



ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

# Как работает реальный центр ГосСОПКА

Георгий Караев

ЗАО «Перспективный мониторинг»

---

# Перспективный мониторинг —



- ГК «ИнфоТеКС»
- Центр мониторинга ИБ
- Пентесты, аудиты, редтиминг
- SDL
- OSINT
- Платформа киберучений



**МОСКОВСКАЯ  
БИРЖА**



  
**infotecs**®



**СПБМТСБ**

Санкт-Петербургская Международная  
Товарно-сырьевая Биржа



# Корпоративный Центр ГосСОПКА класса А с 2017 года

<...>

И мы с вторых печатаем портреты,  
Хоть в этом, право, и не их вина,  
Они - наш флаг, и дети всей планеты  
Проходят в школах эти имена.

Но я прошу, чтоб мы на этом свете,  
Собравшись вместе, хоть когда-нибудь,  
Не позабыли, славя первых этих,  
Всех настоящих первых помянуть.

А. Макаревич

28.02.2019



ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

3



# Центр мониторинга ЗАО «ПМ»



2014

год запуска

23

клиента

28 200

подключенных узлов

30

операторов,  
исследователей,  
аналитиков и  
инженеров

353 млн.

событий за 2018 г.

894

инцидента за 2018 г.

<60 мин.

реагирование на  
инцидент ИБ

8 000

собственных  
сигнатур атак для  
IDS

С 2017 года Центр ГосСОПКА класса А



# Нормативная база

Комплект нормативных правовых актов по вопросам взаимодействия с ГосСОПКА пока не полный, но работать есть с чем.





# Нормативные правовые акты

## Верхнеуровневые документы

- **Основные направления государственной политики** в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012 N 803)
- **Концепция** государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12 декабря 2014 г. N К 1274)



# Нормативные правовые акты

Федеральные законы, указы Президента и постановления правительства

- **Указ Президента Российской Федерации от 22.12.2017 г. № 620** О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (По сути сменил Указ Президента РФ от 15 января 2013 г. N 31с)
- **Федеральный закон от 26.07.2017 N 187-ФЗ** «О безопасности критической информационной инфраструктуры Российской Федерации»



# Нормативные правовые акты



Документы федерального органа исполнительной власти,  
уполномоченного в области обеспечения функционирования ГосСОПКА

- **Приказ ФСБ России от 24 июля 2018 г. № 366** «О Национальном координационном центре по компьютерным инцидентам (НКЦКИ)»
- **Приказ ФСБ России от 24.07.2018 № 367** «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
- **Приказ ФСБ России от 24 июля 2018 г. № 368** «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»



# Нормативные правовые акты

Документы федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования ГосСОПКА

- **Проект приказа ФСБ России «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»**
- **Проект приказа ФСБ России «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»**
- **Проект приказа ФСБ России «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ»**

ПРОЕКТ

# Нормативные правовые акты



## Методические документы ФСБ России

- Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
- Методические рекомендации ФСБ России по обнаружению компьютерных атак на информационные ресурсы Российской Федерации
- Методические рекомендации ФСБ России по установлению причин и ликвидации последствий компьютерных инцидентов связанных с функционированием информационных ресурсов Российской Федерации
- Методические рекомендации НКЦКИ по проведению мероприятий по оценке степени защищенности от компьютерных атак.
- ТРЕБОВАНИЯ к подразделениям и должностным лицам субъектов ГОССОПКА
- РЕГЛАМЕНТ взаимодействия подразделений ФСБ и субъекта ГОССОПКА при осуществлении информационного обмена в области обнаружения предупреждения и ликвидации последствий компьютерных атак



# А это обязательно?

187-ФЗ

Статья 9. Права и обязанности субъектов критической информационной инфраструктуры

Субъект критической информационной инфраструктуры **обязан** незамедлительно информировать о компьютерных инцидентах соответствующие федеральные органы исполнительной власти (НКЦКИ ГосСОПКА, Финцерт ЦБ РФ для финансовых организаций), а также реагировать на компьютерные инциденты в установленном порядке.



