



МИНИСТЕРСТВО ЦИФРОВОГО
РАЗВИТИЯ, ОБОРОННОЙ И
АЭРОКОСМИЧЕСКОЙ
ПРОМЫШЛЕННОСТИ
РЕСПУБЛИКИ КАЗАХСТАН

О СОСТОЯНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



О СОСТОЯНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



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



59/214

СТРАТЕГИЧЕСКИХ
ОБЪЕКТОВ,
ОБЛАДАЮТ
КРИТИЧЕСКОЙ
ИНФРАСТРУКТУРОЙ



3 СЛУЖБЫ РЕАГИРОВАНИЯ
НА КОМПЬЮТЕРНЫЕ
ИНЦИДЕНТЫ (FIRST)



20 КОМПАНИЙ В СФЕРЕ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



О СОСТОЯНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



40

МЕСТО КАЗАХСТАНА В
ГЛОБАЛЬНОМ
ИНДЕКСЕ
КИБЕРБЕЗОПАСНОСТИ



63%

УРОВЕНЬ
ОСВЕДОМЛЕННОСТИ
НАСЕЛЕНИЯ ОБ УГРОЗАХ
КИБЕРБЕЗОПАСНОСТИ



46%

ОБЕСПЕЧЕННОСТЬ
РАБОТНИКАМИ В СФЕРЕ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



О СОСТОЯНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



674 ВЫДЕЛЕННЫХ
ОБРАЗОВАТЕЛЬНЫХ ГРАНТОВ



701 ПОДГОТОВЛЕННЫХ
ГОСЛУЖАЩИХ



19 ПРИСУЖДЕННЫХ
СТИПЕНДИЙ «БОЛАШАК»



70 000 ГОСЛУЖАЩИХ
БЫЛО ОХВАЧЕНО
КИБЕРУЧЕНИЯМИ



5 ПРОФЕССИИ ИМЕЮТСЯ В
ПРОФЕССИОНАЛЬНОМ
СТАНДАРТЕ



4200 ПРОВЕРЯЕМЫХ
СУБЪЕКТОВ



О СОСТОЯНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Создана нормативно-правовая база для обеспечения информационной безопасности государственными органами, квазигосударственным сектором и критически важными объектами ИКИ

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



НАЦИОНАЛЬНЫЙ АНТИКРИЗИСНЫЙ ПЛАН РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ



ОПЕРАТИВНЫЙ ШТАБ
3-5 уровень критичности

Постановка задач по
реагированию на инциденты

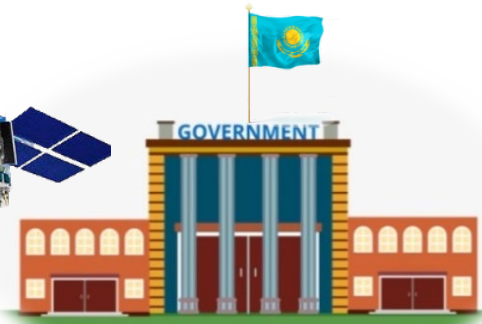
Внесение корректив в
действия в сил и средств

