Региональный семинар МСЭ для стран СНГ и Грузии
«Комплексные аспекты кибербезопасности в инфокоммуникациях»
Одесса, Украина, 15-17 июня 2016 года

Направления совершенствования мер обеспечения кибербезопасности ключевых объектов инфокоммуникаций

БЕЛОРУССКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ СВЯЗИ

Кибербезопасность

Кибербезопасность – это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя (*МСЭ-Т X.1205*).

Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде.

Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде.

Кибербезопасность

ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity

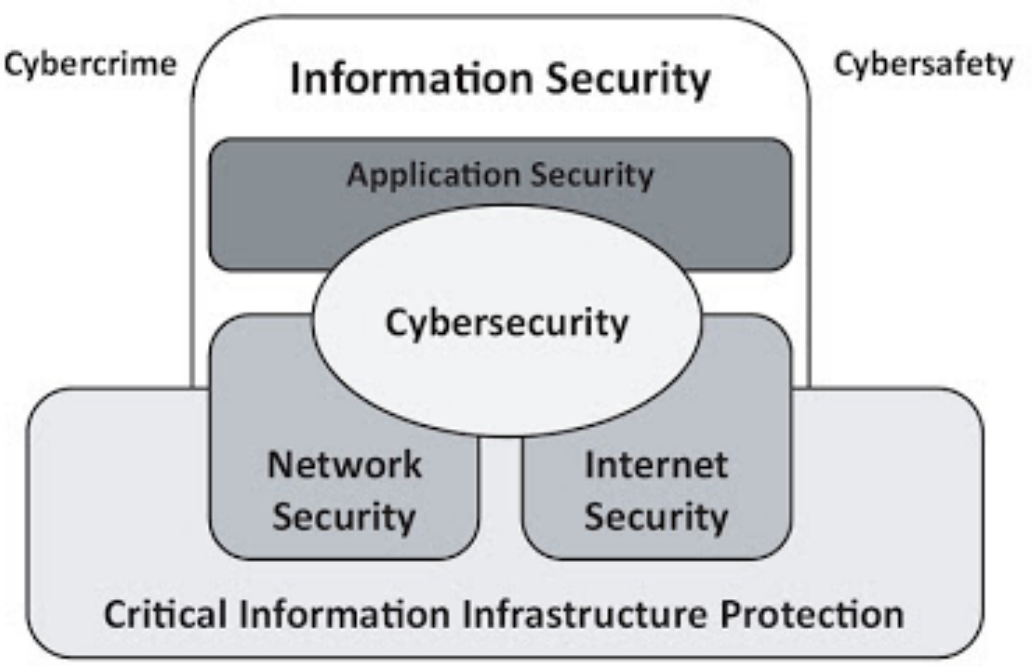


Figure 1 — Relationship between Cybersecurity and other security domains

Кибербезопасность

Киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)

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

Инфокоммуникации

Критическая информационная инфраструктура – совокупность автоматизированных систем управления критически важными объектами и обеспечивающих их взаимодействие информационно-телекоммуникационных (инфокоммуникационных) сетей, предназначенных для решения задач государственного управления, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий.

Ключевые объекты инфокоммуникаций – информационно-управляющие или информационно-телекоммуникационные системы, которые используются для управления критически важными процессами.

Угрозы

- Утечка и обнародование частной информации
- Мошенничество
- Распространение опасного контента
- Воздействие на личность «путем сбора персональных данных» и «атаки на инфраструктуру, используемую гражданами в обычной жизни»

Угрозы

Современные реалии внешних угроз

Технологии нападения развиваются быстрее технологий защиты.

Техники обхода существующих средств защиты совершенствуются.

Количество уязвимостей «нулевого дня» постоянно растет.

Злоумышленники активно используют методы социальной инженерии.

