Житомирська політехніка	Міністерство освіти і науки України Державний університет «Житомирська політехніка»

Лекція 2

Інциденти у сфері високих технологій

Фактично неприховані спроби впливу протиборчих сторін на інформаційний і кіберпростори один одного за рахунок використання засобів сучасної обчислювальної і/або спеціальної техніки й відповідного програмного забезпечення називають ***кібервтручанням*****.**

Під ***інцидентами*** у сфері високих технологій розумітимемо *події, що полягатимуть в реалізації певної загрози та порушенні встановленого рівня безпеки інформаційно-комунікаційних систем.*

Процесом управління інцидентами називатимемо *процес реєстрації інформації про стан безпеки та рівноваги ІКС, передавання інформації в пункти її нагромадження, переробки й аналізу, з ухваленням прийняття рішення та формуванням певного керуючого впливу на об'єкт управління*.

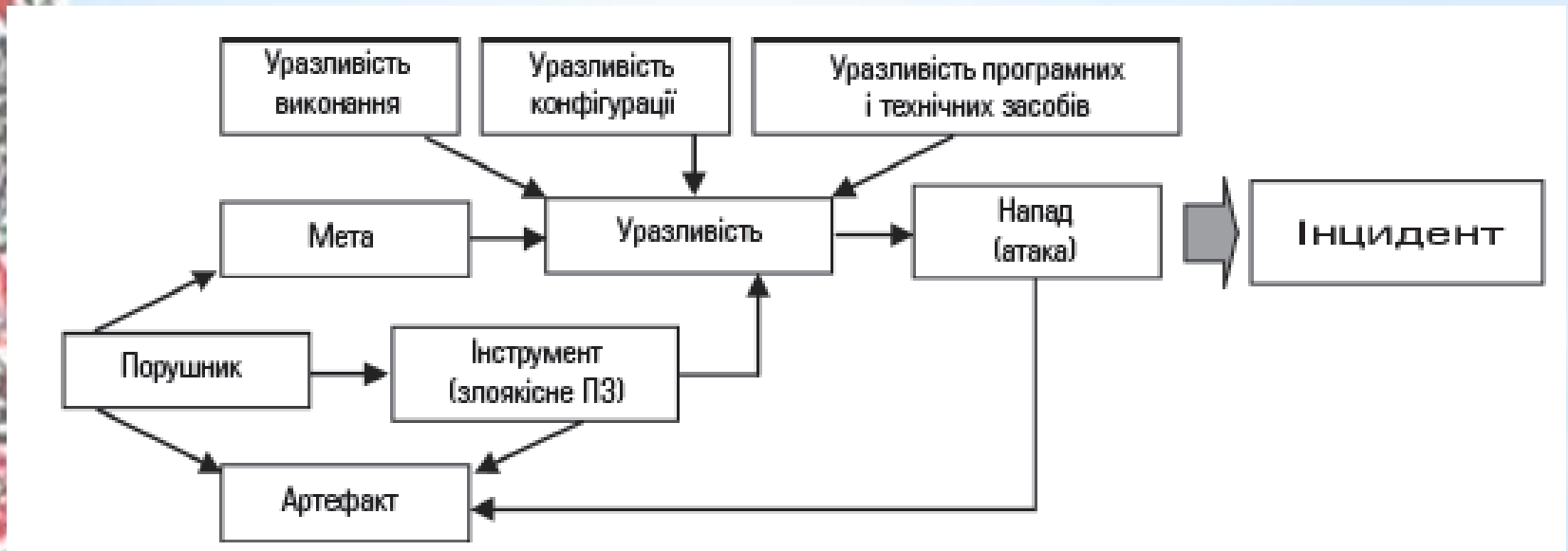


Рис. 1. Діаграма виникнення інцидентів у сфері високих технологій

Інциденти поділяються на:

- власне комп’ютерні інциденти, які полягають, наприклад, у втручанні в роботу обчислювальних систем, порушенні авторських прав на програмне забезпечення, а також у розкраданні даних і комп’ютерного часу;
- інциденти, пов’язані з комп’ютерами, що супроводжують здебільшого протиправні дії з фінансового шахрайства;
- мережні інциденти, що призводять до укладання незаконних угод.

Сім основних груп:

- перехоплення паролів інших користувачів;
- «соціальна інженерія»;
- використання помилок ПЗ і програмних закладок
- використання помилок механізмів ідентифікації користувачів
- використання недосконалості протоколів передавання даних;
- одержання інформації про користувачів стандартними засобами операційних систем;
- блокування сервісних функцій системи, що зазнає атаки.

Класифікація кібернетичних втручань і загроз становить схема, запропонована Конвенцією Ради Європи 2001 року й спрямована на боротьбу з кіберзлочинністю:

1. ***Інциденти, що мають на меті завдати шкоди конфіденційності, цілісності й доступності комп'ютерних даних та систем*** **і реалізуються через:**

• несанкціонований доступ в інформаційне середовище (протиправний навмисний доступ до комп'ютерної системи або її частини, а також до ІР протиборчої сторони, здійснений в обхід систем безпеки);

• втручання в дані (протиправна зміна, ушкодження, вилучення, перекручування або блокування комп'ютерних даних і керуючих команд за допомогою кібератак на інформаційні системи, ресурси та мережі державного і військового управління);

• втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи через розробку та поширення вірусного ПЗ, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби й системи телекомунікацій і зв'язку, на

обробку та передавання інформації, на системи захисту ІР, систем і мереж, програмно-математичне забезпечення, протоколи передавання даних, алгоритми адресації та маршрутизації);

• незаконне перехоплення (протиправне навмисне аудіовізуальне і/або електромагнітне перехоплення не призначених для загального доступу комп'ютерних даних, переданих СІТС в обхід заходів безпеки);

• незаконне використання комп'ютерного й телекомунікаційного обладнання або його повне вилучення.

Класифікація кібернетичних втручань і загроз становить схема, запропонована Конвенцією Ради Європи 2001 року й спрямована на боротьбу з кіберзлочинністю:

2. ***Шахрайство та підробка, пов'язані з використанням комп'ютерів*, а саме:**

- підробка документів із застосуванням комп'ютерних засобів (протиправне навмисне внесення, змінювання, вилучення або блокування комп'ютерних даних, що призводить до зниження вірогідності документів);
- шахрайство із застосуванням комп'ютерних засобів (втручання у функціонування комп'ютерної системи з метою навмисного протиправного одер-

жання економічної вигоди).

