Сучасні підходи до забезпечення кібернетичної безпеки

М. В. Грайворонський

ФТІ НТУУ “КПІ”

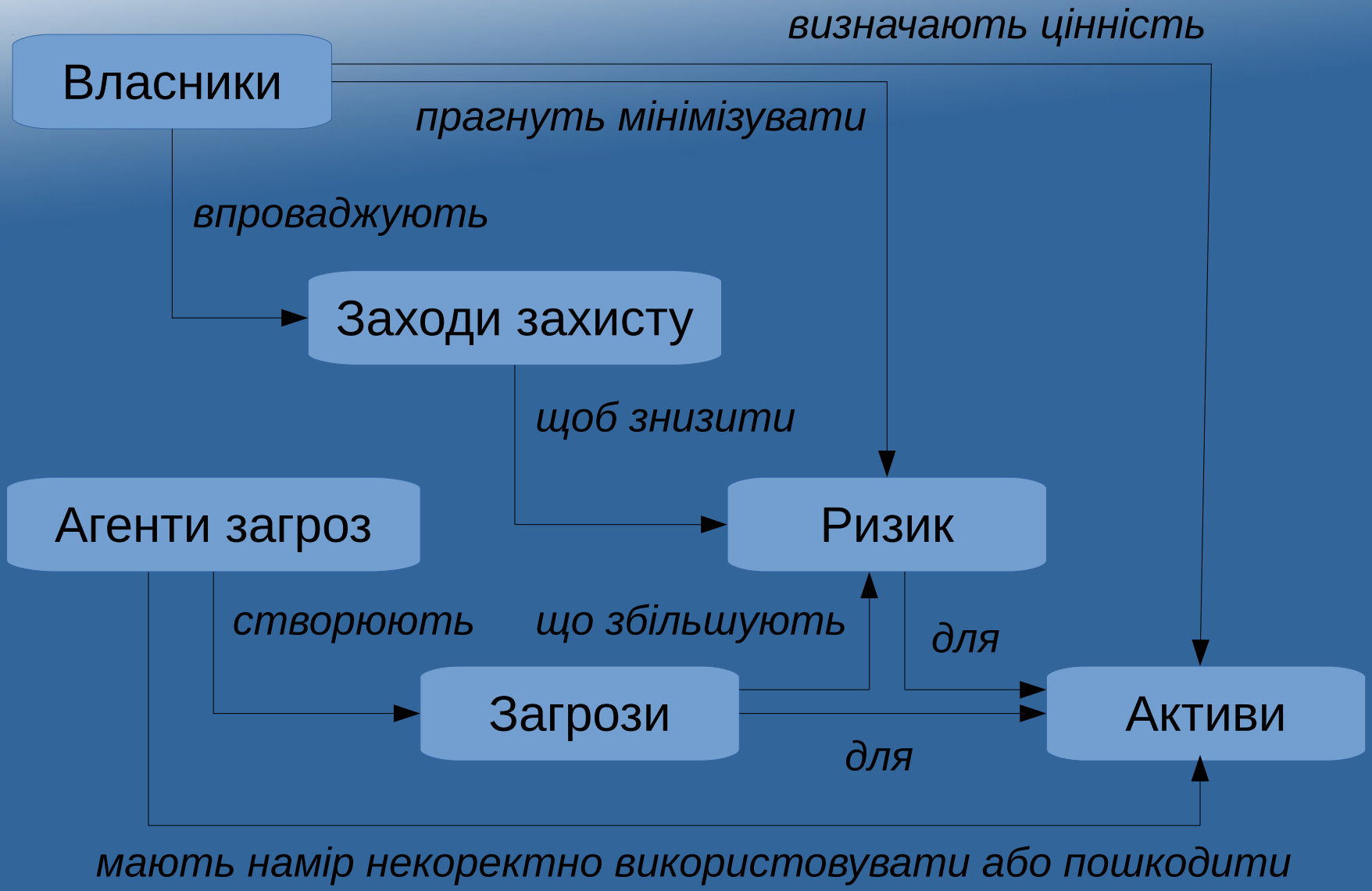
- Поняття кібернетичної безпеки (кібербезпеки)
- Кіберзагрози
- Заходи захисту