ITU NATIONAL CYBERSECURITY STRATEGY GUIDE

Планируй-Делай-Проверяй-Улучшай

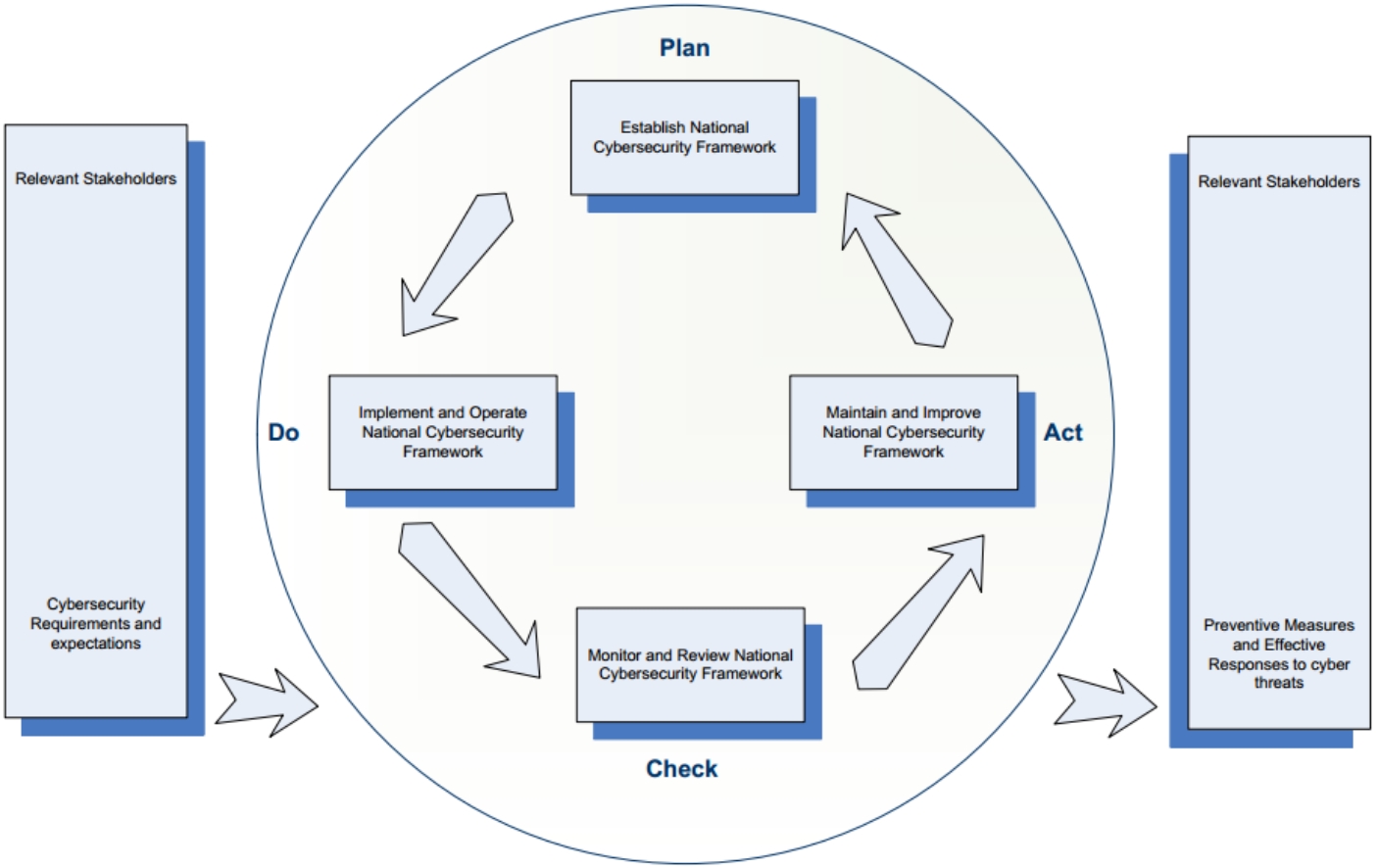


Figure 31 – PDCA Model applied to National Cybersecurity Framework

Процесс обеспечения КБ

I. Определение объектов защиты.

II. Выявление угроз и оценка их вероятности.

III. Оценка возможного ущерба.

IV. Обзор применяемых мер защиты, определение их недостаточности.

V. Определение адекватных мер защиты.

VI. Организационное, финансовое, юридическое и пр. виды обеспечения мер защиты.

VII. Внедрение мер защиты.

VIII. Контроль.

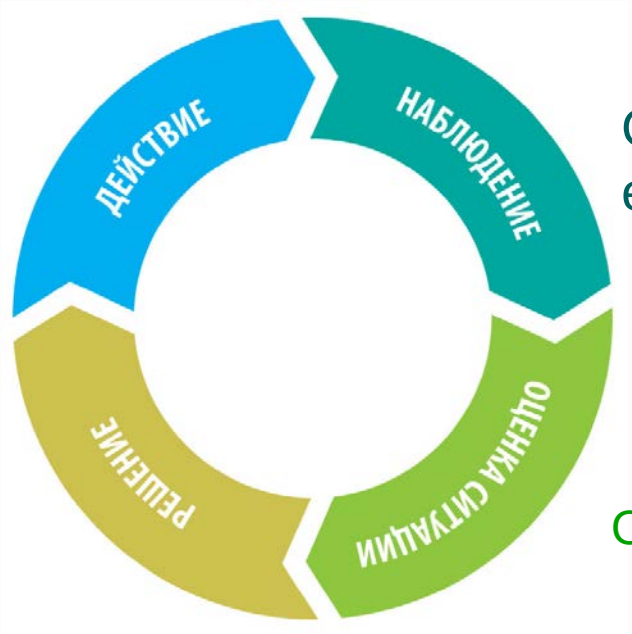
IX. Мониторинг и корректировка внедренных мер.


Жизненный цикл атаки
ДО АТАКИ
Исследование
Внедрение политик
Укрепление
ВО ВРЕМЯ АТАКИ
Обнаружение
Блокирование
Защита
ПОСЛЕ АТАКИ
Локализация
Изолирование
Восстановление
Сеть
Терминал
Мобильное устройство
Виртуальная машина
Облако
Защита в момент времени
Непрерывная защита

Цикл Бойда

Act

Observe



Decide

Orient

Повысить стоимость атаки

Защитные меры, которые:

•не только направлены на предотвращение угроз;

•могут не целиком предотвращать угрозы, а просто делать их реализацию более дорогой и длинной;

•могут быть необязательными;

•ориентированы на угрозы, которые еще не произошли, но могут произойти в скором будущем.

5 шагов для каждого из элементов информационной системы:

•Как усложнить поиск цели?

•Как усложнить проникновение на цель?

•Как усложнить использование цели?

•Как усложнить скрытие атаки?

•Как сделать последствия от атак обратимыми?

Спасибо!