Федеральный закон 187-ФЗ «О безопасности КИИ РФ»

Антон Шипулин
CISSP, CEH, CSSA

Менеджер по развитию решений
по безопасности критической инфраструктуры
Лаборатория Касперского

KASPERSKY lab

Сферы деятельности объектов КИИ попадающие под закон

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

Основные источники принятия решения об отнесении к сфере

- ОКВЭД
- Устав
- Лицензии

Основные мероприятия по 187 ФЗ

- провести категорирование объектов КИИ (3 категории + «Незначимые»);
- обеспечить интеграцию (встраивание) в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА);
- принять организационные и технические меры по обеспечению безопасности объектов КИИ.

Процедура категорирования

- Определение субъектом КИИ перечня всех процессов
- Выявление критических процессов
- Определение объектов КИИ участвующих в критических процессах
- Формирование перечня объектов КИИ, подлежащих категорированию.
- Оценку масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ в соответствии с показателями, указанных в Правилах.
- Присвоение каждому из объектов КИИ одной из категорий значимости.

Показатели критериев значимости

Социальная значимость

- Причинение ущерба жизни и здоровью людей (3-я категория – до 50 чел.; 2-я – 50-500 чел., 1-я – более 500 чел.)
- Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения (в том числе водоснабжения и канализации), транспортной инфраструктуры, сети связи
- Отсутствие доступа к государственной услуге (3-я категория – 24-12 часов; 2-я – 12-6 часов, 1-я – менее 6 часов)

Политическая значимость

- Прекращение или нарушение функционирования государственного органа
- Нарушение условий международного договора Российской Федерации

Экономическая значимость

- Возникновение ущерба субъекту КИИ (снижение уровня дохода на 5-10, 10-15 и более 15% для 3-й, 2-й и 1-й категории соответственно)
- Возникновение ущерба бюджетам Российской Федерации
- Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом КИИ

Экологическая значимость (Вредные воздействия на окружающую среду)

Значимость для обеспечения обороны страны, безопасности государства и правопорядка

- Прекращение или нарушение функционирования пункта управления/ситуационного центра, информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, снижение показателей государственного оборонного заказа

Что после категорирования?

Незначимые объекты КИИ

- Интеграция с ГосСОПКА (Достаточно передачи данных об инцидентах)

Значимые объекты КИИ

- Интеграции в ГосСОПКА (Развертывание технических средств)
- Создание системы безопасности ЗОКИИ (состав на основе категории)
- Реагирование на компьютерные инциденты
- Предоставление на объект КИИ беспрепятственный доступ регуляторам и выполнять их предписания по результатам проверок.

Обеспечение безопасности объектов КИИ

Шаг 1. Формирование требований

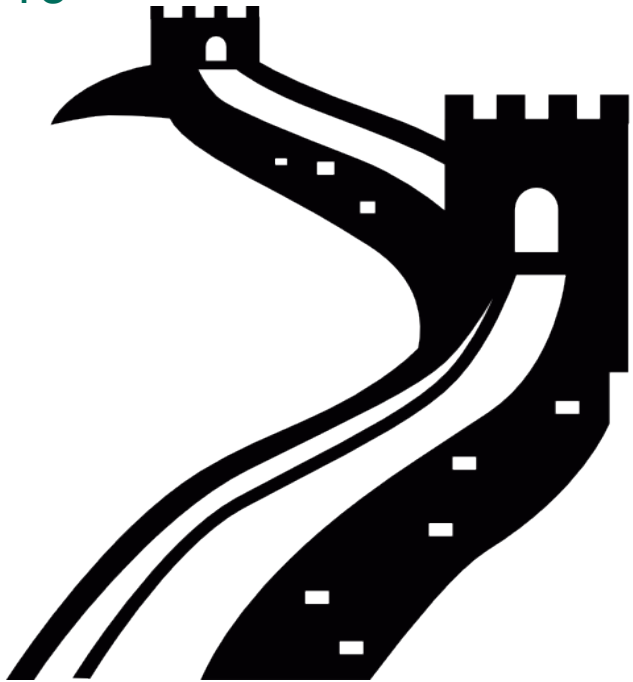
- Формирование требований по ОБ, разработка ТЗ

