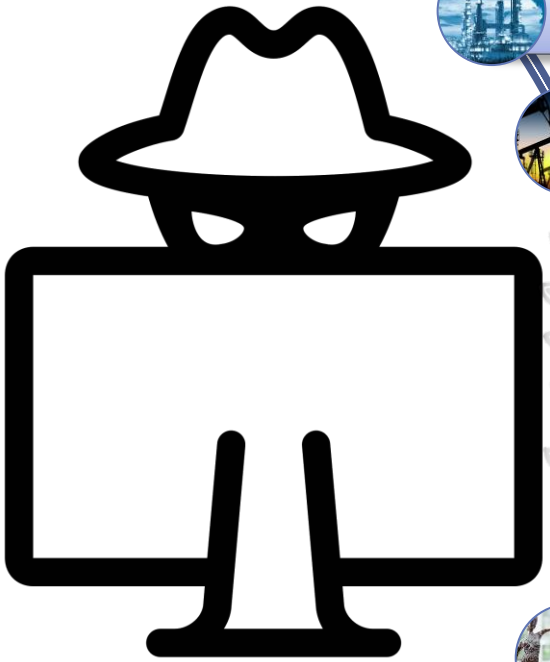
Вопросы реализации Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

КУБАРЕВ Алексей Валентинович
Заместитель начальника управления ФСТЭК России

Компьютерные инциденты в 2020 году



Январь. Нефтегазовая компания Burisma. Взлом почтового сервера

Февраль. Нефтяная компания INA Group. Шифрование серверов

Февраль. Оператор газопровода. Зашифрованы данные одновременно в IT- и OT-сетях

Февраль. Компания NEC. Похищено почти 27 тыс. файлов, включая документы, связанные с контрактами Минобороны Японии

Март. Компания по производству стали и добыче полезных ископаемых Evraz. Вымогательское ПО. Остановлено производство на большинстве заводов

Март. Юридическая компания Epiq Global. Вымогательское ПО. Заражены компьютеры во всех 80 штаб-квартирах компании по всему миру

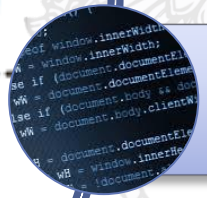
Март. РНПЦ пульмонологии и фтизиатрии Минздрава Беларуси. НСД к компьютерным системам учреждений здравоохранения Беларуси

Май. Производитель банкоматов для кредитных организаций компания Diebold. Вирус-шифровальщик нарушил выполнение некоторых операций

Компьютерные инциденты в 2020 году

Май. Fresenius, крупнейший в Европе оператор частных больниц. Компьютеры компании были взломаны, и кибератака затронула каждую часть деятельности компании по всему миру

Октябрь. Индийский фармацевтический гигант Dr Reddy's. был вынужден отключить все свои серверы центров обработки данных по всему миру на целый день после того, как подвергся кибератаке



Октябрь. Американский поставщик программного обеспечения для здравоохранения eResearchTechnology. подвергся атакам операторов вымогательского ПО, в результате которых были замедлены некоторые медицинские исследования

Сентябрь. Universal Health Services (UHS), предоставляющая услуги в области здравоохранения, была вынуждена отключить свои компьютерные системы вследствие кибератаки

Наблюдения по результатам анализа сведений

- Занижение значимости объектов КИИ
- Игнорирование сроков реализации ФЗ
- Сокрытие объектов КИИ
- Привлечение к категорированию сторонних организаций

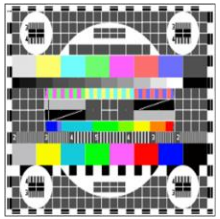
Наблюдения по результатам анализа сведений

