СМОЛЕНСК | 01.11.2018

Практические рекомендации по выполнению требований 187-ФЗ

Горохов Леонид

КОД БЕЗОПАСНОСТИ

ФЗ-187 «КИИ»

Подписан Закон о безопасности критической информационной инфраструктуры России. Он регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Документ определяет основные понятия в этой сфере: «автоматизированная система управления», «безопасность критической информационной инфраструктуры», «значимый объект критической информационной инфраструктуры», «компьютерная атака», «компьютерный инцидент», «критическая информационная инфраструктура», «объекты критической информационной инфраструктуры» и «субъекты критической информационной инфраструктуры».

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 26 ИЮЛЯ 2017 Г. N 187-ФЗ "О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ"

ВЕРХНЕУРОВНЕВО

Определяются полномочия государственных органов РФ в области обеспечения ее безопасности, а также права и обязанности субъектов критической информационной инфраструктуры.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

КТО «ПОД УДАРОМ»

Объекты КИИ – информационные системы, сети, автоматизированные системы управления:

- Госорганов
- Предприятий оборонной промышленности
- Учреждений здравоохранения
- Научных организаций
- Транспортных организаций
- Телеком-операторов
- Организаций кредитно-финансовой сферы
- Предприятий энергетики
- Предприятий топливно-энергетического комплекса
- Предприятий Атомной промышленности
- Предприятий Ракетно-космической промышленности
- Предприятий Горнодобывающей промышленности
- Предприятий Металлургической промышленности
- Предприятий Химической промышленности.
- Организации, которые осуществляют взаимодействие указанных выше систем и сетей

ОБЯЗАННОСТИ

Субьекты КИИ **должны**:

- ✓ Категорировать объекты КИИ которыми они владеют
  - Занизить уровень категорирования нельзя, у ФСТЭК есть право перекатегорирования
- ✓ Создать выделенную службы ИБ КИИ
- ✓ Подключиться к ГосСОПКА согласно требованиям ФСБ
- ✓ Создать систему защиты КИИ согласно требованиям ФСТЭК
- ✓ Регулярно проходить проверки регуляторов
- ✓ Своевременно сообщать об инцидентах ИБ в своей ИТ-инфраструктуре

КРИТЕРИИ ОТНЕСЕНИЯ К КИИ

- Ущерб здоровью людей и окружающей сред
- Нарушение функционирования ГИС
- Нарушение функционирование объектов жизнедеятельности, транспорта, связи
- Причинение значительного ущерба гос.предприятиям или бюджету
- Нарушение функционирования или подмена сайта госоргана
- Нарушение проведения финансовых транзакций
- Отсутствие доступа к госуслугам

А ВСЁ ЛИ ТАК ПЛОХО?

Сам закон, как и его выполнение, очень обеспокоили российские организации в части его исполнения.

Есть понимание того, что надо потратить много денег без видимости реальной ценности мер по защите данных инфраструктур…

Введена уголовная ответственность за действия, направленные против субъекта КИИ. Но пострадать может и сам субъект. Если не защитится…

КОД БЕЗОПАСНОСТИ

ОБ ОТВЕТСТВЕННОСТИ...

Действия субъекта КИИ	Результат действий атакующего	Ответственность
Не защитили объект КИИ	Не жахнуло	Если попадает по критериям – обязанность защитить объект
Не защитили объект КИИ	Жахнуло	274.1 ч.3 «Нарушение правил эксплуатации средств хранения», **до 6 лет лишения свободы** ответственному должностному лицу субъекта КИИ
Защитили объект КИИ	Не жахнуло	
Защитили объект КИИ	Жахнуло	274.1 ч.1 «Создание вредоносного ПО для неправомерного воздействия на КИИ», **до 5 лет лишения свободы** злоумышленнику 274.1 ч.2 «Несанкционированный доступ к информации в КИИ, если он повлек причинение вреда КИИ РФ», **до 6 лет лишения свободы** злоумышленнику

НО!

