МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, ОБОРОННОЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН

Комитет по информационной безопасности

Подходы в государственном регулировании сферы информационной безопасности в РК

Количественные показатели информационной безопасности в сфере ИКТ

100 000 ИНТЕРНЕТ-РЕСУРСОВ, С ДОМЕННЫМИ ИМЕНАМИ .KZ И .ҚАЗ АКТИВНО ПОДДЕРЖИВАЮТСЯ

79 658 ОРГАНИЗАЦИЙ В КАЗАХСТАНЕ, ИСПОЛЬЗУЮТ ИНТЕРНЕТ

35 ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

29 000 ОРГАНИЗАЦИЙ ИМЕЮТ СОБСТВЕННУЮ ИНФРАСТРУКТУРУ

2 ОПЕРАТИВНЫХ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

59/219 СТРАТЕГИЧЕСКИХ ОБЪЕКТОВ, ОБЛАДАЮТ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРОЙ

3 СЛУЖБЫ РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ (FIRST)

20 КОМПАНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Качественные показатели уровня информационной безопасности в РК

40

МЕСТО КАЗАХСТАНА В ГЛОБАЛЬНОМ ИНДЕКСЕ КИБЕРБЕЗОПАСНОСТИ МСЭ ООН

63%

УРОВЕНЬ ОСВЕДОМЛЕННОСТИ НАСЕЛЕНИЯ ОБ УГРОЗАХ КИБЕРБЕЗОПАСНОСТИ

46%

ОБЕСПЕЧЕННОСТЬ РАБОТНИКАМИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Организационные меры по повышению уровня информационной безопасности

674 ВЫДЕЛЕННЫХ ОБРАЗОВАТЕЛЬНЫХ ГРАНТОВ

700 ПОДГОТОВЛЕННЫХ ГОССЛУЖАЩИХ

19 ПРИСУЖДЕННЫХ СТИПЕНДИЙ «БОЛАШАК»

70 000 ГОССЛУЖАЩИХ ОХВАЧЕНО ЭКСПЕРИМЕНТАМИ

5 ПРОФЕССИЙ ОПИСАНЫ В ПРОФЕССИОНАЛЬНОМ СТАНДАРТЕ

4200 ПРОВЕРЯЕМЫХ СУБЪЕКТОВ: государственные юридические лица, квазигоссектор, владельцы частных интегрированных систем