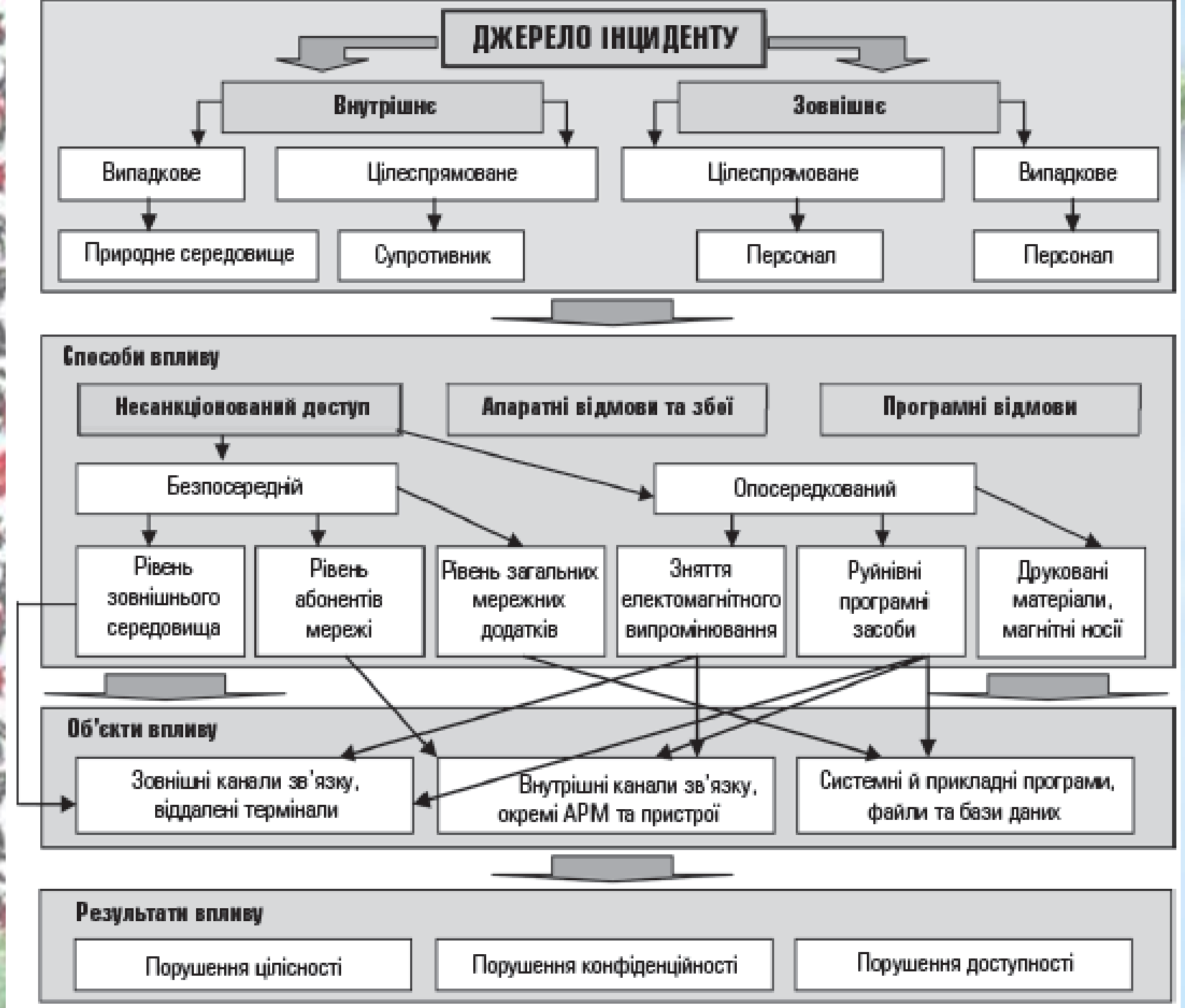
3. ***Інциденти, пов'язані з розміщенням у мережах протиправної інформації*** (наприклад, поширенням дитячої порнографії).

4. ***Інциденти щодо авторських і суміжних прав***.

Узагальнена модель системи управління інцидентами ІБ :

$$Model_{IKC}^{INC} = \\ = (INC, SEC, CRI, KBS, X, Y, S, DMF, AGT, ARS, TRS, IRS, MST, T, SYN),$$

де *INC* — управління інцидентами (внутрішніми та зовнішніми); *SEC* — мета; *CRI* — критерії оцінювання стану безпеки; *KBS* — база знань про внутрішні та зовнішні інциденти; *X* — вхідні впливи; *Y* — реакція на внутрішні та зовнішні інциденти; *S* — стан системи; *DMF* — функція ухвалення (реагування), що поділяється на два етапи: на першому ухвалюється рішення про включення елемента *ARS* до набору *TRS*, а на другому (згідно з результатом виконання першого етапу) — рішення про включення елемента *ARS* до набору *IRS*; *AGT* — множина програмно-реалізованих мобільних інтелектуальних агентів; *ARS* — набір ресурсів інформаційної безпеки, які доступні агентам; *TRS* — тестовий набір ресурсів інформаційної безпеки; *IRS* — інцидентно-орієнтовані набори ресурсів; *MST* — стратегія управління інцидентами; *T* — час; *SYN* — самоорганізація.


ДЖЕРЕЛО ІНЦИДЕНТУ
Внутрішнє
Зовнішнє
Випадкове
Цілеспрямоване
Цілеспрямоване
Випадкове
Природне середовище
Супротивник
Персонал
Персонал
Способи впливу
Несанкціонований доступ
Апаратні відмови та збої
Програмні відмови
Безпосередній
Опосередкований
Рівень зовнішнього середовища
Рівень абонентів мережі
Рівень загальних мережних додатків
Зняття електомагнітного випромінювання
Руйнівні програмні засоби
Друковані матеріали, магнітні носії
Об'єкти впливу
Зовнішні канали зв'язку, віддалені термінали
Внутрішні канали зв'язку, окремі АРМ та пристрої
Системні й прикладні програми, файли та бази даних
Результати впливу
Порушення цілісності
Порушення конфіденційності
Порушення доступності

Найпоширеніші системні події, що спричинені внутрішнім інцидентом:

- *витік конфіденційної інформації;*
- *неправомірний доступ до інформації;*
- *вилучення інформації;*
- *компрометацію інформації;*
- *саботаж;*
- *шахрайство за допомогою ІТ;*
- *аномальну мережну активність;*
- *аномальне поводження бізнес-додатків;*
- *використання активів установи в особистих цілях або в шахрайських операціях.*

Найпоширеніші системні події, що спричинені зовнішнім інцидентом:

- *шахрайство в системах електронного документообігу*;
- *атаки типу «відмова в обслуговуванні» (DoS), у тому числі розподілені (DDoS)*;
- *перехоплення й підміна трафіку*;
- *неправомірне використання бренду установи в мережі Інтернет*;
- *фішинг*;
- *розміщення конфіденційної* (*провокаційної*) *інформації в мережі Інтернет*;
- *злам або спроба зламу мережних вузлів*;
- *сканування порталу установи або мережі, вірусні атаки*;
- *неправомірний доступ до конфіденційної інформації*;
- *анонімні листи* (*листи з погрозами*).

