АО «НАЦИОНАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

ОПЕРАТИВНЫЙ ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

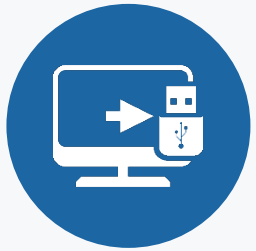
ОБЕСПЕЧЕНИЕ ЗАЩИТЫ
ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ ГОСУДАРСТВЕННЫХ СЛУЖАЩИХ

На территории РК насчитывается более **100 000** персональных компьютеров государственных служащих.
Отсутствие обеспечения защиты персональных компьютеров позволит привести к следующим рискам:

Угроза заражения компьютерными вирусами

Угроза утечки конфиденциальной информации

Неправомерная, скрытая эксплуатация информационно-вычислительных ресурсов (бот-сети, майнинг и т.д.)



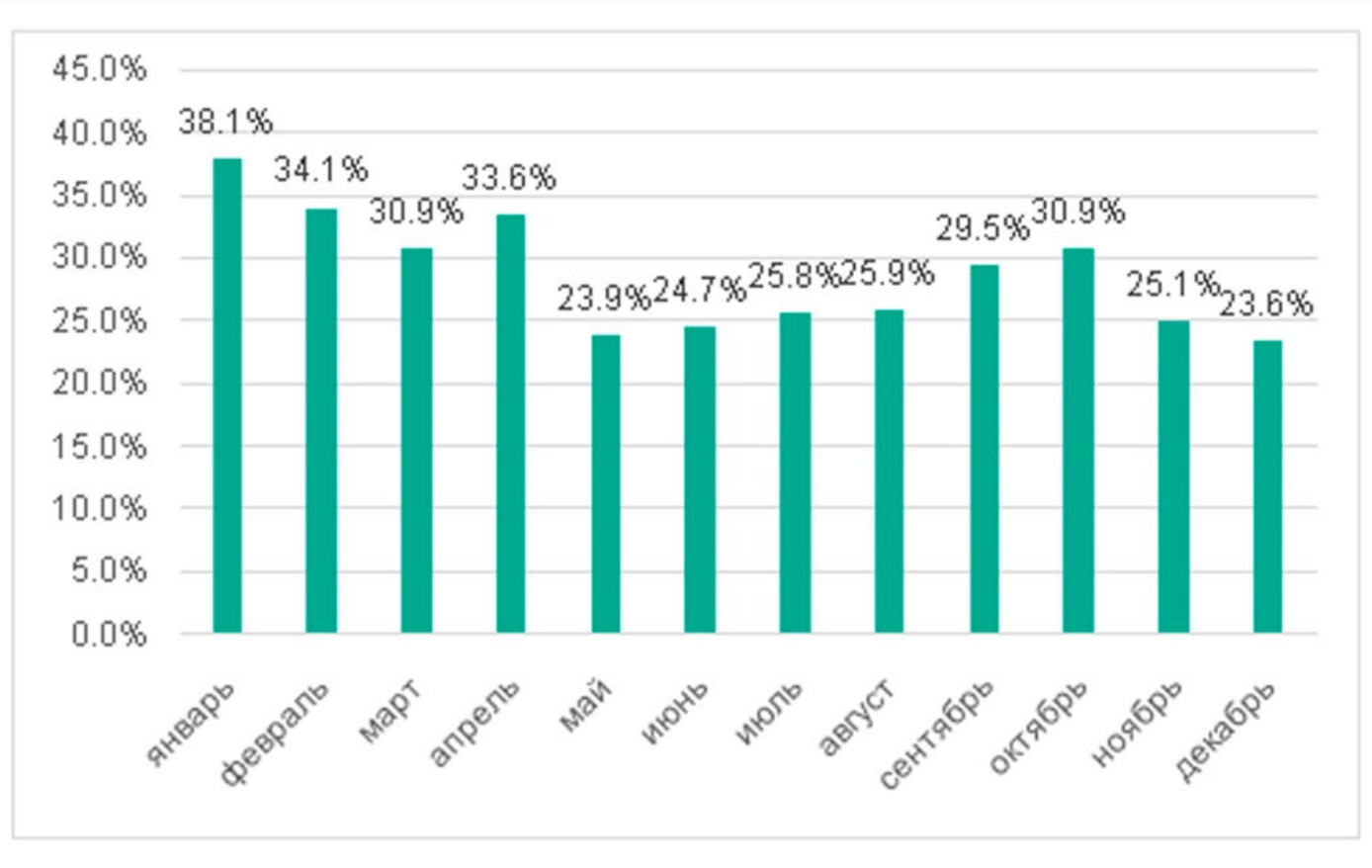
Утечка информации через USB накопитель

Утечка информации путем корпоративной электронный почты

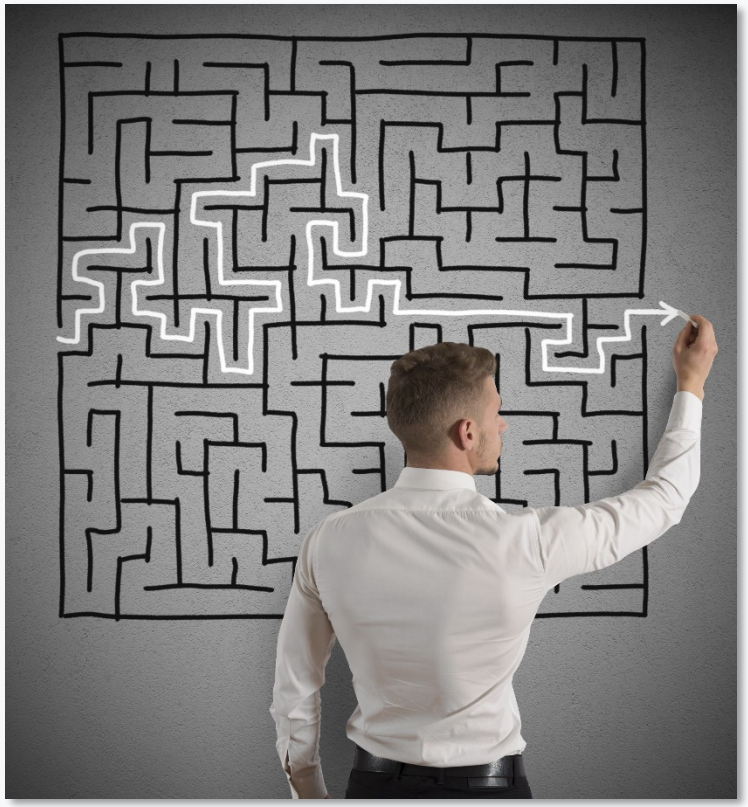
Не актуализированная антивирусная база на персональных компьютерах

АТАКИ НА КАЗАХСТАН

Grey Energy - объекты КВОИКИ
Cobalt – финансовые организации
TajMahal – государственные организации



ПРЕДЛОЖЕНИЯ ПО РЕШЕНИЮ ПРОБЛЕМ
В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНОВ



1. Регулярный технический аудит на соответствие Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности.
2. Совместно с ГТС КНБ РК - проведение на постоянной основе инструментальных обследований информационных систем.
3. Подключение информационных ресурсов государственных органов, КВОИКИ, промышленный сектор, финансовые институты к системе мониторинга Оперативного центра информационной безопасности.
