ГАРДА
ТЕХНОЛОГИИ

БЕЗОПАСНОСТЬ КИИ

КАТЕГОРИРОВАНИЕ ЗАВЕРШЕНО (ДО 1 СЕНТЯБРЯ),
ПОРА ПЕРЕХОДИТЬ К ПРАКТИКЕ

ГАРДА БД

ГАРДА МОНИТОР

ГАРДА ПРЕДПРИЯТИЕ

О КОМПАНИИ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ТЕХНОЛОГИИ — РОССИЙСКИЙ РАЗРАБОТЧИК СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Команда разработчиков обладает многолетним опытом в сфере информационных технологий и создаёт решения для различных задач безопасности.

Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ.

100+
Внедрений на территории России

180 +
Высококвалифицированных сотрудников

10 ЛЕТ
Опыт разработки систем высокой сложности

5
запатентованных технологий собственного исследовательского центра

ПОЛНОСТЬЮ РОССИЙСКИЕ РЕШЕНИЯ

- Собственная технологическая платформа для хранения информации не требует сторонних лицензий.
- Решения сертифицированы ФСТЭК.
- Включены в реестр отечественного программного обеспечения.

ПРОДУКТЫ И РЕШЕНИЯ

ГАРДА ТЕХНОЛОГИИ

АНАЛИТИЧЕСКАЯ ПЛАТФОРМА

ГАРДА АНАЛИТИКА

Построение комплексных систем информационной и экономической безопасности.

ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ

ГАРДА БД

Система аудита и защиты баз данных и веб-приложений, предотвращает возможные утечки информации и повышает надежность защиты.

ГАРДА МОНИТОР

Система мониторинга сетевого трафика, выявления и расследования сетевых инцидентов.

ГАРДА ПРЕДПРИЯТИЕ

DLP-система для защиты от утечек информации и выявления потенциальных угроз информационной безопасности.

ЗАЩИТА ОТ ВНЕШНИХ УГРОЗ

ПЕРИМЕТР

Решение операторского класса для предупреждения, обнаружения и подавления DDoS-атак различного типа в сети передачи данных.

ГАРДА ФИЛЬТР

АПК, предназначенный для фильтрации Интернет-трафика, ограничения доступа к нежелательным доменным именам, указателям страниц сайтов и сетевым адресам сети Интернет.

ФРОД ИНДЕКС

Группа решений для оперативного и эффективного выявления фактов bypass, on-net и off-net фрода в сети оператора связи.

АНТИБОТНЕТ

Аппаратно-программный комплекс анализа Интернет-трафика по сигнатурам бот-сетей.

ГАРДА
ТЕХНОЛОГИИ

ТЕКУЩАЯ СИТУАЦИЯ В ОБЛАСТИ ЗАКОНОДАТЕЛЬСТВА О БКИИ

СТРУКТУРА ЗАКОНОДАТЕЛЬСТВА О БКИИ

ГАРДА ТЕХНОЛОГИИ

187-ФЗ, 193-ФЗ, 194-ФЗ

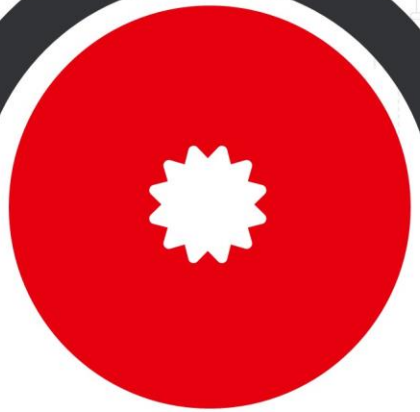
Верхний уровень

ПП-127, ПП-162

Категорирование и госконтроль

Приказы ФСТЭК

- 227, 229, 236
- 235, 239



Приказы ФСБ

- «Рекомендации...», «Выписка...»
- Приказы 366, 367, 368, 196, 281, 282

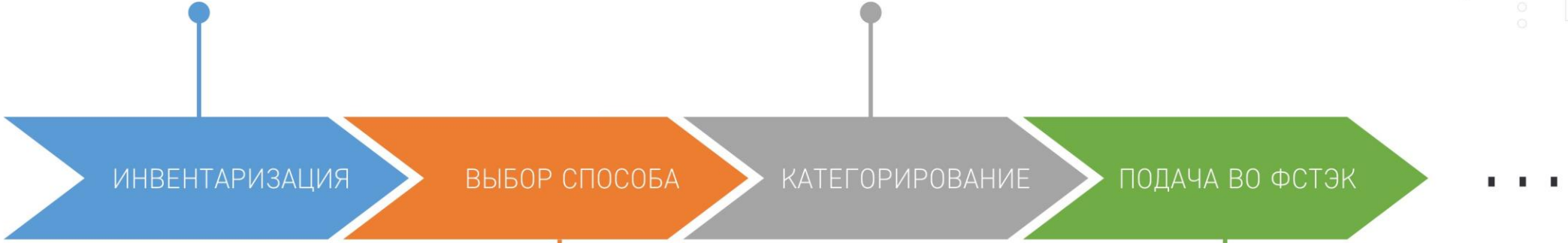
ВЕДОМСТВЕННЫЕ ПРИКАЗЫ (МКС, МИНЭНЕРГО, ЦБ РФ)

АЛГОРИТМ ДЕЙСТВИЙ (ФСТЭК) (ПРОШЛИ)

ГАРДА ТЕХНОЛОГИИ

- Описание систем и процессов
- Привязка к объектам КИИ
- Оценка состояния ИБ и набора СЗИ

- Отраслевая специфика
- Комиссия, акты



- Влияющие на объекты КИИ процессы
- Типовые объекты

ПЕРЕЧЕНЬ ОБЪЕКТОВ

- Вертикаль
- 2 управление
- Управление по ФО

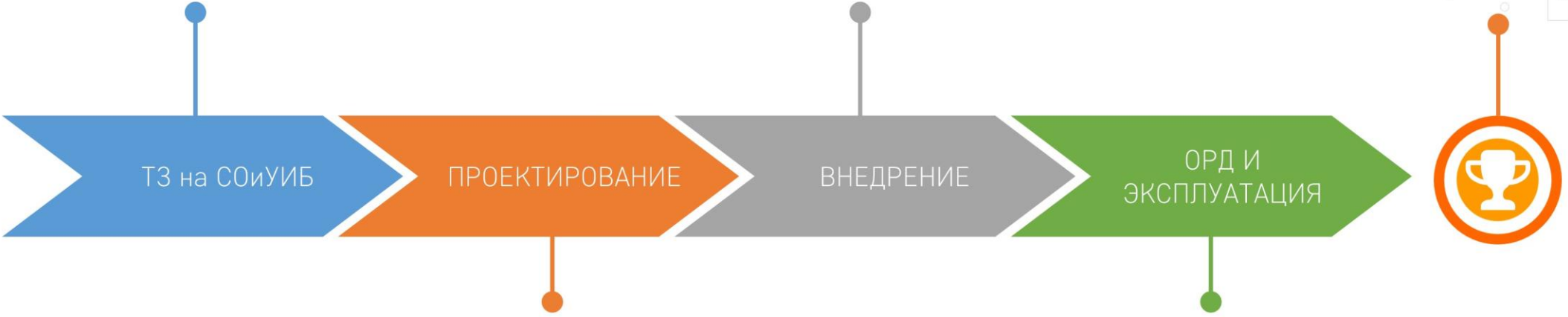
АЛГОРИТМ ДЕЙСТВИЙ (ФСТЭК) (ТЕКУЩИЙ ЭТАП)