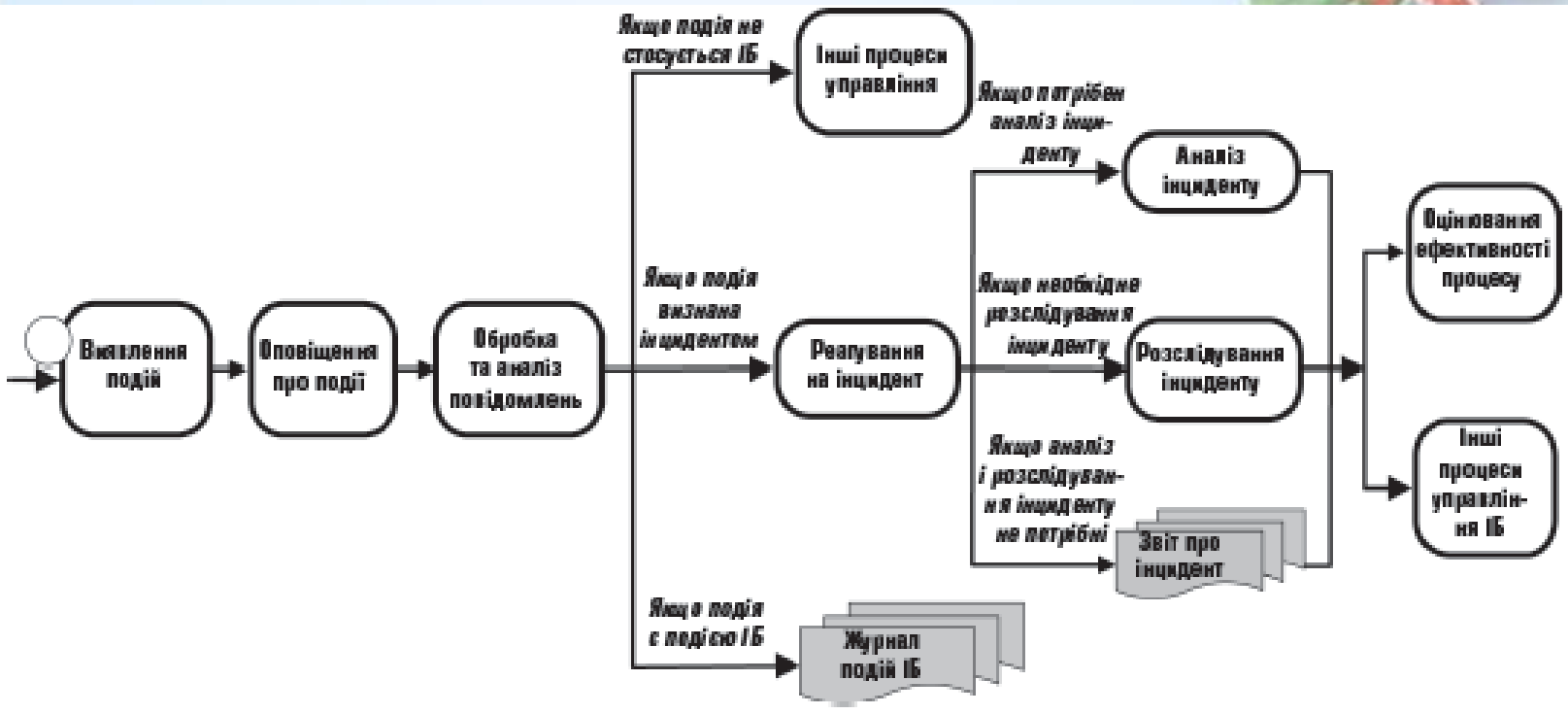


Рис. 3. Процес управління інцидентами ІБ

До найбільш небезпечних інцидентів належать:

1) пошукова оптимізація (SEO — *Search Engine Optimization*), яку застосовують зловмисники для поширення шкідливих програм. Використовуючи технології SEO та вразливість ПЗ, зловмисники посилюють позиції своїх попередньо заражених web-сторінок і в такий спосіб спонукають користувачівзробити запит щодо інтригуючої новини в пошуковій системі, отримати результат, перейти за одним із найбільш верхніх посилань на сторінку зловмисника, запустивши цим самим на своїй ПЕОМ шкідливу програму;
2) експлуатація вразливостей у клієнтському ПЗ, розробленому третьою стороною, наприклад уразливостей так званої нульової доби, що їх застосовують зловмисники для призупинення виконання певних виробничих процесів. Дедалі частіше з цією метою використовуються вразливості в офісних програмах (Word, Excel і PowerPoint) і мультимедіа-програвачах (Real Player, iTunes, QuickTime), а також спеціальні утиліти для перегляду документів (наприклад, Adobe Reader);

До найбільш небезпечних інцидентів належать:

3) цільовий фішинг (*Spear Phishing*), що його застосовують зловмисники для того, аби змусити користувача виконати якусь деструктивну дію на кшталт установлення шкідливого ПЗ на сервері компанії. Із цією метою зловмисники надсилають певним працівникам компанії ретельно підготовлені цільові повідомлення, що мають переконати жертву відкрити шкідливе вкладення або перейти за посиланням на сайт, що містить експлойти для зламу програм на боці користувача;

4) перехоплення браузера (*browser hooking*), що його застосовують зловмисники для розміщення на web-сайтах контенту, який містить шкідливі скрипти (сценарії). Відкриваючи такий сайт, користувач фактично запускає на своїй ПЕОМ відповідні скрипти, тобто надає зловмисникові контроль над власним браузером. Перехоплений у такий спосіб контроль над браузером користувача дозволяє зловмисникові використовувати його як відправну точку для подальших атак на інші системи, у тому числі внутрішні ресурси мережі й серверикомпанії;

До найбільш небезпечних інцидентів належать:

5) масові SQL-ін’єкції, що їх застосовують зловмисники для крадіжки конфіденційних даних з окремих web-додатків і баз даних; зміни вмісту баз даних, які будуть відображатися на web-сайтах; зміни web-контенту й розміщення на сайті шкідливих скриптів для атаки на браузери відвідувачів, а також інших експлойтів, що використовують уразливості ПЗ на боці користувача;

6) атаки на адміністративні web-інтерфейси, що їх застосовують зловмисники для здійснення контролю за певними системами або інфраструктурами (ERP-системами, системами управління HVAC і електропостачанням тощо) за рахунок перехоплення браузера або експлуатації вразливостей ПЗ на боці користувача;

7) атаки на сайти соціальних мереж (Facebook, LinkedIn, Twitter та ін.), що їх застосовують зловмисники для збору критичної інформації про діяльність компанії та технології, використовувані її співробітниками; поширення експлойтів і скриптів із метою перехоплення браузера користувача;

До найбільш небезпечних інцидентів належать:

8) атаки типу «передача хеша» (*pass-the-hash*), що їх застосовують зловмисники для одержання доступу в корпоративний домен за рахунок інтегрованих у Windows-системи пакетів для проведення атак (таких, наприклад, як Metasploit і Nmap). При цьому викрадені хеші використовуються зловмисниками для автентифікації замість паролів;

9) злам устаткування, що за рахунок перехоплення інформації, переданої по шинах даних (*bus sniffing*), зламу прошивань, зміни системного часу (*clock glitching*) та інших витончених атак на обладнання забезпечує зловмисникам можливість обійти захисні механізми й одержати ключі шифрування.

Приклади інцидентів:

1. *Червень 1982 р.* Через активацію програмного забезпечення, отриманого радянськими розвідниками в Канаді, куди, як з'ясувалося згодом, американці попередньо ввели помилкові дані, було здійснено кібератаку проти сибірського газопроводу. Після одержання команди ззовні програма перевищила режим роботи газопроводу настільки, що він вибухнув.

2. *1995 рік.* Банк «Україна» через проникнення в його мережу було пограбовано на суму майже 4 млн дол.

До речі, аналогічні деструктивні інциденти в Україні трапляються дедалі частіше. Найзначніші атаки відбулися 1997 року, коли на кілька годин було заблоковано роботу інтернет-провайдера «Глобал Юкрейн»; 2000 року, коли сталася інформаційна диверсія проти інтернет-провайдера «ukr.net»;

лютий 2012 року - масований кібернапад на державні інтернет-ресурси під час виборчої кампаніїі.

3. *2009 рік*. Здійснено цілеспрямовану атаку GhostNet із центром управління в Китаї, зорієнтовану на понад 100 країн. Вторгнення відбувалося за допомогою повідомлення електронної пошти, при відкритті якого запускалася шкідлива програма із прикріпленого файла. Після встановлення вірус завантажував хакерський інструментарій Ghost Remote Administration Toolkit для дистанційного управління системами. Управляючий сервер у Китаї потім міг надсилати вірусу команди на передавання інформації з комп'ютерів що зазнали атаки. У тому самому 2009 році почалася операція «Аврора», яка, цілком імовірно також виходила з Китаю й мала на меті викрадення інтелектуальної власності й закритої інформації з баз даних високотехнологічних компаній та національних безпекових і оборонних відомств. Атакувальники використовували вразливість класу *use-after-free* в *Internet Explorer*, що уможливлювала псування пам'яті об'єктів HTML. Це дозволяло атакувальнику впровадити сторонній код в область пам'яті, що вивільнялась із вилученням об'єкта. Для цього негайно після вилучення об'єкта на його місці сторонній код створював новий. Атака здійснювалась методом супутного завантаження (*drive-by download*), що відбувалось без відома користувача, у результаті чого його машина зазнавала зараження вірусом.

4. *2010–2012 роки*. Сталися міждержавні інциденти, до яких призвели відомі мережні черв'яки *Duqu*, *Flame* та *Stuxnet*. Останній було розроблено групою фахівців з Ізраїлю та США за участю представників Німеччини й Великобританії. Наслідком його деструктивних дій стало гальмування ядерної програми Ірану. Цьому посприяло виявлення вірусом програмованих логічних контролерів (ПЛК) у автоматизованій системі управління технологічними процесами станції (*Supervisory Control And Data Acquisition*), а також те, що нападникам удалося використати (для впровадження особливого коду в «залізо» ПЕОМ АЕС) чотири невідомі раніше вразливості «нульової доби» («zero-day») у діючих версіях ОС Windows та два дійсні сертифікати від компаній Realtek і JMicron. Саме наявність останніх дала змогу Win32/Stuxnet тривалий час уникати антивірусних радарів.

У процесі докладного вивчення Win32/Stuxnet фахівці відомої лабораторії Касперського дійшли невтішного висновку: поява згаданої шкідливої програми фактично знаменувала собою початок нової ери — ери кібервоєн.

https://ua.interfax.com.ua/news/tag/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8.html

https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BB%D1%96%D0%BA_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA

Рис. 4. Схема функціонування вірусу Win32/Stuxnet

Мережний черв’як Worm.Win32.Flame

виявленого 2012 року фахівцями лабораторії Касперського, то його розробили західні програмісти,як з’ясувалося, виключно з метою ведення кібершпигунства. Основні функції Worm.Win32.Flame такі:

- поширення за допомогою знімних дисків та локальних мереж;
- зараження лише певних ПЕОМ;
- перехоплення мережних пакетів, виявлення мережних ресурсів та збір переліку вразливих паролів;
- сканування диска інфікованої системи щодо наявності визначених розширень та контенту;
- копіювання зображень з екрана користувача в разі активності певних процесів;
- використання мікрофона інфікованої системи для запису звуків із навколишнього середовища;
- передавання інформації на сервери зловмисників;
- використання понад 10 доменів для приймання команд із серверів управління;
- установлення безпечного з’єднання із серверами управління через SSH- та HTTPS-протоколи;
- сумісність з операційними системами Windows XP, Vista та 7.

