NITEC

Первый государственный ОЦИБ (SOC). Тернистый путь первопроходца

Гани Надирханов
управляющий директор АО «НИТ»

Управление администрирования СКЗИ и систем ИБ

ИТОГИ РАБОТЫ ЗА 2018 ГОД

Количество подключенных серверов к SIEM	411 серверов
Количество обнаруженных и заблокированных событий ИБ на IPS*	5 901 746 событий ИБ
Антивирусное ПО установлено на	1 344 рабочих станциях
Количество обнаруженных и заблокированных вирусных угроз	34 176 угроз
Количество писем заблокированных системой защиты почтового трафика (из 1 767 352 писем)	325 349 писем
Количество запросов заблокированных системой защиты веб-трафика (из 3 096 029 478 запросов)	265 419 043 запросов
Количество просканированных серверов и выявленных уязвимостей	4 030 серверов, 167 687 уязвимостей

*IPS - intrusion prevention system (система предотвращения вторжений)

СВЫШЕ 1 500 000 АТАК

НА СЕРВЕРА И ИНФОРМАЦИОННЫЕ РЕСУРСЫ ОРГАНОВ ВЛАСТИ

ИТОГИ РАБОТЫ ПО СОСТОЯНИЮ НА МАРТ 2019 ГОДА

ИБ-системы в 2018 году — **16**

1. Программно-аппаратный комплекс (ПАК) кластер из двух межсетевых экранов следующего поколения
2. ПАК для защиты удаленного доступа
3. ПАК «Интеллектуальный межсетевой экран Веб-приложений»
4. ПАК системы сбора журнальных событий с последующим анализом и корреляцией (расширение)
5. ПАК для защиты от вредоносного кода»
6. ПАК «межсетевых экранов следующего поколения»
7. ПАК по защите электронных ресурсов в сети Интернет (Web Application Firewall)
8. СХД серверное оборудование
9. Сетевой разветвитель
10. Поддержка системы защиты веб-трафика (MWG+MEG) от производителя уровня GOLD
11. Поддержка системы управления событиями информационной безопасности (SIEM) от производителя уровня GOLD
12. Поддержка защиты виртуальных конечных точек от производителя уровня GOLD
13. Поддержка хранилища для SIEM (системы управления событиями информационной безопасности) от производителя уровня GOLD
14. Поддержка интеллектуальной системы безопасности (IPS) от производителя уровня GOLD
15. Поддержка защиты конечных точек от производителя уровня GOLD
16. Поддержка защиты серверов от производителя уровня GOLD

2019 год **+5 новых систем**

ИТОГИ РАБОТЫ ЗА 2018 ГОД

- Разработана и утверждена Схема взаимодействия объектов информатизации посредством внешнего шлюза «электронного правительства»
- Включены работы АСБ в «Состав работ по услугам АО «НИТ» для оказания услуг ГО в рамках договоров»
- Осуществлен перенос прокси-серверов Общества на виртуальные ресурсы
- Введены системы ePolicy Orchestrator для сети администраторов
- Введены системы ИБ Content Security Reporter
- Посещены курсы повышения квалификации 5 работниками АСБ

Успешно проведены пилотные проекты:

- Шифрования сегмента ЕТС ГО МИК РК с использованием СКЗИ Certex VPN. Составлена ПМИ и подготовлен протокол тестирования
- Проверки функционала песочницы от казахстанских и российских производителей
- Тестирования ПАК защиты от вредоносного кода
- Тестирования решений для организации защищенной беспроводной сети

ПЛАН РАБОТЫ НА 2019 ГОД

- Администрирование, конфигурирование, мониторинг работоспособности, мониторинг событий, формирование отчетов с систем ИБ
- Организация процедуры закупа систем ИБ на 2019 год в рамках бюджета Общества
- Внедрение новых систем ИБ в эксплуатацию
- Проведение работ по системам сбора журнальных событий с последующим анализом и корреляцией
- Подключение серверов информационных систем, сопровождаемых Обществом
- Обеспечение антивирусным ПО серверов ИС Общества и рабочих станций пользователей Общества
- Размещение в каждом ОЦИТ и РЦОД промежуточного сервера управления антивирусным ПО и syslog-сервера для сбора журнальных событий на систему SIEM
- Выявление уязвимостей на серверах корпоративной сети и дата-центра
- Осуществление перехода на новый антивирусный продукт
- Обеспечение доступности каналов связи ЕТС ГО с использованием СКЗИ
- Оказание услуг ГО по ИБ в рамках компетенции АСБ согласно утвержденному Каталогу услуг Общества
- Планирование бюджета АСБ на 2020 год