ГАРДА ТЕХНОЛОГИИ

- Написание требований
- Апробация решений

- Инсталляция
- Настройка

Обеспечена бКИИ

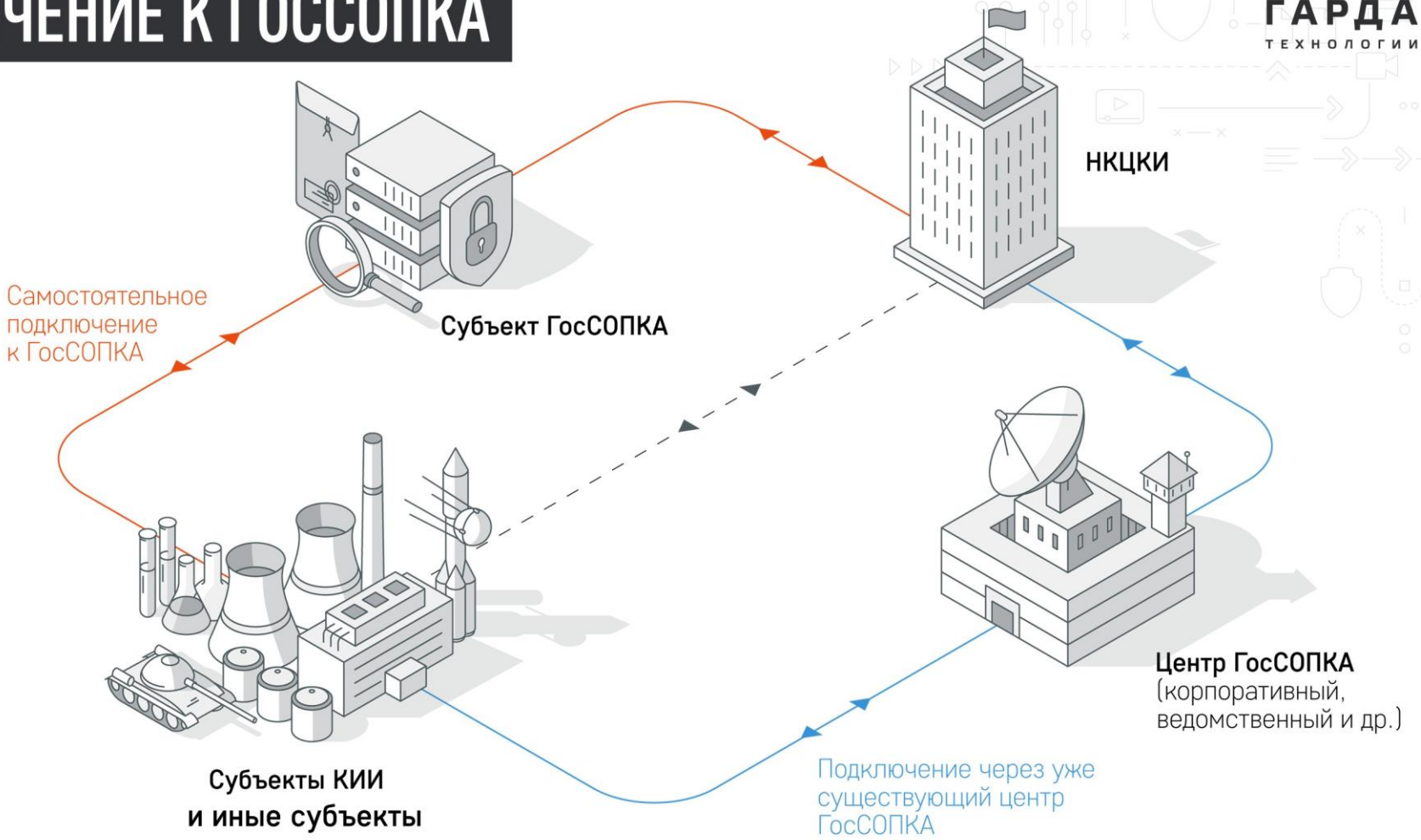


- Проектные решения на процессы и продукты
- Часть ОРД

- Документация
- Оценка эффективности

ПОДКЛЮЧЕНИЕ К ГОССОПКА

ГАРДА
ТЕХНОЛОГИИ



ОТКРЫТЫЙ ВОПРОС ПО ФИН. ОТРАСЛИ

ПРОЕКТ НОВОГО ГОСТ ПО ГОССОПКА

ГАРДА
ТЕХНОЛОГИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

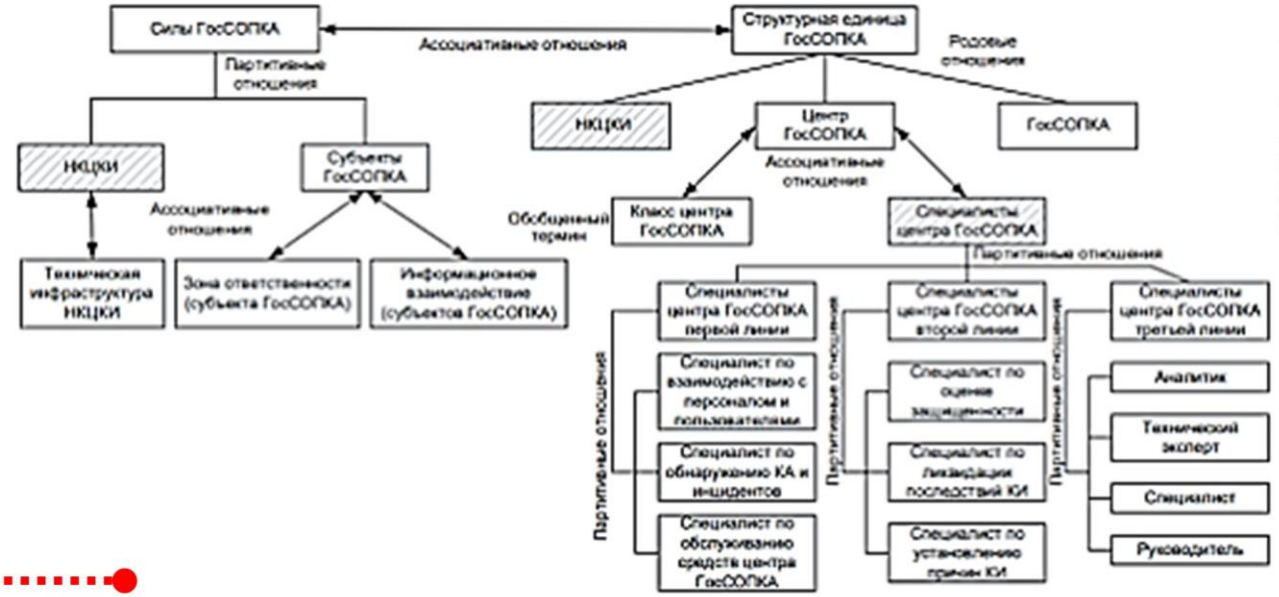
НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р (проект, первая редакция)

Защита информации
ОБНАРУЖЕНИЕ, ПРЕДУПРЕЖДЕНИЕ И ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК И РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ
Термины и определения

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Стандартинформ
202X



- Визуализация терминов => концепция процессов
- Поможет структурировать обучение и понимание
- Можно наглядно доказывать свою позицию (регулятору, руководству) по выстраиванию процессов SOC
- К общему понятийному «знаменателю» ГОСТа полезно также привести свои внутренние документы

ПРОЕКТ ПРИКАЗА О ПОДКЛЮЧЕНИИ ЗО КИИ К ИНТЕРНЕТУ

ГАРДА ТЕХНОЛОГИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« ___ » мая 2020 г. Москва № _____

Об утверждении Порядка согласования
Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования

Только для вновь создаваемых объектов

- Цель подключения значимого объекта к сети связи общего пользования
- Наименование, модель средств обеспечения безопасности значимого объекта, применяемых при его подключении к сети связи общего пользования
- Номера сертификатов или протоколы оценки испытаний
- Копия модели угроз
- Схема организации связи (раньше еще был обязательный перечень СЗИ, его убрали)

ПРОЕКТ ИЗМЕНЕНИЙ В КОАП

ГАРДА ТЕХНОЛОГИИ

СТАТЬЯ 39.24

Нарушение требований в области КИИ по:

- Созданию
- Обеспечению безопасности
- Информированию об инцидентах
- Обмену данными об инцидента

Штраф:

До 50 000₽ – для должностных лиц
До 500 000₽ – для ЮЛ

СТАТЬЯ 39.25

Непредставление сведений по КИИ:

- Во ФСТЭК
- В ФСБ

Штраф:

До 50 000₽ – для должностных лиц
До 500 000₽ – для ЮЛ

ЗА ЧТО НАКАЗЫВАЮТ УЖЕ СЕЙЧАС (1/6)

ГАРДА ТЕХНОЛОГИИ

Прокуратура Приморского края утвердила обвинительное заключение по уголовному делу о неправомерном доступе к системам самообслуживания клиентов оператора сотовой сети

Прокуратура края (Приморский край) . 05 августа 2020, 11:09

Прокуратура Приморского края утвердила обвинительное заключение по уголовному делу в отношении 21-летнего местного жителя. Он обвиняется в совершении преступления, предусмотренного ч. 2 ст. 274.1 УК РФ (неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, повлекший причинение вреда информационной системе).

- При помощи двух подельников получил пароли доступа от модуля «Личный кабинет» системы самообслуживания абонентов
- Осуществлял неправомерный вход в «Личные кабинеты» абонентов, где активировал функцию переадресации входящих вызовов на принадлежащий ему абонентский номер
- Получил доступ к аккаунтам социальной сети, «привязанным» к абонентским номерам сотового оператора, сменить на них пароли доступа, чтобы в дальнейшем использовать их в корыстных целях.
- Компьютерная информация системы самообслуживания абонентов телекоммуникационной компании относится к критической информационной инфраструктуре

ЗА ЧТО НАКАЗЫВАЮТ УЖЕ СЕЙЧАС (2/6)

ГАРДА ТЕХНОЛОГИИ

Уголовные дела

дело № 1-536/2020

Дело | Движение дела | Лица | Стороны | Судебный акт #1 (Приговор)

КОПИЯ

№1-536/2020

28RS0004-01-2020-003397-21

ПРИГОВОРИЛ:

Признать Корнейчука Олега Владимировича виновным в совершении преступления, предусмотренного ч. 4 ст. 274.1 Уголовного Кодекса Российской Федерации, и назначить ему наказание в виде лишения свободы сроком на 3 (три) года.

- Сотрудник оператора связи отправил сведения о расположениях узлов связи (В/Ч, ФСБ, УФСИН, МВД) на личный почтовый ящик (ч.4 ст. 274.1 – с исп. служебного положения)
- Копия сохранилась в памяти облачного хранилища компании «Google», зарегистрированной в США
- Тем самым причинил вред критической информационной инфраструктуре Российской Федерации

ЗА ЧТО НАКАЗЫВАЮТ УЖЕ СЕЙЧАС (3/6)

ГАРДА ТЕХНОЛОГИИ

Во Владивостоке вынесен приговор по уголовному делу в сфере компьютерной информации

Прокуратура края (Приморский край). 03 октября 2019

Ленинский районный суд г. Владивостока вынес приговор по уголовному делу в отношении местной жительницы, которая признана виновной в совершении преступления, предусмотренного ч. 4 ст. 274.1 УК РФ (неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, что повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, совершенное лицом с использованием своего служебного положения).

