Организация мероприятий по обеспечению безопасности объектов КИИ

Докладчик:
Федоров Иван
Заместитель генерального директора
компании «КСБ-СОФТ»

КСБ-СОФТ

1 ноября 2018 года, г. Смоленск

ksb-soft.ru

Законодательство в сфере безопасности критической информационной инфраструктуры

- Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Постановление Правительства РФ от 08 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
- Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказ Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 №236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;
- Приказ Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. N 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Постановление Правительства РФ от 17 февраля 2018 г. N 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Информационное сообщение Федеральной службы по техническому и экспортному контролю от 4 мая 2018 г. N 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации».

Методические документы

Утратили силу

✓С 3 мая 2018 г. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, утвержденные ФСТЭК России 18 мая 2007 г., и Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, утвержденные ФСТЭК России 19 ноября 2007 г., признаны утратившими силу.

Действуют

✓Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г., а также

✓Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.

могут применяться для моделирования угроз безопасности информации на значимых объектах критической информационной инфраструктуры Российской Федерации до утверждения ФСТЭК России соответствующих методических документов.

Информационное сообщение Федеральной службы по техническому и экспортному контролю от 4 мая 2018 г. N 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации».

Перечень потенциальных сфер объектов КИИ

- здравоохранение;
- наука;
- транспорт;
- связь;
- энергетика;
- банковская и иные сферы финансового рынка;
- топливно-энергетический комплекс;
- атомная энергия;
- оборонная и ракетно-космическая промышленность;
- горнодобывающая, металлургическая и химическая промышленность.

Кто такой субъект КИИ?

Как понять, является ли организация субъектом КИИ?

1. **Коды ОКВЭД. Основной и дополнительные**
2. **Коды ОКОГУ (для органов государственной власти)**
3. **Лицензии на виды деятельности**
4. **Устав или положение об организации**

Что такое объект КИИ?

Объект КИИ – это:

Что означает «категорирование объектов КИИ»?

С кем осуществляется взаимодействие при категорировании объектов КИИ?

Чем отличаются значимые объекты КИИ от незначимых?

Объекты КИИ, которым была присвоена одна из категорий, называются в законе **значимыми** объектами КИИ.

Значимый объект КИИ	Незначимый объект КИИ
Установлена одна из категорий значимости	НЕ установлена ни одна из категорий значимости
В обязательном порядке необходимо выполнять требования по обеспечению безопасности информации (Приказы ФСТЭК России №235 и № 239)	Выполнять требования по обеспечению безопасности информации (Приказы ФСТЭК России №235 и № 239) в обязательном порядке НЕ требуется

Категории значимости объектов КИИ

Категорирование объекта КИИ предполагает определение его категории значимости на основе ряда критериев и показателей.

Категория объекта КИИ	Потенциал источника угроз, который следует рассматривать при выборе мер	Требуемый класс СЗИ
1 категория	Высокий	Не ниже 4 класса
2 категория	Базовый усиленный	Не ниже 5 класса
3 категория	Базовый	Не ниже 6 класса

Если объект КИИ не соответствует ни одному из установленных критериев, ему категория не присваивается. В этом случае результаты категорирования все равно должны быть представлены во ФСТЭК России.

Регулирование и надзор

ФСТЭК	ФСБ
• Ведет реестр значимых объектов КИИ • Устанавливает требования по обеспечению безопасности • значимых объектов КИИ • Контролирует выполнение требований по категорированию • объектов КИИ и обеспечению безопасности значимых объектов	• Главный центр ГосСОПКА • Устанавливает порядок информирования об объектах КИИ и инцидентах, определяет состав предоставляемой информации • Обеспечивает установку на объектах КИИ технических средств ГосСОПКА и устанавливает требования к ним • Проводит оценку безопасности объектов КИИ

Прочие регуляторы

Минкомсвязь	Банк России
• Согласовывает требования по обеспечению безопасности объектов КИИ для своей сферы регулирования • Согласовывает порядок установки технических средств ГосСОПКА на объектах КИИ в своей сфере регулирования	• Согласовывает требования по обеспечению безопасности объектов КИИ для своей сферы регулирования • Согласовывает порядок информирования и состав предоставляемых сведений для своей сферы регулирования • Согласовывает порядок установки технических средств • ГосСОПКА на объектах КИИ в своей сфере регулирования • Является центром ГосСОПКА для своей сферы регулирования

