



Державна служба спеціального зв'язку та захисту інформації України



Аспекты практической деятельности
Государственного центра киберзащиты и
противодействия киберугрозам
Госспецсвязи Украины
по обеспечению кибербезопасности и киберзащиты
государственных информационных ресурсов

Худынцев Н.Н.,

Киев - 14-16 мая 2018



Державна служба спеціального зв'язку та захисту інформації України



Общие вопросы

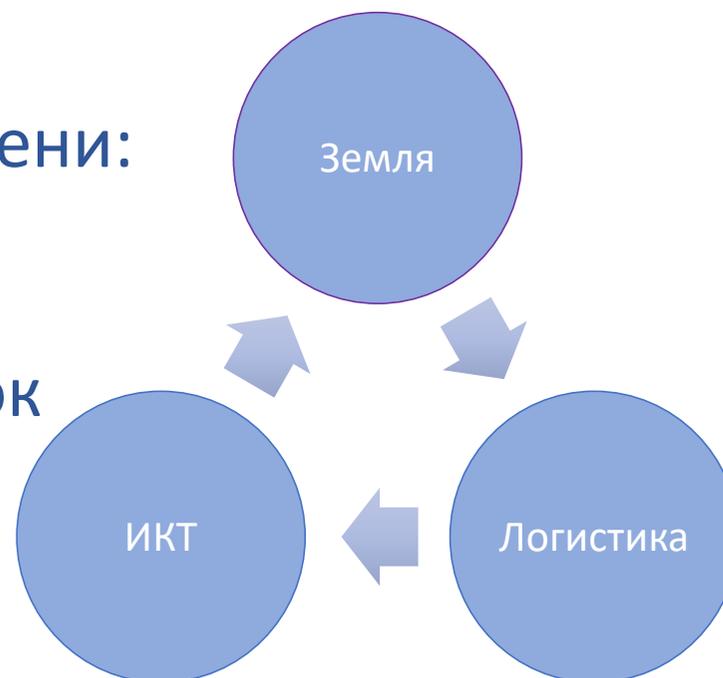


Общие бизнес-процессы



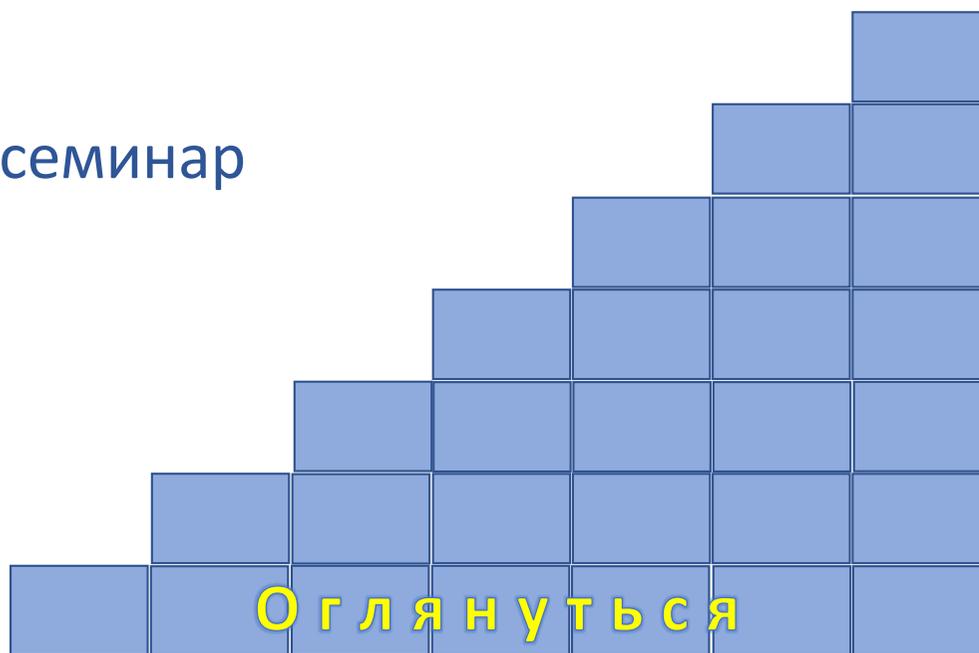


Преимущества по месту и времени:
Земля
ИКТ-ресурсы
Геополитический перекресток





Научно-технический семинар





Научные публикации





Понятная мотивация





Кампус (технопарк)
Кибербезпека агросектора
Цифрова інфраструктура





Научные публикации (коллективные монографии)