# Передаются сведения:

- О категорировании объекта
- О нарушении требований по обеспечению безопасности значимых объектов КИИ (по итогам проведения государственного контроля)
- Информация о компьютерных инцидентах, связанных с функционированием объектов КИИ
- Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Приказ ФСБ России № 367 от  
24 июля 2018 г.  
«Об утверждении Перечня  
информации,  
представляемой в ГосСОПКА  
и Порядка представления  
информации в ГосСОПКА»

Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

## Два способа предоставления информации в НКЦКИ:

- с использованием технической инфраструктуры НКЦКИ
- посредством электронной, факсимильной, почтовой и телефонной связи

Автоматизированное взаимодействие с технической инфраструктурой НКЦКИ сильно экономит силы и время



# ГосСОПКА это не только КИИ



ОГВ

Могут быть  
подключены к  
ГосСОПКА



КИИ

Обязаны быть  
подключены к  
ГосСОПКА





**ГосСОПКА** — территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

**Зона ответственности** — совокупность информационных ресурсов, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

**Субъекты ГосСОПКА** — государственные органы Российской Федерации, российские юридические лица и индивидуальные предприниматели в силу закона или на основании заключенных с ФСБ России соглашений осуществляющие обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

**Центр ГосСОПКА** — структурная единица ГосСОПКА, представляющая совокупность подразделений и должностных лиц субъекта ГосСОПКА, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и реагирование на компьютерные инциденты в своей зоне ответственности.





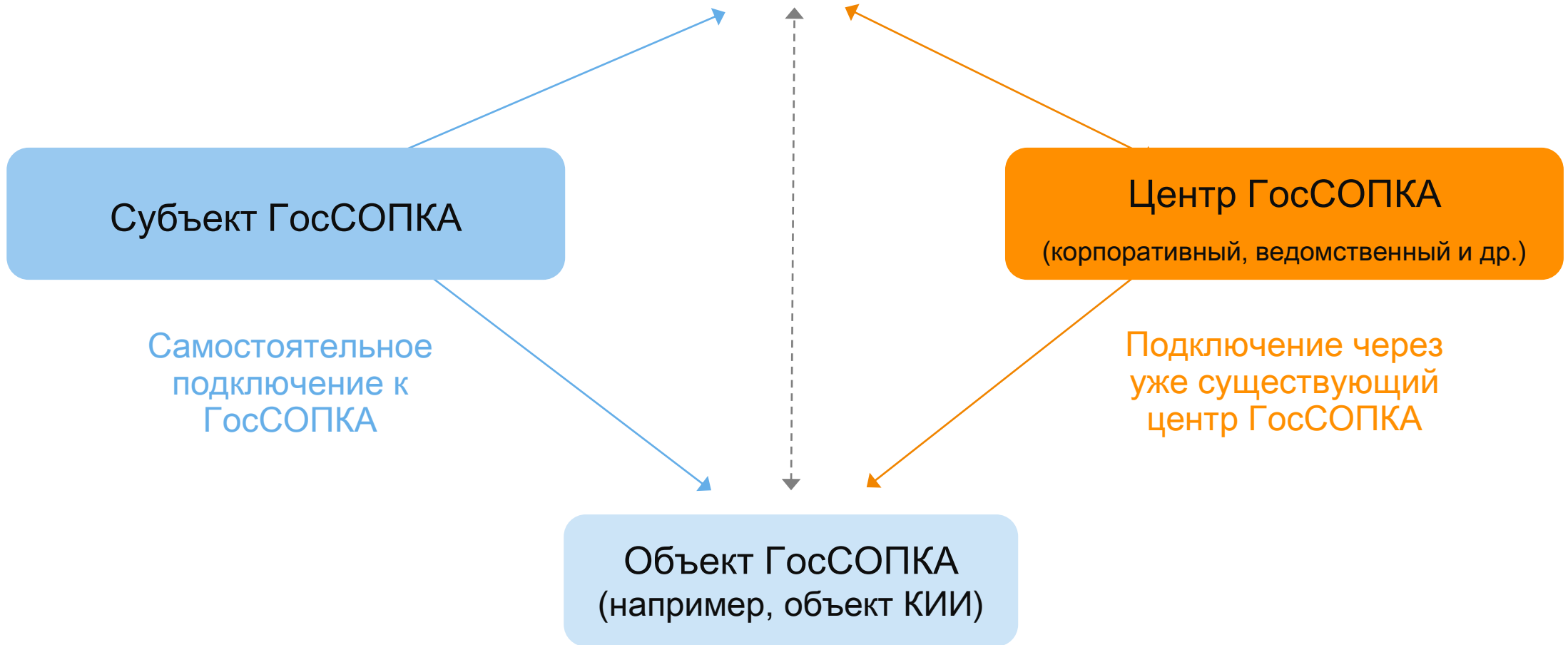
# Технические аспекты

Что делать



# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ



# Что делать?



В случае самостоятельного подключения к ГосСОПКА

---

- ✓ Обеспечить взаимодействие с НКЦКИ
- ✓ Выполнить организационные и технические требования в соответствии с нормативными правовыми актами и методическими рекомендациями
- ✓ Развернуть специализированные системы взаимодействия с технической инфраструктурой НКЦКИ (для значимых КИИ обязательно, остальным опционально).