Нормативная база в сфере информационной безопасности

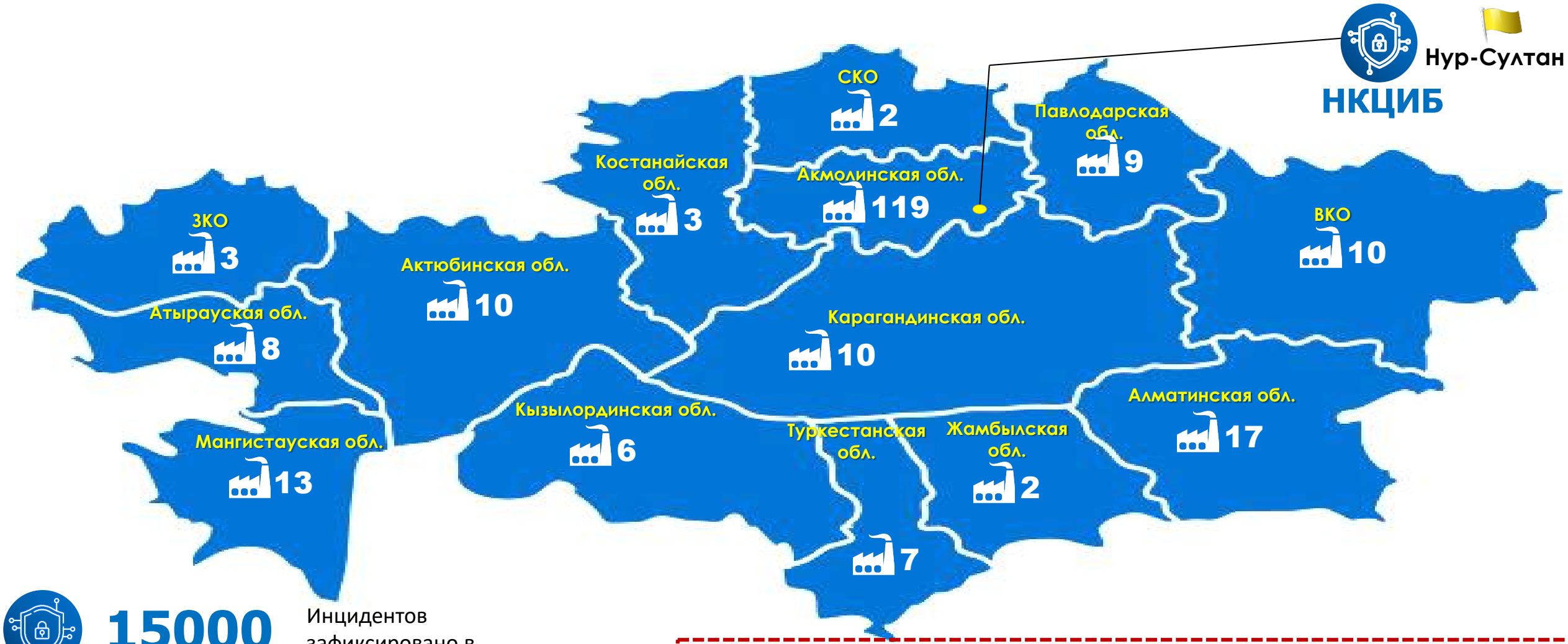
Закон «Об информатизации» от 24 ноября 2015 года (с изменениями и дополнениями по состоянию на 11.04.2019 г.) распространяется на **субъектов информатизации** из числа государственных органов и организаций, квазигосударственный сектор, собственников и владельцев негосударственные системы интегрированные с государственными ИС или отнесенные к КВОИКИ

I
- ✓ **Единые требования** в области информационно-коммуникационных технологий и обеспечения информационной безопасности
- ✓ Правила проведения мониторинга **выполнения единых требований** в области информационно-коммуникационных технологий и обеспечения информационной безопасности

II
- ✓ **Правила и критериии** отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры
- ✓ **Перечень критически важных объектов** информационно-коммуникационной инфраструктуры
- ✓ **Правила проведения мониторинга** обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры

III
- ✓ **Правила обмена информацией**, необходимой для обеспечения информационной безопасности между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности
- ✓ Национальный **антикризисный План** реагирования на инциденты информационной безопасности