- Сотрудница оператора связи скопировала на флешку ПДн абонентов (ч.4 ст. 274.1 – с исп. служебного положения)
- Переслала на электронный адрес знакомого
- Тем самым причинила вред критической информационной инфраструктуре Российской Федерации

ЗА ЧТО НАКАЗЫВАЮТ УЖЕ СЕЙЧАС (4/6)

ГАРДА ТЕХНОЛОГИИ

№

ПРИГОВОР

Именем Российской Федерации

г. Владивосток 25 сентября 2019 года

Ленинский районный суд г. Владивостока Приморского края РФ в составе председательствующего судьи Пасешнюк И.В.,

с участием государственного обвинителя- старшего помощника прокурора Ленинского района г.Владивостока Савченко О.А.,

подсудимой Гагиевой О.С.,

защитника – адвоката Смурова А.Д.,

представителя потерпевшего ПАО «Ростелеком» Ивкова И.Г.,

при секретаре Мельянкиной Е.В., Полевой А.Д.,

рассмотрев в особом порядке в открытом судебном заседании материалы уголовного дела в отношении Гагиевой Олеси Сергеевны, родившейся ДД.ММ.ГГГГ в <адрес>, гражданки РФ, с неоконченным высшим образованием, не военнообязанной, зарегистрированной по адресу: <адрес>, проживающей по адресу: <адрес>, вдовы, иждивенцев не имеющей, работающей <данные изъяты> не судимой,

которой избрана мера пресечения в виде подписки о невыезде и надлежащем поведении,

обвиняемой в совершении преступления, предусмотренного ч.4 ст. 274.1 УК РФ,

- Сотрудница оператора связи отправила на личную почту сведения о КОРПОРАТИВНЫХ клиентах, но содержащих ПДн
- Ч.4 ст.274.1 УК РФ, 3 года лишения свободы условно с лишением права заниматься деятельностью, связанной с доступом к критической информационной инфраструктуре Российской Федерации сроком 2 года

ЗА ЧТО НАКАЗЫВАЮТ УЖЕ СЕЙЧАС (5/6)

ГАРДА ТЕХНОЛОГИИ

ПРИГОВОР

ИМЕНЕМ РОССИЙСКОЙ ФЕДЕРАЦИИ

<адрес> 25 сентября 2019 года

Первомайский районный суд <адрес> края в составе:

председательствующего судьипри секретаре судебного заседания Черненко А.А.Юрковой Н.Д.

с участием государственного обвинителя - пом.прокурора <адрес> Гришиной Ю.В.

защитников Вишнякова В.В.Бондаренко С.Ю.Пасичнюка В.Н.

подсудимыхпредставителя потерпевшего Левина А.С.Литвиненко С.В.Осипова М.А.ФИО11

рассмотрев в открытом судебном заседании в особом порядке принятия судебного решения уголовное дело в отношении:

Левина Александра Сергеевича, родившегося ДД.ММ.ГГГГ в <адрес> края, гражданина РФ, военнообязанного, с высшим образованием, женатого, имеющего на иждивении двух малолетних детей, работающего главным государственным таможенным инспектором ОТО и ТК № ДВЭТП СГГС РФ, зарегистрированного по адресу: <адрес>; проживающего по адресу: <адрес> не судимого;

- обвиняемого в совершении преступления, предусмотренного ч.4 ст.2741 УК РФ;

- избрана мера пресечения в виде подписки о невыезде и надлежащем поведении;

Литвиненко Сергея Викторовича, родившегося ДД.ММ.ГГГГ в <адрес> края, гражданина РФ, военнообязанного, с высшим образованием, женатого, имеющего на иждивении двух малолетних детей, работающего наладчиком станков с ЧПУ, зарегистрированного и проживающего по адресу: <адрес>, не судимого;

- обвиняемого в совершении преступления, предусмотренного ч.4 ст.2741 УК РФ;

- Распределяя между собой преступные роли, Осипов М.А. – сервера, ящик, кошелек, Левин А.С. и Литвиненко С.В. - неправомерный доступ, шифрование, нейтрализация СЗИ
- Действуя умышленно, незаконно осуществили неправомерный доступ к компьютерной информации АО «Восточная верфь», что повлекло за собой нарушение рабочего и производственного процесса и причинение имущественного вреда на сумму 655 034,52 рублей.
- Ч.4 ст.274.1 УК РФ, 2 года лишения свободы условно с лишением права заниматься деятельностью, связанной с доступом к критической информационной инфраструктуре Российской Федерации сроком 2 года

ЗА ЧТО НАКАЗЫВАЮТ УЖЕ СЕЙЧАС (6/6)

ГАРДА ТЕХНОЛОГИИ

Следственный № 11807300001000030

ПОСТАНОВЛЕНИЕ

г. Петропавловск-Камчатский 31 мая 2019 года

Петропавловск-Камчатский городской суд Камчатского края в составе председательствующего судьи Меллер А.В.,

при секретаре Никитиной А.А.,

с участием помощника прокурора г. Петропавловска-Камчатского Курбанова Ш.М.,

обвиняемого ФИО1,

защитника – адвоката Самоделкина О.В.,

рассмотрев в закрытом судебном заседании уголовное дело в отношении

ФИО1, <данные изъяты>, несудимого, не содержавшегося под стражей по настоящему делу,

обвиняемого в совершении преступления, предусмотренного ч. 1 ст. 274.1 УК РФ,

УСТАНОВИЛ:

Органами предварительного следствия ФИО1 обвиняется в том, что 18 апреля 2018 года, находясь на своем рабочем месте по адресу: г. Петропавловск-Камчатский, <адрес>, действуя умышленно, посредством своего рабочего компьютера, не желая блокировки мессенджера «Телеграмм» государственными органами Российской Федерации, использовал компьютерное программное обеспечение «LOIC», интегрированное в сайт «loicjs.weebly.com», заведомо для него предназначенное для неправомерного воздействия на критическую информационную структуру Российской Федерации, для блокирования информации, содержащейся на сайтах «rkn.gov.ru», «vigruzki.rkn.gov.ru». Обратившись к сайту «loicjs.weebly.com», в специальном поле указал адрес сайта «vigruzki.rkn.gov.ru» и нажал кнопку начала действия. После чего в автоматическом режиме компьютерным программным обеспечением «LOIC», содержащемся на сайте «loicjs.weebly.com», использованным ФИО1 в период времени с 11 часов 33 минут до 11 часов 43 минут, отправлено 8072 HTTP-запроса на сайт «vigruzki.rkn.gov.ru». Далее ФИО1 вновь обратившись к сайту «loicjs.weebly.com», в специальном поле указал адрес сайта «rkn.gov.ru» и нажал кнопку начала действия. После чего в автоматическом режиме компьютерным программным обеспечением «LOIC», содержащемся на сайте «loicjs.weebly.com», использованным ФИО1 в период времени с 12 часов 22 минут до 12 часов 34 минут, отправлено 8844 HTTP-запроса на сайт «rkn.gov.ru», которые в соответствии с п.п. 7 и 8 ст. 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» являются объектом критической информационной инфраструктуры Российской Федерации, а в соответствии с приказом Роскомнадзора Российской Федерации от 21 февраля 2013 года № 169 являются информационной системой взаимодействия Роскомнадзора Российской Федерации с операторами связи, с целью исчерпания вычислительных ресурсов веб-сервера, обрабатывающего обращения к Интернет-сайту «vigruzki.rkn.gov.ru», «rkn.gov.ru», что могло привести к невозможности получения доступа к информации, размещенной на указанных сайтах, для других лиц или информационных систем, т.е. привести к её блокированию.

1. САЙТ RKN.GOV.RU – ОБЪЕКТ КИИ, НЕТ ССЫЛОК НА АКТЫ КАТЕГОРИРОВАНИЯ
2. ЯВКА С ПОВИННОЙ
3. С РАБОЧЕГО ПК (ФГБУ «ИНСТУТУТ ВУЛКАНОЛОГИИ...»)
4. ОСВОБОЖДЕН ОТ УО В СВЯЗИ С РАСКАЯНИЕМ

Ч.1 ст. 274.1 УК РФ
– использование компьютерной программы, заведомо предназначенной для неправомерного воздействия на КИИ

ИМПОРТОЗАМЕЩЕНИЕ ДЛЯ ОБЪЕКТОВ КИИ (1/2)

ГАРДА ТЕХНОЛОГИИ

В 239 приказе в текущей редакции:

31. Применяемые в значимом объекте программные и программно-аппаратные средства, в том числе средства защиты информации,

При выборе программных и программно-аппаратных средств, в том числе средств зашиты информации, необходимо учитывать на инфраструктуры на любом из принадлежащих ему значимых объектов критической информационной инфраструктуры со стороны ра

В значимом объекте не допускаются:

наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в том числе сред работниками субъекта критической информационной инфраструктуры;

наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в том числе средствам зашить субъекта критической информационной инфраструктуры;

передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппа стороны субъекта критической информационной инфраструктуры.

Входящие в состав значимого объекта 1 категории значимости программные и программно-аппаратные средства, осуществляю Федерации (за исключением случаев, когда размещение указанных средств осуществляется в зарубежных обособленны представительствах), а также случаев, установленных законодательством Российской Федерации и (или) международными договора

32. При использовании в значимых объектах новых информационных технологий и выявлении дополнительных угроз безопасно разрабатываться компенсирующие меры в соответствии с пунктом 26 настоящих Требований.

ИМПОРТОЗАМЕЩЕНИЕ ДЛЯ ОБЪЕКТОВ КИИ (2/2)

ГАРДА ТЕХНОЛОГИИ

Февральские поправки ФСТЭК не прошли, но «намек понят».