Управление анализа и расследования киберугроз (основа ОЦИБ)

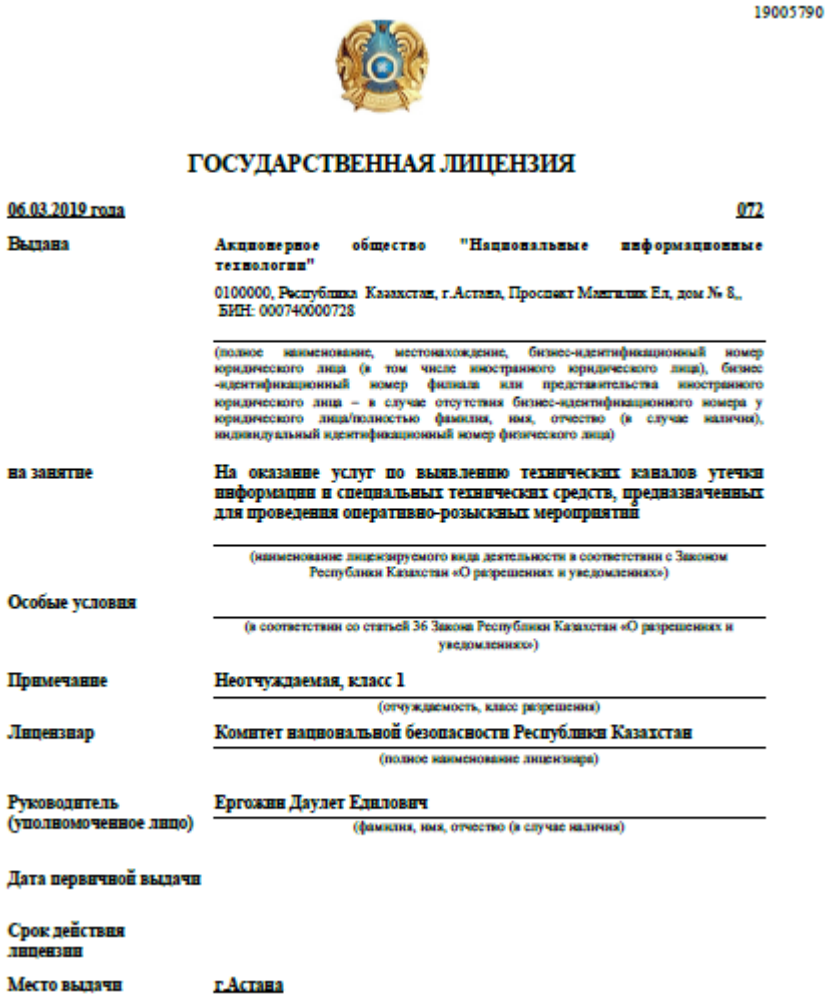
ИТОГИ РАБОТЫ ПО СОСТОЯНИЮ НА МАРТ 2019 ГОДА

Более 2000 подключённых к мониторингу информационных систем

За 1 квартал 2019 года выявлено и заблокировано более 560 тыс. компьютерных атак различных типов.

На постоянной основе проводятся работы по выявлению и устранению инцидентов ИБ.

АО «Национальные информационные технологии» 6 марта 2019 г. получена лицензия №072 на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий.



19005790

ГОСУДАРСТВЕННАЯ ЛИЦЕНЗИЯ

06.03.2019 года — 072

Выдана: Акционерное общество "Национальные информационные технологии"

0100000, Республика Казахстан, г.Астана, Проспект Мангилик Ел, дом № 8,, БИН: 000740000728

(полное наименование, местонахождение, бизнес-идентификационный номер юридического лица (в том числе иностранного юридического лица), бизнес -идентификационный номер филиала или представительства иностранного юридического лица – в случае отсутствия бизнес-идентификационного номера у юридического лица/полностью фамилия, имя, отчество (в случае наличия), индивидуальный идентификационный номер физического лица)

на занятие: На оказание услуг по выявлению технических каналов утечки информации в специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий

(наименование лицензируемого вида деятельности в соответствии с Законом Республики Казахстан «О разрешениях и уведомлениях»)

Особые условия

(в соответствии со статьей 36 Закона Республики Казахстан «О разрешениях и уведомлениях»)

Примечание: Неотчуждаемая, класс 1

(отчуждаемость, класс разрешения)

Лицензиар: Комитет национальной безопасности Республики Казахстан

(полное наименование лицензиара)

Руководитель (уполномоченное лицо): Ергожин Даулет Едилович

(фамилия, имя, отчество (в случае наличия)