Критически важные объекты информационно-коммуникационной инфраструктуры



15000 Инцидентов зафиксировано в 2018 году KZ-CERT

219 КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИКИ

51,1% ОРГАНИЗАЦИЙ В СФЕРЕ IT НЕ ИМЕЮТ СИСТЕМУ УПРАВЛЕНИЯ ИБ

12,2% ОРГАНИЗАЦИЙ ПОЛЬЗУЮТСЯ DLP-СИСТЕМАМИ

17,7% ОРГАНИЗАЦИЙ ИСПОЛЬЗУЮТ МЕЖСЕТЕВЫЕ ЭКРАНЫ

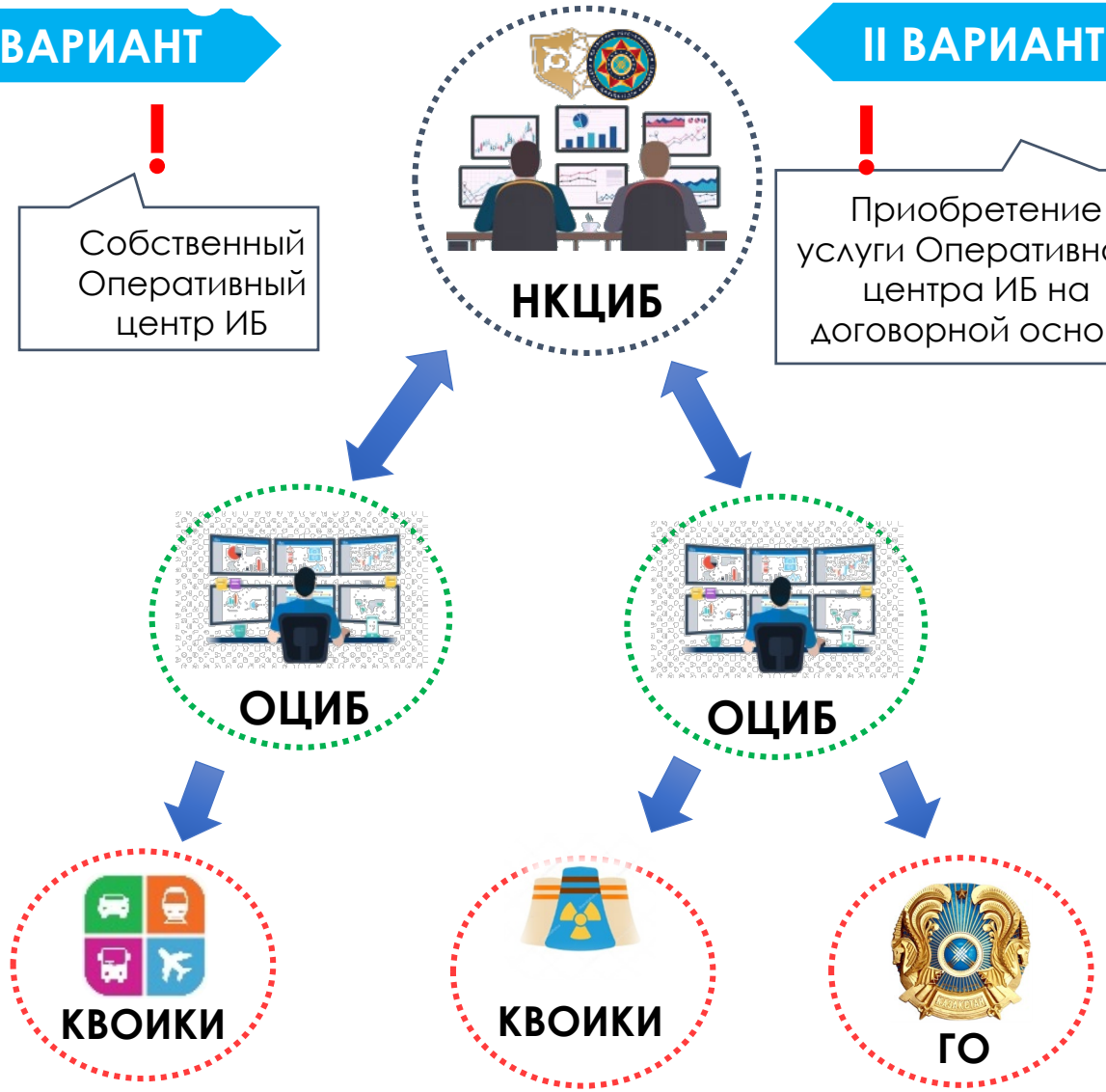
Подходы к организации деятельности Оперативных центров информационной безопасности

I ВАРИАНТ

Собственный Оперативный центр ИБ

II ВАРИАНТ

Приобретение услуги Оперативного центра ИБ на договорной основе



оперативный центр информационной безопасности – юридическое лицо или структурное подразделение юридического лица, осуществляющее **деятельность по защите** электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации

служба реагирования на инциденты информационной безопасности – юридическое лицо или структурное подразделение юридического лица, обеспечивающее анализ информации о событиях информационной безопасности **в целях оказания консультативного и технического содействия в устранении последствий инцидентов информационной безопасности**

Лицензия на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий

Приказ Председателя Комитета национальной безопасности РК Об утверждении квалификационных требований и перечня документов, подтверждающих соответствие им, для осуществления деятельности в сферах обеспечения информационной безопасности и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий.