9. В пункте 31:

в абзаце четвертом слова «не являющихся работниками субъекта критической информационной инфраструктуры» заменить словами «являющихся работниками зарубежных организаций, а также организаций, находящих под прямым или косвенным контролем иностранных физических и (или) юридических лиц»;

в абзаце седьмом слова «1 категории» заменить словами «1 и 2 категорий».

10. Пункт 32 изложить в следующей редакции:

«32. В значимом объекте не допускается техническая поддержка программных и программно-аппаратных средств, в том числе средств зашиты информации, зарубежными организациями, а также организациями, находящимися под прямым или косвенным контролем иностранных физических и (или) юридических лиц.».

ГАРДА
ТЕХНОЛОГИИ

НАШИ ПРОДУКТЫ И КЕЙСЫ ПРИМЕНЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БКИИ

ПРАКТИЧЕСКИЙ ПОДХОД К ЗАЩИТЕ

ГАРДА
ТЕХНОЛОГИИ

ПОМОГАЕМ РЕАЛИЗОВЫВАТЬ ПРАКТИЧЕСКИЙ ПРОЦЕССНЫЙ ПОДХОД, ЗАЛОЖЕННЫЙ В ПРИКАЗЕ ФСТЭК №235 И ДРУГИХ НОРМАТИВНЫХ АКТАХ ФСТЭК И ФСБ

ПРЕДОТВРАЩЕНИЕ НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИЮ, ОБРАБАТЫВАЕМУЮ НА ОБЪЕКТАХ КИИ

ФОКУС ЗА ИНЦИДЕНТАХ, АТАКАХ И ВОЗМОЖНОМ УЩЕРБЕ

ОБНАРУЖЕНИЕ, РЕАГИРОВАНИЕ И РАССЛЕДОВАНИЕ

ПОЧЕМУ РЕАЛЬНАЯ БЕЗОПАСНОСТЬ - ЭТО ВАЖНО

ГАРДА ТЕХНОЛОГИИ

Датский производитель насосов DESMI стал жертвой кибератаки

13:54 / 13 Апреля, 2020

DESMI | кибератака | прои

В результате атаки были отключены все компьютерные системы компании.

SCADA-системы израильской сферы водоснабжения подверглись целевым атакам

Екатерина Быстрова 28 апреля 2020 - 13:18

Государство | Целевые атаки

Мошенники взламывали серверы на АЗС ради бесплатного топлива

14:47 / 3 Июня, 2020

АЗС | взлом | вредоносное

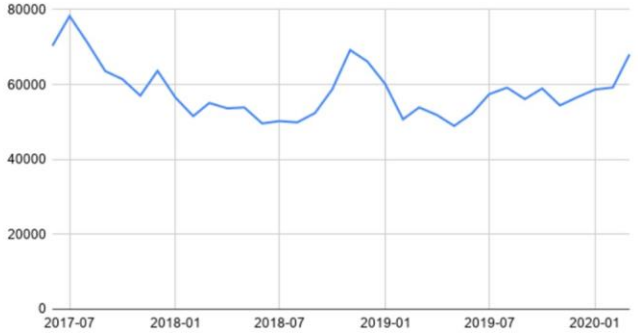
Kaspersky ICS CERT kaspersky

2019 год: главное

- В 2019 году Kaspersky ICS CERT было выявлено 103 уязвимости в промышленных системах, системах IIoT/IoT и других типах решений.
  - 33 из обнаруженных уязвимостей до сих пор не исправлены производителями соответствующих продуктов, хотя они получили для этого всю необходимую

Vulnerable to BlueKeep (CVE-2019-0708)

Shodan - Remote Desktop Port (3388)



Shodan report, March 2020

Shodan - Industrial Control Systems

ЧТО ПРОИСХОДИТ С ВАЖНЫМИ СИСТЕМАМИ

БАЗЫ ДАННЫХ — ОСНОВНОЙ ИСТОЧНИК НАИБОЛЕЕ ЦЕННОЙ КОРПОРАТИВНОЙ ИНФОРМАЦИИ.

КРОМЕ ВЛАДЕЛЬЦЕВ ДАННЫХ ЭТА ИНФОРМАЦИЯ ИНТЕРЕСУЕТ МНОЖЕСТВО ДРУГИХ ЛЮДЕЙ.

ИНСАЙДЕРЫ

Хищения информации сотрудниками с целью продажи конкурентам или использования на новом месте работы.

ХАКЕРЫ

Целенаправленные атаки на базы данных для получения доступа к ним.

ПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ

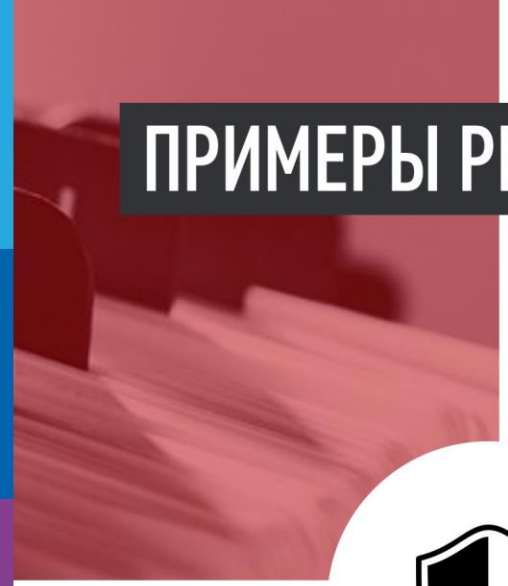
Контроль действий администраторов баз данных.

ХАЛАТНОСТЬ

Случайные утечки данных, совершенные по неосторожности.

ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ

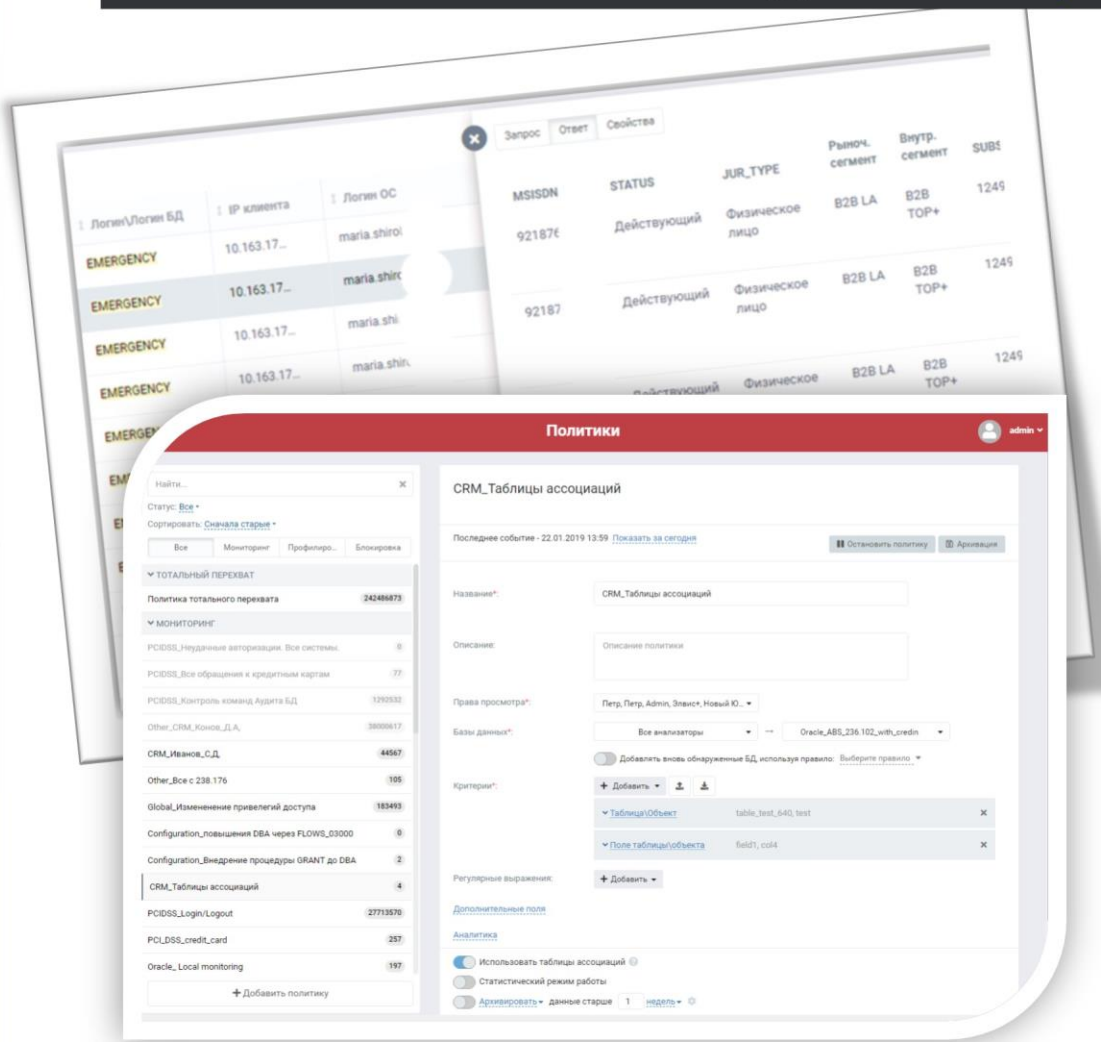
ГАРДА
ТЕХНОЛОГИИ



- Предотвращение выгрузки и продажи критичных данных клиентов, в том числе персональных данных, данных кредитных карт и т.д.
- Контроль манипуляций с клиентскими базами, накрутки KPI менеджерами
- Проверка БД на обезличенность при их передаче (например при их клонировании для целей тестирования)
- Разграничение доступа к СУБД для аттестации информационных систем
- Выявление не оптимально настроенных конфигураций СУБД с точки зрения стандартов и лучших практик по информационной безопасности
- Предотвращение мошенничества и прямых хищений денежных средств с использованием БД и бизнес-приложений компании
- Выявление несанкционированного разворачивания теневых, нелегитимных и неконтролируемых баз данных со стороны администраторов
- И другие

МОНИТОРИНГ КРАЖИ ДАННЫХ (И АДМИНИСТРАТОРАМИ)

ГАРДА ТЕХНОЛОГИИ



ЗАДАЧА

Известно множество способов и попыток слива чувствительных данных (персональных данных, коммерческой тайны) из централизованных систем. Однако, использования только лишь систем специализированных DLP на рабочих местах сотрудников не даёт возможности полного контроля и профилактики выноса важной базы данных.

