Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тамбовский государственный технический университет»

XXI Международная конференция
«Информатика: проблемы, методы, технологии» (IPMT-2021)

Синтез комплексной системы обнаружения компьютерных инцидентов безопасности в критических информационных инфраструктурах

Авторы: Тихомирова Алина Александровна
Яковлев Алексей Вячеславович
Савилова Ульяна Андреевна

Понятие КИИ

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА — совокупность всех объектов КИИ и используемых ими сетей электросвязи

ОБЪЕКТЫ КИИ

информационные системы

информационно-телекоммуникационные сети

автоматизированные системы управления

СУБЪЕКТЫ КИИ

государственные органы

государственные учреждения

российские юр. лица, ИП (которые владеют объектами КИИ и обеспечивают их взаимодействие)

ОТРАСЛИ КИИ

здравоохранение, наука, транспорт, связь, финансы, атомная и топливная энергетика, промышленность (горнодобывающая, металлургическая, химическая, оборонная, ракетно-космическая)

Этапы реализации требований 187-ФЗ

Категорирование объектов КИИ

ПП-127

- Инвентаризация процессов
- Определение критических процессов
- Выделение объектов КИИ
- Оценка возможных последствий (Анализ угроз)
- Сопоставление с показателями (ПП-127)
- Присвоение категории

Включение в Перечень объектов КИИ (ФСТЭК)

Безопасность значимых объектов КИИ

Приказы ФСТЭК 235, 239

- Защита от неправомерного доступа к информации, обрабатываемой объектом КИИ
- Защита от негативных воздействий, в результате которых может быть нарушено и (или) прекращено функционирование объекта КИИ
- Восстановление функционирования объектов КИИ

