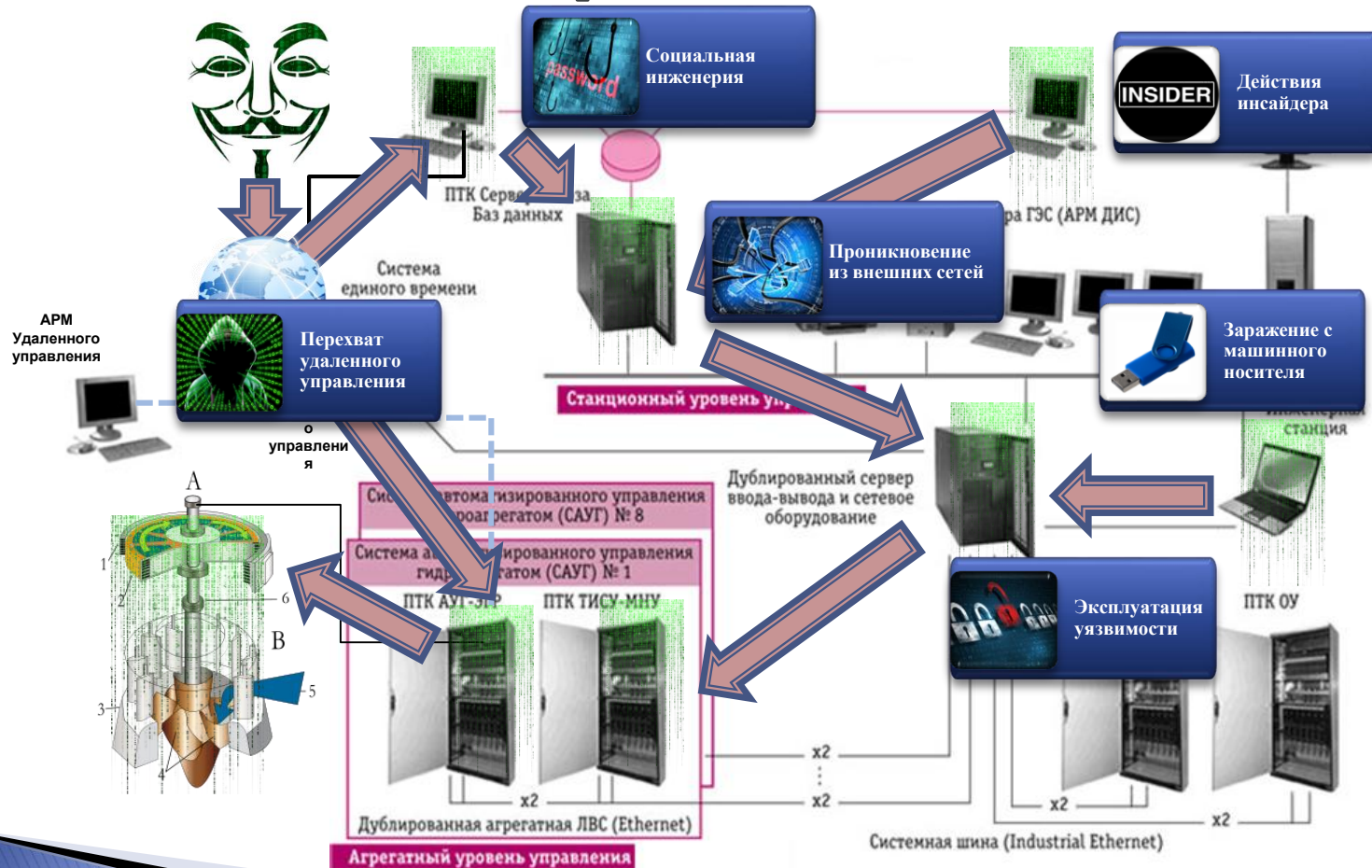


Вопросы реализации Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»



КУБАРЕВ Алексей Валентинович
Заместитель начальника управления ФСТЭК России

Компьютерные атаки на АСУ ТП



Последствия компьютерных атак на АСУ ТП



Контроль над режимом работы оборудования



Несанкционированное управление оборудованием



Несрабатывание защиты при возникновении аварийной ситуации



Введение в заблуждение персонала



Изменение показаний устройств



Меры по обеспечению безопасности ЗО КИИ



ФЕДЕРАЛЬНЫЙ ЗАКОН

от 26 июля 2017 г. № 187-ФЗ

«О безопасности критической
информационной
инфраструктуры
Российской Федерации»

**Разработка перечней объектов,
подлежащих категорированию**

Категорирование объектов КИИ

**Создание и обеспечение функционирования
систем безопасности значимых объектов КИИ**

**Принятие мер по обеспечению
безопасности значимых объектов КИИ**

Осуществление взаимодействия с ГосСОПКА



Наблюдения по результатам анализа сведений



Занижение значимости объектов КИИ



Игнорирование сроков реализации ФЗ



Соккрытие объектов КИИ



Привлечение к категорированию сторонних организаций



Наблюдения по результатам анализа сведений



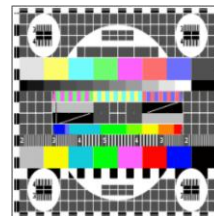
Уполномоченные лица низкого уровня

Непрофильные подразделения безопасности



Отсутствуют необходимые организационно-распорядительные документы по ОБ КИИ

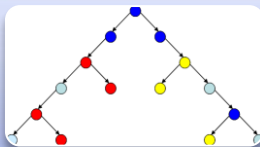
Не реализуются меры по информированию персонала субъектов КИИ



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



Наблюдения по результатам анализа сведений



Импортное ПО и
оборудование



Связи с внешними сетями



Низкий потенциал
нарушителя



Реализован лишь базовый
набор мер



Первоочередные меры по повышению уровня безопасности КИИ

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 ОБ КИИ



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.**



Внесение изменений в Требования ... 239



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«20» февраля 2020 г.