Квалификационные требования к Оперативным центрам информационной безопасности

СТАТУС ЮРИДИЧЕСКОГО ЛИЦА или СТРУКТУРНОГО ПОДРАЗДЕЛЕНИЯ ЮРИДИЧЕСКОГО ЛИЦА

СПЕЦИАЛЬНО ВЫДЕЛЕННОЕ ПОМЕЩЕНИЕ

1) на праве собственности или иного законного основания;

2) оборудовано автоматическими системами охранной и пожарной сигнализации.

ПЕРЕЧЕНЬ ТРЕБОВАНИЙ К РАБОТНИКАМ ОЦИБ

1) **не менее 3 специалистов**, имеющих дипломы о высшем и (или) профессиональном техническом образовании **по профилю ИБ** (защите информации);

2) **не менее 2 специалистов**, имеющих сертификаты по направлению **аудита** требованиям международного стандарта **ISO 27001**;

3) **не менее 1 специалиста** по направлению **компьютерной криминалистики** (например, EC-Council Certified Security Analyst, GIAC Certified Forensic Analyst и другие);

4) **не менее 1 специалиста** по направлению **реверс-инжиниринга и (или) анализа вредоносных программ** (например, GIAC Reverse Engineering Malware и другие);

5) **не менее 1 специалиста** по направлению **этичного хакинга и (или) тестирования на проникновение** (например, Offensive Security Certified Professional, EC-Council Certified Ethical Hacker, GIAC Penetration Tester и другие);

6) **не менее 2 специалистов** по направлению **администрирования серверных операционных систем** (например, Red Hat Certified System Administrator, Microsoft Certified Solutions Associate и другие).

Квалификационные требования к Оперативным центрам информационной безопасности

МИНИМАЛЬНЫЙ НАБОР ПОИСКОВЫХ СРЕДСТВ

1) средства защиты клиентов от угроз информационной безопасности:

- решение класса next-generation firewall или unified threat management;
- система обнаружения угроз на рабочих станциях и реагирования на них (Endpoint Threat Detection and Response);
- средство проактивного поиска и обнаружения угроз (Threat Hunting);
- средство предотвращения утечки информации (DLP).

2) средства мониторинга и реагирования на инциденты информационной безопасности:

- система управления событиями информационной безопасности (SIEM);
- платформа реагирования на инциденты (IRP);
- платформа управления информацией об угрозах (Threat Intelligence Platform);
- средство динамического анализа вредоносных программ типа «песочница».

3) средства аудита информационной безопасности и тестирования на проникновение в информационные системы и ресурсы:

- сетевой сканер;
- сканер уязвимостей;
- сканер уязвимостей веб-приложений;
- средство эксплуатации уязвимостей;
- внешний Wi-Fi адаптер с направленной антенной.

ДОПОЛНИТЕЛЬНЫЕ ТРЕБОВАНИЯ К ЛИЦЕНЗИАТУ

1) наличие **методики оказания услуг** по выявлению технических каналов утечки информации и СТС оперативным центром информационной безопасности;

2) **осуществление заявленного вида деятельности** в полном соответствии с методикой;

3) **информирование лицензиара** о заключенных договорах (контрактах) на оказание услуг;

4) **предоставление ежеквартального электронного отчета** по оказанным услугам по выявлению технических каналов утечки информации и СТС оперативным центром информационной безопасности.

Договор о совместных работах по обеспечению информационной безопасности

ПРЕДМЕТ ДОГОВОРА

эксплуатация средств и систем обеспечения ИБ, используемых ГО либо предоставляемых поставщиком услуг аутсорсинга;

реализация отдельных целостных процессов системы обеспечения ИБ или их частей:

выявление компьютерных атак на информационно-коммуникационной инфраструктуру сторон;

анализ безопасности кода приложений;

мониторинг и анализ событий ИБ;

проведение тестирования на проникновение;

анализ защищенности информационно-коммуникационной инфраструктуры;

обеспечение безопасности веб-доступа и электронной почты;

организация управления инцидентами ИБ в том числе во взаимодействии НКЦИБ;

оповещение о новых угрозах и признаках атак (Treat Intelligence).

