infotecs

Решения от InfoTeCS
Защита от компьютерных атак

Григорьев Дмитрий
Руководитель обособленного подразделения

disclaimer

Регулирование безопасности КИИ сейчас находится в фазе активной подготовки нормативно-правовых актов. Презентация является лишь экспертным мнением, основанном на изучении существующих документов и личном опыте.

Для получения более полной информации о подключении своих организаций к ГосСОПКА направляйте соответствующие запросы в Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и другие подразделения ФСБ России отвечающие за координацию в данной сфере.

©2017, ОАО «ИнфоТеКС».

Элементы ГосСОПКА

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

©2017, ОАО «ИнфоТеКС».

Регулирование вопросов защиты ГИС, ПДн, КИИ

- Приказ ФСТЭК России от 14 марта 2014 г. N 31 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
- Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

©2017, ОАО «ИнфоТеКС».

Регулирование вопросов центров мониторинга компьютерных атак

- «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», № 149/2/7-200 от 24.12.2016 г.
- Временный порядок включения в состав ГосСОПКА корпоративных центров

- Постановление Правительства РФ от 15.06.2016 N 541 "О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам лицензирования отдельных видов деятельности»
- Перечень контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержден Директором ФСТЭК России в апреле 2017 г.

©2017, ОАО «ИнфоТеКС».

Что нас ждет?

Федеральный закон от 26 июля 2017 г. N 187 «О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральный закон от 26.07.2017 N 193-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

Федеральный закон от 26.07.2017 N 194-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации»

©2017, ОАО «ИнфоТеКС».

Ожидаемые НПА

В настоящее время ведется разработка нормативных и правовых актов, регулирующих вопросы взаимодействия с ГосСОПКА. До конца года ожидаются:

- положение по ведомственным и корпоративным центрам ГосСОПКА;
- регламент взаимодействия с НКЦКИ.

Более 10 НМД от ФСТЭК России

- ❑ Проект Постановления Правительства РФ "Об утверждении показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, а также порядка и сроков осуществления их категорирования" (по состоянию на 25.09.2017) (подготовлен ФСТЭК России)

- ❑ Проект Указа Президента РФ "О федеральном органе исполнительной власти, уполномоченном в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации" (по состоянию на 30.08.2017)

©2017, ОАО «ИнфоТеКС».

Федеральный закон от 26 июля 2017 г. N 187 «О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Настоящий Федеральный закон вступает в силу с **1 января 2018 года.**

©2017, ОАО «ИнфоТеКС».

Федеральный закон от 26 июля 2017 г. N 187 «О безопасности критической информационной инфраструктуры Российской Федерации»

Субъекты критической информационной инфраструктуры

- государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели
- которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления,
- функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности
- российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей

©2017, ОАО «ИнфоТеКС».

Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются

ТЗКИ

- предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации

ТЗКИ

- недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры

ТЗКИ

- восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации

ГосСОПКА

- непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

©2017, ОАО «ИнфоТеКС».

Меры по обеспечению безопасности критической информационной инфраструктуры РФ

Общие обязанности субъекта КИИ	Категорировать объекты КИИ и уведомить ФСТЭК России обо всех своих объектах и присвоенных категориях
	Обязан выполнить требования НМД ФСТЭК России по ОБИ КИИ
	Обязан реагировать на КА в порядке утвержденном ФСБ России
	Обязан незамедлительно информировать ФСБ России об инциденте
	Обязан оказать содействие должностным лицам ФСБ России в деятельности, связанной с предупреждением, обнаружением и ликвидацией последствий инцидента
	Обязан обеспечить выполнение порядка, ТУ установки и эксплуатации ТС ГосСОПКА, если они установлены на объекте КИИ

©2017, ОАО «ИнфоТеКС».

Меры по обеспечению безопасности критической информационной инфраструктуры РФ

К обязанностям оператора связи отнесено обеспечение выполнения утвержденных в соответствии с Федеральным законом "О безопасности критической информационной инфраструктуры Российской Федерации" порядка, технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи и их сохранности, в случае их установки в сети электросвязи, используемой для организации взаимодействия объектов критической информационной инфраструктуры РФ

©2017, ОАО «ИнфоТеКС».