Организация мероприятий по
восстановлению

Установление
причин и условий

Оповещение собственников
и владельцев

Ограничение доступа к
зарубежным сегментам



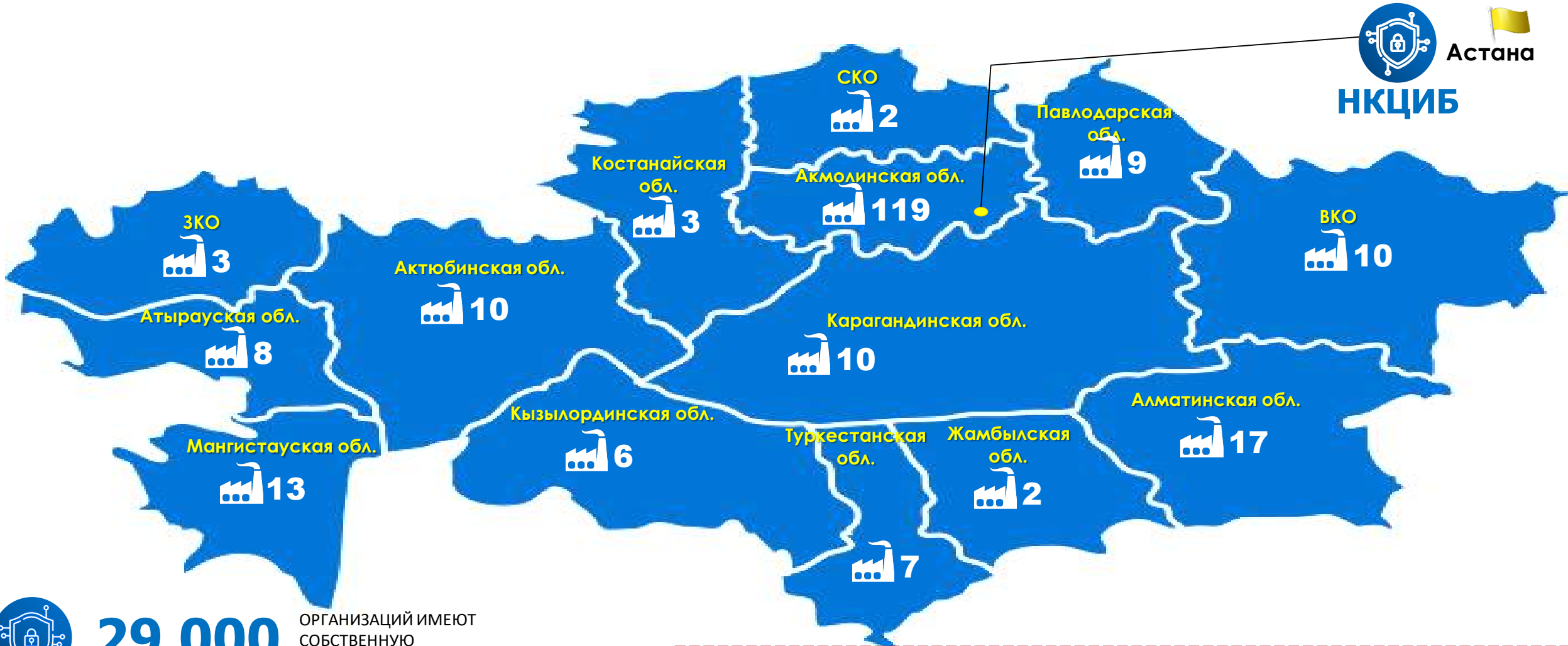


ОБЪЕКТЫ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ



Астана

НКЦИБ



29 000

ОРГАНИЗАЦИЙ ИМЕЮТ СОБСТВЕННУЮ ИНФРАСТРУКТУРУ



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



СИСТЕМА ЗАЩИТА ОБЪЕКТА ИКИ





О СОСТОЯНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

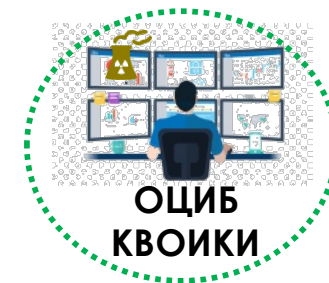
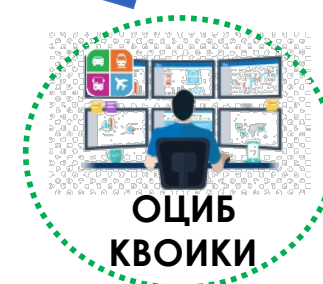
I ВАРИАНТ

Приобретение
услуги Оперативного
центра ИБ



II ВАРИАНТ

Собственный
Оперативный
центр ИБ





КВАЛИФИЦИРОВАННЫЕ ТРЕБОВАНИЯ ПО ОКАЗАНИЮ УСЛУГ ОЦИБ



СТАТУС ЮРИДИЧЕСКОГО ИЛИ ФИЗИЧЕСКОГО ЛИЦА



СПЕЦИАЛЬНО ВЫДЕЛЕННОЕ ПОМЕЩЕНИЕ

- 1) на праве собственности или иного законного основания;
- 2) оборудовано автоматическими системами охранной и пожарной сигнализации.



ПЕРЕЧЕНЬ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 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).



КВАЛИФИЦИРОВАННЫЕ ТРЕБОВАНИЯ ПО ОКАЗАНИЮ УСЛУГ ОЦИБ



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.



МИНИСТЕРСТВО ЦИФРОВОГО
РАЗВИТИЯ, ОБОРОННОЙ И
АЭРОКОСМИЧЕСКОЙ
ПРОМЫШЛЕННОСТИ
РЕСПУБЛИКИ КАЗАХСТАН

СПАСИБО ЗА ВНИМАНИЕ!