Уполномоченные лица низкого уровня

Непрофильные подразделения безопасности

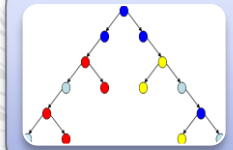
Нет ОРД

Не реализуются меры по информированию



Наблюдения по результатам анализа сведений

Многие объекты эксплуатируются множеством организаций



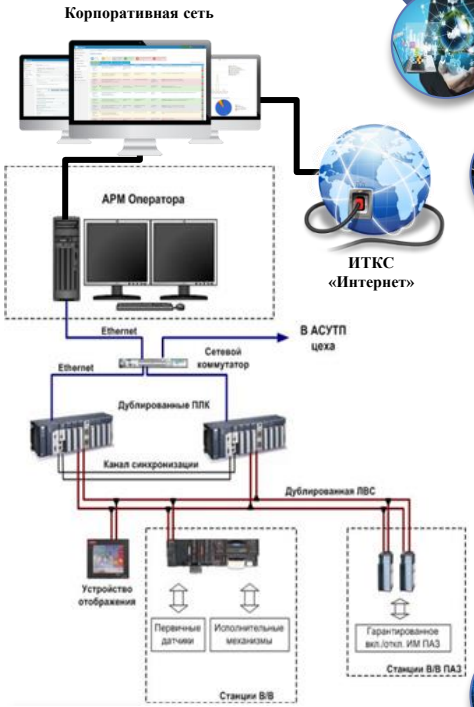
Многие объекты являются территориально распределенными

Применение СЗИ, не прошедших оценку соответствия

Не рассматриваются угрозы, реализуемые внешним нарушителем

Не рассматривается возможность реализации компьютерных инцидентов

Факторы, влияющие на защищенность значимых объектов КИИ



- Расширение масштаба применения ИТ для управления технологическими процессами
- Подключение к внешним сетям, в том числе корпоративным
- Непринятие мер по обеспечению сетевой безопасности АСУ
- Применение импортного ПО и оборудования
- Наличие уязвимостей ПО (от 25 до 38 на одном объекте)
- Наличие удаленных каналов связи с производителями оборудования
- Недооценка возможностей нарушителей безопасности информации

Наблюдения на объектах

Планы конкретных мероприятий по реализации ФЗ отсутствуют

Специалисты по ОБКИИ в подчинении у Служб ИТ, отсутствуют или перегружены

ОРД в соответствие требованиям ФЗ не приведены

Не все УБИ определены или нейтрализованы

Персонал об УБИ и правилах безопасной работы не осведомлён

Наблюдения на объектах

Не все объекты КИИ категорированы

Не все уязвимости нейтрализованы

САВЗ и СОВ не обновляются

СЗИ настроены некорректно

Персонал с инструкциями не ознакомлен

Наблюдения на объектах

- Применение наложенных СЗИ, пагубно влияющих на технологический процесс
- Не все технические меры по ОБКИИ приняты
- Не минимизированы права доступа
- Оценка соответствия СЗИ и систем ОБ не осуществлена
- АРМ администрирования компонентов ЗОКИИ в их состав не входят
- Модернизация ОБКИИ не спланирована

Наблюдения на объектах

Не осуществляется учет и контроль съемных МНИ и подключаемых СВТ

АРМ управления СЗИ не защищаются

SOC не готов к APT

Инструкции персоналу перегружены

Категорирование создаваемых объектов не проводится

И, конечно, удалёночка

Общая учётка на всю семью

Нет идентификации и аутентификации

Экран не гасим

Нет даже антивируса

Параллельно с работой играем в Доту с той же учётки

И, конечно, удалёночка

Уязвимые VPN-клиенты

RDP со всех СВТ

Незащищенный криптографией RDP

Уязвимые Web-сервисы

Требования к функционированию системы безопасности значимых объектов

планирование и разработка мероприятий по обеспечению безопасности значимых объектов

реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов

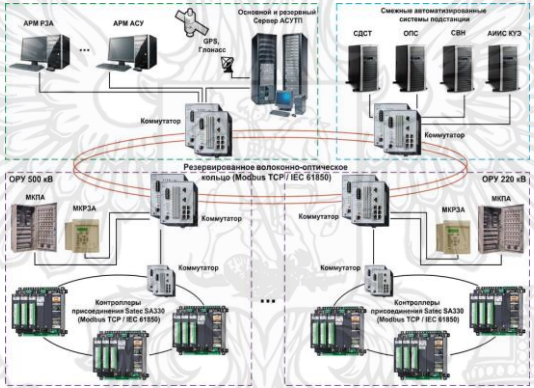
контроль состояния безопасности значимых объектов

совершенствование безопасности значимых объектов

Состав мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Определение угроз безопасности объекта

Поддержание уровня безопасности объекта в ходе его эксплуатации



Формирование требований по обеспечению безопасности объекта

Оценка соответствия принятых мер по обеспечению безопасности объекта

Внедрение организационных и технических мер по обеспечению безопасности объекта

Первоочередные меры по повышению уровня безопасности критической информационной инфраструктуры

Созданы штатные службы или подразделения по обеспечению безопасности объектов КИИ