Давайте посмотрим на всё с другой стороны…

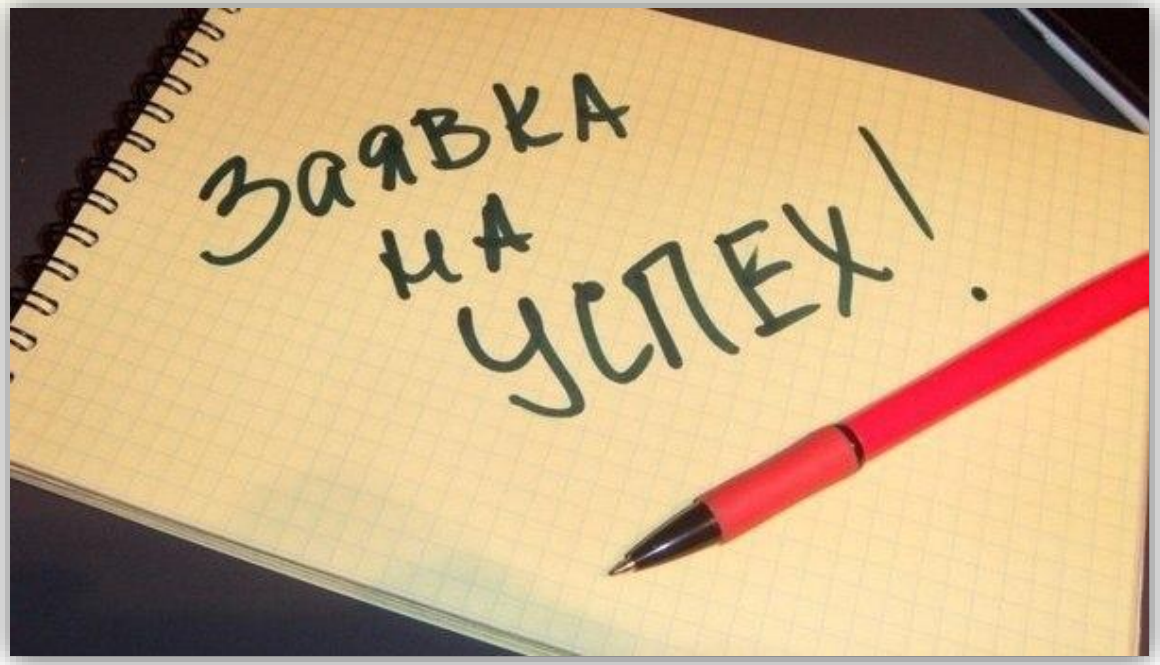
ОФИЦИАЛЬНО информационная безопасность станет независимой от ИТ

В рамках требований регуляторов появятся бюджеты именно на решения по информационной безопасности

Будет серьезная востребованность в специалистах по информационной безопасности

Закон направлен на попытку реализации планов по цифровому суверенитету страны. Это стратегия!

В ЧЁМ ПЛЮСЫ?



КАДРЫ! Они появятся!

Рост компетенций и экспертизы по информационной безопасности со стороны простых граждан и сотрудников организаций.

Если субъект КИИ ранее озадачивался защитой своей инфраструктуры и своих данных, то данный закон его из колеи не выбьет. У него практически всё есть!

КОД БЕЗОПАСНОСТИ

ТРЕБОВАНИЯ ФСТЭК

Направление	Endpoint	Network	Virtualization
Идентификация и аутентификация (ИАФ)	+	+	+
Управление доступом (УПД)	+	+	+
Ограничение программной среды (ОПС)	+		+
Защита машинных носителей информации (ЗНИ)	+		
Аудит безопасности (АУД)	+	+	+
Антивирусная защита (АВЗ)	+		
Предотвращение вторжений (компьютерных атак) (СОВ)	+	+	
Обеспечение целостности (ОЦЛ)	+	+	+
Обеспечение доступности информации (ОДТ)	+	+	+
Защита технических средств и систем (ЗТС)	Организационные меры		
Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	+ (+Терминал, MDM)	+	+
Реагирование на инциденты информационной безопасности (ИНЦ)	+	+	+
Управление конфигурацией (УКФ)	+		+
Управление обновлениями программного обеспечения (ОПО)	+		+
Планирование мероприятий по обеспечению безопасности (ПЛН)	Организационные меры		
Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	+	+	+
Информирование и обучение персонала (ИПО)	Организационные меры		

КОД БЕЗОПАСНОСТИ

ТРЕБОВАНИЯ ФСБ

Направление	Продукт
Обнаружение компьютерных атак	SIEM
Предупреждение компьютерных атак	Сканер уязвимостей
Ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты	исходя из требований – управление инцидентами на основе SIEM
Поиск признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ	СОВ/СОА
Криптографическая защита обмена информацией необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак	СКЗИ

СКЗИ
строго сертифицированные

Отсутствие НДВ в ПО

Средства защиты должны быть РОССИЙСКИМИ

КОД БЕЗОПАСНОСТИ

СРЕДСТВА ЗАЩИТЫ ПО ФСТЭК

Что потребуется для защиты	Что мы можем предложить
СЗИ от НСД	Secret Net Studio (АРМ), vGate (виртуализация), Secret MDM (мобильные устройства)
Межсетевой экран	АПКШ «Континент» (сеть), Secret Net Studio (АРМ)
Средство обнаружения вторжений	АПКШ «Континент» (сеть), Secret Net Studio (АРМ)
Средства антивирусной защиты	Secret Net Studio
Средства контроля защищенности	---
Средства управления событиями безопасности	---
Средства защиты каналов передачи данных	АПКШ «Континент»