Шаг 2. Разработка орг. и тех. мер по ОБ

- Моделирование угроз
- Проектирование системы безопасности
- Разработка эксплуатационной документации

Шаг 3. Внедрение орг. и тех. мер по ОБ

- Установка и настройка СЗИ
- Разработка документов по ОБ
- Предварительные испытания
- Опытная эксплуатация
- Выявление уязвимостей
- Приемочные испытания



Обеспечение безопасности объектов КИИ

Шаг 4. ОБ во время эксплуатации

- Планирование мероприятий по ОБ
- Периодический анализ угроз
- Администрирование подсистемы безопасности
- Управление подсистемой безопасности
- Обеспечение действий в нештатных ситуациях
- Информирование и обучение персонала
- Контроль за соблюдение безопасности

Шаг 5. ОБ при выводе из эксплуатации

- Архивирование информации
- Уничтожение (стирание) данных и/или носителей
- Архивирование или уничтожение ЭД

Что такое ГосСОПКА

- Совокупность технической составляющей, обслуживающего персонала и регламентов, предназначенная для обеспечения и контроля состояния информационной безопасности в Российской Федерации и диппредставительствах страны за рубежом
- Техническая составляющая (средства ОПЛ КА) будет состоять из центров ГосСОПКА, объединённых в иерархическую структуру по ведомственно-территориальному признаку, и подключённых к ним технических средств, установленных в конкретных объектах КИИ
- Государство будет выступать в качестве регулятора и координатора (не собственника)
- Единого собственника не будет: каждый из элементов будет принадлежать тому, кто за него заплатил

Решения «Лаборатории Касперского» для центров ГосСОПКА

Функции центра ГосСОПКА / объект КИИ	Продукты «Лаборатории Касперского»	Сервисы «Лаборатории Касперского»
Инвентаризация информационных ресурсов	Не имеется*	Частично может быть выполнено при работах по анализу защищённости
Выявление уязвимостей информационных ресурсов	Не имеется*	Анализ защищённости (в первую очередь, тестирование на проникновение – «penetration testing»)
Анализ угроз информационной безопасности	Не имеется*	Набор сервисов по анализу угроз информационной безопасности
Повышение квалификации персонала информационных ресурсов	Kaspersky Awareness	Сервисы по обучению (навыкам использования конкретных средств, повышение уровня осведомлённости в области информационной безопасности и т.д.)
Обеспечение процесса обнаружения компьютерных атак	KATA, KICS, KES, KSV, KPSN, KDP	Сервисы по анализу целевых компьютерных атак и компьютерных вирусов
Анализ данных о событиях безопасности	KATA, KICS, KES, KPSN, KDP, как источники соответствующей информации; KSM и KSC, как её агрегаторы	Набор сервисов по анализу угроз информационной безопасности
Регистрация инцидентов	KATA, KICS, KES, KPSN, KDP, как источники соответствующей информации; KSM и KSC, как её агрегаторы	Kaspersky Managed Protection
Реагирование на инциденты и ликвидация их последствий	KATA EDR (релиз в начале 2018 года)	Сервисы по расследованию инцидентов
Установление причин инцидентов	Не имеется*	Сервисы по расследованию инцидентов
Анализ результатов устранения последствий инцидентов	Не имеется*	Может быть реализовано путём добавления соответствующих работ в контракт по расследованию инцидентов