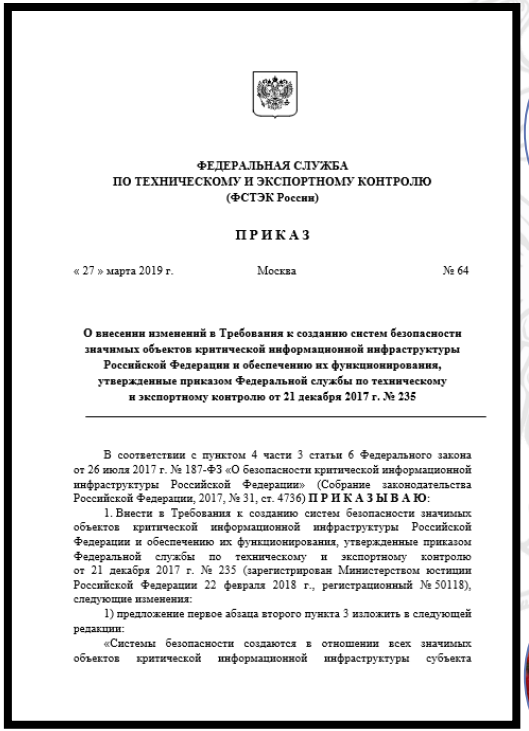
Проведена инвентаризация ПО и оборудования, входящих в состав объектов КИИ

Разработаны организационно-распорядительные документы, регламентирующие защиту значимых объектов КИИ

Основные меры обеспечения безопасности объектов КИИ:

- усиление мер по защите периметра автоматизированных систем управления технологическими процессами
- принятие мер по поддержанию безопасного состояния систем
- постоянный мониторинг безопасности систем
- управление инцидентами информационной безопасности

Разработка нормативных правовых актов по обеспечению безопасности критической информационной инфраструктуры



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« 27 » марта 2019 г. Москва № 64

О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю**:

1. Внести в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 (зарегистрирован Министерством юстиции Российской Федерации 22 февраля 2018 г., регистрационный № 50118), следующие изменения:

1) предложение первое абзаца второго пункта 3 изложить в следующей редакции:

«Системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры субъекта

Уточнен порядок создания систем безопасности в филиалах (представительствах) и подчиненных организациях интегрированных структур

Установлены требования к образованию специалистов по безопасности значимых объектов КИИ

Вступление в силу с 1 января 2021 г.

Государственный контроль в области обеспечения безопасности критической информационной инфраструктуры

Постановление Правительства Российской Федерации
от 17 февраля 2018 г. № 162

Об утверждении порядка осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

Устанавливает правила осуществления ФСТЭК России и ее территориальными органами мероприятий по государственному контролю в области обеспечения безопасности значимых объектов КИИ РФ

Виды контроля

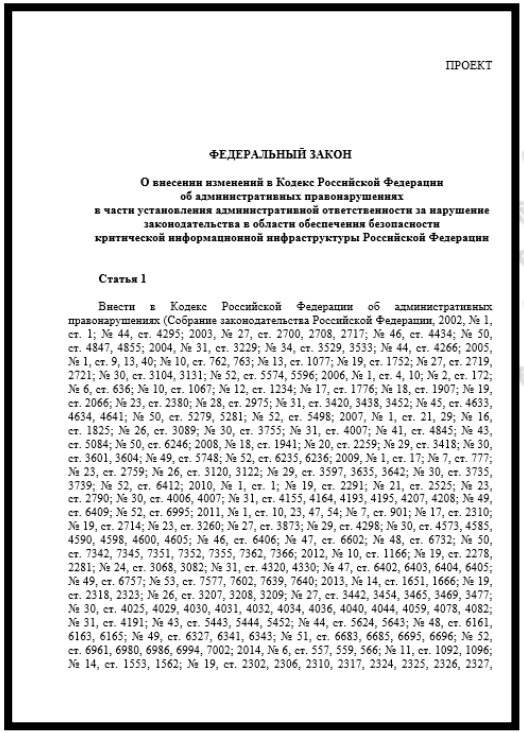
Плановый

- Истечение 3 лет со дня внесения сведений об объекте КИИ в Реестр
- Истечение 3 лет со дня осуществления последней плановой проверки

Внеплановый

- Истечение срока выполнения субъектом КИИ предписания об устранении выявленного нарушения
- Возникновение компьютерного инцидента, повлекшего негативные последствия
- Поручение Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора

Разработка нормативных правовых актов по обеспечению безопасности критической информационной инфраструктуры