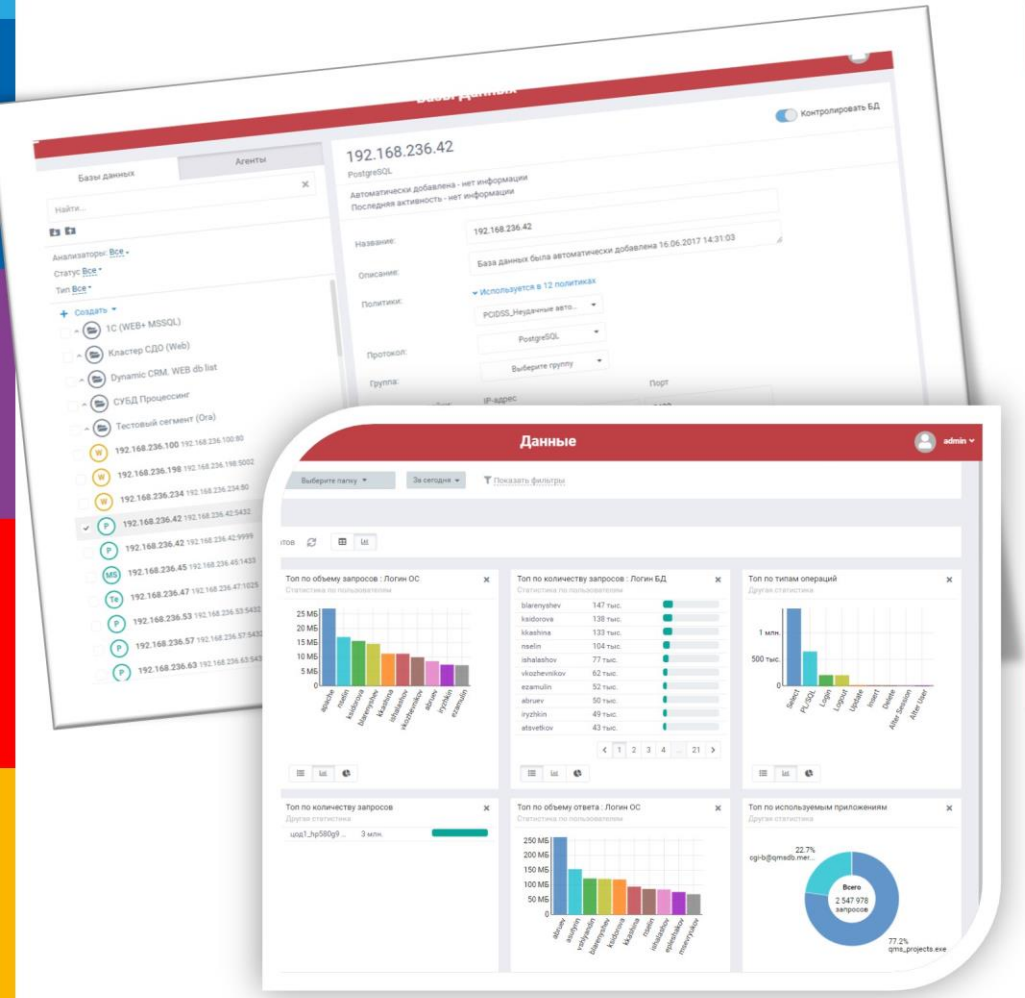
КАК ПОМОГАЕТ ГАРДА БД

Гарда БД контролирует и фиксирует все обращения непосредственно в базах данных, на которых работают ERP, CRM и другие системы. Гарда БД не оставляет белых пятен для службы ИБ и позволяет обнаружить:

- Большие единовременные выгрузки из баз данных
- Выгрузки из баз данных небольшими кусками в течение определенного времени
- Попытки злоумышленника воспользоваться ИТ-инструментами, отладочными программами
- Попытки администраторов выгрузить данные, напрямую подключившись к СУБД

ОБНАРУЖЕНИЕ НЕЛЕГИТИМНЫХ КОПИЙ «БОЕВЫХ» БД

ГАРДА ТЕХНОЛОГИИ



ЗАДАЧА

В крупных организациях с множеством систем и баз данных, нередко разворачиваются «тестовые контуры» с более мягкими требованиями по защите и ограничению доступа к ним. По требованиям информационной безопасности данные в таких «зеркальных» системах не должны быть реальными, а замененными на сгенерированные. Зная, что все обращения к действующим «боевым» базам данных контролируются, некоторые сотрудники в корыстных целях могут создать новую базу, а затем произвести настройку основной базы данных таким образом, что бы ежедневно небольшое количество информации автоматически передавалось из основной базы в новую, не вызывая при этом подозрений. Кроме того, нельзя исключать случаи обычной халатности или действий по незнанию.

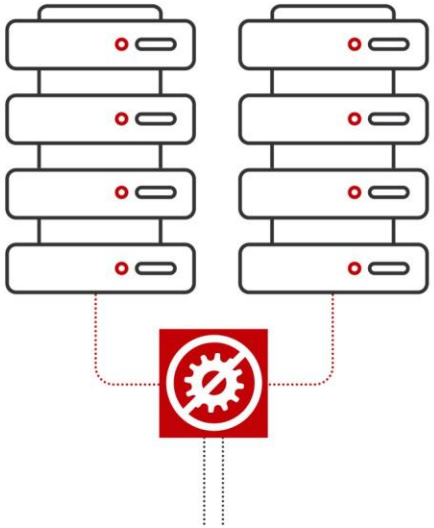
КАК ПОМОГАЕТ ГАРДА БД

В Гарде БД есть функционал сканирования, призванный выявлять все развернутые БД в инфраструктуре компании. Во время сканирования Гарда БД обнаруживает и автоматически классифицирует все новые базы, в том числе определяя их как «теневые» копии основных баз данных.

Кроме того, Гарда БД проверяет базы данных на наличие уязвимостей и даёт рекомендации по их устранению.

ПРИМЕНЕНИЕ НА ОБЪЕКТАХ КИИ

ГАРДА
ТЕХНОЛОГИИ



1 АУДИТ ДЕЙСТВИЙ СЕТЕВЫХ- И БД- АДМИНИСТРАТОРОВ КИИ

2 ЗАЩИТА КРИТИЧНЫХ БД КИИ

3 ВЫЯВЛЕНИЕ «ЛЕВЫХ» БД НА ОБЪЕКТАХ КИИ

4 ДЕТЕКЦИЯ СПЕЦИФИЧНЫХ ИНЦИДЕНТОВ (БД + ПРОМ. ИС)

5 ФИКСАЦИЯ И РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ, СВЯЗ. С ДОСТУПОМ

НАЛОЖЕННОЕ СЕРТИФИЦИРОВАННОЕ СЗИ

ГАРДА ТЕХНОЛОГИИ

АТТЕСТАЦИЯ ИС ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ В СЛУЧАЕ ПРИМЕНЕНИЯ НЕСЕРТИФИЦИРОВАННЫХ СУБД

- Описан технологический процесс обработки информации и ЗИ
- Использованы средства защиты в соответствии с требованиями и моделью угроз
- В части защиты СУБД и приложений использована Гарда БД

НАЗНАЧЕНИЕ СИСТЕМЫ

- Ведение СЭД
- Пром. ERP предприятия (проектирование и часть производства)
- Ведение бухгалтерского и кадрового учета организации
- Информация по клиентам и проектам

ГАРДА БД

- Контроль доступа и активности в базах данных
- Мониторинг локальных действий администраторов в особо критичных БД
- Внедрение и работа в структуре систем организации:
  - Гибкие возможности по выбору платформ
  - Модульность комплекса
  - Сбор событий в нескольких распределенных точках инфраструктуры