СРЕДСТВА ЗАЩИТЫ ПО ФСБ

Что потребуется для защиты	Что мы можем предложить
SIEM	-
Сканеры уязвимостей	-
Средство обнаружения вторжений	АПКШ «Континент» (СОВ)
Средства обнаружения атак	АПКШ «Континент» (СОА)
Средства криптографической защиты информации	АПКШ «Континент»

КОД БЕЗОПАСНОСТИ

КОНКРЕТИКА

3 категория	2 категория	1 категория
Антивирус	Антивирус	Антивирус
СЗИ от НСД для АРМ и серверов	СЗИ от НСД для АРМ и серверов	СЗИ от НСД для АРМ и серверов
СЗИ от НСД для виртуальной инфраструктуры	СЗИ от НСД для виртуальной инфраструктуры	СЗИ от НСД для виртуальной инфраструктуры
Сканер уязвимостей	Сканер уязвимостей	Сканер уязвимостей
Система сбора и анализа событий безопасности	Система сбора и анализа событий безопасности	Система сбора и анализа событий безопасности
Система контроля подключенных USB-устройств	Система контроля подключенных USB-устройств	Система контроля подключенных USB-устройств
Межсетевой экран (сетевой, хостовый)	Межсетевой экран (сетевой, хостовый)	Межсетевой экран (сетевой, хостовый)
Система защиты информации на мобильных устройствах	Система защиты информации на мобильных устройствах	Система защиты информации на мобильных устройствах
Система управления обновлениями ПО	Система управления обновлениями ПО	Система управления обновлениями ПО
Система защищенного удаленного доступа	Система защищенного удаленного доступа	Система защищенного удаленного доступа
Система резервного копирования	Система резервного копирования	Система резервного копирования
Защита от DoS и DDoS-атак	Защита от DoS и DDoS-атак	Защита от DoS и DDoS-атак
	Система обнаружения вторжений	Система обнаружения вторжений
	Модуль доверенной загрузки	Модуль доверенной загрузки
	Анти-спам	Анти-спам

КОД БЕЗОПАСНОСТИ

КОНКРЕТИКА ПО КБ

3 категория	2 категория	1 категория
Антивирус	Антивирус	Антивирус
СЗИ от НСД для АРМ и серверов	СЗИ от НСД для АРМ и серверов	СЗИ от НСД для АРМ и серверов
СЗИ от НСД для виртуальной инфраструктуры	СЗИ от НСД для виртуальной инфраструктуры	СЗИ от НСД для виртуальной инфраструктуры
Сканер уязвимостей	Сканер уязвимостей	Сканер уязвимостей
Система сбора и анализа событий безопасности	Система сбора и анализа событий безопасности	Система сбора и анализа событий безопасности
Система контроля подключенных USB-устройств	Система контроля подключенных USB-устройств	Система контроля подключенных USB-устройств
Межсетевой экран (сетевой, хостовый)	Межсетевой экран (сетевой, хостовый)	Межсетевой экран (сетевой, хостовый)
Система защиты информации на мобильных устройствах	Система защиты информации на мобильных устройствах	Система защиты информации на мобильных устройствах
Система управления обновлениями ПО	Система управления обновлениями ПО	Система управления обновлениями ПО
Система защищенного удаленного доступа	Система защищенного удаленного доступа	Система защищенного удаленного доступа
Система резервного копирования	Система резервного копирования	Система резервного копирования
Защита от DoS и DDoS-атак	Защита от DoS и DDoS-атак	Защита от DoS и DDoS-атак
	Система обнаружения вторжений	Система обнаружения вторжений
	Модуль доверенной загрузки	Модуль доверенной загрузки
	Анти-спам	Анти-спам

КОД БЕЗОПАСНОСТИ

СОВСЕМ КОНКРЕТНО

3 категория	2 категория	1 категория
SECRET NET STUDIO (СЗИ от НСД, Контроль устройств) АПКШ Континент (СКЗИ, МЭ) vGate (СЗИ ВИ) + Антивирус SIEM Сканер уязвимостей Резервное копирование	SECRET NET STUDIO (СЗИ от НСД, Контроль устройств) АПКШ Континент (СКЗИ, МЭ, СОВ) vGate (СЗИ ВИ) ПАК СОБОЛЬ (АПМДЗ) + Антивирус SIEM Сканер уязвимостей Резервное копирование	SECRET NET STUDIO (СЗИ от НСД, Контроль устройств) АПКШ Континент (СКЗИ, МЭ, СОВ) vGate (СЗИ ВИ) ПАК СОБОЛЬ (АПМДЗ) + Антивирус SIEM Сканер уязвимостей Резервное копирование

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Горохов Леонид
l.gorokhov@securitycode.ru
+7 (495) 982 30 20 (*580)
+7 (917) 585 74 66