- Система защищенного доступа к сети Интернет в Украине
- Система обработки и хранения данных в Украине
- Национальная телекоммуникационная сеть
- Национальная система кибербезопасности и Система киберзащиты государственных информационных ресурсов и объектов критической информационной инфраструктуры
- Телекоммуникационные сети доступа: организационные и нормативно-правовые аспекты



Научно-техническое общество (НТО)

- Корпорация MITRE (США)
- НТТ Plank (Германия)
- НТТ Fraunhofer (Германия)
- НДО NASK (Польша)
- ...
- ОО ??? (Украина)
- НТО ??? (Украина)
- НИИ ??? (Украина)
- неприбыльная организация
- неправительственная организация
- членство юридических лиц
- проектно-бюджетное финансирование
- прозрачное финансирование
- инфраструктурные проекты
- участие в международном разделении труда



Государственно-частное партнерство (ГЧП)

- Сферы: информационная безопасность, кибербезопасность, киберзащита, защита информации, телекоммуникации, информационно-телекоммуникационные технологии, большие базы данных (в том числе единые реестры)
- предмет
- формат договора
- условия конкурса
- процедура
- выбор партнеров
- реализация (внедрение, эксплуатация)



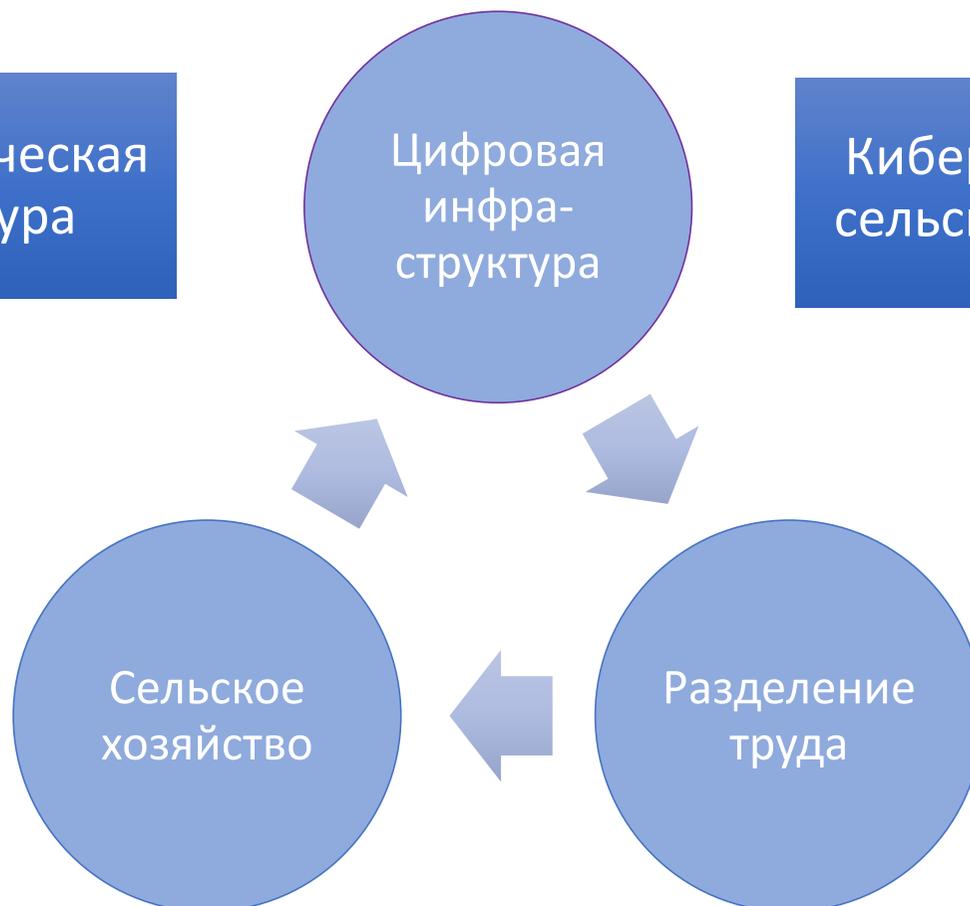
Мировая критическая инфраструктура

Цифровая инфраструктура

Киберзащита ИТС: сельское хозяйство

Сельское хозяйство

Разделение труда





Державна служба спеціального зв'язку та захисту інформації України



Нормативные вопросы



Указ Президента України № 96/2016 от 15.03.2016

«О решении Совета национальной безопасности и обороны Украины от 27 января 2016

«О Стратегии кибербезопасности Украины»

