ВТОРАЯ КОНФЕРЕНЦИЯ
«ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИЙ»

Анализ опыта формирования и реализации стратегий и программ кибербезопасности в странах Европейского Союза

Анищенко В.В., к.т.н., CISA
(Ассоциация «Инфопарк» / ООО "СОФТКЛУБ")

IT-SECURITY CONFERENCE-2016,
29-30 марта 2016
Академия управления при Президенте Республики Беларусь, Минск

Необходим ли национальный нормативно-методический базис кибербезопасности?

Кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

Киберпространство образуется совокупностью коммуникационных каналов и технологической инфраструктуры в информационном пространстве для использования в любой деятельности личности, организаций, государства.

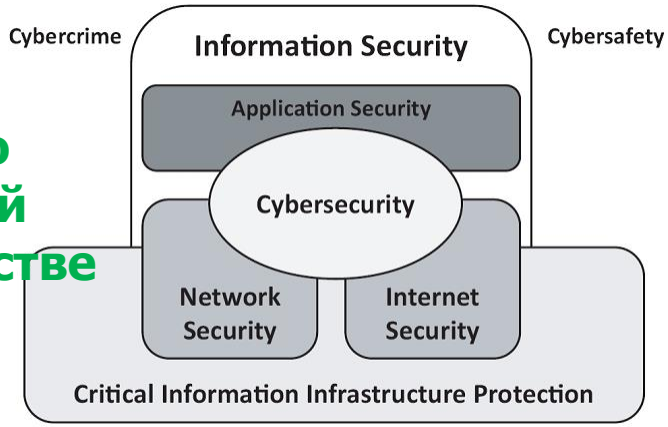


Figure 1 — Relationship between Cybersecurity and other security domains

Кибербезопасность - совокупность технологий, процессов и практик, предназначенных для защиты сетей, компьютеров, программ и данных от атак, от разрушения или несанкционированного доступа.

Необходим ли национальный нормативно-методический базис кибербезопасности?

Термин «кибербезопасность» не выделяется из понятия «информационная безопасность» и не используется отдельно в НПА и ТНПА РБ.

Регулирование киберпространства исключительно на национальном уровне невозможно в силу его трансграничности.

Целесообразно установить соответствие между белорусским и европейскими нормативными актами, чтобы активизировать участие в международной работе в области кибербезопасности.

February 2013: EU Cybersecurity Strategy "An Open Safe and Secure Cyberspace"

Приоритеты

Стратегии кибербезопасности ЕС «Открытое безопасное и защищенное киберпространство»:

1. Достижение киберустойчивости
2. Радикальное сокращение киберпреступности
3. Развитие киберзащиты, как составной части Европейской Общей Политики Безопасности и Обороны (ОПБО)
4. Развитие индустриальных и технологических ресурсов для кибербезопасности
5. Установление политики международного киберпространства ЕС

February 2013: EU Cybersecurity Strategy
1. Достижение киберустойчивости

SoftClub

ІNFOPARK

Цель - повышение уровня готовности к кибербезопасности государств-членов ЕС

Стратегия требует формирования:

- Национальных стратегий кибербезопасности и планов сотрудничества
- Национальных компетентных органов по кибербезопасности
- Групп реагирования на компьютерные инциденты (Computer Emergency Response Team - CERT)

February 2013: EU Cybersecurity Strategy
1. Достижение киберустойчивости

Директивой NIS Европейского Парламента и Европейской Комиссии от 07.12.2015

по «Сетевой и информационной безопасности»

законодательно установлены требования по управлению рисками и представлению данных об инцидентах компетентным органам для отраслей:

1. **Энергетика: электроснабжение, газоснабжение и нефтепереработка**
2. **Кредитно-финансовые учреждения и биржи**
3. **Транспорт: воздушный, морской, железнодорожный**
4. **Здравоохранение**
5. **Поставщики ключевых услуг доступа в Интернет**
6. **Органы государственного управления**

February 2013: EU Cybersecurity Strategy
1. Достижение киберустойчивости

Повышение осведомленности: всеобщая ответственность

- Месяц кибербезопасности (октябрь)
- Чемпионы по кибербезопасности
- Кибер- образование и профессиональная подготовка (ENISA)

February 2013: EU Cybersecurity Strategy
2. Радикальное сокращение киберпреступности

Приоритеты в борьбе с киберпреступностью:

- Строгое и эффективное законодательство
- Улучшенные операционные возможности
- Более эффективное сотрудничество
- Наращивание потенциала

February 2013: EU Cybersecurity Strategy
2. Радикальное сокращение киберпреступности

Директивы ЕС по борьбе с киберпреступностью:

Директива об атаках на информационные системы
- Принята в 2013 году, реализация к 2015 году

Директива о сексуальном насилии, сексуальной эксплуатации детей и детской порнографии
- Передана для реализации в страны-члены ЕС в конце 2013 года

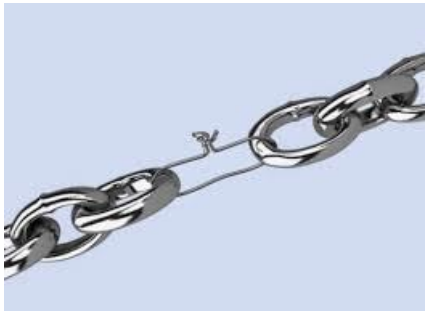
Ратификация и продвижение Будапештской конвенции Совета Европы по борьбе с киберпреступностью

February 2013: EU Cybersecurity Strategy
3. Развитие киберзащиты

SoftClub

INFOPARK

Укрепление самого слабого звена:

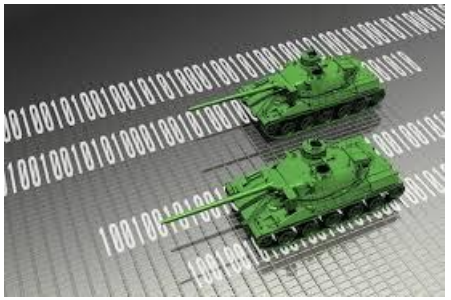


- Укрепление устойчивости связи и информационных систем поддержки обороны и национальной безопасности государств-членов и миссий ЕС и штаб-квартиры.

- Концентрация на развитии способности обнаруживать, реагировать и восстанавливаться от сложных киберугроз.

- Создание основ политики кибероборонны ЕС.

February 2013: EU Cybersecurity Strategy
3. Развитие киберзащиты



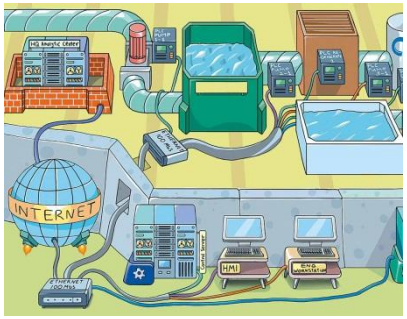
Проект рекомендаций по политике кибероборонь включает в себя:

1. Усиление защиты сетей связи ОПБО.
2. Развитие потенциала кибероборонь государств-членов в части ОПБО.
3. Содействие военно-гражданскому сотрудничеству и синергия за счёт более широкого представительства ключевых персон киберпространства ЕС из соответствующих органов ЕС и из частного сектора.
4. Улучшение возможностей для подготовки, образования и тренировок.
5. Сотрудничество с международными партнерами (например, НАТО, Совместными Центрами передового опыта кибероборонь ...).

February 2013: EU Cybersecurity Strategy
4. Развитие ресурсов для кибербезопасности

Развитие индустриальных и технологических ресурсов для кибербезопасности:

Обеспечение безопасности цепей создания добавленной стоимости:



- Государственно-частная платформа по кибербезопасности и рекомендации по кибербезопасности посредством цепей создания добавленной стоимости в ИКТ (платформа NIS).
- Рекомендации по стандартам и передовым практикам (через ENISA).
- Ускорение научно-технологических инвестиций, в том числе, через программу Horizon 2020.

February 2013: EU Cybersecurity Strategy
5. Политика международного киберпространства

Политика международного киберпространства ЕС:

- Свобода интернета и права человека.
- Нормы в киберпространстве, международная безопасность.
- Укрепление потенциала в третьих странах.
- Содействие Будапештской конвенции по борьбе с киберпреступностью.
- Подотчетность и стабильность Интернета.
- Отношения с партнерами и международными Организации: Совет Европы, ОБСЕ, ООН, НАТО, ОЭСР …

ENISA: Work programme 2016
Including multiannual planning

SoftClub

ÍNFOPARK

enisa European Network and Information Security Agency

Направления деятельности Агентства ЕС по Сетевой и Информационной Безопасности (European Union Agency for Network and Information Security - ENISA):

