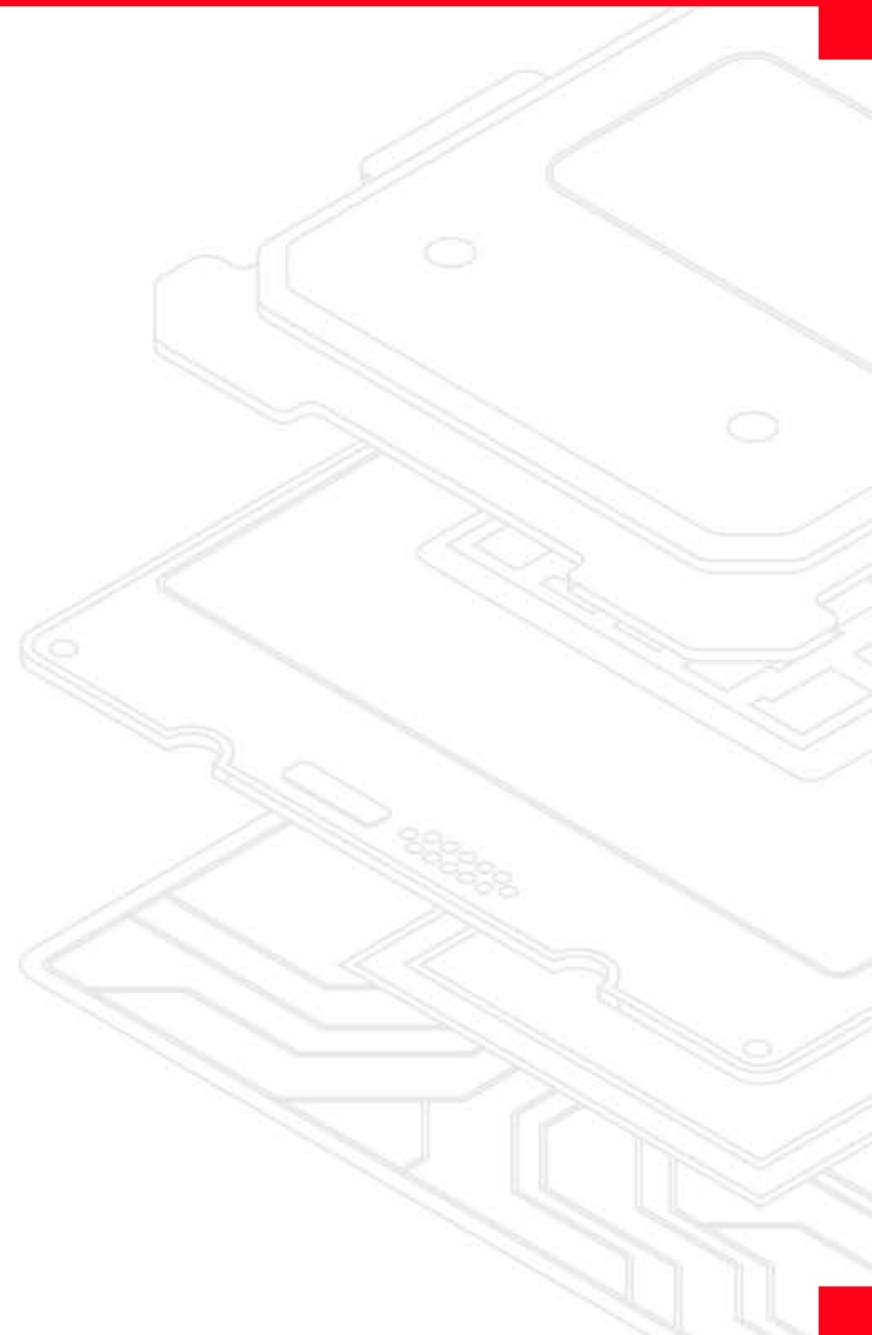


НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

О взаимодействии субъектов ГосСОПКА с Национальным координационным центром по компьютерным инцидентам

Анатолий Грачев



187-ФЗ «О безопасности объектов КИИ Российской Федерации»



Недостаточная защищенность информационных ресурсов

ФСБ России постоянно фиксирует попытки скрытого внедрения ВПО в информационные системы различных секторов экономики Российской Федерации

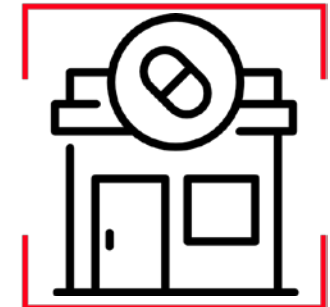
Успешные атаки осуществляются и на системы, на защиту которых потрачены немалые средства