ЗАЩИЩАЕМЫЕ РЕСУРСЫ

- СУБД Microsoft SQL
- СУБД PostgreSQL
- пром. ERP
- СЭД
- 1С
- БД веб-сервера

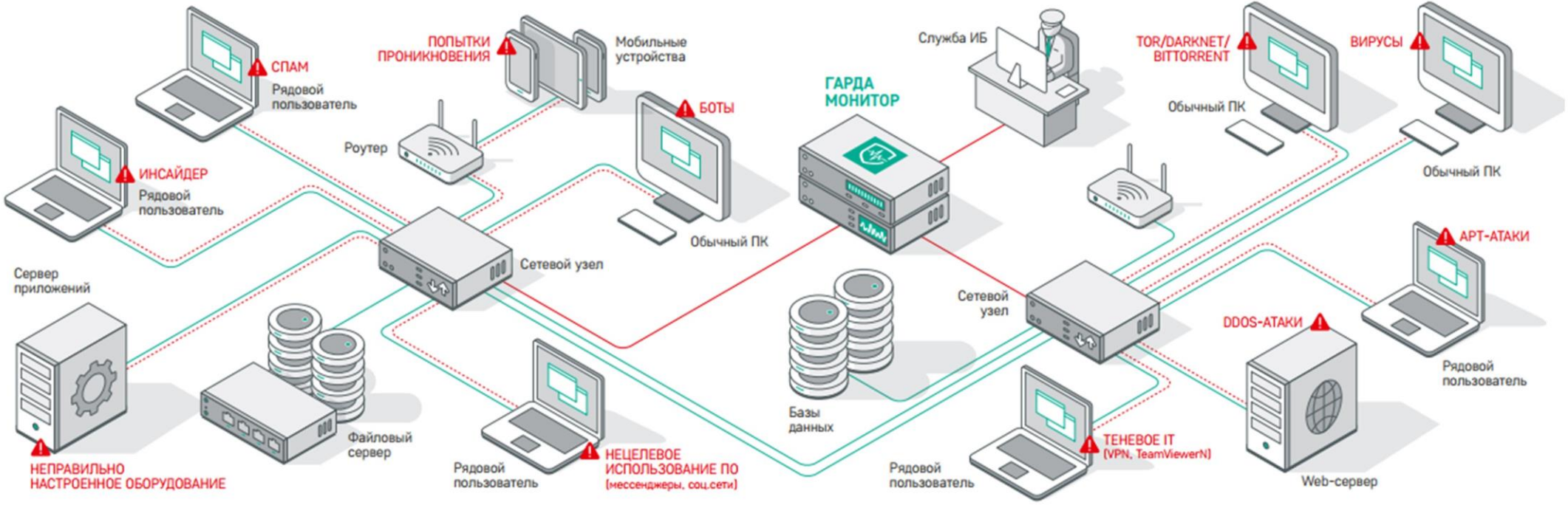
ИТОГ:

УСПЕШНАЯ АТТЕСТАЦИЯ ПО ТРЕБОВАНИЯМ БИ

ЧТО ПРОИСХОДИТ В СЕТИ КОМПАНИИ

ГАРДА
ТЕХНОЛОГИИ

- ЗАПИСЬ СЕТЕВОГО ТРАФИКА
- ВЫЯВЛЕНИЕ АНОМАЛИЙ
- ОБНАРУЖЕНИЕ КИБЕРАТАК И ВИРУСОВ
- КОНТРОЛЬ «ТЕНЕВЫХ» ТЕХНОЛОГИЙ В СЕТИ
- ВЫЯВЛЕНИЕ ОШИБОК ИТ
- РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ



ИНСТРУМЕНТ ДЛЯ ЕЖЕДНЕВНОЙ РАБОТЫ

ГАРДА ТЕХНОЛОГИИ

«ГАРДА МОНИТОР» ПОЗВОЛЯЕТ

- ☑ Навести порядок в сети компании
- ☑ Обнаружить аномалии и потенциально уязвимые места сети
- ☑ Анализировать сетевые события
- ☑ Оценить, что предшествовало инциденту и каковы последствия
- ☑ Проверить корректность настройки IT-оборудования
- ☑ Выявить нецелевое использование ресурсов
- ☑ Обеспечить тотальный контроль сети

ПОМОГАЕТ ДИРЕКТОРУ ПО ИБ:

- Обнаружить попытки взлома критических бизнес-ресурсов и нелегитимного доступа к конфиденциальным данным
- Получить оперативную сводку по угрозам безопасности, в т.ч. сведения о попытках атак на инфраструктуру
- Увидеть подробную статистику по нарушениям политик безопасности в компании

ПОМОГАЕТ АНАЛИТИКУ SOC:

- Проводить подробное расследование инцидентов
- Собирать артефакты попыток совершения атаки
- Обнаруживать следов злонамеренного сканирования портов, служб и сервисов
- Выявить присутствие хакеров внутри корпоративной инфраструктуры

ПОМОГАЕТ ОФИЦЕРУ ИБ:

- Выявлять и детектировать вредоносную активность и сетевые атаки
- Инвентаризировать используемые устаревшие и уязвимые протоколы
- Выявлять использование нелегального шифрования, нелегального удаленного доступа (прокси, TOR, VPN и др.)

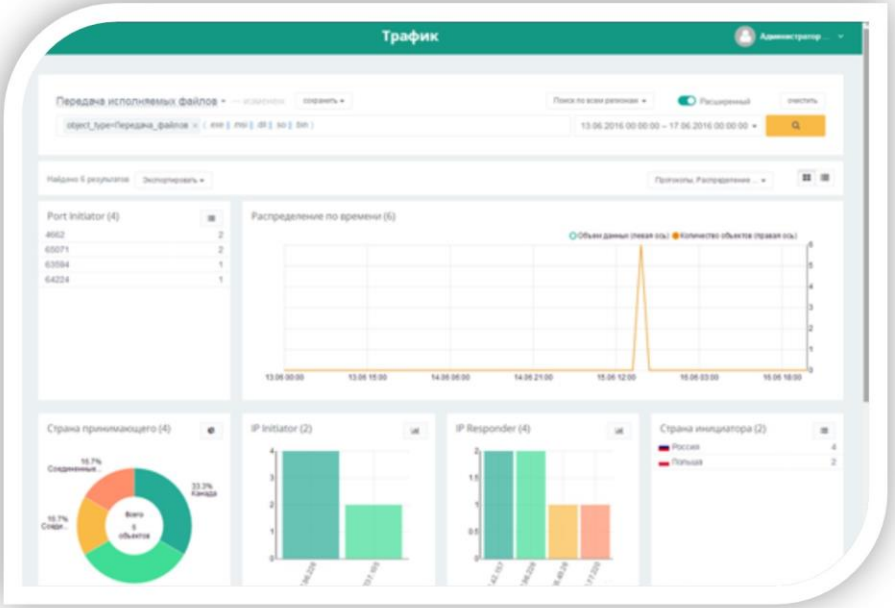
ПОМОГАЕТ РУКОВОДИТЕЛЮ ПО ИТ:

- Собирать статистику используемых протоколов и сетевых служб
- Повышать прозрачность сетевых потоков компании
- Выявить «всплески» и «провалы» в сетевой активности
- Выявить нецелевое использование корпоративных ресурсов

МАЙНИНГ НА РАБОЧЕМ МЕСТЕ

ГАРДА
ТЕХНОЛОГИИ

ЧЕМ ОПАСНО?