Федеральный закон от 26.07.2017 N 187-ФЗ обязывает субъекта КИИ

Обеспечить безопасность объекта КИИ

- Техническая защита конфиденциальной информации
- Провести категорирование объекта КИИ
- *Выполняем требования приказов ФСТЭК России 17, 21, 31*
- *Выполняем требования ФСБ России в части использования средств криптографической защиты информации*
- *Выполняем требования ведомственных нормативно-методических документов*
- Противодействие компьютерным атакам
- При необходимости установить технические средства сегмента ГосСОПКА
- Обеспечить взаимодействие объекта КИИ с ГосСОПКА
- Эксплуатация ведомственного (корпоративного) центра мониторинга подключенного к ГосСОПКА*

©2017, ОАО «ИнфоТеКС».

Технические средства сегмента ГосСОПКА

- Средства взаимодействия персонала
- Средства взаимодействия с Главным центром ГосСОПКА
- Средства инвентаризации информационных систем
- Средства выявления уязвимостей
- Средства анализа событий безопасности
- Средства учета и обработки инцидентов

©2017, ОАО «ИнфоТеКС».

Элементы ГосСОПКА

Создание собственного ведомственного центра / или подключение через ведомственный центр созданный в интересах объектов КИИ

Подключение через существующий корпоративный Центр мониторинга

©2017, ОАО «ИнфоТеКС».

Определение функций главного центра ГосСОПКА

©2017, ОАО «ИнфоТеКС».

Разделение функционала ГосСОПКА

Центры мониторинга

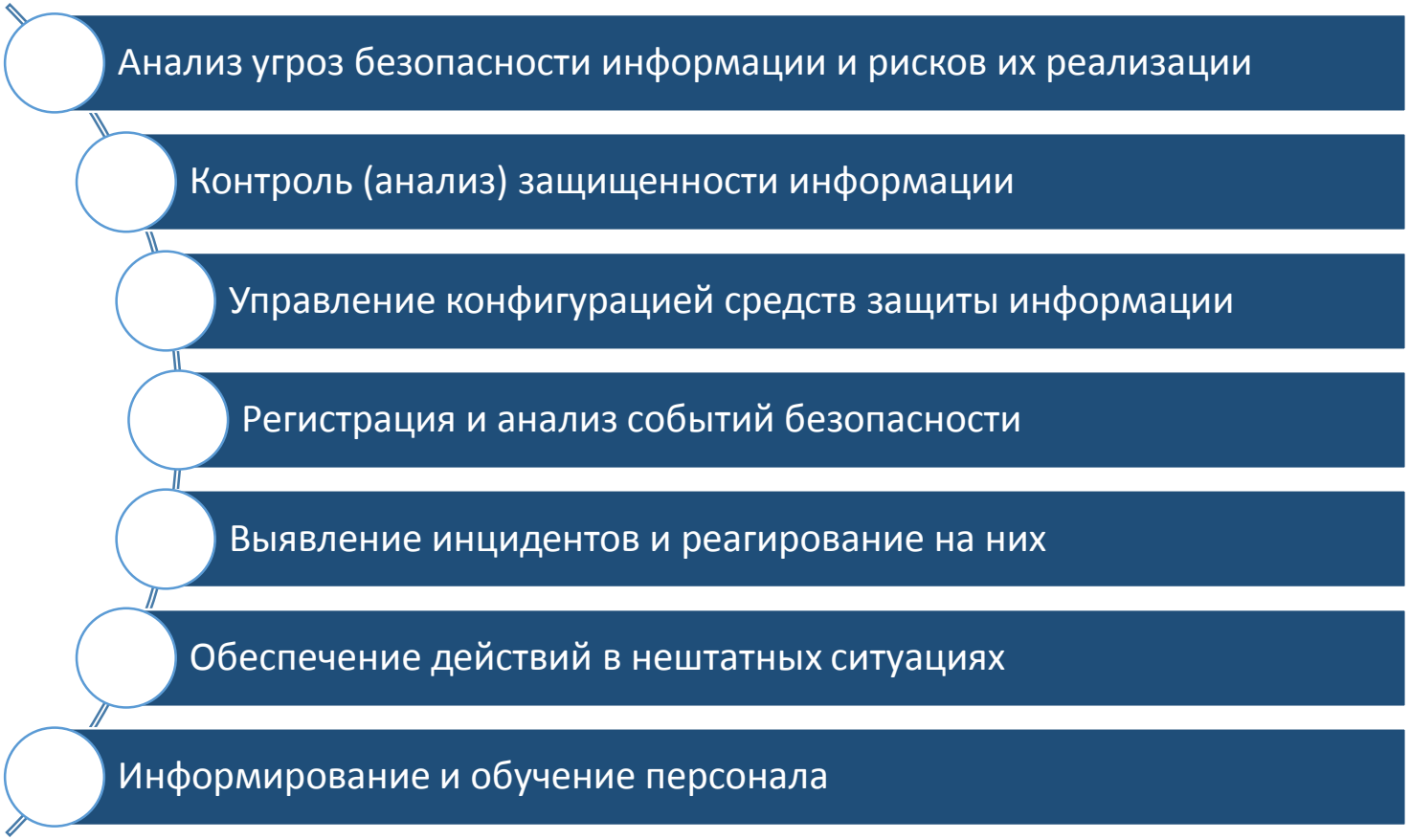
- формируют и предоставляют сведения об информационных ресурсах
- выявляют и анализируют сведения об уязвимостях ПО и оборудования
- проводят мероприятия по оценке степени защищенности
- **выявляют КА** в круглосуточном режиме
- осуществляют сбор и анализ сведений о КИ
- проводят **мероприятия по реагированию** и **ликвидации последствий** КА и КИ
- предоставляют в НКЦКИ сведения об инфраструктуре, состоянии защищенности, а также о выявляемых КА и КИ