В случае подключения через сторонний корпоративный сегмент

---

- ✓ Заключение соглашения с корпоративным центром
- ✓ Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности корпоративного центра.



# Какие функции выполняют центры ГосСОПКА

# Глобально:



1. Сбор сведений о контролируемой инфраструктуре.
2. Непрерывный мониторинг и выявление КА и инцидентов.
3. Информирование, реагирование, расследование.
4. Передача сведений в НКЦКИ.

Подробнее →

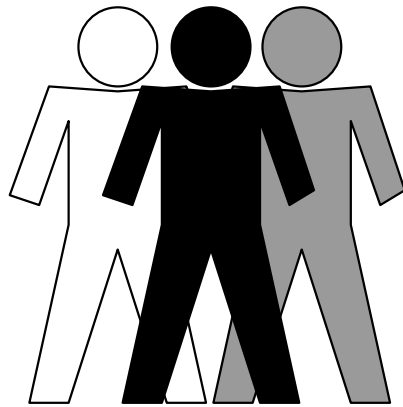
Функции	Центры ГосСОПКА		
	Класса А	Класса Б	Класс В
Взаимодействие с НКЦКИ при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты, в том числе в части информационно-аналитического и прогностического обеспечения функционирования ГосСОПКА, предоставление в НКЦКИ сведений о состоянии защищенности информационных ресурсов от компьютерных атак и информации о компьютерных инцидентах в соответствии с установленным порядком;	+	+	+
Разработка документов, регламентирующих процессы обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов и реагирования на компьютерные инциденты;	+	+	+
Эксплуатация средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, выявление ошибок в работе средств и направление производителю средств информации о выявленных ошибках, а также актуализация средств используемых для обеспечения защиты информационных ресурсов, направление в НКЦКИ предложений по совершенствованию средств;	+	+	+
Прием сообщений об инцидентах от персонала и пользователей информационных ресурсов;	+	+	+
Регистрация компьютерных атак и компьютерных инцидентов;	+	+	+
Анализ событий информационной безопасности;	+	+	+
Инвентаризация информационных ресурсов;	+	+	+
Анализ угроз информационной безопасности, прогнозирование их развития и направление в НКЦКИ результатов;	+	+	
Составление и актуализация перечня угроз информационной безопасности для информационных ресурсов;	+	+	
Выявление уязвимостей информационных ресурсов;	+	+	
Формирование предложений по повышению уровня защищенности информационных ресурсов;	+	+	
Составление перечня последствий компьютерных инцидентов;	+	+	
Ликвидация последствий компьютерных инцидентов;	+		
Анализ результатов ликвидации последствий инцидентов;	+		
Установление причин компьютерных инцидентов.	+	+	

# Необходимые ресурсы



Силы ГосСОПКА

Средства ГосСОПКА



Кадровое обеспечение

Средства  
обнаружения,  
средства  
предотвращения,  
средства ликвидации  
последствий



# Силы ГосСОПКА



# Персонал



## Первая линия

Взаимодействие с пользователями

Анализ событий и обнаружение компьютерных атак и инцидентов

Регистрация инцидентов ИБ и оповещение заинтересованных лиц

## Вторая линия

Помощь в расследовании и установлении причин инцидентов

Координация действий при реагировании на инциденты ИБ

Анализ уязвимостей, анализ защищенности, тестирование на проникновение

## Третья линия

Подготовка и улучшение нормативной базы, описание сценариев выявленных инцидентов

Разработка сигнатурных правил и правил корреляции

Углубленный анализ Инцидентов ИБ, сбор доказательной базы

# Специалисты 1 линии



Специалист по взаимодействию с персоналом и пользователями

- Прием сообщений персонала и пользователей
- Подготовка информации для предоставления в НКЦКИ
- Взаимодействие с НКЦКИ

Специалист по обнаружению компьютерных атак и инцидентов

- Анализ событий информационной безопасности
- Регистрация компьютерных атак и инцидентов

Специалист по обслуживанию средств центра ГосСОПКА

- Обеспечение функционирования средств, размещаемых в центре ГосСОПКА, а также дополнительных средств защиты информационных систем