Создание СОИБ

Взаимодействие с ГосСОПКА

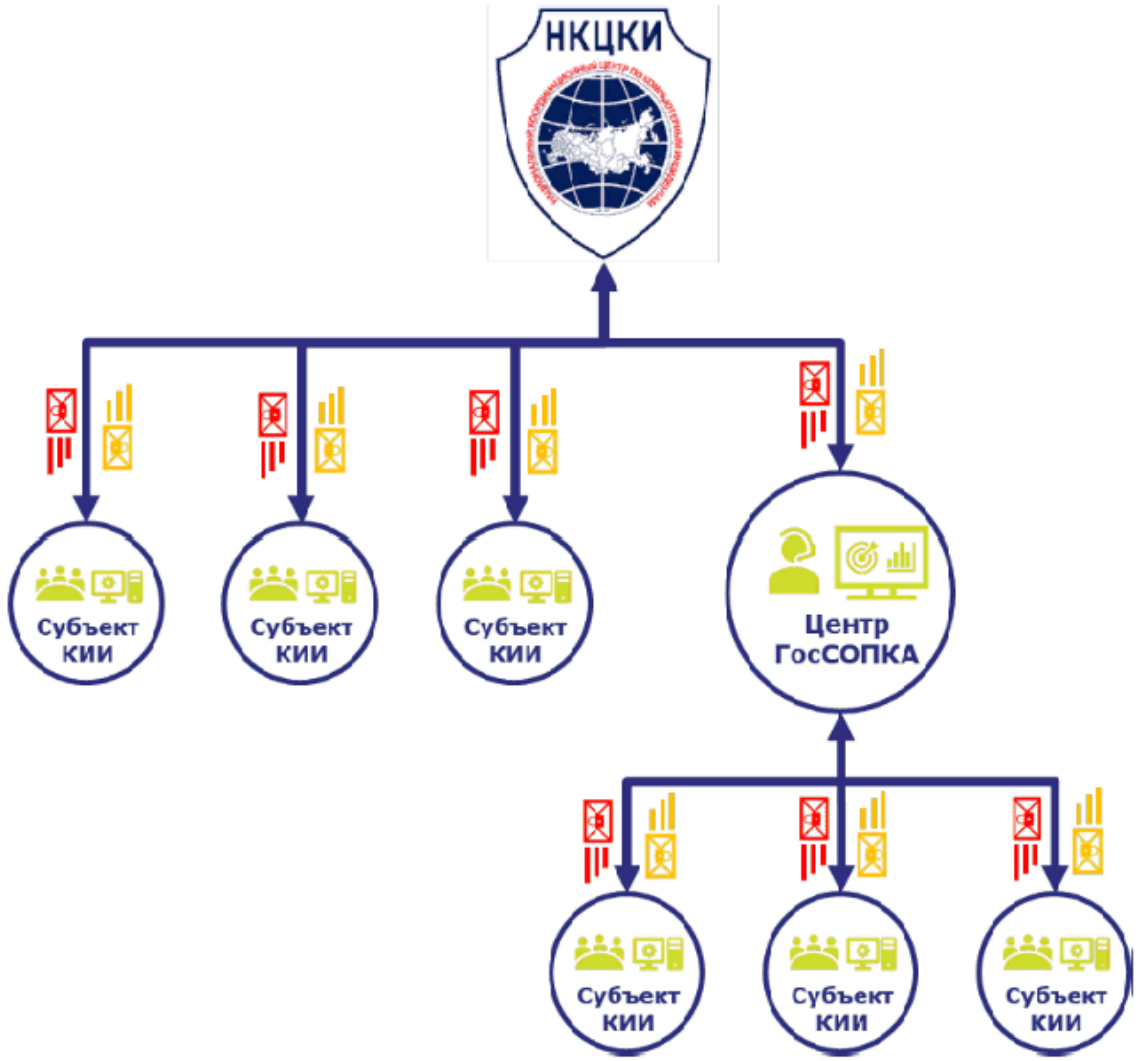
НКЦКИ

- Субъекты КИИ, у которых есть значимые объекты КИИ, обязаны подключиться к ГосСОПКА

ГОССОПКА

Взаимодействие субъектов КИИ с ГосСОПКА

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки



Базовые категории и типы компьютерных инцидентов безопасности

Категория компьютерного инцидента и его международное обозначение	Тип компьютерного инцидента и его международное обозначение
Заражение вредоносным программным обеспечением (malware)	Внедрение в контролируемый объект КИИ модулей вредоносного программного обеспечения (malware infection)
Распространение вредоносного программного обеспечения (malware distribution)	Использование контролируемого объекта КИИ для распространения вредоносного программного обеспечения (malware command and control)
Нарушение или замедление работы контролируемого информационного ресурса (availability)	Компьютерная атака типа «отказ в обслуживании», направленная на контролируемый объект КИИ (dos)
	Распределенная компьютерная атака типа «отказ в обслуживании», направленная на контролируемый объект КИИ (ddos)
	Несанкционированный вывод объекта КИИ из строя (sabotage)
	Непреднамеренное отключение объекта КИИ (outage)
Несанкционированный доступ в систему (intrusion)	**Успешная эксплуатация уязвимости на контролируемом объекте КИИ (application compromise)**
	Компрометация учетной записи на контролируемом объекте КИИ (account compromise)
Сбор сведений с использованием информационно-коммуникативных технологий (information gathering)	Прослушивание (захват) сетевого трафика контролируемого объекта КИИ (traffic hijacking)
	Социальная инженерия, направленная на компрометацию объекта КИИ (social engineering)
Нарушение безопасности информации (information content security)	Несанкционированное разглашение информации, обрабатываемой на контролируемом объекте КИИ (unauthorised access)
	Несанкционированное изменение информации, обрабатываемой на контролируемом объекте КИИ (unauthorised modification)
Распространение информации с неприемлемым содержимым (abusive content)	Рассылка спам-сообщений с контролируемого объекта КИИ (spam)
	Публикация на контролируемом объекте КИИ запрещенной законодательством РФ информации (prohibited content)

Структура ГосСОПКА

Синтез комплексной системы обнаружения компьютерных инцидентов безопасности в КИИ

Множество альтернатив средств обнаружения инцидентов

Средства обнаружения инцидента malware	Средства обнаружения инцидента availability	Средства обнаружения инцидента information gathering	Средства обнаружения инцидента intrusion
Norton Antivirus Plus	Group-IB Fraud Hunting Platform	Kaspersky Anti Targeted Attack	Страж NT 4.0
McAfee Total Protection	Anti-DDoS Qrator	Kaspersky Industrial CyberSecurity	Secret Net 7
Kaspersky Total Security	CloudFlare DDoS Attack Protection	ViPNet IDS HS	ViPNet SafeBoot 1.4
Kaspersky Security Center 10	Kaspersky DDoS Protection	Kaspersky Private Security Network	Secret Disk 5
Dr.Web Enterprise Security Suite	ViPNet TIAS	Детектор атак «Континент»	Соболь 4.0
ESET NOD32 Secure Enterprise Pack	ViPNet IDS 2.0	Рубикон	vGate-S 4.1
Avira Total Security Suite	Cisco ASA FirePOWER 6.2	Аргус 1.5	Secret Net LSP