Характерна відмінність черв’яка Worm.Win32.Flame від інших троянів полягає в наявності прихованого алгоритму дії та широкого спектра «бойових» можливостей

Можливості троянських вірусних програм Stuxnet, Duqu та Flame

Характеристика програми	Stuxnet	Duqu	Flame
Дата впровадження	Червень-вересень 2012 р.	Вересень 2011 р.	Травень 2012 р.
Призначення	Ураження автоматизованих систем управління атомною інфраструктурою Ірану (АВС у м. Бушер та завод зі збагачення урану в м. Натанз)	Збір конфіденційної інформації про особливості функціонування стратегічно важливих ядерних та індустріальних об'єктів	Цілеспрямований систематичний збір даних (офісні документи, креслення тощо), можливість модифікації інформації
Географія поширення	Іран, Норвегія, країни Близького Сходу	Близький Схід	
Спосіб поширення	Мережа Інтернет, знімні носії інформації типу USB Flash Drive		
Мови програмування	Асемблер, C, C++	C, програмна архітектура Microsoft Visual C++	C, C++, ША
Обсяг файла	До 0,5 Мбіт	Від 0,06 до 0,23 Мбіт	Понад 20 Мбіт
Розмір програмного коду	Близько 10 тис. рядків	6–8 тис. рядків	750 тис. рядків (базовий модуль — 650 тис. рядків / 6 Мбіт; найменший модуль — 70 тис. рядків (170 — зашифровані)
Принцип дії	Ґрунтується на використанні вразливостей (помилок) ОС Microsoft Windows		
Можливість самодублювання і самознищення	Самодублювання	Самодублювання та самознищення	Самознищення
Алгоритм маскування присутності в системі	Використання фальшивих сертифікатів компаній «Realtek Semicon ductof» та «JMicron Technology»	—	Використання дійсних сертифікатів компанії «Microsoft»
Інші особливості	Залучення до розробки значних технічних та фінансових ресурсів		

Заходи із захисту інформації (мереж і систем) від кіберзагроз та їхній аналіз

№ з/п	Відповідно до рекомендацій американської IT-компанії «SANS»		Відповідно до вимог НД ТЗІ України
1	2		3
1	Інвентаризація дозволених для підмикання пристроїв, а також пристроїв, підмикених не санкціоновано		Реалізація функціонального профілю безпеки (ФПБ) «Автентифікація отримувача» унеможливлює відмову від одержання і забезпечує однозначне встановлення факту одержання певного об'єкта певним користувачем
2	Інвентаризація дозволеного для встановлення ПЗ, а також ПЗ, установленого на ПЕОМ мережі не санкціоновано		Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення готових інформації, які існують, але не контролюються іншими ФПБ
3	Безпечне настроювання апаратного й програмного забезпечення для серверів, робочих станцій і ноутбуків	*Образи, з яких здійснюється встановлення систем, мають бути попередньо налаштовані для забезпечення необхідного рівня захисту та протестовані*	Реалізація ФПБ «Самотестування» дозволяє комплексу засобів захисту інформації перевіряти і на підставі цього гарантувати правильність функціонування та цілісність певної множини функцій ІТС
4	Безпечне настроювання мережних пристроїв	*Налаштовування міжмережних екранів, маршрутизаторів, комутаторів і т. ін.*	Реалізація ФПБ «Самотестування» дозволяє комплексу засобів захисту інформації перевіряти і на підставі цього гарантувати правильність функціонування та цілісність певної множини функцій ІТС
5	Захист периметра мережі	*Забезпечуваний міжмережними екранами, проксі, DMZ і системами IPS рівень захисту мережі має бути перевірений сканерами вразливостей*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення потоків інформації, які існують, але не контролюються іншими ФПБ
6	Супровід, моніторинг і аналіз журналів реєстрації подій		Реалізація ФПБ «Реєстрація» дозволяє контролювати небезпечні для ІТС дії. Рівні цієї послуги ранжуються залежно від гнучкості вибірковості контролю, складності засобів аналізу даних журналів реєстрації та здатності до виявлення потенційних порушень
7	Безпека прикладного ПЗ	*Розроблене й придбане ПЗ має бути протестоване за допомогою автоматизованих засобів аналізу або засобів ручного тестування на проникнення*	Реалізація ФПБ «Самотестування» дозволяє комплексу засобів захисту інформації перевіряти і на підставі цього гарантувати правильність функціонування та цілісність певної множини функцій ІТС
8	Контроль використання адміністративних привілеїв	*Проведення моніторингу використання й відстежування облікових записів, що мають адміністративні привілеї*	Реалізація ФПБ «Розподіл обов'язків» дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні цієї послуги ранжуються на підставі вибірковості керування можливостями користувачів і адміністраторів

1	2		3
9	Контроль доступу на основі принципу «потрібен знати»	*Відокремлення критичних даних від менш критичних та забезпечення контролю доступу до них*	Реалізація ФПБ «Адміністративна (довірча) конфіденційність» та «Адміністративна (довірча) цілісність» дозволяє адміністратором або спеціально авторизованому користувачеві керувати потоками інформації від користувачів до захищених об'єктів. Рівні цієї послуги ранжуються на підставі повноти захисту та вибірковості керування
10	Постійний аналіз уразливостей їх усунення	*Упровадження ефективних засобів для сканування, які дозволяють порівнювати здобуті результати зі результатами попереднього сканування для визначення змін, що відбулися*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення наявних потоків інформації, не контрольованих іншими ФПБ
11	Моніторинг і контроль облікових записів	*Застосовування самостійно розроблених скриптів або спеціалізованих додатків для аналізу вмісту журналів реєстрації подій*	Реалізація ФПБ «Ідентифікація і автентифікація» дозволяє комплексу засобів захисту інформації визначити і перевірити особистість користувача, що намагається одержати доступ до ІТС. Рівні цієї послуги ранжуються залежно від кількості задіяних механізмів автентифікації
12	Захист від шкідливого коду	*Використання адміністративних функцій або операційних систем забезпечення безпеки кінцевих точок для перевірки функціонування засобів захисту від шкідливих програм і системи IPS/IDS рівня хосту на всіх ГЕОМ мережі*	—
13	Обмеження та контроль мережевих портів, протоколів і служб	*Відключення невикористовуваних служб і протоколів, блокування непотрібних для роботи портів, установлення мінімережевих екранів рівня хосту для підвищення захисту*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення наявних потоків інформації, не контрольованих іншими ФПБ
14	Захист і контроль бездротових пристроїв	*Застосовування спеціалізованих IDS. Сканування та моніторинг для виявлення фізичних бездротових мереж*	Реалізація ФПБ «Конфіденційність при обміні» та «Цілісність при обміні» дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, або її модифікації під час їх експорту/імпорту через незахищене середовище
15	Запобігання витоку даних	*Використання рішень DLP для виявлення спроб викрадення критичних даних зсередині мережі компанії, а також іншої підозрілої активності*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення наявних потоків інформації, не контрольованих іншими ФПБ