- национальная система кибербезопасности
- организационно-техническая модель национальной системы кибербезопасности
- государственный центр киберзащиты
- система независимого аудита информационной безопасности
- сеть команд реагирования на компьютерные чрезвычайные события
- система технической и криптографической защиты информации
- единая система ситуационных центров профильных органов государственной власти сектора безопасности и обороны
- защищенная интегрированная система электронных государственных реестров, баз данных, дата-центров
- единые дата-центры резервного хранения информации и сведений государственных электронных информационных ресурсов
- система хранения, передачи и обработки данных государственных реестров и баз данных



- механізм обміну інформацією між державними органами, частним сектором і громадянами про загрози критичній інформаційній інфраструктурі
- галузеві індикатори стану кібербезпеки
- система контррозвідального і оперативно-розшукового забезпечення кібербезпеки
- контакт-центр для повідомлень про випадки злочинів і шахрайства в кіберпросторі
- блокування операторами і провайдерами телекомунікацій спеціально ідентифікованих інформаційних ресурсів (сервісів)



Указ Президента України № 32/2017 от 13.02.2017 «О решении Совета национальной безопасности и обороны Украины от 29 декабря 2016» Об угрозах кибербезопасности государства и неотложные меры по их нейтрализации »

- протокол совместных действий субъектов обеспечения кибербезопасности, владельцев (распорядителей) объектов критической информационной инфраструктуры во время выявления, предупреждения, пресечения кибератак и киберинцидентов, а также при устранении их последствий - КМУ, утверждение, 3 мес.
- единые основной и резервный защищенные дата-центры хранения информации и сведений государственных электронных информационных ресурсов - КМУ, обеспечение создания, 6 мес.
- механизм дополнительного стимулирования мотивации к труду специалистов по кибербезопасности, задействованных в секторе безопасности и обороны Украины, прежде всего путем совершенствования системы оплаты их труда - КМУ, отработка, 6 мес.
- национальная телекоммуникационная сеть с подключением информационно-телекоммуникационных систем органов государственной власти, других государственных органов, предприятий, учреждений и организаций государственной формы собственности - КМУ, обеспечение создания и развертывания, 1 год



Указ Президента України № 183/2017 от 11.07.2017

«О решении Совета национальной безопасности и обороны Украины от 10 июля 2017 года» О неотложных мерах по финансированию потребностей национальной безопасности и обороны Украины в 2017 году »

- государственная система специальной связи и защиты информации (укрепление потенциала кибернетической безопасности) - Администрация Госспецсвязи - 250,0 млн. гривен



Указ Президента Украины № 254/2017 от 30.08.2017

«О решении Совета национальной безопасности и обороны Украины от 10 июля 2017» О состоянии выполнения решения Совета национальной безопасности и обороны Украины от 29 декабря 2016 «Об угрозах кибербезопасности государства и неотложные меры по их нейтрализации», введенного в действие Указом Президента Украины от 13 февраля 2017 № 32 »

- определение Госспецсвязи органом, ответственным за сохранение резервных копий информации и сведений государственных электронных информационных ресурсов, а также по установлению порядка передачи, хранения и доступа к этим копиям - КМУ
- внедрение механизма обязательного согласования с Госспецсвязью проектов (задач) создания и развития информационно-телекоммуникационных систем государственных органов, предприятий, учреждений и организаций государственной формы собственности - КМУ
- механизм привлечения физических и юридических лиц на условиях аутсорсинга к выполнению задач киберзащиты государственных электронных информационных ресурсов в рамках развития государственно-частного партнерства - КМУ