# Специалисты 2 линии



Специалист по  
оценке  
защищенности

- Проведение инвентаризации информационных ресурсов
- Выявление уязвимостей
- Сбор и анализ выявленных уязвимостей и угроз
- Установление соответствия требований по информационной безопасности принимаемым мерам

Специалист по  
ликвидации  
последствий  
компьютерных  
инцидентов

- Координация действий при реагировании на компьютерные инциденты и приведение в штатный режим работы
- Взаимодействие с НКЦКИ

Специалист по  
установлению  
причин  
компьютерных  
инцидентов

- Установление причин компьютерных инцидентов
- Анализ последствий инцидентов и подготовка перечня компьютерных инцидентов
- Взаимодействие с НКЦКИ

# Специалисты 3 линии



Аналитик-методист

- Анализ информации, предоставляемой специалистами 1-й и 2-й линий
- Выявление и анализ угроз информационной безопасности
- Прогнозирование развития угроз
- Разработка рекомендаций по доработке нормативных и методических документов

Технический эксперт

- Экспертная поддержка в соответствии со специализацией (ВПО, настройка средств защиты, применение специализированных технических средств, оценка защищенности и т.п.)
- Формирование предложений по повышению уровня защищенности

Специалист

- Нормативно-правовое и методическое сопровождение деятельности центра ГосСОПКА

Руководитель

Управление деятельностью центра ГосСОПКА  
Взаимодействие с НКЦКИ



# Практическое применение

## СБОР СОБЫТИЙ



Сетевые IDS



Хостовые IDS



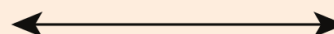
DNS, DHCP, AV,  
VPN, FW, Mail...



## АНАЛИЗ И ВЫЯВЛЕНИЕ



TIAS



LogCollector

## ОБОГАЩЕНИЕ И РЕАГИРОВАНИЕ



Фиды угроз  
и уязвимостей



TI Platform



Incident  
Management



ТИ НКЦКИ

# Инвентаризация



Центр ГосСОПКА



НКЦКИ



Контролируемая инфраструктура заказчика

# Система инвентаризации



Inventory System Search REPORTS JSON

Advanced Monitoring resources list MSK-W0038 Software List

Host Name	Timestamp	os_version	arch	Application Name	Version	CVE count	Approve
MSK-W0038	1515745587	Майкрософт Windows 10 Корпоративная	64-разрядная			0	X
MSK-W0057	1517401048	Майкрософт Windows 10 Корпоративная	64-разрядная	64 Bit HP CIO Components Installer	13.2.1	0	✓
MSK-W0326	1515745985	Майкрософт Windows 10 Корпоративная	64-разрядная	7-Zip 17.01 beta (x64)	17.01 beta	0	✓
MSK-W0603	1515745813	Майкрософт Windows 10 Корпоративная	64-разрядная	7-Zip 9.20 (x64 edition)	9.20.00.0	2	✓
MSK-W1595	1515745810	Майкрософт Windows 10 Корпоративная	64-разрядная	Adobe Reader XI (11.0.23) MUI	11.0.23	26	✓

Selected: Adobe Reader XI (11.0.23) MUI cpe:"cpe:/a:adobe:acrobat\_reader" cve:26

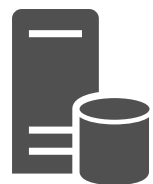
- ! CVE-2013-3346 (cvss:10) v
- ! CVE-2013-3342 (cvss:10) v
- ! CVE-2013-3341 (cvss:10) v
- ! CVE-2013-3340 (cvss:10) v
- ! CVE-2013-3339 (cvss:10) v
- ! CVE-2013-3338 (cvss:10) v
- ! CVE-2013-3337 (cvss:10) v
- ! CVE-2013-2736 (cvss:10) v



# Обработка уязвимостей



Публичные  
базы  
уязвимостей



bdu.fstec.ru

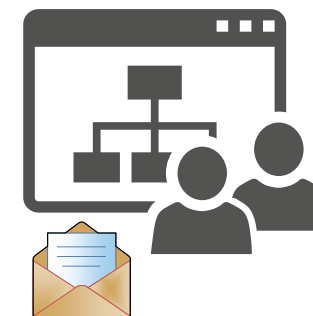
Обработка, агрегация и  
формирование базы  
уязвимостей