Взаимодействие со ФСТЭК России.
Оценка соответствия показателям критериев значимости

По завершению категорирования сведения о его результатах должны направляться субъектом КИИ во ФСТЭК России для ведения реестра значимых объектов КИИ. В реестр включается следующая информация:

- ✓наименование значимого объекта КИИ;
- ✓наименование субъекта КИИ;
- ✓сведения о взаимодействии значимого объекта КИИ и сетей электросвязи;
- ✓сведения о лице, эксплуатирующем значимый объект КИИ;
- ✓присвоенная категория значимости;
- ✓сведения о программных и программно-аппаратных средствах, используемых на значимом объекте КИИ;
- ✓меры, применяемые для обеспечения безопасности значимого объекта КИИ.

Регулятор проверяет представленные материалы и при необходимости направляет замечания, которые должен учесть субъект КИИ. Если субъект КИИ не предоставит данные о категорировании, ФСТЭК России вправе потребовать эту информацию. Решение комиссии оформляется актом категорирования.

Порядок ведения реестра значимых объектов КИИ определяется приказом ФСТЭК России от 06.12.2017 №227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».

Представление информации в реестр и ведение реестра значимых объектов КИИ

Реестр представляет собой единую систему учета, хранения и представления информации в бумажном или электронном виде о значимых объектах КИИ.

В ходе формирования и ведения Реестра осуществляются:

✓оценка полноты и достаточности сведений об объектах КИИ;

✓проверка соблюдения субъектами КИИ порядка категорирования;

✓проверка правильности присвоения объектам КИИ одной из категорий значимости.

Решение о включении сведений о значимом объекте КИИ в Реестр принимается в течение 30 дней со дня получения ФСТЭК России сведений от субъекта КИИ.

Изменение категории значимости объектов КИИ

Изменения категории значимости объектов КИИ в реестр вносятся только на основе сведений, представляемых субъектами КИИ.

Изменение категории значимости может произойти:

✓По мотивированному решению ФСТЭК по результатам проверки, выполненной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ;

✓Объект перестал соответствовать критериям значимости и показателям их значений;

✓Субъект КИИ был реорганизован, ликвидирован или произошли изменения в его организационно-правовой форме.

Субъект КИИ не реже чем один раз в 5 лет осуществляет пересмотр установленной категории значимости и сообщает об изменениях в ФСТЭК.

Обеспечение безопасности объектов КИИ

«Для категорирования объектов критической информационной инфраструктуры субъекты критической информационной инфраструктуры могут привлекать организации, имеющие соответствующую лицензию на деятельность в области защиты информации».

Приказ Федеральной службы по техническому и экспортному контролю "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (подготовлен ФСТЭК России от 17.12.2017)

Система безопасности значимого объекта КИИ

Реализация требований к ИБ включает в себя 5 базовых шагов:

Система безопасности значимого объекта КИИ

Создаваемые системы безопасности должны соответствовать требованиям, предъявляемым к:

✓Силам обеспечения безопасности значимых объектов КИИ;

✓Программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ;

✓Организационно-распорядительным документам по безопасности значимых объектов;

✓Функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Порядок создания системы и требования к принимаемым мерам безопасности определяются приказом ФСТЭК России от 21.12.2017 №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

Система безопасности значимого объекта КИИ

Для значимых объектов КИИ, помимо интеграции в ГосСОПКА, субъекты КИИ должны:

✓Создать систему безопасности значимого объекта КИИ;

✓Реагировать на компьютерные инциденты. Порядок реагирования на компьютерные инциденты должен быть подготовлен ФСБ России до конца апреля текущего года;

✓Предоставлять на объект КИИ беспрепятственный доступ регуляторам и выполнять их предписания по результатам проверок. Законом предусматриваются как плановые, так и внеплановые проверки.