- механізм додаткового стимулювання мотивації к труду спеціалістів Міністерства оборони, Госпесцсв'язи, Служби безпеки, Національної поліції, Національного банку, розвідувальних органів, приймаючих неопосередковане участь в організації і реалізації заходів протидії кіберзагрозам - КМУ, введення, 3 міс.
- законопроект об установленні обов'язкового узгодження з Госпесцсв'яззю завдань (проектів) Національної програми інформатизації - КМУ, підготовка і внесення на розгляд ВСУ, 3 міс.
- модернізація ситуаційних центрів по кібербезпеці Служби безпеки України і Госпесцсв'язи - КМУ, забезпечення фінансування, 6 міс.
- проектування захищеного центру обробки даних для розміщення державних електронних інформаційних ресурсів - КМУ, забезпечення фінансування, впродовж 2017
- пріоритетне підключення к національній телекомунікаційній мережі державних органів в відповідності з переліком - КМУ, організація, впродовж 2017
- Національний центр оперативного-технічного управління мережами телекомунікацій України - КМУ, заходи по створенню впродовж 2017



- требования относительно осуществления идентификации и аутентификации источников полученных обновлений программного обеспечения, которое используется для обработки государственных информационных ресурсов - Администрация Госспецсвязи, внедрение, 3 мес.
- единая интерактивная база данных о киберинцидентах - Администрация Госспецсвязи, создание, 3 мес.
- система информационного обмена о киберугрозах - Администрация Госспецсвязи, обеспечение модернизации, 3 мес.
- требования к техническим средствам, применяемым для мониторинга блокировки (ограничения) доступа к информационным ресурсам (сервисам) - Администрация Госспецсвязи, СБУ, разработка, 1 мес.



Указ Президента України №283 / 2017 от 25.09.2017

«О решении Совета национальной безопасности и обороны Украины от 13 сентября 2017» О Концепции реформирования и дальнейшего развития системы управления государством в условиях чрезвычайного положения и в особый период »

- система управления государством в условиях чрезвычайного положения и в особый период



Закон України «Об основных принципах обеспечения кибербезопасности Украины» №2163-19 от 05.10.2017

- национальная телекоммуникационная сеть и национальная система кибербезопасности
- организационно-техническая модель киберзащиты - Администрация Госспецсвязи, внедрение
- Государственный центр киберзащиты (ГЦК)- Администрация Госспецсвязи, обеспечение функционирования
- правительственная команда реагирования на компьютерные чрезвычайные события CERT-UA
- организационно-техническая модель киберзащиты - ГЦК, внедрение
- основные составляющие системы защищенного доступа государственных органов к сети Интернет - ГЦК, обеспечение создания и функционирования
- система антивирусной защиты информационных ресурсов - ГЦК, обеспечение создания и функционирования
- аудит информационной безопасности и состояния киберзащиты объектов критической информационной инфраструктуры - ГЦК
- система обнаружения уязвимостей и реагирования на киберинциденты и кибератаки по объектам киберзащиты - ГЦК, обеспечение создания и функционирования



- система взаємодія команд реагування на комп'ютерні надзвичайні події - ГЦК, забезпечення створення та функціонування
- сценарії реагування на кіберзагрози, заходи по протидії, програми та методики кіберзахисту - ГЦК, розробка та створення
- єдина (універсальна) система індикаторів кіберзагроз
- вимоги (правила, інструкції) по безпечному використанню мережі Інтернет та надання електронних послуг державними органами
- індикатори стану кібербезпеки
- система контррозвідального забезпечення кібербезпеки
- порядок функціонування НТМ - КМУ
- Державний реєстр кіберінцидентів - ведення, CERT-UA



Державна служба спеціального зв'язку та захисту інформації України



Технические вопросы



Инфраструктурные проекты

- Национальная телекоммуникационная сеть (НТС)
- Система защищенного доступа органов государственной власти к сети Интернет (СЗДИ)
- Единые основной и резервный защищенные дата-центры хранения информации и сведений государственных электронных информационных ресурсов (ЕЦХД)
- Система обработки и хранения данных государственных информационных ресурсов (СОХД)
- Системы межведомственной мобильной и стационарной телефонной связи (СММС и СМСТС)
- Система киберзащиты государственных информационных ресурсов и объектов критической информационной инфраструктуры (СКЗ)

