



Обеспечение киберзащиты государства в контексте требований Закона Украины «Об основных принципах кибербезопасности Украины»

Т.В.О. ДИРЕКТОРА ДЕПАРТАМЕНТА ФОРМИРОВАНИЯ И РЕАЛИЗАЦИИ
ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ КИБЕРЗАЩИТЫ
ПОЛКОВНИК ЦИПЛИНСЬКИЙ Ю.И.

Одесса - 2018

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ УКРАИНЫ

(УКАЗ ПРЕЗИДЕНТА УКРАИНЫ № 96 от 15.03.2016)

Развитие безопасного, стабильного и надежного
киберпространства

Киберзащита государственных электронных информационных
ресурсов и информационной инфраструктуры, предназначенной
для обработки информации

Киберзащита критической инфраструктуры

Развитие потенциала сектора безопасности и обороны в
сфере обеспечения кибербезопасности

Борьба с киберпреступностью

БАЗОВЫЕ ДОКУМЕНТЫ ПО ВОПРОСАМ КИБЕРБЕЗОПАСНОСТИ



ЗАКОН УКРАИНЫ

«Об основных принципах обеспечения кибербезопасности Украины»

05.10.2017

принято
Верховной Радой Украины

20.10.2017

подписано Председателем
Верховной Раді України

07.11.2017

подписано
Президентом Украины

09.05.2018

Вступает в силу

**Является основоположным нормативно-
правовым актом в сфере обеспечения
кибербезопасности государства**



ЗАКОН УКРАИНЫ «Об основных принципах обеспечения кибербезопасности Украины»

- определяет правовые и организационные основы обеспечения защиты жизненно важных интересов человека и гражданина, общества и государства, национальных интересов Украины в киберпространстве;
- структурирует положения о национальной системы кибербезопасности;
- вводит механизмы применения лучших европейских и мировых практик и стандартов.

ОСНОВНЫЕ СУБЪЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ УКРАИНЫ



Совет национальной безопасности
и обороны Украины
(Национальный координационный центр кибербезопасности)

Основные субъекты обеспечения кибербезопасности



Государственная служба
специальной связи и защиты
информации Украины
(Правительственный CERT-UA)



Служба
безопасности
Украины



Министерство
внутренних дел
Украины
(Национальная
полиция)



Министерство
обороны Украины
(Генеральный
штаб ВСУ)



Разведывательные
органы Украины



Национальный
банк Украины

Другие субъекты
обеспечения
кибербезопасности

- другие государственные органы
- распорядители объектов критической инфраструктуры
- независимые организации и эксперты

РНБО

Национальный координационный
центр кибербезопасности

Технологическая система
киберзащиты

организационно-техническая модель
киберзащиты, система аудита
информационной безопасности

Оперативная составляющая
кибербезопасности

разведывательные, контрразведывательные,
оперативно-розыскные, правоохранные
меры

Сектора
профдеятельности
(операторы,
провайдеры)

ИТ-системы
госорганов

Частный
сектор

Критическая
инфраструктура

ОБЪЕКТЫ

Защищенность
(ИТС, информресурс)

Госспецсвязи,
НБУ

Активная защита
(Реагирование,
Противо-
действие)

Госспецсвязи,
НБУ, МОУ,
Генштаб ВСУ

Правопорядок
(киберпреступность)

СБУ,
Нацполиция

Киберразведка, борьба с
кибертерроризмом

СБУ, СВР,
ГУР МО

ОСНОВНЫЕ СУБЪЕКТЫ

Объектами киберзащиты являются:

- ▶ коммуникационные системы всех форм собственности, в которых обрабатываются национальные информационные ресурсы и/или используемых в интересах органов государственной власти, органов местного самоуправления, правоохранительных органов и воинских формирований, образованных в соответствии с законом;
- ▶ объекты критической информационной инфраструктуры;
- ▶ коммуникационные системы, которые используются для удовлетворения общественных потребностей и/или реализации правоотношений в сферах электронного управления, электронных государственных услуг, электронной коммерции, электронного документооборота.

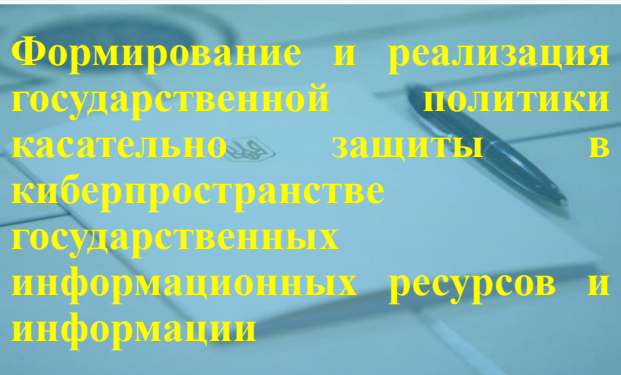
Ответственность за обеспечение киберзащиты

Ответственность за

- обеспечение киберзащиты коммуникационных и технологических систем объектов критической инфраструктуры
- защиты технологической информации в соответствии с требованиями законодательства
- за безотлагательное информирование правительственной команды реагирования на компьютерные чрезвычайные события Украины CERT-UA об инцидентах кибербезопасности
- за организацию проведения независимого аудита информационных безопасности на таких объектах

возлагается на владельцев и/или руководителей предприятий, учреждений и организаций, отнесенных к объектам критической инфраструктуры.