- Поняття кібернетичної безпеки (кібербезпеки)
- Кіберзагрози
- Заходи захисту

Традиційні поняття із захисту інформації

- Безпека інформації
  - Конфіденційність, цілісність, доступність
- Захист інформації
  - Діяльність, спрямована на забезпечення безпеки інформації
- Інформаційна безпека
  - Безпека інформації + захист від інформації (інформаційні війни тощо)
- Information security = безпека інформації або інформаційна безпека

Онтологія*



* ISO/IEC 15408 (“Common Criteria”)

Розуміння кібербезпеки (варіанти)

- “Нічого нового”
- Кібербезпека – безпека кібернетичних систем
- Кібербезпека включає наступальні дії
- Кібербезпека – зниження кіберризиків
- Кібербезпека – безпека інформації у кіберпросторі

Погляд 1: Нічого принципово нового

- Численні фахівці з комп'ютерної безпеки вважають, що **Кібербезпека (або кіберзахист) – це лише новий термін, який означає саме те, чим вони займались протягом останніх десятиліть**

(Нові слова допомагають збільшити фінансування)

Бюджет на інформаційну безпеку

Бюджет на кібербезпеку

Погляд 2: Кібербезпека – це безпека кібернетичних систем

- Суттєва мета кібернетики – це розуміння і визначення функцій та процесів систем, які мають мету і які беруть участь у циклічних ланцюгах, що переходять від дії до сприйняття, далі до порівняння з кінцевою метою, і знову до дії.
- **Кібернетика** охоплює багато різних дисциплін, деякі з яких дійсно є можливими цілями для кібератак. Наприклад:
  - Штучний інтелект;
  - Робототехніка;
  - Системи керування;
  - Системи підтримки прийняття рішень;
  - Соціальні системи

Погляд 3: Кібербезпека включає наступальні дії (offensive actions)

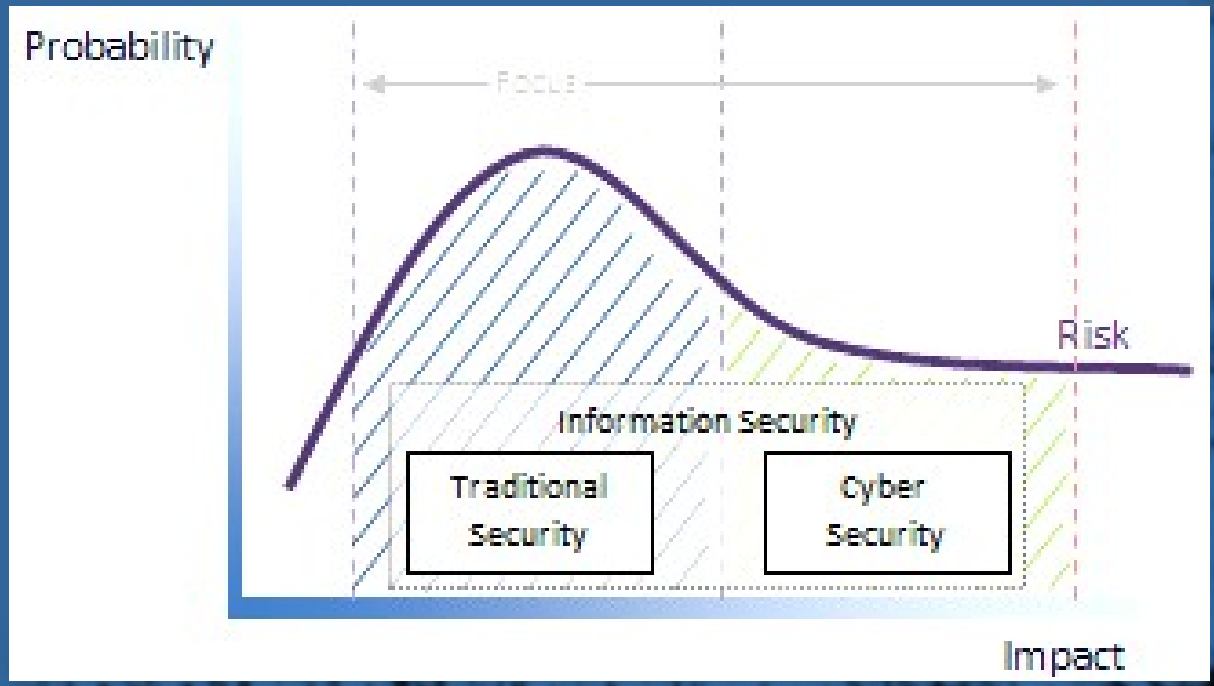
- Видавництво Gartner доручило аналітикам розробити визначення терміну “Кібербезпека” “Definition: Cybersecurity”, для класифікації публікацій
- Результати роботи аналітиків:
- ***“Кібербезпека охоплює широке коло практичних дій, засобів і концепцій, що тісно пов’язані з інформаційною безпекою. Кібербезпека відрізняється тим, що вона включає застосування інформаційних технологій для наступальних дій для атакування супротивників.”***