ФСБ России

- предоставляет сведения об угрозах информационной безопасности в отношении информационных ресурсов, находящихся в зоне ответственности центров
- взаимодействует с уполномоченными органами иностранных государств, международными и неправительственными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты
- участвует в совместных мероприятиях по оценке степени защищенности
- участвует в мероприятиях по ликвидации последствий компьютерных атак

©2017, ОАО «ИнфоТеКС».

К мерам защиты информации используемым при реализации ГосСОПКА относятся



©2017, ОАО «ИнфоТеКС».

При создании Центров Мониторинга ГосСОПКА реализуются следующие функции

©2017, ОАО «ИнфоТеКС».

Что можем предложить?

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

- Подключение к Корпоративному центру мониторинга (ГосСОПКА)
- Подключение к системе управления инцидентами (Сервис)
- Подключение к системе управления уязвимостями (Сервис) *(Банк данных угроз безопасности информации (БДУ БИ) ФСТЭК России, National Vulnerability Database (NVD) NIST, Red Hat Bugzilla, Debian Security Bug Tracker, CentOS Mailing List)*
- Пентесты на проникновение в периметр
- Пентесты на проникновение в корпоративной сети
- Расследование инцидентов
- Выявление уязвимостей
- Анализ защищенности ПО и практики безопасной разработки (SDL)*

** Приказ № 31 п. 18.14. Меры по обеспечению безопасной разработки прикладного и специального программного обеспечения **должны обеспечивать выявление, анализ и устранение разработчиком уязвимостей программного обеспечения автоматизированной системы управления, определенного заказчиком, на всех этапах (стадиях) его разработки**, а также контроль принимаемых мер по выявлению, анализу и устранению уязвимостей со стороны заказчика и (или) оператора автоматизированной системы управления.*

©2017, ОАО «ИнфоТеКС».