ЦМ



Пользователи  
Реагирование



Хранение сведений — 3 года

Сопоставление данных

# Обработка уязвимостей



**Vulnerability Prevention**

Уязвимости | Продукты | Компоненты | Отчеты | Мой профиль | Выход (Demo)

## Уязвимость #7117

[Комментарии \(2\)](#)

Статус	новая	создана	09/06/2017 14:39
Статус Аналитика	подтверждена	обновлена	07/08/2017 13:45
CVE	CVE-2017-2636		
Продукт	Linux Server 1		
Уязвимое ПО	linux_kernel - 3.10.1		
CPEs	21		
Ответственный	нет (назначить)		

### CVE-2017-2636

**Комментарий**

Состояние гонки существует в drivers/tty/n\_hdlc.c ядра Linux при обращении к списку n\_hdlc.tbuf. Данная уязвимость позволяет локальным, непривилегированным пользователям повысить уровень своих привилегий или вызвать отказ в обслуживании (двойное освобождение), используя настройку дисциплины линии HDLC.

**Уровень опасности:** Высокий  
**Воздействие:** Повышение привилегий  
**Вектор атаки:** Локальный

**Описание**

Race condition in drivers/tty/n\_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.

**Ссылки**

MLIST	<a href="http://www.openwall.com/lists/oss-security/2017/03/07/6">http://www.openwall.com/lists/oss-security/2017/03/07/6</a>	03/07/2017
BID	<a href="http://www.securityfocus.com/bid/96732">http://www.securityfocus.com/bid/96732</a>	03/13/2017

**Cvss v3**

SCORE	7.8
SCOPE	UNCHANGED
Вектор доступа (AV)	LOCAL
Сложность доступа (AC)	LOW
Privileges Required (PR)	LOW
User Interaction (UI)	NONE
Воздействие на конфиденциальность (C)	HIGH
Воздействие на целостность (I)	HIGH
Воздействие на доступность (A)	HIGH

**Cvss v2**

SCORE	7.2
Вектор доступа (AV)	LOCAL
Сложность доступа (AC)	LOW

# Обработка уязвимостей



Вы не получаете уведомления о новых или незакрытых уязвимостях по почте.  
Вы можете [настроить](#) рассылку и список уязвимостей на главной странице.  
Вы можете [экспортировать](#) уязвимости из списка ниже.

## Список уязвимостей с CVSS выше или равным 0.5 (6)

Отобразить назначенные мне (4)

Поиск

поиск

Поиск по полям: #, CVE, Комментарий, Описание



#	V2: AV	V2: Score	V3: AV	V3: Score	CVE	Статус	Продукт	Компоненты	Ответственный	Создана	Обновлена	Client Status Changed At
7512	NETWORK	10.0	NETWORK	9.8	CVE-2015-8812	новая	Linux Server 1	linux_kernel - 3.10.1	developer	09/06/2017 14:39	07/08/2017 14:31	27/06/2017 12:54
7117	LOCAL	7.2	LOCAL	7.8	CVE-2017-2636	новая	Linux Server 1	linux_kernel - 3.10.1		09/06/2017 14:39	07/08/2017 13:45	28/06/2017 06:11
7063	NETWORK	9.3	NETWORK	8.1	CVE-2017-0143	новая	APM Windows msk-w0423	windows_10 - 1511		02/06/2017 17:37	07/08/2017 12:32	27/06/2017 12:55
6997	NETWORK	9.3	NETWORK	8.8	CVE-2016-0184	новая	APM Windows msk-w0423	windows_10 - 1511		02/06/2017 17:34	07/08/2017 15:18	27/06/2017 12:56
5544	NETWORK	10.0	NETWORK	9.8	CVE-2016-0705	в работе	Linux Server 1	openssl - 1.0.1e-2+deb7u13		29/02/2016 16:07	07/08/2017 12:45	27/06/2017 12:55
5535	NETWORK	10.0	NETWORK	9.8	CVE-2016-4275	новая	APM Windows msk-w0423	flash_player - 10.0.0.584		11/10/2016 14:53	07/08/2017 12:49	17/10/2016 15:32

# Сведения по уязвимостям



Ввод в эксплуатацию	Ежемесячно	Ежеквартально	Ежегодно
анализ документации	сетевое и системное сканирование	контроль устранения ранее выявленных уязвимостей	тестирование на проникновение
анализ исходного кода	контроль выполнения требований безопасности		оценка соответствия мер защиты

# LogCollector



— система обработки данных, предназначенная для сбора и анализа событий от разнородных источников в информационной сети