Основные задачи безопасности

- ✓ Предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами КИИ, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
- ✓ Недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов КИИ;
- ✓ Восстановление функционирования значимых объектов КИИ, в том числе за счет создания и хранения резервных копий необходимой для этого информации;
- ✓ Непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, которое осуществляется в соответствии со статьей 5 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

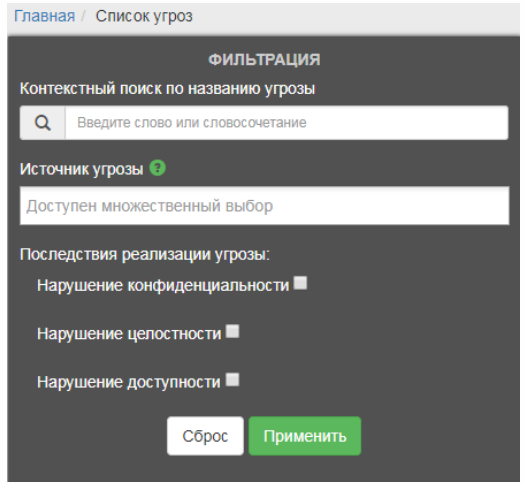
Угрозы безопасности КИИ

Существует множество классификаций угроз безопасности

По природе возникновения:
a)человеческий фактор
b)угрозы среды (естественные), возникшие в результате явлений, не зависящих от человека
По способу осуществления:
a)Случайные
b)Целенаправленные (преднамеренные)
В зависимости от источника:
a)субъект доступа
b)материальный объект
c)физическое явление

В зависимости от расположения источника угроз:
a)внутренние
b)внешние
По степени воздействия:
a)пассивные
b)Активные
По способу доступа к защищаемым ресурсам:
a)угрозы, использующие стандартный доступ
b)нестандартный (скрытый) доступ
По использованию нарушителями физического и технического доступа и др.

БДУ ФСТЭК https://bdu.fstec.ru/threat



Что нужно сделать для обеспечения безопасности объекта КИИ?

1. Категорирование
2. Установление требований
3. Анализ УБИ и разработка (уточнение) МУ
4. Проектирование
5. Разработка рабочей документации
6. Внедрение
7. Испытания

Обеспечение безопасности объектов КИИ

Создание (модернизация) системы защиты

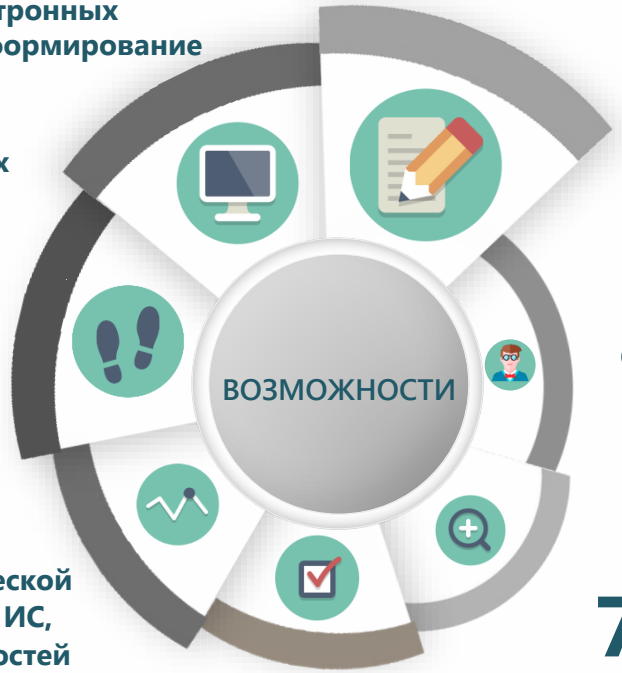
- ✓ Установление требований к обеспечению безопасности
- ✓ Разработка модели угроз безопасности информации
- ✓ Проектирование системы защиты информации
- ✓ Разработка рабочей документации на систему защиты информации
- ✓ Внедрение мер защиты информации
- ✓ Сопровождение средства защиты информации
- ✓ Контроль состояния безопасности

ПК «АльфаДок»* - отечественное решение для управления мероприятиями по защите информации

Призер конкурса
«Лучшие информационно-аналитические инструменты 2017»
Аналитического центра при правительстве РФ

Лауреат конкурса
«Лучшее ИТ решение для здравоохранения 2018»