- “Застосування терміна “кібербезпека” як синоніма захисту інформації чи безпеки інформаційних технологій вводить в оману споживачів і професіоналів у сфері інформаційної безпеки і приховує критичну різницю між цими дисциплінами.”

Погляд 4: Кібербезпека – це зниження кіберризиків

- Кіберризики – це група ризиків з дуже потужним впливом, що включає:
  - Спрямовані атаки
  - Програмні і апаратні закладки в обладнанні
  - Шпигунів і інформаторів
  - Експлуатацію вразливостей в застарілому обладнанні
  - тощо
- Більшість кібер-ризиків донедавна вважали настільки малоймовірними, що їм не приділяли увагу

(by Menny Barzilay, published at ISACA News)



Recommendation X.1205 “Overview of Cybersecurity”

Definition:

- **Cybersecurity** is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets
- Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment
- Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment
- The general security objectives comprise the following:
  - **Availability;**
  - **Integrity, which may include authenticity and non-repudiation;**
  - **Confidentiality**

ISO/IEC 27032
“Guidelines for cybersecurity”

- Під кібербезпекою розуміють властивість захищеності активів від загроз конфіденційності, цілісності, доступності у кіберпросторі (*Cyberspace*)
- Кіберпростір – це комплексне віртуальне середовище, що не має фізичного втілення, сформоване в результаті діяльності людей, програм і сервісів в мережі Інтернет шляхом мережних і комунікаційних технологій

- Коли говорять про “кібервійни” або “кібервійська”, мають на увазі зовсім інше!
- Відомі кібератаки поза Інтернет (Stuxnet)

Місце кібербезпеки згідно ISO 27032

Онтологія*

* ISO/IEC 27032 (“Guidelines for cybersecurity”)

- Поняття кібернетичної безпеки (кібербезпеки)
- Кіберзагрози
- Заходи захисту

Загрози злочинів у кіберпросторі зростають

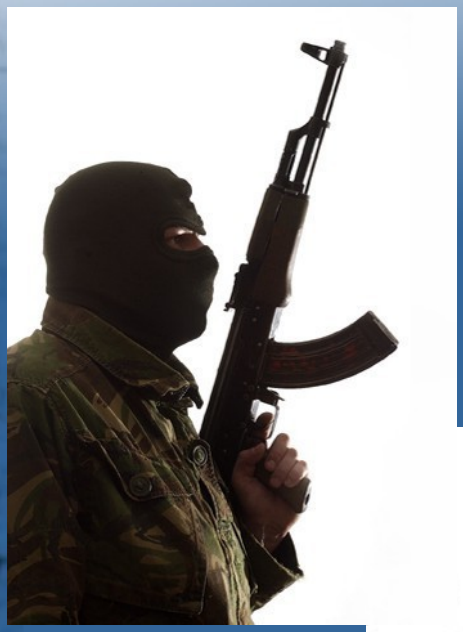
Norton Cybercrime Report
(*усі цитують*)