Дата первичной выдачи

Срок действия лицензии

Место выдачи: г.Астана

Планы и перспективы SOC-2019

- Вступление в сообщество Forum of Incident Response and Security Teams (FIRST)
- Разработка и утверждение процессов Security Operation Center
- Переход на круглосуточный режим работы мониторинга 24/7
- Создание оперативного центра мониторинга ИБ (Security Operation Center) на базе АО «НИТ», оказание услуг мониторинга состояния информационной безопасности ГО. Лицензия 072 от 06.03.2019
- Настройка сетевого взаимодействия между экземплярами платформы обмена информации о вредоносном ПО (MISP) ГТС КНБ и АО НИТ
- Своевременное оповещение Национального координационного центра информационной безопасности

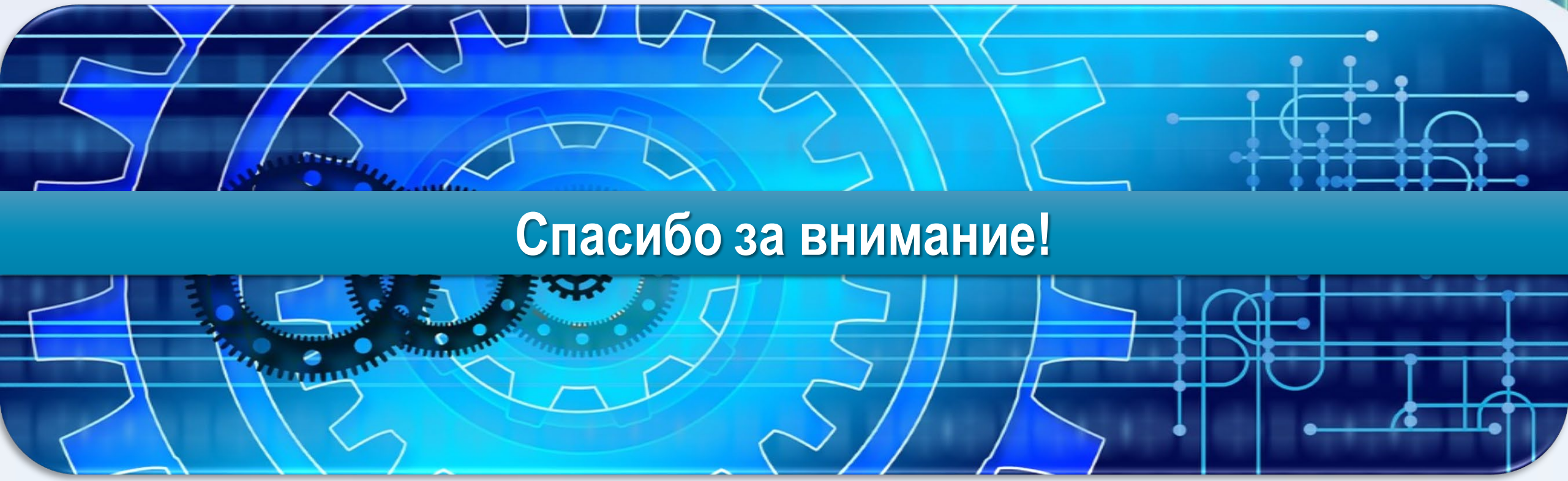
ПЛАН РАБОТЫ НА 2019 ГОД

1	Поиск уязвимостей сетевых служб ИТ ресурсов Общества. Поиск уязвимостей операционных систем и прикладного программного обеспечения ИТ ресурсов Общества
2	Анализ данных, полученных в результате мониторинга событий в системе сбора журнальных событий SIEM
3	Проведение тестов на исследование защищенности ИТ ресурсов общества (Penetration Test). Поиск уязвимостей операционных web сервисов Общества. Закрытие обнаруженных уязвимостей ИТ ресурсов Общества.
4	Техническое и программное сопровождение внедрения системы сбора журнальных событий SIEM Настройка форм отчетности, Создание и настройка правил корреляции, Создание парсеров для источников данных
5	Мониторинг и регистрация инцидентов в системы сбора журнальных событий с последующим анализом и корреляцией
6	Взаимодействие с государственными органами по вопросам информационной безопасности, Прием сообщений о возможных инцидентах и угрозах от KZ-CERT
7	Уведомление государственных органов о зарегистрированных инцидентах в зоне ответственности государственных органов (хостинговые платформы, колокейшн)

недостаток методологической информации

Какие события категоризировать как инциденты?

Каковы этапы проведения анализа и расследования?



Спасибо за внимание!