Органы
государственной власти



Юридические лица



Индивидуальные
предприниматели

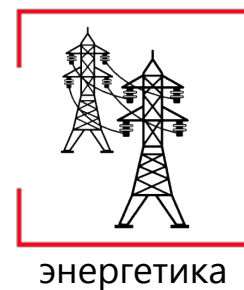
Перечень дополнительных НПА к 187-ФЗ

 ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ П Р И К А З № _____ Москва ПОЛОЖЕНИЕ о Национальном координационном центре по компьютерным инцидентам № 366 от 24.07.2018	 ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ П Р И К А З № _____ Москва Перечень информации, предоставляемой в ГосСОПКА № 367 от 24.07.2018	 ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ П Р И К А З № _____ Москва ПОРЯДОК обмена информацией о компьютерных инцидентах № 368 от 24.07.2018
 ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ П Р И К А З № _____ Москва Порядок, технические условия установки и эксплуатации средств ГосСОПКА	 ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ П Р И К А З № _____ Москва ПОРЯДОК информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятие мер ликвидации последствий	 ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ П Р И К А З № _____ Москва ТРЕБОВАНИЯ к средствам обнаружения, предупреждения, ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

Охват информационных ресурсов системой ГосСОПКА



Возможные инциденты в объектах КИИ



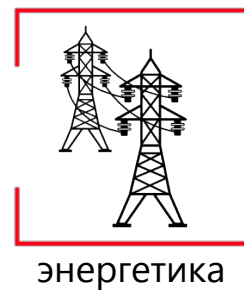
Атаки на процессинг банковских карт?

Возможные инциденты в объектах КИИ



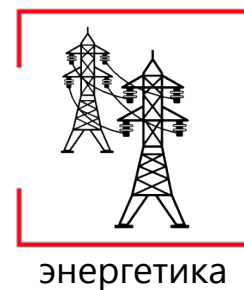
Атаки на трейдинговые системы?

Возможные инциденты в объектах КИИ



Компрометация АРМ КБР?

Возможные инциденты в объектах КИИ



Воздействия на банкоматы?

Проблема противодействия компьютерным атакам

Владельцы информационных ресурсов зачастую замалчивают факты успешных компьютерных атак на их системы и сети, опасаясь ущерба деловой репутации или из-за нежелания проводить организационно-технические мероприятия



Категории и типы компьютерных инцидентов

Категории инцидентов	Типы инцидентов
Внедрение вредоносного программного обеспечения	Заражение ВПО
Распространение ВПО	Использование контролируемого ресурса для распространения ВПО
	Попытки внедрения модулей ВПО
Нарушение или замедление работы контролируемого информационного ресурса	Компьютерная атака типа “отказ в обслуживании”
	Распределенная компьютерная атака типа “отказ в обслуживании”
	Несанкционированный вывод системы из строя
	Непреднамеренное отключение системы (без злого умысла)
Несанкционированный доступ в систему	Успешная эксплуатация уязвимости
	Компрометация учетной записи
Попытки НСД в систему или к информации	Попытки эксплуатации уязвимости
	Попытки авторизации в информационном ресурсе
Сбор сведений с использование ИКТ	Сканирование информационного ресурса
	Прослушивание (захват) сетевого трафика
	Социальная инженерия
Нарушение безопасности информации	Несанкционированное разглашение информации
	Несанкционированное изменение информации
Распространение информации с неприемлемым содержанием	Рассылка незапрашиваемых электронных сообщений
	Публикация запрещенной законодательством РФ информации
Мошенничество с использованием ИКТ	Злоупотребление при использовании информационного ресурса
	Публикация мошеннического информационного ресурса
Наличие уязвимости или недостатков конфигурации	

I – по телекоммуникационным каналам сети Интернет:

- 1) заполнением унифицированной карточки сообщения на портале НКЦКИ
- 2) направлением Пакетов с унифицированными карточками сообщений

II – посредством электронной, почтовой, факсимильной и телефонной связи

I – Интерактивный обмен запросами и уведомлениями через портал НКЦКИ (т.н. Личный кабинет субъекта ГосСОПКА)

II – Автоматизированный обмен Пакетами с унифицированной карточкой сообщения через техническую инфраструктуру НКЦКИ

Пакет – электронный файл в формате JSON

Для взаимодействия используется RESTful API в технической инфраструктуре НКЦКИ

Благодарю за внимание

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