У 2007 році доходи кіберзлочинців вперше перевищили доходи від торгівлі наркотиками

У 2012 році за деякими оцінками вони сягнули **110 мільярдів доларів США**

Цілі кібератак

Кіберзлочинці



Кібертерористи

“Хактивісти”

Шпигуни
(конкуренти,
іноземні розвідки)

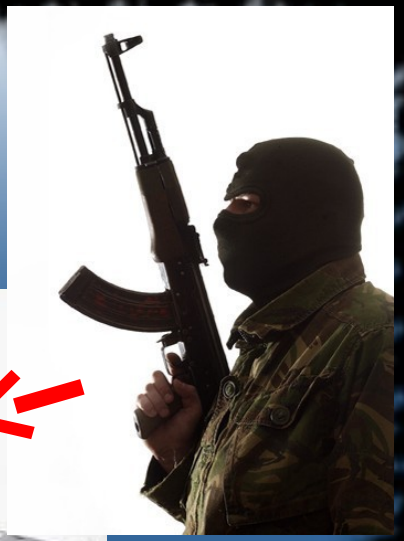
Кіберзагрози

- Таргетовані атаки (Advanced Persistent Threat)
- Кібертероризм (вплив на системи керування)
- Кібервійни
- Хактивізм
- Зловживання у соціальних мережах (вплив на суспільство)
- Атаки на банківські системи (викрадення грошей)
- Атаки на електронний уряд
- Апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання

Кіберзагрози

Hacktivists

Internet



Confidential

SCADA

Дві тактики атак на комп'ютерні системи

1) Застосувати *вірус, троянський кінь, черв'як*, маючи на меті компрометацію якомога більшої кількості систем
   - В результаті створюють *ботнет* — мережу скомпрометованих комп'ютерів
   - В подальшому ботнети застосовують для організації розподілених атак на відмову в обслуговуванні (DDOS) або для іншої злочинної діяльності в Інтернеті
2) Проводити атаку прицільно (*“таргетована атака"*) для компрометації комп'ютерів конкретної установи або конкретних користувачів
   - Якщо спроба атаки була неуспішною, готують нову спробу (*Advanced Persistent Threat – APT*)
   - Застосовують спеціально сконструйоване шкідливе програмне забезпечення. Заради успіху атаки на розробку таких програм виділяють значні кошти
   - Для таргетованої атаки може здійснюватись впровадження в атаковану організацію шпигунів і інформаторів, а також атаки на “треті сторони”, що надають сервіси тим, кого атакують.

Кіберзброя – шкідливе програмне забезпечення (malware)