4. Создание на базе ОЦИБ АО «НИТ» академии информационной безопасности для государственных служащих занятых в сфере информационной безопасности квазигосударственного сектора.
5. Дооснащение центра техническими и программными средствами.

УСЛУГИ

ОПЕРАТИВНОГО ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «НИТ»

Наименование услуг

- Технический аудит (pentest), обследование информационных систем на соответствие требованиям информационной безопасности
- Мониторинг обеспечения информационной безопасности, а также защита е-правительства
- Мониторинг безопасного функционирования е-правительства
- Мониторинг интернет-ресурсов Государственных органов в целях их безопасного использования и реагирование на инциденты ИБ
- Взаимодействие с национальным координационным центром информационной безопасности (НКЦИБ)
- Разработка средств защиты информации в части обнаружения, анализа и предотвращения угроз для обеспечения устойчивого функционирования информационных систем и сетей телекоммуникаций Государственных органов
- Координация по вопросам мониторинга обеспечения ИБ, защиты и безопасного функционирования ОИ ЭП, казахстанского сегмента Интернета, а также КВОИКИ, реагирования на инциденты информационной безопасности с проведением совместных мероприятий по обеспечению ИБ
- Сбор, анализ и обобщение информации оперативных центров ИБ об инцидентах информационной безопасности на объектах ИКИ ЭП и других КВОИКИ
- Мониторинг и реагирование на инциденты ИБ компаний, не включённых в список ГО и КВОИКИ