Парсер логов

Система визуализации

Нереляционная БД

Агент сбора логов

Анализ событий

Система очередей

&gt; Search... (e.g. status:200 AND extension:PHP)

Options

Refresh

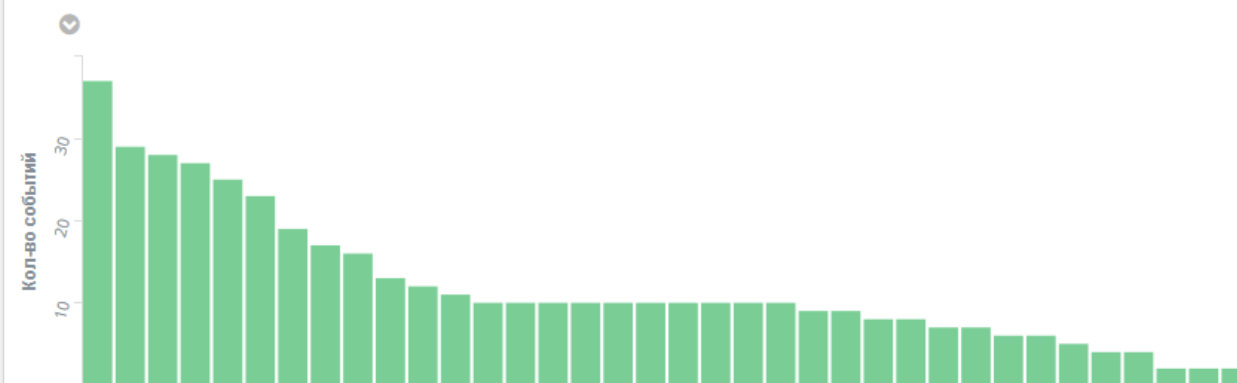
Add a filter +

Кол-во хостовых событий до агрегации

# 34,787

Sum of baseEventCount

HS Хосты по событиям



Всего хостовых событий

# 436

Count

Сетевые со...

# 8

Count

Узел

Select...

Критичность

Select...