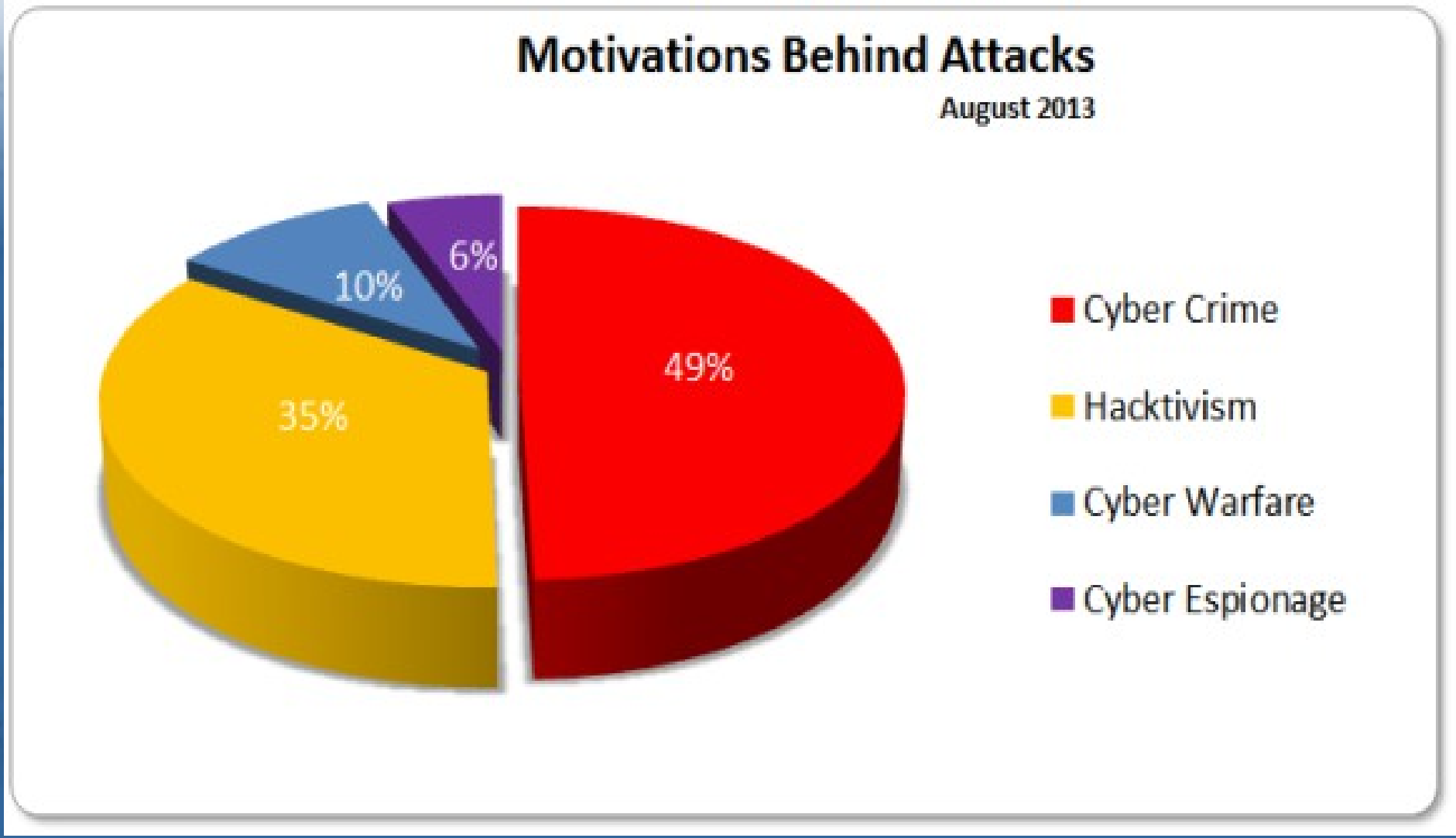
- Класичні комп’ютерні віруси (virus)
- Мережні черв'яки (worms)
- “Троянські коні” (trojan)
- Спеціальні засоби (експлойти, генератори ключів тощо)

Програмні закладки

- Програми або окремі функції програм, які приховано впроваджують у комп'ютерну систему, і які протягом тривалого часу функціонують у системі, порушуючи політику безпеки.
  - Програмні закладки можуть впроваджуватись вірусом, троянським конем, черв'яком або безпосередньо користувачем-зловмисником.
- Функції:
  - перехоплення і передавання інформації (Spyware)
  - порушення функціонування систем (“логічні бомби”)
  - утиліти віддаленого адміністрування (люки, backdoor);
  - Несанкціонована робота з мережею
    - Інтернет-клікери;
    - проксі-сервера;
    - організація DoS і DdoS атак;
  - психологічний тиск на користувача:
    - реклама (Adware);
    - злі жарти і містифікації.
- Руткіти (rootkit) – програмні закладки або їхні компоненти, призначені для приховування слідів присутності зловмисника чи зловмисної програми у системі.