Москва

№ 35

О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

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), пунктом 2 и подпунктом 9.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2017, № 48, ст. 7198; 2018, № 20, ст. 2818), **П Р И К А З Ы В А Ю:**

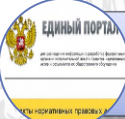
1. Внести в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 (зарегистрирован Министерством юстиции Российской Федерации 26 марта 2018 г., регистрационный № 50524) (с изменениями, внесенными приказом Федеральной службы по техническому



Разработан во исполнение поручений Президента и Правительства Российской Федерации



При разработке **учтено мнение** экспертов крупнейших субъектов КИИ



Прошли **общественное обсуждение**



Согласованы с **Минкомсвязью России**



Утверждены приказом ФСТЭК России от 20 февраля 2020 г. № 35



Зарегистрирован Минюстом России
11 сентября 2020 г. № 59793



Внесение изменений в Требования ... 239



Определены признаки модернизации ЗО КИИ



Определены требования по безопасности к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности ЗО КИИ



Введены новые требования к СЗИ (6 УД) – с 1 января 2023 г.

Проверяются на этапе предварительных испытаний САМОСТОЯТЕЛЬНО или лицензиатом



Введены требования к СППО, обеспечивающему выполнение функций ЗО КИИ по назначению – с 1 января 2023 г.

Проверка САМОСТОЯТЕЛЬНО, лицензиатом или интегратором на этапе проектирования



Смягчены требования по удаленному взаимодействию ЗО КИИ



Введены условия допущения удаленного доступа к компонентам объектов КИИ и определены меры по обеспечению безопасности такого доступа



Новые требования к СППО

Требования по безопасной разработке:

- наличие **руководства по безопасной разработке** программного обеспечения;
- **проведение анализа угроз** безопасности информации программного обеспечения;
- наличие **описания структуры программного обеспечения на уровне подсистем и результатов сопоставления функций программного обеспечения и интерфейсов, описанных в функциональной спецификации, с его подсистемами** (для 1 категории)

Требования к поддержке безопасности:

- наличие процедур отслеживания и исправления обнаруженных ошибок и уязвимостей ПО;
- определение способов и сроков доведения разработчиком (производителем) ПО до его пользователей информации об уязвимостях, о компенсирующих мерах по защите информации или ограничениях по применению ПО, способов получения пользователями ПО его обновлений, проверки их целостности и подлинности;
- наличие процедур информирования субъекта КИИ об окончании производства и (или) поддержки ПО (для 1 категории)

Требования к испытаниям по выявлению уязвимостей:

- проведение **статического анализа** исходного кода программы;
- проведение **фаззинг-тестирования** программы, направленного на выявление в ней уязвимостей;
- проведение **динамического анализа** кода программы (для 1 категории)

Оценка путем анализа материалов, представленных разработчиком (производителем СПО)



Компенсирующие меры для организации



определение лиц и устройств, которым разрешен УД к ПО и П-АС 3О, предоставление им минимальных полномочий при доступе к этим средствам;



контроль доступа к ПО и П-АС 3О;



ЗИ и данных при их передаче по каналам связи при УД к ПО и П-АС 3О;



мониторинг и регистрация действий лиц, которым разрешен УД к ПО и П-АС 3О, а также инициируемых ими процессов, анализ этих действий в целях выявления фактов неправомерных действий;



обеспечение невозможности отказа лиц от выполненных действий при осуществлении УД к ПО и П-АС 3О



Порядок согласования подключения ЗО КИИ к ССОП



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«28» мая 2020 г.

Москва

№ 45

Об утверждении Порядка согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования

В соответствии с пунктом 3 Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры, утвержденных постановлением Правительства Российской Федерации от 8 июня 2019 г. № 743 (Собрание законодательства Российской Федерации, 2019, № 24, ст. 3099), **П Р И К А З Ы В А Ю:**

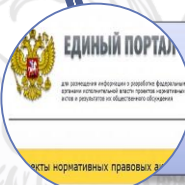
Утвердить прилагаемый Порядок согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛЕЗНЕВ



Разработан во исполнение постановления
Правительства Российской Федерации



Прошел **общественное обсуждение**



Утвержден приказом ФСТЭК России
от 28 мая 2020 г. № 75



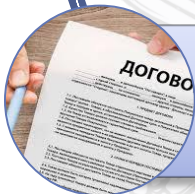
Зарегистрирован Минюстом России
15 сентября 2020 г. № 59866



Согласование подключения



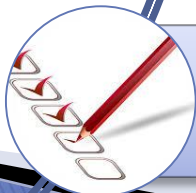
До ввода ZO в действие



**До заключения договора с оператором
связи**



**В случае подключения ZO до внесения
его в реестр согласование не требуется**



**Форма запроса на согласование в
приложении к Порядку**



Основания для отказа в согласовании



Представление неполных сведений и документов



Несоответствие СЗИ декларированным



Несоответствие СЗИ Требованиям по ОБ 30 КИИ и Требованиям по созданию систем ОБ 30 КИИ и обеспечению их функционирования



Спасибо за внимание!

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



КУБАРЕВ Алексей Валентинович

Заместитель начальника управления ФСТЭК России