Clear form

Cancel changes

Apply changes

Активность реестра

# 152

100000 to 199999 - sid

Файловая активность

# 97

200000 to 299999 - sid

Активность процесса

# 77

300000 to 399999 - sid

Системная активность

# 1

400000 to 499999 - sid

Логины

# 104

500000 to 599999 - sid

Изменения пользователей, групп

# 5

600000 to 699999 - sid

Зарезервировано

# 0

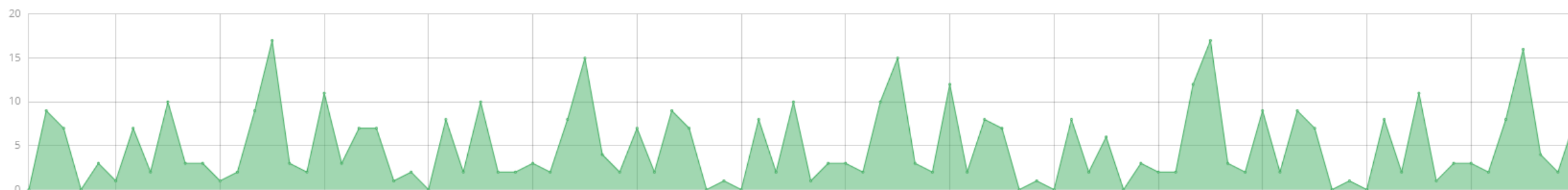
700000 to 799999 - sid

Linux

# 0

800000 to 999999 - sid

Распределение событий



# Система управления инцидентами



Расследование Организации

Инциденты

## Найденные инциденты

ID	Время фиксации	Название	Уровень	Количество событий	Статус	Тип	Пораженные активы	Состояние
DEMO-91	18.10.2018 14:34	Заражение хоста трояном LoadMoney	Высокий	1	Новый	Эксплуатация уязвимостей	8.8.8.8:53	Неподтвержденный
DEMO-90	18.10.2018 14:34	Заражение хоста трояном LoadMoney	Высокий	1	Новый	Эксплуатация уязвимостей	8.8.8.8:53	Неподтвержденный
DEMO-88	18.10.2018 14:33	Классификатором выявлено подозрительное событие	Высокий	45	Новый	Эксплуатация уязвимостей	192.168.0.1:3389, 192.168.0.1...	Неподтвержденный
DEMO-89	18.10.2018 14:33	Классификатором выявлено подозрительное событие	Высокий	45	Новый	Эксплуатация уязвимостей	192.168.0.1:3389, 192.168.0.1...	Неподтвержденный
DEMO-86	18.10.2018 14:33	Классификатором выявлено подозрительное событие	Высокий	45	Новый	Эксплуатация уязвимостей	192.168.0.1:3389, 192.168.0.1...	Неподтвержденный
DEMO-87	18.10.2018 14:33	Классификатором выявлено подозрительное событие	Высокий	45	Новый	Эксплуатация уязвимостей	192.168.0.1:3389, 192.168.0.1...	Неподтвержденный
DEMO-84	18.10.2018 14:33	Заражение хоста трояном LoadMoney	Высокий	1	Новый	Эксплуатация уязвимостей	192.168.122.2:53	Неподтвержденный
DEMO-85	18.10.2018 14:33	Заражение хоста трояном LoadMoney	Высокий	1	Новый	Эксплуатация уязвимостей	192.168.122.2:53	Неподтвержденный
DEMO-82	18.10.2018 14:33	Заражение хоста трояном LoadMoney	Высокий	1	Новый	Эксплуатация уязвимостей	192.168.122.2:53	Неподтвержденный
DEMO-83	18.10.2018 14:33	Заражение хоста трояном LoadMoney	Высокий	1	Новый	Эксплуатация уязвимостей	192.168.122.2:53	Неподтвержденный
DEMO-80	18.10.2018 14:33	Потенциальная попытка проведения атаки SQL-injection на узел контролиру...	Высокий	10	Новый	Эксплуатация уязвимостей	192.168.0.2:80	Неподтвержденный
DEMO-81	18.10.2018 14:33	Потенциальная попытка проведения атаки SQL-injection на узел контролиру...	Высокий	10	Новый	Эксплуатация уязвимостей	192.168.0.2:80	Неподтвержденный
DEMO-78	18.10.2018 14:33	Потенциальная попытка проведения атаки SQL-injection на узел контролиру...	Высокий	10	Новый	Эксплуатация уязвимостей	192.168.0.2:80	Неподтвержденный
DEMO-79	18.10.2018 14:33	Потенциальная попытка проведения атаки SQL-injection на узел контролиру...	Высокий	10	Новый	Эксплуатация уязвимостей	192.168.0.2:80	Неподтвержденный
DEMO-77	17.10.2018 13:26	Классификатором выявлено подозрительное событие	Высокий	19	Новый	Эксплуатация уязвимостей	192.168.122.2:53, 128.199.86...	Неподтвержденный
DEMO-76	17.10.2018 13:24	Потенциальная попытка проведения атаки SQL-injection на узел контролиру...	Высокий	10	Новый	Эксплуатация уязвимостей	192.168.0.2:80	Неподтвержденный
DEMO-75	17.10.2018 13:24	Заражение хоста трояном LoadMoney	Высокий	1	Новый	Эксплуатация уязвимостей	192.168.122.2:53	Неподтвержденный
DEMO-74	17.10.2018 09:42	Потенциальная попытка проведения атаки SQL-injection на узел контролиру...	Высокий	10	Новый	Эксплуатация уязвимостей	192.168.0.2:80	Неподтвержденный
DEMO-72	17.10.2018 09:42	Потенциальная попытка проведения атаки SQL-injection на узел контролиру...	Высокий	10	Новый	Эксплуатация уязвимостей	192.168.0.2:80	Неподтвержденный
DEMO-71	17.10.2018 09:42	Потенциальная попытка проведения атаки SQL-injection на узел контролиру...	Высокий	10	Новый	Эксплуатация уязвимостей	192.168.0.2:80	Неподтвержденный
DEMO-73	17.10.2018 09:42	Потенциальная попытка проведения атаки SQL-injection на узел контролиру...	Высокий	10	Новый	Эксплуатация уязвимостей	192.168.0.2:80	Неподтвержденный
DEMO-67	17.10.2018 09:42	Классификатором выявлено подозрительное событие	Высокий	22	Новый	Эксплуатация уязвимостей	192.168.122.2:53, 128.199.86...	Неподтвержденный
DEMO-68	17.10.2018 09:42	Классификатором выявлено подозрительное событие	Высокий	22	Новый	Эксплуатация уязвимостей	192.168.122.2:53, 128.199.86...	Неподтвержденный
DEMO-69	17.10.2018 09:42	Классификатором выявлено подозрительное событие	Высокий	22	Новый	Эксплуатация уязвимостей	192.168.122.2:53, 128.199.86...	Неподтвержденный
DEMO-70	17.10.2018 09:42	Классификатором выявлено подозрительное событие	Высокий	22	Новый	Эксплуатация уязвимостей	192.168.122.2:53, 128.199.86...	Неподтвержденный