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ
ITM
www.itmcongress.ru



2 ведение электронных журналов и формирование отчетов

1 разработка и актуализация документации по защите информации

3 планирование внутренних проверок и оценка готовности к проверкам регуляторов

8 обучение сотрудников

4 формирование моделей угроз и действий нарушителя

5 оценка технической защищенности ИС, анализ уязвимостей

7 мониторинг и контроль деятельности подведомственных организаций

6 категорирование объектов КИИ

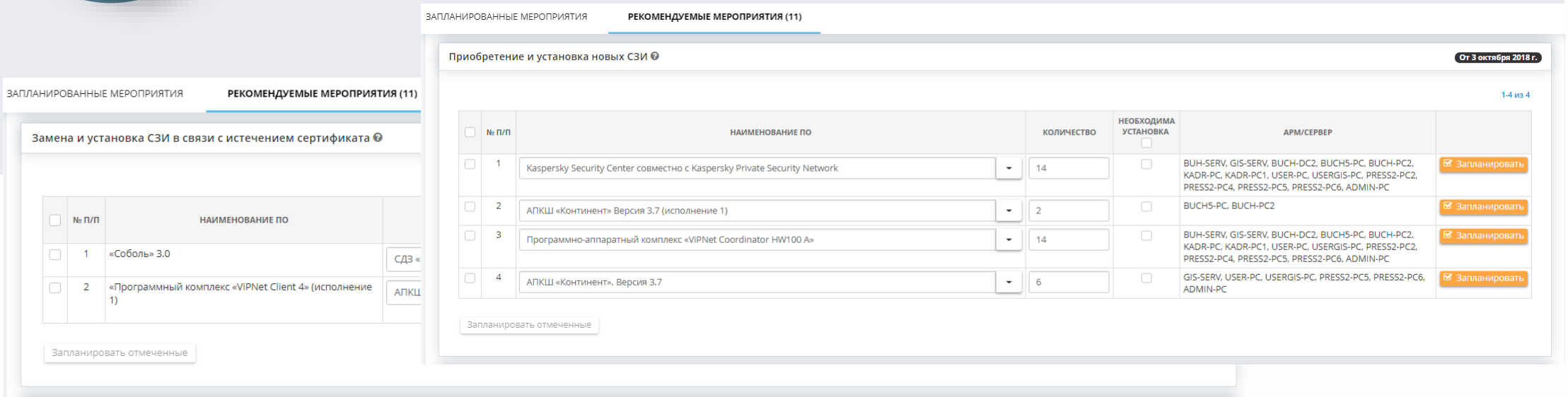
***Входит в Единый реестр российских программ для электронных вычислительных машин и баз данных – ссылка**

Планирование работ по защите информации

NEW!

ФОРМИРОВАНИЕ И ВЫГРУЗКА ПЛАНА РАБОТ:

- **Автоматизированный подбор рекомендуемых мероприятий** по приобретению, замене, продлению лицензий СЗИ, аттестации/ переаттестации информационных систем и т.д.)
- Планирование **индивидуальных** мероприятий
- Планирование **на определенный период**



Сервис обучения

NEW!

ОРГАНИЗАЦИЯ СИСТЕМАТИЧЕСКОГО ОБУЧЕНИЯ СОТРУДНИКОВ:

- ☑ Повышение уровня осведомленности специалистов, обрабатывающих персональные данные
- ☑ Повышение квалификации специалистов по защите информации
- ☑ Соответствие требованиям регуляторов **пп.6 п.1 ст.18.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»**

ФУНКЦИОНАЛ:

- ☑ Создание курсов и тестов
- ☑ Формирование групп обучения
- ☑ Формирование отчётов о ходе обучения и результатах тестирования

БЕСПЛАТНЫЕ КУРСЫ ПО ЗАЩИТЕ ПДн ОТ «КСБ-СОФТ»:

- ➢ **для органов государственной власти**
- ➢ **для медицинских организаций**
- ➢ **для образовательных учреждений**

Заполните анкету и получите **демо-доступ**

Закажите **пилотный проект** для тестирования функционала с точки зрения персонального использования и контроля подведомственных учреждений

Проконсультируйтесь со специалистами компании «КСБ-СОФТ»

ООО «КСБ-СОФТ»
ksb-soft.ru
8 (8352) 322-322
sec@keysystems.ru

КСБ-СОФТ