1	2		3
16	Забезпечення безпеки мережі	*Застосування найкращих практичних досягнень у сфері безпеки при проектуванні мережі, а також при настроюванні маршрутизаторів, комутаторів, критичних серверів, міжмережевих екранів, компонентів безпеки й груп користувачів ПЕОМ*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення потоків інформації, не контрольованих засобами ФПБ
17	Тестування на проникнення	*Наслідування дій комп'ютерних злочинників при визначенні мети і підходів до проведення тестів на проникнення. Використовування відомостей про виявлені недоліки для підвищення безпеки*	Випробування КСЗІ в цілому та комплексу засобів захисту інформації (як складової КСЗІ або як окремого об'єкта експертизи в галузі ТЗІ — обов'язковий етап при створенні КСЗІ в ІТС. Вимоги до випробувань визначаються відповідними критеріями і кратній
18	Організація реагування на інциденти	*Періодичне проведення навчань і практичне відпрацювання процедур реагування на інциденти на основі певних сценаріїв*	Одна з неодмінних умов створення та функціонування КСЗІ в ІТС — наявність служби захисту інформації в ІТС, на яку покладаються загальні організаційні та координаційні роботи, пов'язані із захистом інформації в ІТС, підтримання необхідного рівня захищеності інформації та ресурсів ІТС
19	Організація дій із відновлення даних	*Упровадження надійних і безпечних процедур резервного копіювання важливих даних*	Реалізація ФПБ «Відкочування» уможливлює відміну операцію або послідовності операцій і повернення (відкочування) захищеного об'єкта до попереднього стану. Ресурси цієї послуги ранжуються на підставі множини операцій, для яких забезпечується відкочування
20	Оцінювання навиків навчених щодо безпеки, проведення необхідних тренінгів	*Оцінювання знань і навичок співробітників із питань безпеки та проведення в разі потреби додаткового навчання*	Одна з функцій служби захисту інформації в ІТС полягає в організації професійної підготовки та підвищення кваліфікації користувачів ІТС із питань захисту інформації, проведення занять та контрольних перевірок

Якщо було зафіксовано порушення кібербезпеки на ОІД, то співробітники служби безпеки компанії (організації, установи) мають вжити таких заходів:

1) ідентифікувати інцидент і переконатися, що він насправді відбувався;
2) локалізувати область ІТ-інфраструктури, задіяної в інциденті;
3) обмежити доступ до об’єктів, задіяних в інциденті;
4) повідомити підрозділ інформбезпеки про факт виникнення інциденту;
5) залучити компетентних фахівців для консультування;
6) створити групу з розслідування інциденту, скласти план робіт зі збору доказів і відновлення систем, а також забезпечити ведення протоколу подій;
7) забезпечити схоронність і належне оформлення доказів, для чого зняти енергозалежну інформацію із системи, яка працює; зібрати в реальному часі інформацію про інцидент; відімкнути від мережі живлення;

Якщо було зафіксовано порушення кібербезпеки на ОІД, то співробітники служби безпеки компанії (організації, установи) мають вжити таких заходів:

8) у присутності третьої незалежної сторони вилучити й опечатати носії інформації з доказовою базою, знявши образи та іншу інформацію для подальшого її аналізу та зберігання. При цьому необхідно:

• оформити протоколом всі операції з носіями інформації;

• задокументувати процес на фото- або відеокамеру;

• подати докладний опис об’єктів, що містять інформацію, даних, які витягаються, а також місць їх зберігання;

• зберегти опечатані об’єкти разом зі складеним протоколом у надійному місці до передачі носіїв на дослідження;

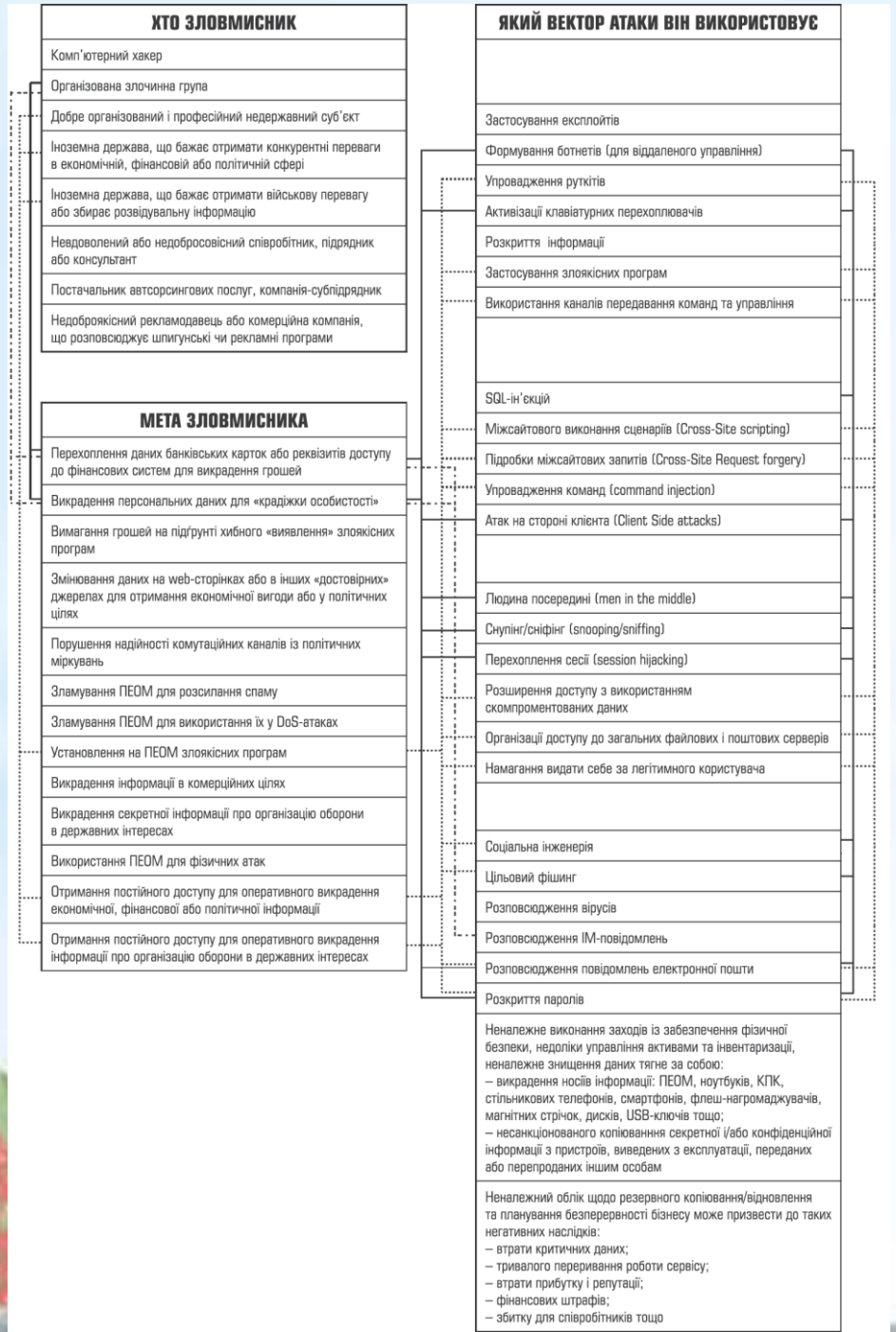
9) після збереження та оформлення речових доказів відновити роботоздатність ІС;