ИТОГИ РАБОТЫ

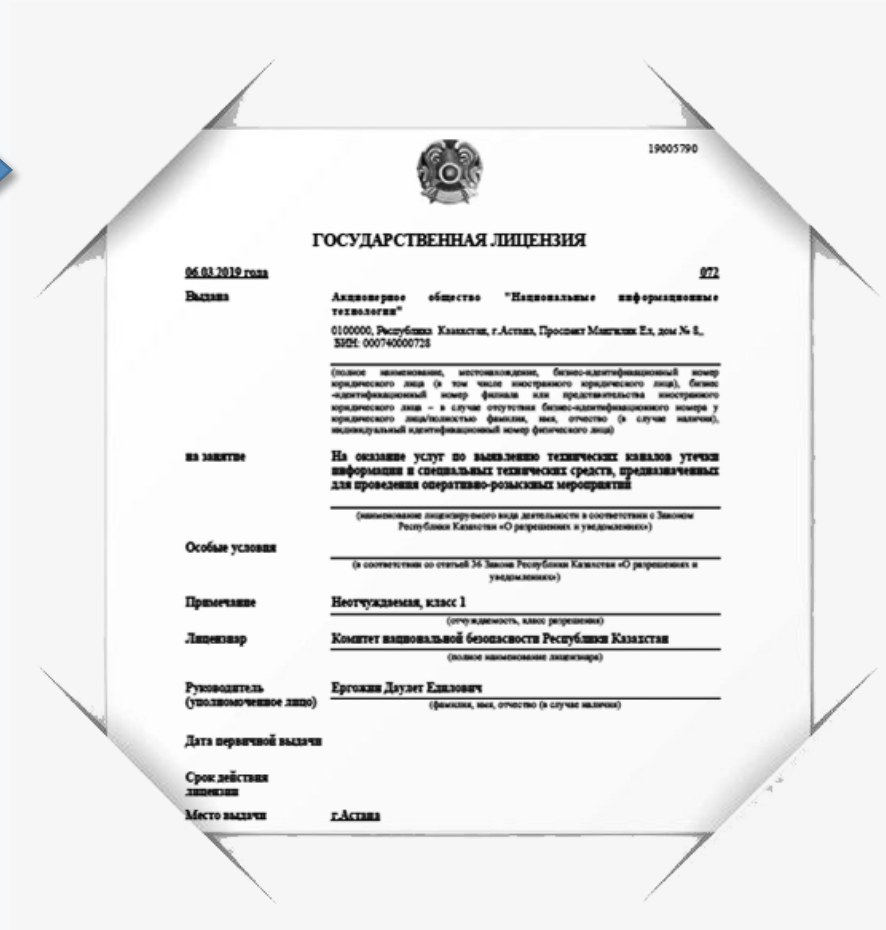
ПО СОСТОЯНИЮ НА МАЙ 2019 ГОДА

АО «НИТ» получена лицензия №72 от 6 марта 2019 г. на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий.

Сформирован кадровый состав сотрудников ОЦИБ, в том числе круглосуточной дежурной смены

Осуществлен переезд ОЦИБ в здание Дома министерств, для дальнейшего подключения к мониторингу информационных систем ГО

Завершены работы по переходу ОЦИБ на круглосуточный режим работы 24/7.



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 и 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 Елдосович

(фамилия, имя, отчество (в случае наличия))

Дата первичной выдачи

Срок действия лицензии

Место выдачи: г.Астана

ПЛАН РАБОТ ОЦИБ

2019 – 2020 г.г.

1. Разработка и утверждение процессов Security Operation Center
2. Настройка сетевого взаимодействия между экземплярами платформы обмена информации о вредоносном ПО (MISP) ГТС КНБ и АО НИТ
3. Своевременное оповещение Национального координационного центра информационной безопасности согласно концепции о разделении ролей Национального координационного центра информационной безопасности и Оперативного центра информационной безопасности Акционерного общества «Национальные информационные технологии» в сфере обеспечения информационной безопасности объектов информатизации государственных органов Республики Казахстан
4. Увеличение количества подключаемых к ОЦИБ источников информационных систем в целях мониторинга и оперативного реагирования на инциденты информационной безопасности
5. Вступление в сообщество Forum of Incident Response and Security Teams (FIRST)

NITEC

ТЕХНИЧЕСКОЕ ОСНАЩЕНИЕ ОПЕРАТИВНОГО ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Платформа оперативного центра информационной безопасности

МЕЖДУНАРОДНЫЕ АНАЛИТИЧЕСКИЕ ЦЕНТРЫ ИБ

KZ-CERT

FIRST — Improving Security Together

Forum of Incident Response and Security Teams

APWG

Anti-Phishing Working Group

СИСТЕМА ВИЗУАЛИЗАЦИИ

ИНТЕЛЕКТУАЛЬНАЯ ПЛАТФОРМА ОБНАРУЖЕНИЯ УГРОЗ

ATD используют общий индикатор компрометации через обмен индикаторами STIX (выражения структурированной информации об угрозе)

ATD (продвинутая защита от угроз безопасности)

TIE Server (сервер обмена данными об угрозах безопасности)

Индикатор компрометации от надежного источника и независимого источника ATD

СЛУЖБА СБОРА ИНФОРМАЦИИ ОБ УГРОЗАХ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

GTI CTIP

СИСТЕМА МОНИТОРИНГА И АНАЛИЗА СОБЫТИЙ

Системы защиты информации

Любые другие источники (серверы, АРМы, СУБД, ОС, прикладные системы, сетевые устройства и прочее)

Ядро системы (SIEM)

IT-системы

АСУ ТП

Системы технической защиты

Национальный координационный центр информационной безопасности **(НКЦИБ)** – структурное подразделение республиканского государственного предприятия на праве хозяйственного ведения "Государственная техническая служба" КНБ РК

ОПЕРАТИВНЫЙ ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