Договор о совместных работах по обеспечению информационной безопасности

СОДЕРЖАНИЕ ДОГОВОРА

обязанности и разделение зоны ответственности собственника и поставщика услуг аутсорсинга;

требования к показателям качества деятельности поставщика услуг и создания условий непрерывности предоставления услуг (требования к SLA) и к инструментам по мониторингу этого уровня;

требования к гарантиям поставщика услуг (в том числе финансовым) в случае наступления риска нарушения ИБ;

требования к инфраструктуре оказания услуг, включая инфраструктуру обеспечения ИБ и обеспечения непрерывности выполнения функций и их восстановления после инцидентов ИБ;

порядок разбора конфликтов в случае нарушения поставщиком услуг условий оказания услуг;

минимальный срок выполнения условий расторжения соглашения об аутсорсинге существенных функций;

условия привлечения поставщиком услуг субподрядчиков и др.

Планируемые изменения законодательства в сфере информационной безопасности

Законопроект по вопросам регулирования цифровых технологий

1) Определение приоритетных секторов экономики в которых необходимо создание отраслевых центров ИБ;

2) Установление ответственности отраслевых госорганов за информацию о КВОИКИ;

3) Введение обязательности ежегодного аудита для организаций и предприятий среднего и крупного бизнеса;

4) Выделение категорий организаций и предприятий, для которых подключение к Интернету обязательно через Шлюзы доступа;

5) Создание реестра операторов персональных данных.

6) Внесение изменений в Перечень продукции и услуг, подлежащих обязательной сертификации, в части служебной информации, персональных данных и КВОИКИ

Техническое регулирование и стандартизация

1) Включение в ЕТ требований соблюдения стандартов:

- ИСО/МЭК 27034 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность приложений;

- СТ РК IEC/PAS 62443 СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ ЗАЩИЩЕННОСТЬ (КИБЕРБЕЗОПАСНОСТЬ) СЕТИ И СИСЕТЕМЫ;

2) Гармонизация стандарта ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования;

3) Формирование **Реестра** доверенного программного обеспечения и продукции электронной промышленности на основе стандарта **ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий;**

4) Испытания негосударственных информационных систем из числа КВОИКИ **Органами подтверждения соответствия**, а не ГТС;

5) Поощрение использования практики **Open Web Application Security Project** (OWASP): Руководство OWASP, Обзорное Руководство по Коду OWASP, Топ-10 OWASP и др;

Экосистема обеспечения безопасности национальной информационной инфраструктуры

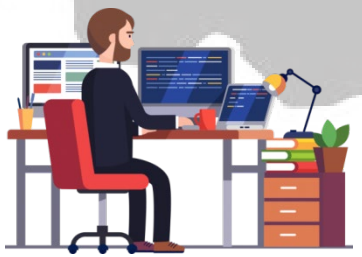
ОЦИБ

НКЦИБ

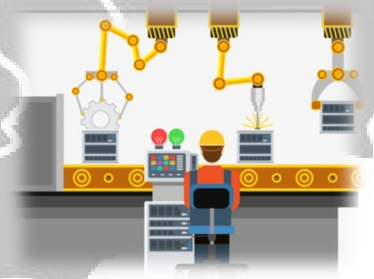
ОЦИБ

объекты информационно-коммуникационной инфраструктуры

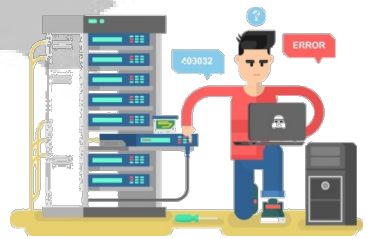
Субъекты НТД, ВУЗы, ССУЗы, школы



Разработчики ПО



Службы реагирования



Лаборатории ОПС

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, ОБОРОННОЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН

СПАСИБО ЗА ВНИМАНИЕ!