1 СЛОЖНО ДОКАЗАТЬ РЕАЛЬНЫЙ УЩЕРБ

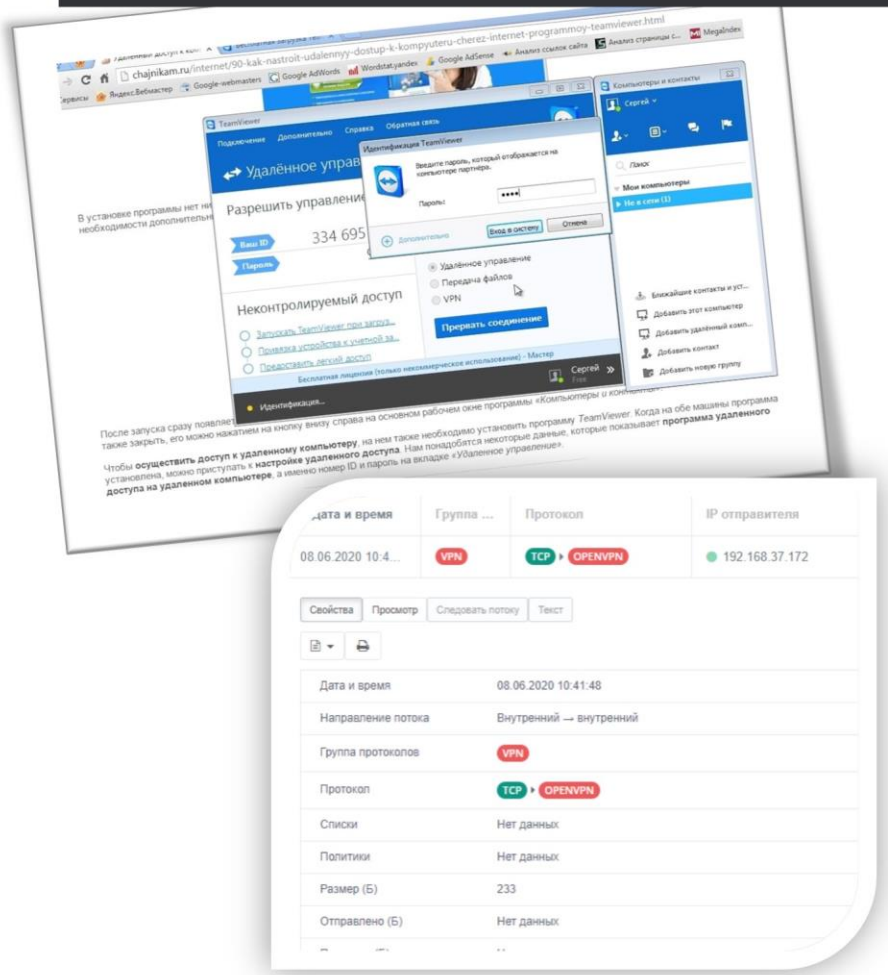
2 ВИРУСЫ ПОД ВИДОМ МАЙНЕР-КЛИЕНТОВ

3 НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ ВРЕМЕНИ

4 CRYPTOJACKING – МАЙНЕРЫ-ВРЕДОНОСЫ

НЕЛЕГАЛЬНЫЙ УДАЛЕННЫЙ ДОСТУП ИЗ ДОМА

ГАРДА ТЕХНОЛОГИИ



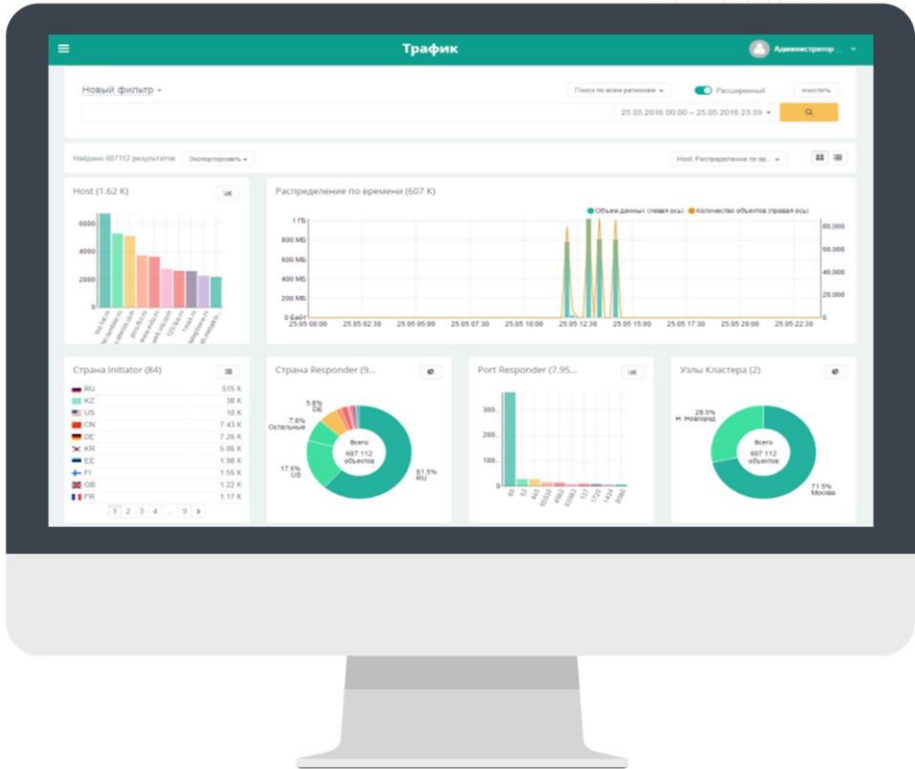
ЧЕМ ОПАСНО?

1. ПОТЕРЯ КОНТРОЛЯ ДОСТУПОВ
2. ПОДКЛЮЧЕНИЕ ИЗ ЛЮБЫХ ЛОКАЦИЙ
3. ВРЕДОНОСНАЯ АКТИВНОСТЬ ВНУТРИ
4. СЛОЖНОСТИ ПРИ РАССЛЕДОВАНИИ

ЗАЩИТА ОТ ЗАРАЖЕНИЯ ВРЕДОНОСНЫМ ПО И ВНЕШНИХ АТАК

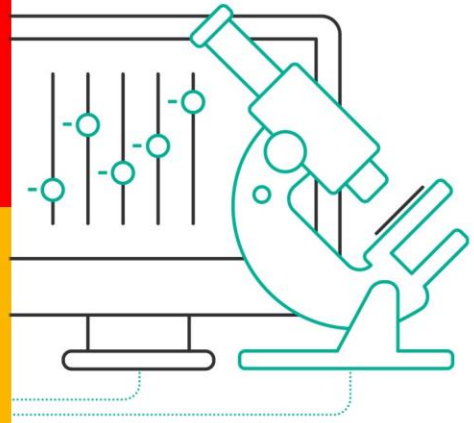
КОНТРОЛИРУЕМ ИНФРАСТРУКТУРУ ПРЕДПРИЯТИЯ НА ВСЕХ УРОВНЯХ: РАБОЧИЕ МЕСТА, БИЗНЕС- И ПРОИЗВОДСТВЕННЫЕ СИСТЕМЫ, СЕТЕВОЙ ТРАФИК

- Целевые и DDOS-атаки, попытки проникновений в сеть извне
- Контроль вирусных заражений, недопущение распространения эпидемий в инфраструктуре, в том числе шифровальщиков и «уничтожителей»
- Пресечение случаев майнинга криптовалюты
- Вычисление долговременного присутствия злоумышленников в инфраструктуре
- Мониторинг трафика иностранного происхождения и darknet-соединений



ПРИМЕНЕНИЕ НА ОБЪЕКТАХ КИИ

ГАРДА
ТЕХНОЛОГИИ



1 ОЦЕНКА ТЕКУЩЕГО СОСТОЯНИЯ СЕТИ И КОНРОЛЬ ИЗМЕНЕНИЙ

2 ЗАПИСЬ И ХРАНЕНИЕ ВСЕГО СЕТЕВОГО ТРАФИКА

3 ДЕТЕКЦИЯ СПЕЦИФИЧЕСКИХ ДЛЯ АСУ ТП УГРОЗ

4 РАСПРЕДЕЛЕННАЯ УСТАНОВКА, КОНТРОЛЬ ИЗ ЦЕНТРА SOC/СОПКА

5 ПАССИВНОЕ ВНЕДРЕНИЕ, НЕ ОКАЗЫВАЕТ ВЛИЯНИЕ НА СЕТЬ

ЧТО ПРОИСХОДИТ НА РАБОЧИХ УСТРОЙСТВАХ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ПРЕДПРИЯТИЕ

#1 Выявляет нарушения и угрозы уже на пилоте

#2 Контролирует все каналы, позволяет восстановить полную картину бизнес-коммуникаций в любой момент

#3 Контролирует рабочее время сотрудников, блокирует недопустимые действия

#4 Блокирует передачу конфиденциальных данных

#5 Помогает в расследовании инцидентов безопасности

ПРИНЦИП РАБОТЫ DLP

ГАРДА
ТЕХНОЛОГИИ

КОНТРОЛЬ ИНФОРМАЦИОННЫХ ПОТОКОВ

- Анализатор трафика контролирует сетевые каналы на соответствие передаваемых данных установленным политикам ИБ.
- Агент рабочего места контролирует ПК и подключенные к нему устройства, обеспечивает выполнение заданных политик ИБ

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ

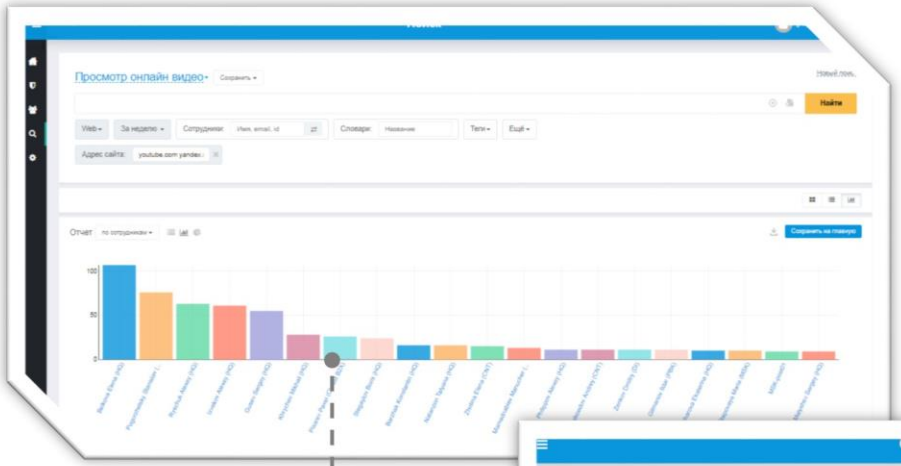
- Система предоставляет гибкие возможности для администрирования и управления процессами перехвата данных
- Анализ данных для определения инцидентов безопасности и построения отчётности

ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ ХРАНЕНИЯ И ПОИСКА

- Система обеспечивает запись и хранение данных, передаваемых в компании
- Постоянный мониторинг данных со всех подключенных к системе информационных каналов