1) Сетевая и информационная безопасность и кибер-безопасность

2) CERT (Центр реагирования на компьютерные инциденты)

3) Защита и устойчивость критической информационной инфраструктуры (Critical Information Infrastructure Protection (CIIP) and Resilience)

ENISA: Work programme 2016
Including multiannual planning

Сетевая и информационная безопасность и кибер-безопасность
(Network and Information Security and Cyber-security)

Предусматривает:

- Деятельность CERT - Центров реагирования на компьютерные инциденты;

- Обеспечение защиты и устойчивости критической информационной инфраструктуры (Critical Information Infrastructure Protection (CIIP) and Resilience);

- Управление рисками (Risk Management).

ENISA: Work programme 2016
Including multiannual planning

CERT (Центр реагирования на компьютерные инциденты)

Computer Emergency Response Teams (CERTs, aka CSIRTs)

Центры реагирования на компьютерные инциденты (CERTs или CSIRTs) являются ключевым инструментом для защиты критически важных объектов информатизации или информационных инфраструктур (CIIP – КВОИ). Каждая страна, подключенная к сети Интернет, должна иметь возможности эффективно реагировать на инциденты информационной безопасности.

CERTs должны выступать в качестве первичных поставщиков услуг безопасности для правительства и граждан. В то же время, они должны выступать в качестве банков знаний и выполнять образовательную функцию.

ENISA: Work programme 2016
Including multiannual planning

Защита и устойчивость критической информационной инфраструктуры
(Critical Information Infrastructure Protection (CIIP) and Resilience)

Разработка лучших практик и рекомендаций

Для планов действий в чрезвычайных и непредвиденных ситуациях, для стратегий кибер-безопасности, для минимальных мер безопасности Интернет-провайдеров, для надежного обмена информацией и др., в частности касающихся:

- **разработки безопасного ПО;**
- **безопасности смартфонов;**
- **Веб-безопасности;**
- **бот-сетей;**
- **безопасности технологий облачных вычислений;**
- **сетевой и информационной безопасности в финансовом секторе и т.п.**

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ЭСТОНИИ 2014-2017

ВВЕДЕНИЕ
1. АНАЛИЗ ТЕКУЩЕЙ СИТУАЦИИ
2. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ
3. ОБЩИЕ ЦЕЛИ СТРАТЕГИИ ДО 2017 ГОД

Увеличить потенциал по обеспечению кибербезопасности и повысить осведомленность населения о киберугрозах.

Подцель 1: Обеспечить защиту информационных систем, лежащих в основе служб жизнеобеспечения

Подцель 2: Совершенствование борьбы с киберпреступностью

Подцель 3: Развитие национального потенциала в кибероборонe

Подцель 4: Страна борется с угрозами кибербезопасности

Подцель 5: Страна развивает межгосударственное сотрудничество

5. СТОРОНЫ, СВЯЗАННЫЕ СО СТРАТЕГИЕЙ

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ЭСТОНИИ 2014-2017

Подцель 1: Обеспечить защиту информационных систем, лежащих в основе служб жизнеобеспечения

1.1. Обеспечить для важных служб альтернативные решения

1.2. Управление взаимозависимостью важных служб

1.3. Обеспечение безопасности ИКТ инфраструктуры и служб

1.4. Преодоление киберугроз для государственного и частного сектора

1.5. Внедрение национальной системы контроля в сфере кибербезопасности

1.6. Обеспечение целостности цифровых ресурсов государства

1.7. Продвижение международного сотрудничества в сфере защиты инфраструктуры особо важной информации

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ЭСТОНИИ 2014-2017

Подцель 2: Совершенствование борьбы с киберпреступностью

2.1. Обеспечение выявления киберпреступности

2.2. Повышение общественной осведомленности о киберрисках

2.3. Развитие международного сотрудничества в борьбе с киберпреступностью

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ЭСТОНИИ 2014-2017

Подцель 3: Развитие национального потенциала в кибероборонe

3.1. Синхронизация военного планирования и подготовка к гражданским чрезвычайным ситуациям

3.2. Развитие коллективной киберзащиты и международного сотрудничества

3.3. Развитие военного потенциала в сфере кибероборонe

3.4. Обеспечение высокого уровня осведомленности о роли кибербезопасности в обеспечении национальной обороны