ПРОЕКТ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Кодекс Российской Федерации
об административных правонарушениях
в части установления административной ответственности за нарушение
законодательства в области обеспечения безопасности
критической информационной инфраструктуры Российской Федерации

Статья 1

Внести в Кодекс Российской Федерации об административных правонарушениях (Собрание законодательства Российской Федерации, 2002, № 1, ст. 1; № 44, ст. 4295; 2003, № 27, ст. 2700, 2708, 2717; № 46, ст. 4434; № 50, ст. 4847, 4855; 2004, № 31, ст. 3229; № 34, ст. 3529, 3533; № 44, ст. 4266; 2005, № 1, ст. 9, 13, 40; № 10, ст. 762, 763; № 13, ст. 1077; № 19, ст. 1752; № 27, ст. 2719, 2721; № 30, ст. 3104, 3131; № 52, ст. 5574, 5596; 2006, № 1, ст. 4, 10; № 2, ст. 172; № 6, ст. 636; № 10, ст. 1067; № 12, ст. 1234; № 17, ст. 1776; № 18, ст. 1907; № 19, ст. 2066; № 23, ст. 2380; № 28, ст. 2975; № 31, ст. 3420, 3438, 3452; № 45, ст. 4633, 4634, 4641; № 50, ст. 5279, 5281; № 52, ст. 5498; 2007, № 1, ст. 21, 29; № 16, ст. 1825; № 26, ст. 3089; № 30, ст. 3755; № 31, ст. 4007; № 41, ст. 4845; № 43, ст. 5084; № 50, ст. 6246; 2008, № 18, ст. 1941; № 20, ст. 2259; № 29, ст. 3418; № 30, ст. 3601, 3604; № 49, ст. 5748; № 52, ст. 6235, 6236; 2009, № 1, ст. 17; № 7, ст. 777; № 23, ст. 2759; № 26, ст. 3120, 3122; № 29, ст. 3597, 3635, 3642; № 30, ст. 3735, 3739; № 52, ст. 6412; 2010, № 1, ст. 1; № 19, ст. 2291; № 21, ст. 2525; № 23, ст. 2790; № 30, ст. 4006, 4007; № 31, ст. 4155, 4164, 4193, 4195, 4207, 4208; № 49, ст. 6409; № 52, ст. 6995; 2011, № 1, ст. 10, 23, 47, 54; № 7, ст. 901; № 17, ст. 2310; № 19, ст. 2714; № 23, ст. 3260; № 27, ст. 3873; № 29, ст. 4298; № 30, ст. 4573, 4585, 4590, 4598, 4600, 4605; № 46, ст. 6406; № 47, ст. 6602; № 48, ст. 6732; № 50, ст. 7342, 7345, 7351, 7352, 7355, 7362, 7366; 2012, № 10, ст. 1166; № 19, ст. 2278, 2281; № 24, ст. 3068, 3082; № 31, ст. 4320, 4330; № 47, ст. 6402, 6403, 6404, 6405; № 49, ст. 6757; № 53, ст. 7577, 7602, 7639, 7640; 2013, № 14, ст. 1651, 1666; № 19, ст. 2318, 2323; № 26, ст. 3207, 3208, 3209; № 27, ст. 3442, 3454, 3465, 3469, 3477; № 30, ст. 4025, 4029, 4030, 4031, 4032, 4034, 4036, 4040, 4044, 4059, 4078, 4082; № 31, ст. 4191; № 43, ст. 5443, 5444, 5452; № 44, ст. 5624, 5643; № 48, ст. 6161, 6163, 6165; № 49, ст. 6327, 6341, 6343; № 51, ст. 6683, 6685, 6695, 6696; № 52, ст. 6961, 6980, 6986, 6994, 7002; 2014, № 6, ст. 557, 559, 566; № 11, ст. 1092, 1096; № 14, ст. 1553, 1562; № 19, ст. 2302, 2306, 2310, 2317, 2324, 2325, 2326, 2327,

- Нарушение сроков категорирования объектов КИИ
- Нереализация Требований по созданию систем безопасности ЗО КИИ и обеспечению их функционирования
- Нереализация Требований по обеспечению безопасности ЗО КИИ
- Нарушение порядка реагирования на инциденты
- Нарушение порядка информирования об инцидентах
- Нарушение порядка и сроков представления информации в ГосСОПКУ

Первая заповедь ИБ

Общая защищенность системы равняется защищенности наименее защищенной её части

Спасибо за внимание!

Вопросы?

Вопросы реализации Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

КУБАРЕВ Алексей Валентинович
Заместитель начальника управления ФСТЭК России