Команда ЦМ ЗАО "Перспективный Мониторинг"

infotecs

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

CEH (Certified Ethical Hacker)

OSCP (Offensive Security Certified Professional)

CSA (Certified Security Analyst)

HFI (Computer Hacking Forensic Investigator)

eWPT (eLearnSecurity Web Application Penetration Tester)…

Аналитик уязвимостей

Сигнатурный аналитик

Аналитик IDS/COA

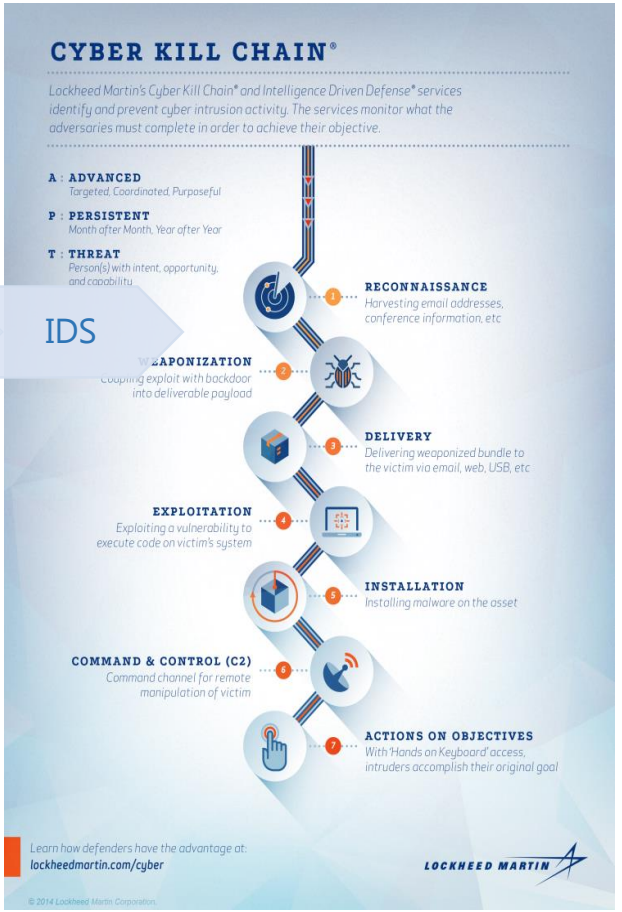
Аналитик инцидентов

Более 60 высококвалифицированных технических специалистов

©2017, ОАО «ИнфоТеКС».

Что можем предложить из средств защиты информации и СКЗИ?

Разведка	Firewall	IDS	VPN	
Выбор оружия	Threat Intelligence			
Доставка	DNS Security	E-mail Security	Web Security	IDS
Взлом	Firewall	IDS	Network Antivirus	
Установка	Host Firewall	Host Antivirus	Host VPN	
Управление	DNS Security	Web security	IDS	
Работа по целям	Anomaly analytics			