10) при проведенні дослідження джерел інформації забезпечити незмінність доказів (працювати тільки з копією);

11) у процесі розслідування забезпечити коректну взаємодію із зацікавленими підрозділами та зовнішніми організаціями;

12) закінчивши розслідування, оформити відповідний звіт та скласти рекомендації зі зниження ризиків виникнення аналогічних інцидентів у майбутньому.

Окрім цього слід своєчасно налаштувати ПЗ АРМ (РСт) та програми міжмережного екрана (Firewall) для безпечного доступу до ресурсів мережі Інтернет і ЛОМ, заборонити копіювання та запуск на виконання невідомих програм або програм, отриманих із несертифікованих джерел, обмежувати права доступу користувачів до об’єктів файлової системи та запуску системних програм, керувати розмежуванням доступу.



Карта кіберзагроз містить ключові елементи, які мають місце майже в кожній атаці, і пропонує кроки проведення успішних атак та контзаходи для захисту від них. Будь-яка атака може бути подана у вигляді певного шляху на карті. Як приклад наведено три варіанти атак: викрадення даних банківських карток та фінансової інформації, цілеспрямовані атаки мотивованого і кваліфікованого зловмисника та пошукова оптимізація

ЯКИМИ ЦІЛЬОВИМИ СИСТЕМАМИ ЗЛОВМИСНИК КОРИСТУВАВСЯ ДЛЯ ПРОНИКНЕННЯ ?	ЯКИЙ ЗАХИСТ МОЖЕ ЗУПИНИТИ ЗЛОВМИСНИКА
	Захисний рівень № 1 — проактивне забезпечення безпеки ПЗ
Робочі станції	Сканери безпеки додатків, що працюють за принципом «білого ящика»
Ноутбуки	Сканери безпеки додатків, що працюють за принципом «чорного ящика»
КПК	Оцінювання загроз на рівні мережі
Флешки	Оцінювання загроз на рівні хостів
Бітові пристрої з USB (цифрові фоторамки, камери, плеєри)	Тестування додатків на проникнення
	Оцінювання можливостей додатків щодо забезпечення безпеки
	Захисний рівень № 2 — блокування атак на рівні мережі
Стільникові телефони та смартфони	Виявлення та запобігання вторгненням (IDS/IPS)
Офісні АТС та інфраструктура телефонії	Запобігання вторгненням через безпроводові мережі (WIPS)
Мережні пристрої	Аналіз мережної активності та визначення шаблона «нормальної» поведінки (базового рівня мережної активності)
Безпроводові мережі	Міжмережні екрани, корпоративні антивіруси, UTM-пристрої
Міжмережні екрани	
Обладнання IDS/IPS	Шлюзи повідомлень для забезпечення безпеки та засобів захисту від спаму
Маршрутизатори	Міжмережні екрани прикладного рівня (WAF)
Комутатори	Керовані сервіси безпеки
DNS-сервери	**Захисний рівень № 3 — блокування атак на рівні хоста**
Поштові сервери	Захист кінцевих точок, у тому числі антивірусне та антишпигунське ПЗ, персональний міжмережний екран, система IPS на рівні хоста тощо
	Процедура реагування на інциденти та проведення криміналістичного аналізу
Сервери баз даних	Контроль доступу до мережі (NAC)
Мережі VPN	Засоби контролю цілісності системи
Периферійні пристрої («розумні» принтери)	Засоби підвищення захищеності конфігурацій
	Обмежене використання адміністративних облікових записів
	Захисний рівень № 4 — виявлення та усунення уразливостей
	Засоби сканування мережі для виявлення підімкнених засобів
	Управління уразливостями
	Тестування на проникнення в мережу, етичне зламування
	Управління патчами і конфігураціями, забезпечення відповідності вимогам
	Захисний рівень № 5 — безпечна підтримка уповноважених користувачів
	Управління ідентифікацією та доступом
	Захист даних на мобільних пристроях та носіях інформації
	Шифрування даних, що підлягають зберіганню, а також резервних копій
	Засоби моніторингу контенту
	Захист авторських прав і даних від витоку
	Віртуальні приватні мережі
	Захисний рівень № 6 — засоби для управління безпекою
	Управління логами, інформацією та подіями безпеки (SIEM)
	Знищення носіїв інформації та пам'яті мобільних пристроїв
	Підвищення кваліфікації в галузі безпеки
	Тренінги для підвищення обізнаності
	Корпоративні засоби криміналістичного аналізу
	Стратегічне управління, засоби управління ризиками та відповідністю
	Безперервність бізнесу та відновлення після аварій

