрес ФСТЭК России. В ходе проведения отраслевого мониторинга выясняется, что полномочия генерального директора организации, отраженные в Уставе, не включают в себя принятие решений в части защиты информации ограниченного доступа. Соответствующими полномочиями наделен только Совет директоров.

Требование:
Постановление Правительства РФ от 08 февраля 2018 г. № 127, п.11, перечисление «а)»

Обратите внимание:
Руководитель организации и председатель комиссии по категорированию должны иметь соответствующие полномочия для обеспечения легитимности результатов категорирования.

Сфера деятельности

Фабула:
Предприятие осуществляет разработку и производство автомобильной техники, в том числе пассажирских автобусов. Деятельность не относится к одной из сфер по 187-ФЗ. При этом имеет лицензию на услуги местной телефонной связи, за исключением услуг местной телефонной связи с использованием таксофонов и средств коллективного доступа и оказывает первичную медико-санитарную помощь населению поселка, в котором расположено.

Требование:
Федеральный закон от 26 июля 2017 г. № 187-ФЗ, Статья 2, перечисление «8)»

Обратите внимание:
Правоприменение положений Федерального закона от 26 июля 2017 г. № 187-ФЗ к организации необходимо осуществлять не по видам деятельности, а по продукции и услугам, которые оно производит или оказывает.

Идентификация объектов КИИ

Фабула:
Предприятие в ходе процедуры категорирования отнесла все ИС, АСУ, ИТКС (а также все, что хоть отдаленно имеет элементы информационной инфраструктуры) к объектам КИИ, включив их в соответствующий Перечень. Считая, что включение в Перечень не влечет никаких последствий для них, если в последствие объектам КИИ не будет присвоена одна из категорий значимости.

Требование:
Федеральный закон от 26 июля 2017 г. № 187-ФЗ, Статья 9, перечисление «2)»

Постановление Правительства РФ от 08 февраля 2018 г. № 127, п.14, перечисление «б)»

Обратите внимание:
В отношении всех объектов КИИ, включенных в Перечень необходимо осуществлять информирование о компьютерных инцидентах в адрес ГосСОПКА. При формировании Перечня объектов КИИ обязательно проводить выявление критических процессов. Необходимо установить четкую связь влияния элемента информатизации на результативность критического процесса.

Обеспечение безопасности объекта КИИ

Федеральный закон от 26 июля 2017 г. № 187-ФЗ, Статья 10, п. 1

«Субъект КИИ….создает систему безопасности такого объекта и обеспечивает ее функционирование»

Приказ ФСТЭК России от 25 декабря 2017 г. № 239, п.28

Оценка СЗИ на соответствие требованиям по безопасности в форме обязательной сертификации, испытаний или приемки

«Кто наблюдает ветер, тому не сеять, и кто смотрит на облака, тому не жать»

Приказ ФСТЭК России
от 21 декабря 2017 г. № 235, п.36

Внутренняя оценка или внешняя оценка (внешний аудит) состояния безопасности значимых объектов критической информационной инфраструктуры

Приказ ФСТЭК России от 25 декабря 2017 г. № 239, п.13.3, пер. «е)»
Построение Центра мониторинга, подключение к Ведомственному Центру мониторинга компьютерных инцидентов

Отраслевой центр компетенций по ИБ в промышленности Минпромторга России

https: //ock.gammaural.ru

t.me/ockgammaural