Задания Администрации Госспецсвязи



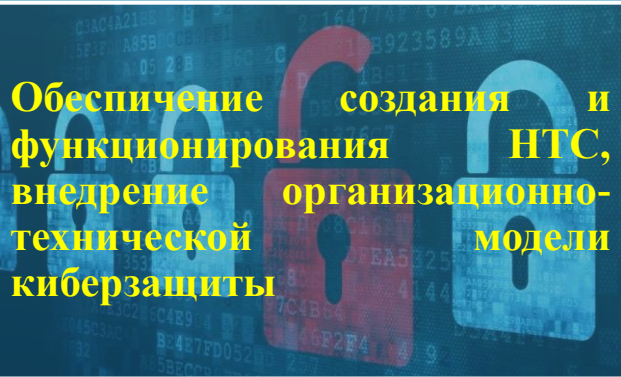
Формирование и реализация государственной политики касательно защиты в киберпространстве государственных информационных ресурсов и информации



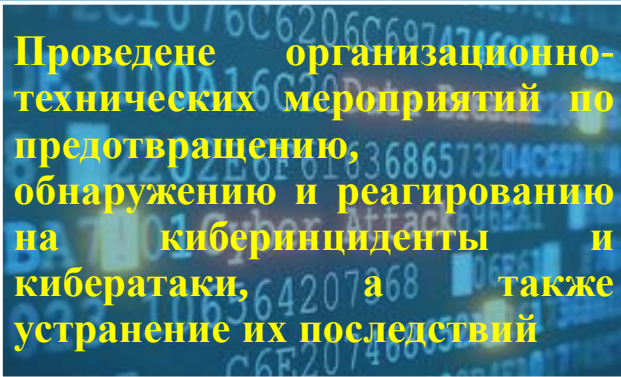
Координация деятельности остальных субъектов обеспечения кибербезопасности касательно киберзащиты



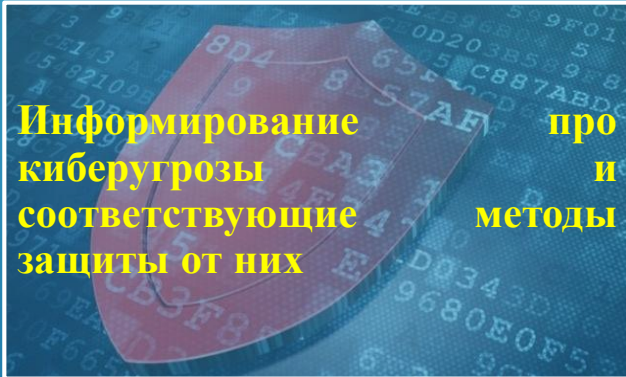
Формирование и реализация государственной политики касательно киберзащиты объектов критической информационной инфраструктуры



Обеспечение создания и функционирования НТС, внедрение организационно-технической модели киберзащиты



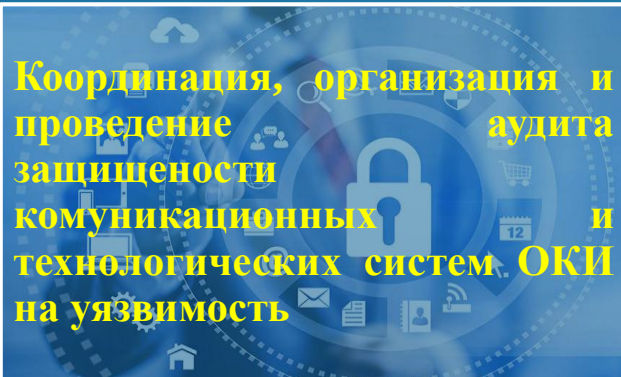
Проведение организационно-технических мероприятий по предотвращению, обнаружению и реагированию на киберинциденты и кибератаки, а также устранение их последствий



Информирование киберугрозы и соответствующие методы защиты от них



Обеспечение внедрения аудита информационной безопасности на ОКИ, установление требований к аудиторам информационной безопасности