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ЭСТОНИИ 2014-2017

Подцель 4: Страна борется с угрозами кибербезопасности

4.1. Подготовка следующего поколения профессионалов в сфере кибербезопасности

4.2. Развитие смарт проектирования решений по кибербезопасности

4.3. Поддержка развития предприятий, обеспечивающих кибербезопасность, и решений национальной кибербезопасности

4.4. Предотвращение рисков безопасности в новых решениях

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ЭСТОНИИ 2014-2017

Подцель 5: Страна развивает межгосударственное сотрудничество

5.1. Разработка законодательной базы для обеспечения кибербезопасности

5.2. Поддержание политики международной кибербезопасности

5.3. Более тесное сотрудничество с союзниками и партнерами

5.4. Развитие потенциала Европейского Союза

СТРАТЕГИЯ КИБЕРБЕЗОПАСНОСТИ ЭСТОНИИ 2014-2017

5. СТОРОНЫ, СВЯЗАННЫЕ СО СТРАТЕГИЕЙ

Министерство экономики и коммуникаций координирует разработку и реализацию политики и стратегии кибербезопасности.

План действий определяет перечень мероприятий и бюджет стратегии, а также лиц, ответственных за реализацию каждой части стратегии.

Стоимость реализации четырехлетней стратегии - около 16 миллионов евро.

Доклад о реализации плана действий - должен ежегодно представляться Правительству Республики и должен включать предложения по улучшению плана действий.

Стратегия не изменяет полномочий различных ведомств, ответственных за кибербезопасность.

Сетевая и информационная безопасность и кибер-безопасность

Основа для гармонизации

ТКП 483-2013 (01019) Информационные технологии и безопасность Безопасность эксплуатации и надежное функционирование критически важных объектов информатизации. Общие требования

Разработан в базисе **СТБ ISO/IEC 27001-2011** ИТ. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

Рекомендуется локализация и внедрение стандарта **ISO/IEC 27032:2012 «ИТ. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности»**, который устанавливает принципы: *обмена информацией, координации, разрешения инцидентов*.

Помогает отражать атаки:
– атаки с применением социального инжиниринга,
– хакерство,
– вредоносные приложения (malware),
– шпионские приложения (spyware),
– другое нежелательное программное обеспечение.

Предложения в проект СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ Беларуси на 2017-2020

Направления деятельности по кибербезопасности в Республике Беларусь:

1) развитие национальной системы защиты от кибератак и предупреждения киберугроз, поощрение развития государственно-частного партнерства (ГЧП) по созданию защитных механизмов и систем кибероборонь;

2) развитие и обновление в соответствии с текущими и перспективными киберугрозами средств повышения безопасности и надежности критически важных объектов информатизации (КВОИ);

3) совершенствование мер обеспечения информационной безопасности государственных информационных ресурсов в киберпространстве;

4) разработка моделей и процессов партнерства государства, бизнеса и граждан в области кибербезопасности;

5) формирование программ цифровой грамотности населения и культуры безопасного поведения в киберпространстве;

6) развитие межгосударственного сотрудничества для дальнейшего повышения глобального уровня кибербезопасности;

7) совершенствование нормативно-правового базиса обеспечения кибербезопасности.

Совершенствование нормативно-правового базиса обеспечения кибербезопасности Беларуси

- разработка руководств по проведению аудита и созданию механизмов обновления требований и рекомендаций по кибербезопасности в отношении государственных информационных систем, сетей, КВОИ на основе ГЧП;

- совершенствование законодательства в сфере кибербезопасности с учетом возможности гармонизации правовых норм в сфере кибербезопасности с Европейским Союзом в рамках реализации инициативы по Гармонизации цифровых рынков стран Восточного партнерства и ЕС;

- расширение практики привлечения экспертного сообщества, профильных научных и профессиональных ассоциаций к подготовке проектов нормативных документов в области кибербезопасности;

- дальнейшее совершенствование права, касающегося административной и уголовной ответственности за преступления, совершенные в киберпространстве;

- формирование предложений по дальнейшему упрощению взаимодействия с иностранными уполномоченными органами при расследовании инцидентов кибербезопасности;

- подготовка нормативно-правовой базы для применения технологий цифровой трансформации: мобильных приложений, виртуализации, облачных вычислений, ЦОД и др.

ВТОРАЯ КОНФЕРЕНЦИЯ
«ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИЙ»

INFOPARK

SoftClub

Спасибо за внимание!

Владимир Анищенко

u.anishchanka@softclub.by

SecurITy conference