Решения «Лаборатории Касперского» для центров ГосСОПКА

Функция обеспечения информационной безопасности	Продукты «Лаборатории Касперского»	Место установки
Антивирусная защита (включая регистрацию инцидентов, блокирование, предупреждение и ликвидация последствий)	KES, KESS, KSV, KICS, KPSN	Узлы (сервера и рабочие станции) контролируемого объекта КИИ
Обнаружение компьютерных атак (включая регистрацию инцидентов, блокирование, предупреждение и ликвидация последствий	KES, KSV, KESS, KPSN	Узлы (сервера и рабочие станции) контролируемого объекта КИИ
	KATA, KICS, Защита почты, серверов совместной работы, Proxy серверов.	Каналы связи контролируемого объекта КИИ
	KICS	Сервера и рабочие станции SCADA, каналы связи АСУ ТП
	KDP	Каналы связи контролируемого объекта КИИ (возможна установка на площадках операторов связи и/или маршрутизация сетевого трафика через специализированные центры «очистки»)
Межсетевое экранирование	KES, KSV	Узлы (сервера и рабочие станции) контролируемого объекта КИИ (персональное межсетевое экранирование на уровне конкретного узла)
	Не имеется	Каналы связи контролируемого объекта КИИ («очистка» сетевого трафика при поступлении соответствующей команды, временная блокировка внешних IP-адресов)
Агрегация информации мониторинга/регистрация, анализ и установление причин инцидентов	KATA, KSC	Центр ГосСОПКА (возможен аутсорсинг)
Комплексная защита от компьютерных атак	KATA, KES, KSV, KICS, KDP	Серверная группировка (сервера соответствующего назначения), мобильные устройства, базы данных

Ответственность

№	Новая статья 274.1 в УК РФ (дела по ней рассматривает ФСБ)	Ответственность
1	Создание, распространение, использование ПО либо иной компьютерной информации для неправомерного воздействия на КИИ	До **5 лет**, со штрафом
2	Неправомерный доступ к охраняемой информации в КИИ, повлекший причинение вреда КИИ	До **6 лет**, со штрафом
3	Нарушение правил эксплуатации и правил доступа, повлекшее причинение вреда КИИ	До **6 лет**, с лишением права занимать должность
4	Все предыдущие деяния по сговору или с использованием служебного положения	До **8 лет**, с лишением права занимать должность
5	Все предыдущие деяния, повлекшие тяжкие последствия	До **10 лет**, с лишением права занимать должность

Давайте обсудим?

Антон Шипулин
CISSP, CEH, CSSA
Менеджер по развитию решений по безопасности критической инфраструктуры

Лаборатория Касперского
Москва, Ленинградское шоссе, д.39А, стр.3
T: (495) 797 8700 #1746
Anton.Shipulin@kaspersky.com
www.kaspersky.ru
https://ics.kaspersky.com
https://ics-cert.kaspersky.ru

KASPERSKY lab

Присоединяйтесь к сообществу

RUSCADASEC.RU

RUSCADASEC RU | EN Главная Группы Встречи Контакты

RUSCADASEC - это некоммерческая инициатива по развитию русскоязычного международного открытого сообщества специалистов про промышленной кибербезопасности / кибербезопасности АСУ ТП. Целями инициативы являются повышение осведомлённости и квалификации специалистов по безопасности и промышленной автоматизации, развитие профессиональных связей между специалистами и организациями, содействие развитию рынка, развитие связей с профильными международными сообществами, и в итоге повышение уровня безопасности на промышленных предприятиях. Инициатива включает в себя онлайн площадки, живые встречи и профильные конференции, в рамках которых участники следят за текущим состоянием темы, обсуждают организационные и технические вопросы, обмениваются опытом, идеями. Всегда рады новым участникам сообщества и открыты к идеям по развитию сообщества и помощи в их реализации. Присоединяйтесь к нам!

Наши онлайн площадки

Присоединяйся к чату Telegram

Присоединяйся к группе Facebook

Следи за нами в Twitter

Дружественные глобальные онлайн площадки

SANS ICS Industrial Control Systems — SANS ICS Community forum

SCADASEC mailing list

Встречи сообщества и дружественные конференции

Неформальные встречи

COLABORATORY Industrial Cybersecurity Meetup

Industrial CyberSecurity Meetup

КОНФЕРЕНЦИЯ Информационная безопасность АСУ ТП КВО

Конференция ИБ АСУ ТП КВО

KASPERSKY Industrial Cybersecurity Conference

Industrial Cybersecurity Conference

phd Positive Hack Days

Positive Hack Days

АИС

Безопасность КВО ТЭК

Связь с администраторами

Шипулин Антон
LinkedIn | Facebook | Twitter | Telegram

Тамеев Даниил
LinkedIn | Facebook

Подольный Вадим
Linkedin | Facebook

Карпов Илья
LinkedIn | Facebook | Telegram

Дружинин Евгений
Facebook | Telegram

Савков Борис
Telegram