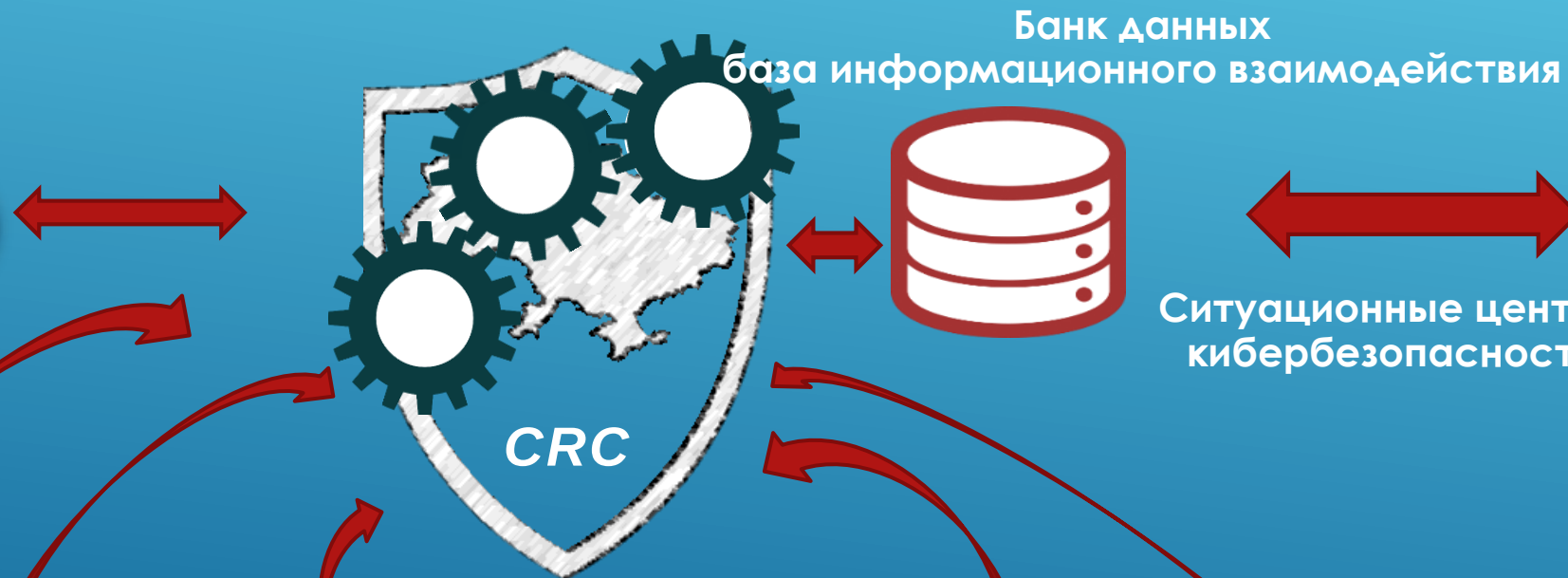
Координация, организация и проведение аудита защищенности коммуникационных и технологических систем ОКИ на уязвимость



Обеспечение функционирования Государственного центра киберзащиты, правительственной команды CERT-UA



Центр реагирования на киберугрозы Госспецсвязи (Cyber Threat Response Centre, CRC)



CERT (SCIRT)
отраслевые

Объекты критической информационной инфраструктуры



Правительственная команда реагирования команда реагирования на компьютерные чрезвычайные происшествия Укрины (CERT-UA)

- ▶ Реагирование на киберинциденты
- ▶ Накопление и проведение анализа данных про киберинциденты
- ▶ Предоставление собственникам объектов киберзащиты практической помощи по вопросам предотвращения обнаружения и нейтрализации последствий киберинцидентов
- ▶ Содействие при решении вопросов киберзащиты и противодействия киберугрозам

Взаимодействует с более чем
400 командами CERT (CSIRT) из более 80 стран



Организационно-техническая модель: система как сенсор безопасности

Эволюция: автономные мероприятия —> Cyber Cloud, Cyber Greed —> Национальная система киберзащиты



2018 : финансовый, банковский,
военный, энергетический, транспортный секторы

Государственно- частное взаимодействие в сфере кибербезопасности

Создание системы
своевременного выявления,
предупреждения и
нейтрализации киберугроз.
Волонтерская помощь.

Повышение цифровой
грамотности граждан и
культуры безопасности

Создание платформы
обмена информацией
между государственными
органами, частным
сектором и гражданами

Партнерства и координации
команд реагирования
на компьютерные
чрезвычайные события

Привлечение экспертного
потенциала, научных
учреждений,
профессиональных
объединений

Оказание консультативной и
практической помощи

Формирование инициатив и
создание авторитетных
консультационных пунктов

Внедрение механизма
общественного контроля

Периодического проведения
национального саммита с
профессиональными
поставщиками бизнес-услуг

Создание системы
подготовки кадров

Тесное взаимодействие с
стейкхолдерами
относительно
киберобороны



Государственная служба специальной связи и защиты информации Украины



СПАСИБО ЗА ВНИМАНИЕ!

ЦИПЛИНСЬКИЙ Ю.И.

YTSIPLINSKIY@DSSZZI.GOV.UA