Синтез комплексной системы обнаружения компьютерных инцидентов безопасности в КИИ

Усечение множества альтернатив средств обнаружения инцидентов

Средства обнаружения инцидента malware	**Средства обнаружения инцидента availability**	**Средства обнаружения инцидента information gathering**	**Средства обнаружения инцидента intrusion**
Kaspersky Security Center 10	Kaspersky DDoS Protection	ViPNet IDS HS	Secret Net 7
Dr.Web Enterprise Security Suite	ViPNet TIAS	Детектор атак «Континент»	ViPNet SafeBoot 1.4
ESET NOD32 Secure Enterprise Pack	ViPNet IDS 2.0	Рубикон	Secret Disk 5
	Cisco ASA FirePOWER 6.2	Аргус 1.5	Соболь 4.0
			Secret Net LSP

Синтез комплексной системы обнаружения компьютерных инцидентов безопасности в КИИ

Сравнение альтернатив средств обнаружения заражения вредоносным программным обеспечением

Альтернатива	Kaspersky Security Center 10	Dr.Web Enterprise Security Suite	ESET NOD32 Secure Enterprise Pack	Сумма баллов
Kaspersky Security Center 10	–	1	1	**2**
Dr.Web Enterprise Security Suite	0	–	0	0
ESET NOD32 Secure Enterprise Pack	0	1	–	1

Лучшей альтернативой средства обнаружения заражения вредоносного программного обеспечения для синтезируемой системы является Kaspersky Security Center 10

Синтез комплексной системы обнаружения компьютерных инцидентов безопасности в КИИ

Сравнение альтернатив средств обнаружения инцидентов нарушения или замедления работы контролируемого информационного ресурса

Альтернатива	Kaspersky DDoS Protection	ViPNet TIAS	ViPNet IDS 2.0	Cisco ASA FirePOWER 6.2	Сумма баллов
Kaspersky DDoS Protection	–	1	0	0	1
ViPNet TIAS	0	–	0	0	0
ViPNet IDS 2.0	1	1	–	1	**3**
Cisco ASA FirePOWER 6.2	1	1	0	–	2

Лучшая альтернатива средства обнаружения компьютерных инцидентов нарушения или замедления работы контролируемого информационного ресурса для синтезируемой системы – ViPNet IDS 2.0

Синтез комплексной системы обнаружения компьютерных инцидентов безопасности в КИИ

Сравнение альтернатив средств обнаружения несанкционированного сбора сведений

Альтернатива	ViPNet IDS HS	Детектор атак «Континент»	Рубикон	Аргус 1.5	Сумма баллов
ViPNet IDS HS	–	1	1	1	**3**
Детектор атак «Континент»	0	–	0	1	1
Рубикон	0	1	–	0	1
Аргус 1.5	0	0	1	–	1

Лучшей альтернативой средства обнаружения несанкционированного сбора сведений с использованием информационно-коммуникативных технологий для синтезируемой системы является ViPNet IDS HS

Синтез комплексной системы обнаружения компьютерных инцидентов безопасности в КИИ

Сравнение альтернатив средств обнаружения несанкционированного доступа в систему

Альтернатива	Secret Net 7	ViPNet SafeBoot 1.4	Secret Disk 5	Соболь 4.0	Secret Net LSP	Сумма баллов
Secret Net 7	–	1	1	1	1	**4**
ViPNet SafeBoot 1.4	0	–	0	1	1	2
Secret Disk 5	0	1	–	1	1	3
Соболь 4.0	0	0	0	–	1	1
Secret Net LSP	0	0	0	0	–	0

Лучшей альтернативой средства обнаружения несанкционированного доступа для синтезируемой системы будет Secret Net 7

СПАСИБО ЗА ВНИМАНИЕ!