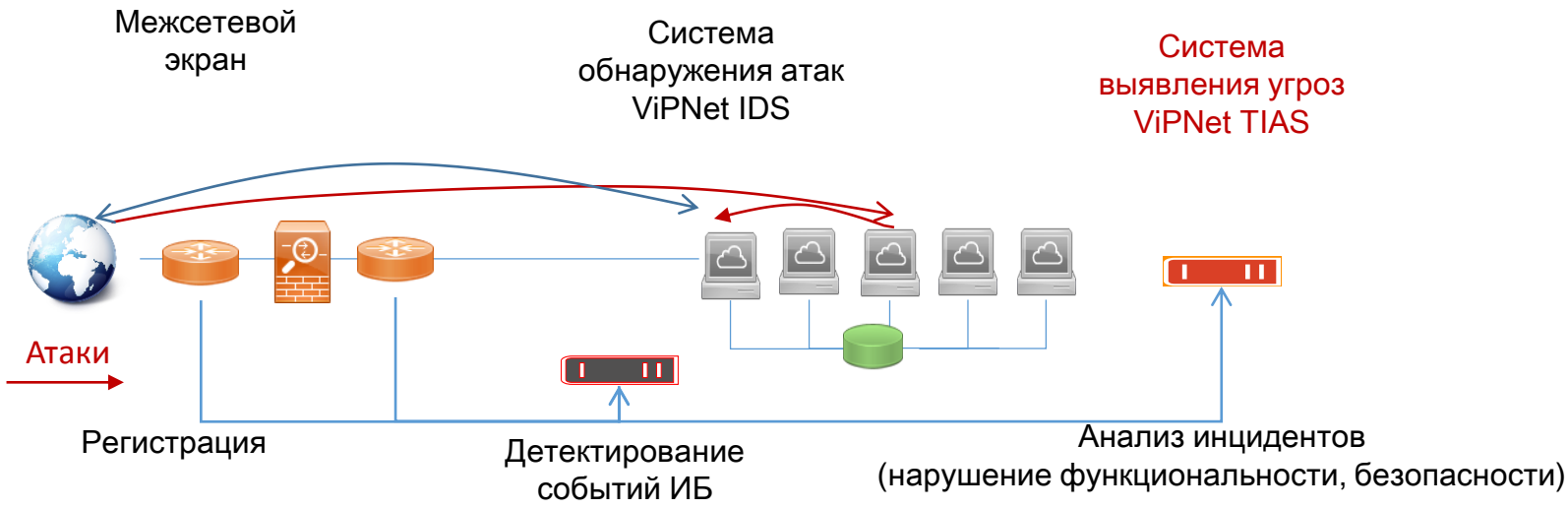


©2017, ОАО «ИнфоТеКС».

Что можем предложить?

©2017, ОАО «ИнфоТеКС».

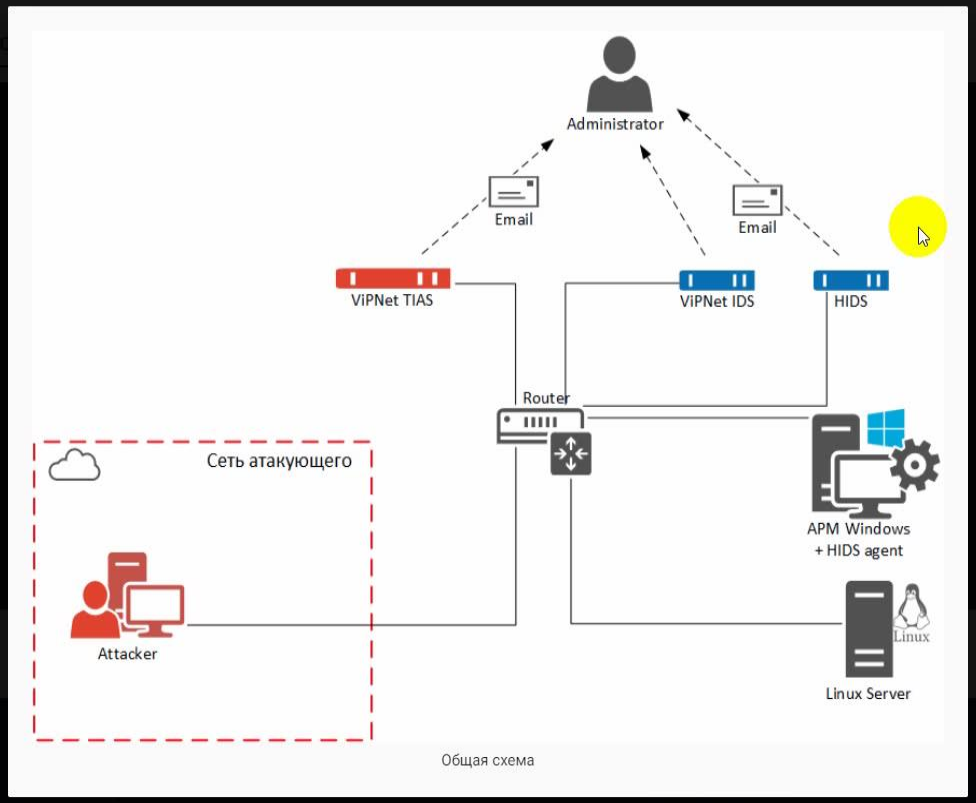
Threat Intelligence Analytics System оптимизация работы с событиями