Реальні атаки у кіберпросторі

- У 2010 році було виявлено шкідливе програмне забезпечення ***Stuxnet***, яке продемонструвало реальність загроз, які до того вважали лише уявними
  1. Програма була здатна атакувати локальні мережі, не підключені до Інтернету
  2. Програма була призначена для атаки на промислове обладнання ядерного об'єкта
  3. Програма була розроблена великою і добре скоординованою групою розробників
- Пізніше виявили зразки програмного забезпечення, яке мало розвідувальні функції, і було розроблене такими ж великими і професійними групами
  - Приклади таких програмних засобів – **DuQu**, **Flamer**, **Red October**
  - Як з'ясувалось, деякі з масштабних розвідувальних операцій у кіберпросторі проводились протягом майже десяти років
  - Цілі – США, Західна Європа (джерело атак – Китай), Близький Схід (ймовірне джерело – США), Росія, Казахстан, Білорусь, Україна (???)



Data from Hackmageddon.com (only essential attacks)

Приклади потенційних і фактичних атак на системи керування

- Computers and manuals seized in Al Qaeda training camps full of SCADA information related to dams and related structures.
- Ohio Davis-Besse Nuclear power plant safety monitoring system was offline for 5-hours due to Slammer Worm in January 2003.
- In 2000, former employee Vitek Boden release a million liters of water into the coastal waters of Queensland, Australia.
- In 2003, the east coast of America experienced a blackout, while not the cause, many of the related systems were infected by the Blaster worm
- In 1992, former Chevron employee disabled it's emergency alert system in 22 states, which wasn't discovered until an emergency happened that needed alerting.
- In 1997, a teenager breaks into NYNEX and cuts off Worcester Airport in Massachusetts for 6 hours, affecting both air and ground communications.
- In the action to liberate Kosovo, NATO used information warfare techniques against the Serbs, Russian hackers attacked NATO computers, Chinese hackers (in response to accidental U.S. bombing of Chinese embassy) attacked United States computers.
- In 2000, the Russian government announced that hackers succeeded in gaining control of the world's largest natural gas pipeline network (owned by Gazprom).

- Поняття кібернетичної безпеки (кібербезпеки)
- Кіберзагрози
- Заходи захисту

Забезпечення кібербезпеки

- Антивірусний захист
- Комплексні системи захисту інформації
- Системи управління інформаційною безпекою
- Перевірка відповідності системи захисту
- Навчання користувачів і підготовка фахівців

Антивірусний захист

- Принципово цей метод полягає в тому, щоби на підставі різних ознак виявити і знешкодити програми, які створені для того, щоби порушити безпеку інформації в системі
  - Сигнатурний пошук
  - Поведінковий (евристичний) аналіз
  - Незмінність файлів
- Антивірусний захист є одним із базових компонентів захисту сучасних систем
- Не слід переоцінювати його надійність – таргетовані атаки, як правило, успішно його обходять

Комплексні системи захисту інформації

- Вимоги щодо створення КСЗІ і підтвердження її відповідності встановлена Законом України
- Вимоги до КСЗІ встановлені системою НД ТЗІ
- Можна сказати, що по своїй суті КСЗІ є необхідною компонентою будь-якої інформаційної системи, безвідносно до вимог захисту інформації у конкретній системі
- Суттєвий недолік КСЗІ – статичність
  - Вимоги до КСЗІ формулюють на підставі обстеження об'єкта, далі розробляють модель загроз, оцінюють ризики, розробляють політику безпеки, інтегрують КСЗІ і проводять державну експертизу з метою підтвердження її відповідності
  - Будь-які зміни у технологіях оброблення інформації і інформаційних потоках у системі вимагають повторного обстеження і внесення змін у модель загроз, переоцінки ризиків, корегування політики безпеки і т.д.