# Карточка инцидента



Инциденты / demo-36

Отправить в НКЦКИ

Редактировать

## ⚠ Потенциальная попытка проведения атаки SQL-injection на узел контролируемой инфраструктуры

Создан 4 месяца назад  
Изменен несколько секунд назад

Тип: Эксплуатация уязвимостей

Уровень: Высокий

Система: Demo DemoNetwork

Зафиксирован: 17.10.2018 09:41

Необходимо содействие НКЦКИ

Состояние: неподтвержденный

Статус: Новый

Пользователь: TIAS

Наблюдатели: TIAS

Описание:

Рекомендации 4

Предпринятые действия: Нет данных

Наблюдается активность проведения попыток SQL Injection

- TIAS 17.10.2018 09:41  
Отключить пораженный актив от вычислительной сети
- Роман Кобцев 28.02.2019 09:23  
Заблокировать на межсетевом экране IP-адрес атакующего
- Роман Кобцев 28.02.2019 09:24

События 10 | История | Комментарии | Пораженные активы | Влияние | Файлы | Контакты



vipnet\_ids\_ns

Порт получателя	IP получателя	Порт отправителя	IP отправителя	Событие	Группа	Дата	Приоритет	Протокол	ID сенсора	Сенсор	Правило
80	192.168.0.2	56735	91.59.66.41	92158		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...
80	192.168.0.2	56736	91.59.66.41	92159		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...
80	192.168.0.2	56737	91.59.66.41	92161		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...
80	192.168.0.2	56738	91.59.66.41	92163		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...
80	192.168.0.2	56739	91.59.66.41	92165		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...
80	192.168.0.2	56740	91.59.66.41	92167		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...
80	192.168.0.2	56742	91.59.66.41	92169		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...
80	192.168.0.2	56743	91.59.66.41	92171		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...
80	192.168.0.2	56744	91.59.66.41	92173		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...
80	192.168.0.2	56746	91.59.66.41	92177		17.10.2018 08:47	3	TCP	458180614	10.0.24.201	ET WEB_SERVER Possible SQL Injection Att...



# Рекомендации по реагированию



 Рекомендации <span>1</span>	 Предпринятые действия <span>1</span>
Администратор <span style="float: right;">04.09.2018 14:42</span>	Администратор <span style="float: right;">04.09.2018 14:42</span>
Провести антивирусную проверку	Оповещена группа реагирования

# Проблемы



При построении своего Центра

1. ДО-РО-ГО!
2. Нужна лицензия.
3. Нехватка ресурсов на реагирование.

В процессе взаимодействия

1. Страх передать информацию.

# Помогаем не только клиентам



Сработала  
сигнатура на IDS



Майнер на  
сайте банка



Нашли  
безопасника

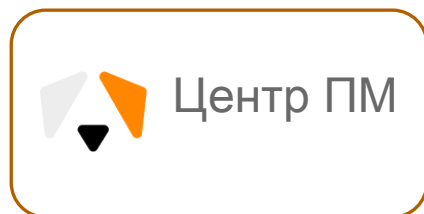


Отправили  
рекомендации



[cert@amonitoring.ru](mailto:cert@amonitoring.ru)

# Выводы



## Ресурсы

- ✓ Выявление КА и КИ
- ✓ Реагирование
- ✓ Разработка правил
- ✓ Выявление уязвимостей
- ✓ Адаптация новых источников данных
- ✓ Экспертная поддержка
- ✓ Сбор и передача сведений в НКЦКИ

## Техническое обеспечение

- ✓ Средства сбора и анализа событий
- ✓ Средства выявления аномалий
- ✓ Система управления уязвимостями
- ✓ Система управления инцидентами
- ✓ Отправка сведений в НКЦКИ



**Защитимся сообща.  
Подключайтесь!**

Реагирование

Предупреждение

**ГОССОПКА**

Ликвидация

Обнаружение

**2019 год**



Спасибо за  
внимание!

И подключайтесь к  
ГосСОПКА

# Георгий Караев

Руководитель направления

[Georgy.Karaev@amonitoring.ru](mailto:Georgy.Karaev@amonitoring.ru)