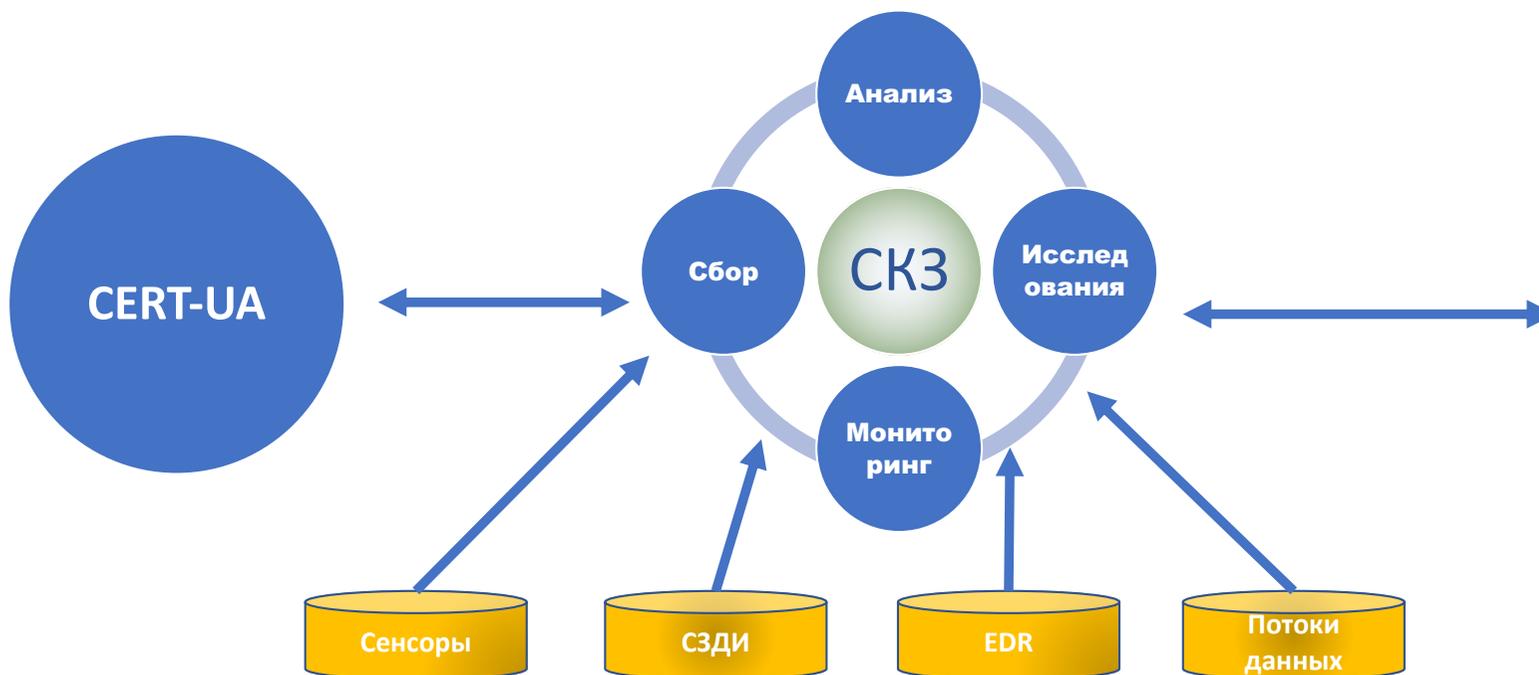


Задачи СКЗ

- Сбор информации об угрозах в ИТС ОГВ и на объектах критической информационной инфраструктуры
- Аналитика и информирование команды реагирования CERT-UA на киберинциденты и киберугрозы, методы защиты
- Координация деятельности субъектов обеспечения кибербезопасности



Взаимодействие СКЗ с субъектами обеспечения кибербезопасности



Объекты критической информационной инфраструктуры





Ожидаемые результаты

- Повышение уровня киберзащиты объектов киберзащиты
- Уменьшение количества уязвимостей ИТС ОГВ и объектов критической информационной инфраструктуры
- Создание интерфейса организационно-технического взаимодействия субъектов национальной системы кибербезопасности
- Расширение государственно-частного партнерства в сфере кибербезопасности и киберзащиты
- Укрепление национальной обороноспособности и устойчивости ИТС ОГВ к угрозам в киберпространстве



Державна служба спеціального зв'язку та захисту інформації України



БЛАГОДАРЮ ЗА ВНИМАННЯ!