Системи управління інформаційною безпекою

- СУІБ (Information Security Management System, ISMS) є складовою загальної системи менеджменту, що базується на підході бізнес-ризиків під час створення, впровадження, функціонування, моніторингу, аналізу, підтримки й удосконалення безпеки інформації.
- В основу розроблення СУІБ покладено модель PDCA:
  - Планування (Plan) — етап розроблення СУІБ, створення переліку активів, оцінювання ризиків і добирання заходів;
  - Дія (Do) — етап реалізації і впровадження відповідних заходів;
  - Перевірка (Check) — етап оцінювання ефективності та продуктивності СУІБ, що переважно виконують внутрішні аудитори;
  - Удосконалення (Act) — виконання превентивних та коригуючих дій.

Системи управління інформаційною безпекою – стандарти

- Практичні правила, рекомендації та специфікації у сфері безпеки інформації для створення, розвитку і підтримки СУІБ містяться у серії стандартів ISO/IEC 27000
  - ISO/IEC 27001:2005 (Системи управління інформаційною безпекою — Вимоги) — стандарт, за яким організація може бути сертифікована;
  - ISO/IEC 27002:2012 (Практичні правила управління безпекою інформації) — набір практичних правил, які зручно застосовувати як для підвищення рівня безпеки інформації в організації, так і для аудиту
  - ISO/IEC 27005:2008 (Управління ризиками інформаційної безпеки) — стандарт, що надає рекомендації з управління безпекою інформації на основі підходу керування ризиками;
  - \item ISO/IEC 27006:2007 (Вимоги до організацій, що проводять аудит та сертифікацію систем управління інформаційною безпекою) — настанова з акредитації сертифікаційних організацій.

Перевірка відповідності системи захисту

- Сертифікація систем і засобів захисту
  - Сертифікація є основною, міжнародно визнаною процедурою перевірки відповідності
  - Засоби захисту можуть проходити сертифікацію за різними стандартами, зокрема, ISO/IEC 15408 (Common Criteria)
  - СУІБ сертифікують за стандартом ISO/IEC 27001
- Державна експертиза систем і засобів захисту
  - В Україні перевірку відповідності проводять у вигляді державної експертизи згідно Положення про державну експертизу і ряду НД ТЗІ
- Аудит
  - Незалежна перевірка стану безпеки інформації
  - Аудит часто проводять на відповідність вимогам стандарту ISO/IEC 27002
- Тестування на проникнення (*penetration testing, pentest*)
  - Проводять окремо або як частину комплексного аудиту
  - Передбачає здійснення модельних атак, метою яких є демонстрація можливості подолання систем захисту і компрометації системи
  - Цей вид випробувань систем набув особливої популярності в контексті кібербезпеки

Навчання користувачів і підготовка фахівців

- Рівень кібербезпеки критично залежить від коректності дій користувачів і кваліфікації фахівців
- Навчання користувачів завжди було одною із важливих складових побудови системи захисту (КСЗІ або СУІБ)
- Різні організації проводять навчання і сертифікацію фахівців
  - Сертифікації охоплюють широке коло завдань, які повинні розв'язувати адміністратори і менеджери систем
  - У контексті кібербезпеки слід виділити курси підготовки фахівців із конструювання експлойтів і такі сертифікації, як наприклад CEH – Certified Ethical Hacker
- Все більшої популярності набувають змагання з проникнення у комп'ютерні системи (CTF – Capture The Flag)

Напрями наукових досліджень

- Моделі поведінки шкідливого програмного забезпечення
- Методи захисту програм, методи подолання захисту програм
- Математичні моделі безпеки, адекватні реальним системам
- Методи пошуку і видобування інформації в кіберпросторі
- Методи впливу на людей через кіберпростір
- Криптологія

Висновки:

- Кіберпростір вже став територією активного протистояння
- Сучасні комп'ютерні системи є вразливими
- Атаки здійснюються за допомогою спеціально розробленого програмного забезпечення, що використовує вразливості комп'ютерних систем
- Виявлення таких атак ускладнюється тим, що вони здійснюються на обмежену кількість спеціально визначених цілей, не викликають збоїв і відмов комп'ютерів, і тому тривалий час не потрапляють у поле зору дослідників з антивірусних лабораторій
- Методи захисту не завжди ефективні — вимагають розвитку

- Кібербезпека — актуальна проблема сучасності