МОНИТОРИНГ АКТИВНОСТИ

ГАРДА ТЕХНОЛОГИИ



ТОП УЧЕТОК ПО КРИТЕРИЯМ НА РАБОЧЕМ МЕСТЕ

ОТЧЁТ ПО РАБОЧЕМУ ДНЮ СОТРУДНИКА

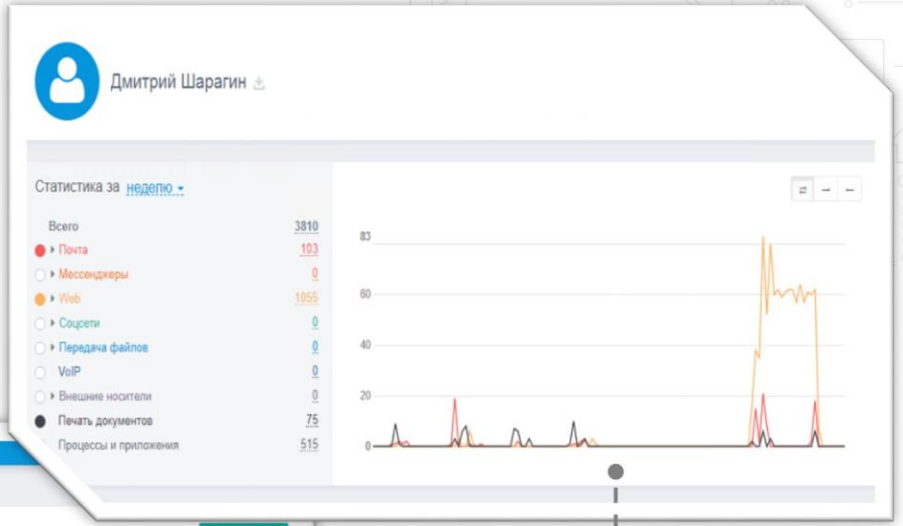


ГРАФИК АКТИВНОСТИ

ПРИМЕНЕНИЕ НА ОБЪЕКТАХ КИИ

ГАРДА
ТЕХНОЛОГИИ

1. УСТАНОВКА ЛЕГКИХ АГЕНТОВ (В Т.Ч. НА СТАРЫЕ ОС)
2. ТОТАЛЬНАЯ ЗАПИСЬ ВСЕХ ДЕЙСТВИЙ НА АРМ
3. ЗАПРЕТ НОСИТЕЛЕЙ И ПРИЛОЖЕНИЙ
4. ВЫЯВЛЕНИЕ «ТЕНЕВЫХ» ИТ В УСЛОВИЯХ ЗАПРЕТОВ НА АСУ ТП
5. ФИКСАЦИЯ ЮРИДИЧЕСКИ ЗНАЧИМЫХ ФАКТОВ

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

ГАРДА МОНИТОР

ВЫЯВЛЕНИЕ
И РАССЛЕДОВАНИЕ
СЕТЕВЫХ ИНЦИДЕНТОВ

ГАРДА БД

АУДИТ И ЗАЩИТА
БАЗ ДАННЫХ
И ВЕБ-ПРИЛОЖЕНИЙ

ГАРДА ПРЕДПРИЯТИЕ

КОНТРОЛЬ И АНАЛИЗ
ИНФОРМАЦИОННЫХ
ПОТОКОВ
КОМПАНИИ

ГАРДА АНАЛИТИКА

ПЛАТФОРМА
ИНФОРМАЦИОННОЙ
И ЭКОНОМИЧЕСКОЙ
БЕЗОПАСНОСТИ

ПЕРИМЕТР

ПРЕДУПРЕЖДЕНИЕ,
ОБНАРУЖЕНИЕ
И ПОДАВЛЕНИЕ
DDOS-АТАК

ФРОД ИНДЕКС

БОРЬБА
С МОШЕННИЧЕСТВОМ
И ГАРАНТИРОВАНИЕ
ДОХОДОВ ОПЕРАТОРОВ
СВЯЗИ

+ ОКАЗАНИЕ ЦЕНТРОМ УСЛУГ МОНИТОРИНГА И ЗАЩИТЫ ДЛЯ СУБЪЕКТОВ КИИ ПО СЕРВИСНОЙ МОДЕЛИ

ПРИКАЗ ФСТЭК №239 & НАШИ РЕШЕНИЯ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ПРЕДПРИЯТИЕ

ФСТЭК

	Защита машинных носителей информации (ЗНИ)			
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации			
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+	+	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации			+
ЗНИ.7	Контроль подключения машинных носителей информации	+	+	+
	Аудит безопасности (АУД)			
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.9	Анализ действий пользователей			+
	Обеспечение целостности (ОЦЛ)			
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			+
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		+	+
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+

	Реагирование на компьютерные инциденты (ИНЦ)			
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+
	Управление конфигурацией (УКФ)			
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+

ГАРДА БД

ФСТЭК

	Реагирование на компьютерные инциденты (ИНЦ)			
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+
	Аудит безопасности (АУД)			
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.9	Анализ действий пользователей			+
	Обеспечение целостности (ОЦЛ)			
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			+
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		+	+
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+

ГАРДА МОНИТОР

	Реагирование на компьютерные инциденты (ИНЦ)			
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+

	Аудит безопасности (АУД)			
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.9	Анализ действий пользователей			+

ТЕХНИЧЕСКИЕ СРЕДСТВА ГОССОПКА (1/2)

ГАРДА ТЕХНОЛОГИИ

(Приказ №196)

НАИМЕНОВАНИЯ КЛАССА СРЕДСТВА ГОССОПКА	ГАРДА БД, ГАРДА ПРЕДПРИЯТИЕ	ГАРДА МОНИТОР
Средства для обнаружения компьютерных атак	+	+
Средства для предупреждения компьютерных атак	+	+
Средства для ликвидации последствий компьютерных атак		
Средства поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры (ППКА)		+
Средства обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак*	+	+

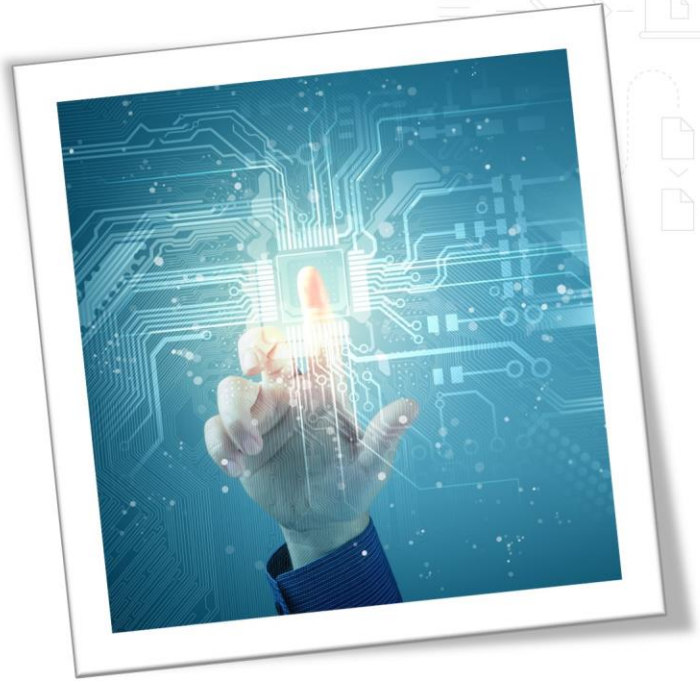
ТЕХНИЧЕСКИЕ СРЕДСТВА ГОССОПКА (2/2)

ГАРДА ТЕХНОЛОГИИ

КАТЕГОРИЯ ИНЦИДЕНТА	ГАРДА БД / ГАРДА ПРЕДПРИЯТИЕ	ГАРДА МОНИТОР
Заражение вредоносным программным обеспечением (malware)	+	+
Распространение вредоносного программного обеспечения (malware distribution)	+	+
Нарушение или замедление работы контролируемого информационного ресурса (availability)		+
Несанкционированный доступ в систему (intrusion)	+	+
Попытки несанкционированного доступа в систему или к информации (intrusion attempt)	+	+
Сбор сведений с использование ИКТ (information gathering)	+	+
Нарушение безопасности информации (information content security)	+	+
Распространение информации с неприемлемым содержимым (abusive content)	+	+
Мошенничество с использованием ИКТ (fraud)	+	+
Уязвимость (vulnerability)		+

ЧЕК-ЛИСТ/ПОЛЕЗНЫЕ СОВЕТЫ ПОСЛЕ КАТЕГОРИРОВАНИЯ

1. ВЫСТРОЙТЕ/ПРОВЕДИТЕ РЕВИЗИЮ ПРОЦЕССОВ
2. СОГЛАСУЙТЕ ОБМЕН С ФСБ (НЕ ТОЛЬКО ЗО КИИ!)
3. НЕ ЗАБЫВАЙТЕ ПРО РЕАЛЬНУЮ ИБ
4. ПОСТАРАЙТЕСЬ СОГЛАСОВАТЬ С ДРУГИМИ НПА
5. ИСПОЛЬЗУЙТЕ УЖЕ ВЫПУЩЕННЫЕ ОРД В СВОИХ ЦЕЛЯХ



ПОЛЕЗНЫЕ МАТЕРИАЛЫ ПО КИИ

ГАРДА ТЕХНОЛОГИИ

НАИМЕНОВАНИЕ	ССЫЛКА
Типовой план мероприятии по теме КИИ от ДИТ Москвы	https://www.mos.ru/dit/documents/informatcionnaia-bezopasnost/view/226311220/
Методические материалы ДИТ Москвы	https://www.mos.ru/dit/documents/informatcionnaia-bezopasnost
Методические материалы АРСИБ	http://aciso.ru/files/docs/metodichka_2.0.pdf
Методические материалы АДЭ (в основном – в области связи)	http://www.rans.ru/images/metrecKII.pdf
Методические материалы Минэнерго	https://minenergo.gov.ru/view-pdf/11357/102517
Практика по теме КИИ от Норникеля (в отношении судов)	https://club-bip.ru/ru/news/art-24
Письмо ФСТЭК про удалёнку на КИИ	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/290-inye/2060-pismo-fstek-rossii-ot-20-marta-2020-g-n-240-84-390
Метод. материалы Минздрава	http://portal.egisz.rosminzdrav.ru/materials/3635

РЕШЕНИЯ «ГАРДА»

ГАРДА
ТЕХНОЛОГИИ

"ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БИЗНЕСА И ГОСУДАРСТВА"

г. Нижний Новгород, пр. Гагарина, 50\9
8 (831) 422 12 21

г. Москва, Мичуринский пр-т, д. 27, корп. 5
8 (495) 540 05 27

info@gardatech.ru

/gardatechnologies

/garda_tech