Логи / события / инциденты

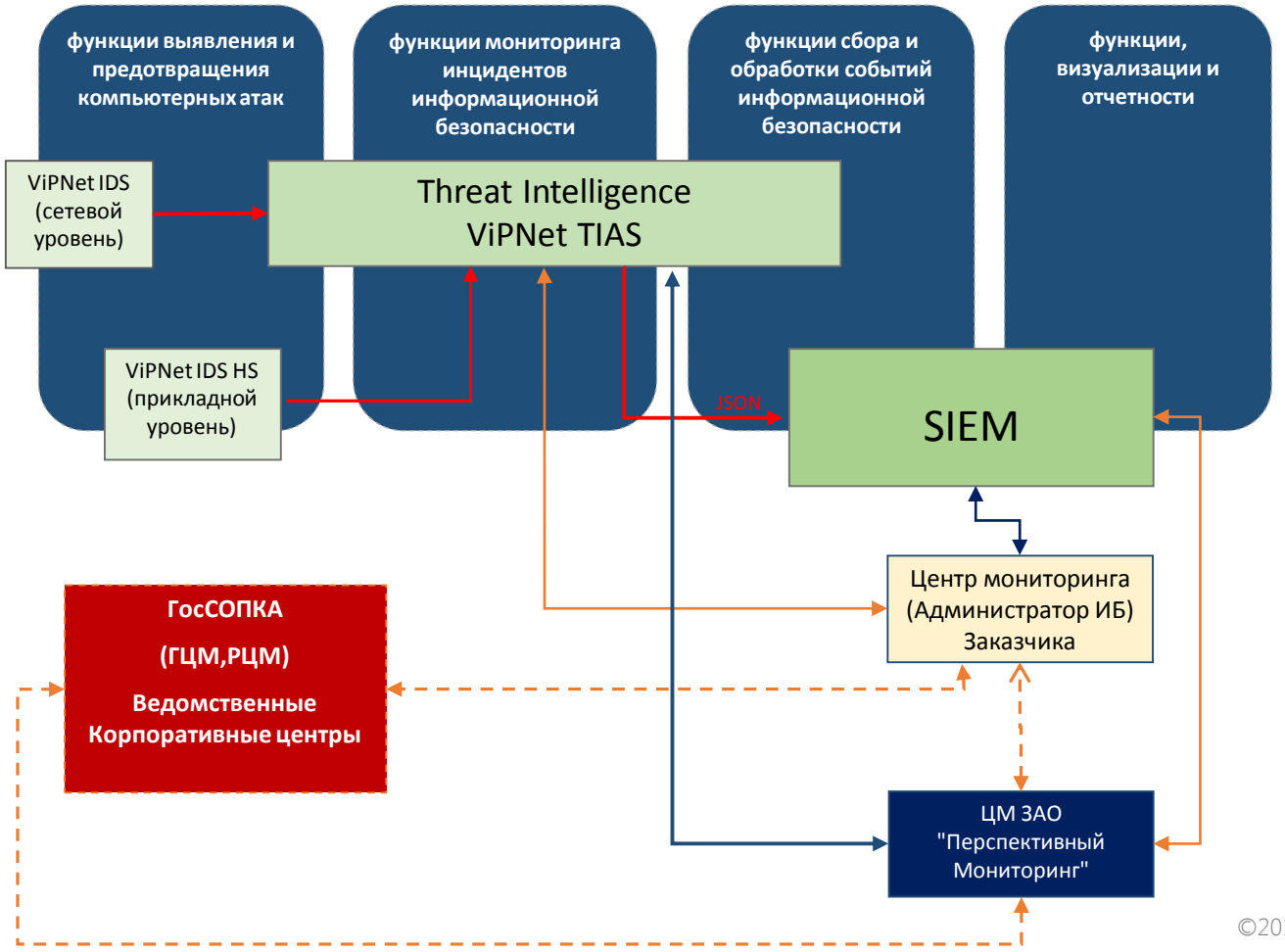
©2017, ОАО «ИнфоТеКС».

Демонстрация работы



©2017, ОАО «ИнфоТеКС».

