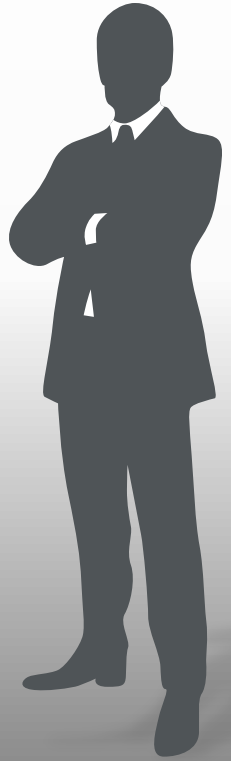
Государственная
техническая служба

Практическая реализация взаимодействия между НКЦИБ и ОЦИБ



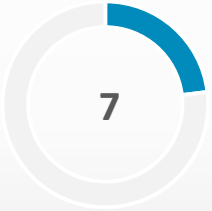
Директор департамента
инструментального анализа РГП «ГТС»

Искаков Медет

Государственная техническая служба

Практическая реализация взаимодействия между НКЦИБ и ОЦИБ

КВОИКИ



ОЦИБ

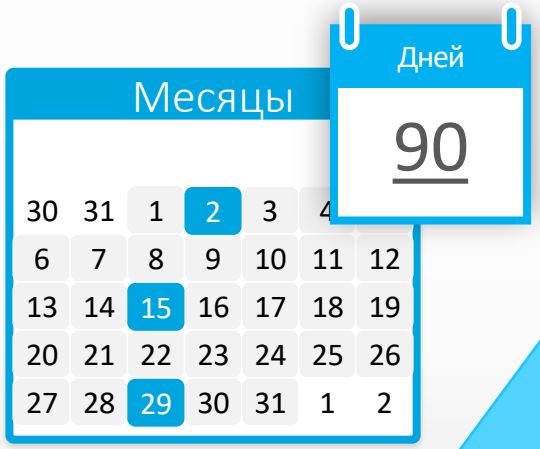
НКЦИБ

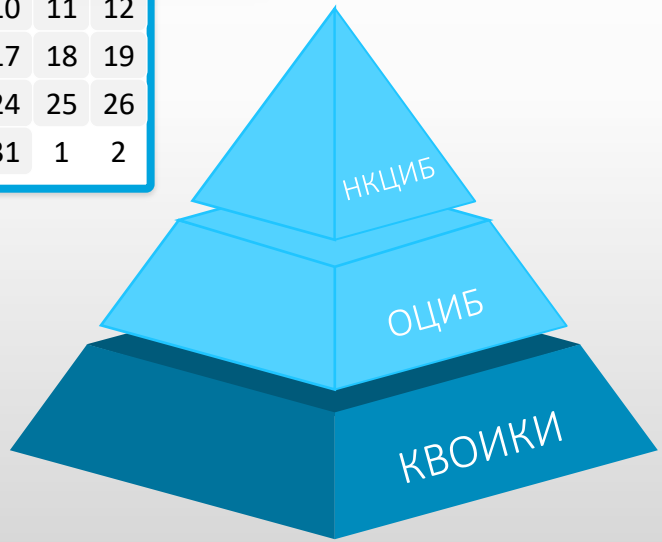
- КВОИКИ – Критически важные объекты информационно-коммуникационной инфраструктуры
- ОЦИБ – Оперативный центр информационной безопасности
- НКЦИБ – Национальный координационный центр информационной безопасности

Общее взаимодействие регулируется на основе Закона РК «Об информатизации»

Государственная техническая служба

КВОИКИ





Собственник или владелец КВОИКИ обеспечивает подключение информационной системы к системе мониторинга обеспечения ИБ КВОИКИ к техническим средствам ОЦИБ, а также определяет ответственного по ИБ КВОИКИ в течение девяноста календарных дней со дня включения в перечень КВОИКИ, утверждаемый согласно подпункту 4) статьи 6 Закона. (пункт 20 Правил*)

Правила проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и КВОИКИ, утвержденные Приказом МОАП РК от 28.03.2018 №52/НҚ

Государственная техническая служба

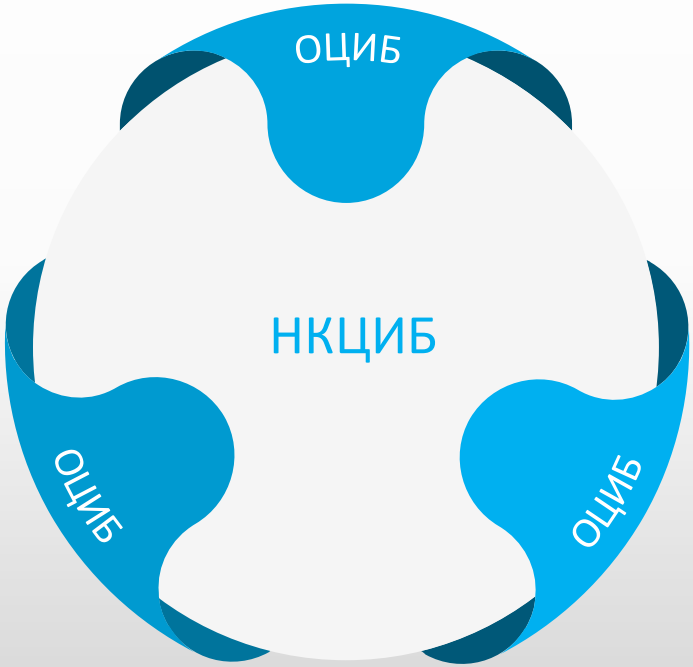
Оперативный центр информационной безопасности

ОЦИБ осуществляет мониторинг обеспечения информационной безопасности КВОИКИ ОИ, не относящихся к объектам информатизации "электронного правительства"(подпункт 3) пункта 1 статьи 7-2. Закона).

Государственная техническая служба

Национальный координационный центр информационной безопасности

НКЦИБ осуществляет сбор, анализ и обобщение информации оперативных центров информационной безопасности об инцидентах ИБ на объектах ИКИ «ЭП» и других КВОИКИ (подпункт 3) пункта 1 статьи 7-4 Закона)



- Сбор данных
- Круглосуточный мониторинг 24/7
- Единая точка взаимодействия

Государственная техническая служба

Взаимодействие между НКЦИБ и ОЦИБ

Для оперативного взаимодействия НКЦИБ с ОЦИБ в рамках Правил в НКЦИБ развернута веб-платформа MISP, к которой подключены все ОЦИБ.

Для регламентации процессов взаимодействия заключены Соглашения о взаимодействии по обнаружению, анализу и реагированию на угрозы/инциденты информационной безопасности посредством веб-платформы Malware information sharing platform НКЦИБ с указанными организациями.

Взаимодействие осуществляется согласно правилам обмена информацией необходимой для обеспечения ИБ между ОЦИБ и НКЦИБ, утвержденных приказом МОАП РК от 19.03.2018 №48/НҚ

Государственная
техническая служба

С начала текущего года НКЦИБ посредством MISP было направлено 1167 уведомлений

Другие организации

11 уведомлений

Банки второго уровня

105 уведомлений

ЦА ГО РК

46 уведомлений

Государственная
техническая служба

Спасибо за внимание!