TIAS и SIEM



©2017, ОАО «ИнфоТеКС».

Центр мониторинга разработка бюллетени при эпидемии

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

AM–2017–ALE–0627-02

Вредоносное ПО Petya

Описание угрозы	Программа шифровальщик Petya является модифицированной версией обнаруженного в 2016 году вредоносного ПО – Petya. Заражение происходит после открытия почтового вложения, которое эксплуатирует уязвимость CVE-2017-0199. Для распространения по другим компьютерам сети эксплуатирует уязвимость в SMB - MS17-010 (EternalBlue)
На что направлена	Семейство операционных систем Microsoft Windows
Способ реализации	Если после запуска вредонос получил привилегии администратора, и на компьютере отсутствует файл C:\Windows\perfc, то Petya подменяет загрузочную запись MBR, и в течение пары часов шифрует е файлы на диске, после чего компьютер перезагружается. Если административные привилегии отсутствуют, файлы шифруются без подмены загрузочной записи и перезагрузки Распространя PsExec, по T Для удаленно учетные запи EternalBlue
Дата выявления / публикации	27.06.17
Базовые меры по противодействию	Обновить MS Обновить MS Обновить баз Минимизиро Не скачивать Не переходит особенно есл Контролиров Заблокироват – 84.200. – hxxp:// – 111.90. – COFFE Для защиты е

	узлов не происходит.
Ссылки на источники	https://www.ptsecurity.com/ru-ru/about/news/283092/ https://xakep.ru/2017/06/27/petya-outbreak/ Сигнатуры для IDS доступны: http://amonitoring.ru/article/detail.php?ELEMENT_ID=178
Прочая информация	Для выявления атаки Petya могут быть использованы следующие индикаторы: – наличие файла **C:\Windows\perfc** – наличие файла **C:\Windows\perfc.dat** – наличие файла **C:\myguy.xls.hta** – наличие файла **%APPDATA%\10807.exe** – наличие задачи в планировщике Windows с пустым именем и действием на перезагрузку **"%WINDIR%\system32\shutdown.exe /r /f"** – запуск команды **Remote WMI, "process call create "C:\\Windows\\System32\\rundll32.exe \\"C:\\Windows\\perfc.dat\\" #1"** – срабатывание сигнатур на IDS: AM Exploit SMB MS-17-010 metasploit scan request (sid: 3006209) AM Exploit SMB MS-17-010 metasploit scan FID trans (sid: 3006210) AM Exploit SMB MS-17-010 Success STATUS_INSUFF_SERVER_RESOURCES response (sid: 3006211) AM Exploit EternalBlue check version SMB (sid: 3006267) AM Exploit EternalBlue overflow SMB (sid: 3006268) AM Exploit EternalBlue answer SMB x64 (sid: 3006269) AM Exploit EternalBlue answer SMB x86 (sid: 3006270)

©2017, ОАО «ИнфоТеКС».

Где получить информацию?

Представительство InfoTeCS в Новосибирске	*Дмитрий Григорьев* *Руководитель обособленного подразделения* *Фрунзе 86,оф. 705* *e-mail: Dmitry.Grigoryev@infotecs.ru* *T: +7 -965-821-6767* *T: +7(383) 319-04-68 доб. 3151* *Сайт: infotecs.ru* *Канал InfoTeCS Docs YouTube*
Исследовательская компания «Перспективный мониторинг»	Роман Кобцев Директор по развитию бизнеса *e-mail:* Roman.Kobtsev@amonitoring.ru Т.: +7 (495) 737-6192 доб.5273 *Сайт:* amonitoring.ru *Сайт:* habrahabr.ru
Компания Axoft	Михаил Богаченко Продакт-менеджер по направлению ИБ в регионе ул. Фрунзе 86, Офис 301, Новосибирск *e-mail:* mikhail.bogachenko@axoftglobal.com T: +7-903- 999-5949

Партнеры компании ИнфоТеКС
https://infotecs.ru/partners/list/

©2017, ОАО «ИнфоТеКС».

infotecs

Благодарим
за внимание!