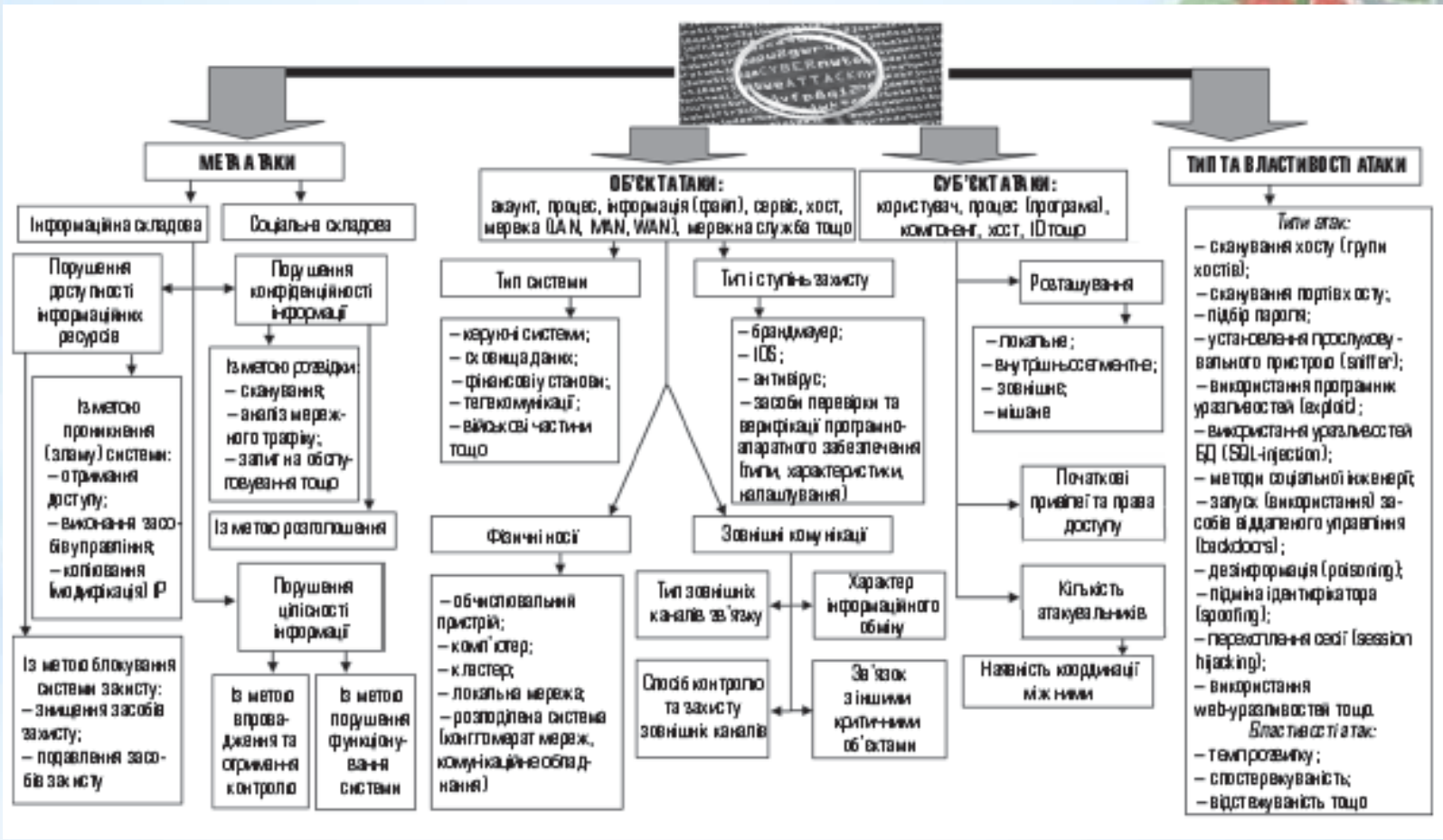
Карта кіберзагроз характеризує ключові елементи, притаманні майже кожній атаці, що призводять до ефективних атак, і описує заходи із захисту від них. Будь-яка атаку може бути представлена у вигляді певного шляху на карті. Наприклад, на ній позначено три варіанти атак: викрадення даних банківських карт та фінансової інформації (суцільні лінії), цілеспрямовані атаки мотивованого і кваліфікованого зловмисника (пунктирні лінії) та пошукова оптимізація (штрихпунктирні лінії)

ТОП-9 найбільш небезпечних векторів атак

1	**Пошукова оптимізація (SEO — Search Engine Optimization)**	Спосіб розповсюдження злоякісних програм. Коли відбуваються певні події, інформація про які з'являється в усіх новинах, зловмисники використовують технології SEO, аби підняти позиції своїх попередньо заражених web-сторінок у результатах видачі пошукових систем. Коли користувач зробить у пошуковій системі запит до новини, яка його цікавить, він, отримавши результат, почне рух згідно з одним із верхніх посилань і потрапить на сторінку зловмисника, яка намагатиметься завантажити й запустити на ПЕОМ користувача злоякісну програму завдяки уразливості ПЗ користувача
2	**Експлуатація уразливостей у клієнтському ПЗ, розробленому третьою стороною**	Оскільки операційні системи (ОС) стали значно безпечнішими, зловмисники дедалі частіше переходять до використання уразливостей у сторонньому ПЗ, що працює в ОС, передусім у Word, Exel та Power Point, мультимедіа-програвачах — Real player, QuickTime тощо, а також у спеціальних утилітах для перегляду документів, наприклад Adobe Reader. Доволі часто зловмисники використовують у своїх атаках уразливості «нульової доби», для яких розробник ще не випустив патч, який виправляє недоліки уразливого ПЗ
3	**Цільовий фішинг (Spear phising)**	Зловмисники надсилають певним особам (передусім керівникам) у компанії цільові й реалістичні сценарії (повідомлення), аби спонукати жертву відкрити злоякісне вкладення або перейти за посиланням на сайт, який містить експлойти для зламування програм на боці користувача

4	**Перехоплення браузера (browser hooking)**	Експлуатуючи уразливості, що дозволяють здійснювати міжсайтове виконання сценаріїв на довірених web-сайтах, зловмисники розміщують контент, який містить злоякісні скрипти (сценарії). Коли користувач відкриває такий сайт, браузер на його ПЕОМ запускає ці крипти та надає зловминику контроль над самим браузером користувача. Перехоплений таким чином контроль над браузером користувача дозволяє зловмиснику використати його як точку відліку для подальших атак на інші системи, зокрема на внутрішні ресурси мережі та сервери компанії
5	**Сайти соцмереж як засіб крадіжки інформації та розповсюдження злоякісних програм**	Зловмисники використовують популярні соцмережі типу FaseBook, LinkedIn, Twitter для збору критичної інформації про діяльність компанії. Більш того, вони розповсюджують експлойти та скрипти для перехоплення браузера через сайти соцмереж
6	**Масові SQL-ін'єкції**	Протягом багатьох років атаки, що використовували SQL-ін'єкції, зосереджувались на крадіжці конфіденційних даних в окремих web-додатках та базах даних (БД). Останнім часом зловмисники розширили спектр використання SQL-ін'єкцій за допомогою автоматизованого ПЗ, яке дозволяє одночасно атакувати тисячі web-додатків. Замість викрадення даних сучасні атаки на основі SQL-ін'єкцій найчастіше намагаються змінити вміст БД, які будуть відображатися на web-сайтах, спотворити web-контент, розмістити на сайті злоякісні скрипти для атаки на браузери користувачів, а також інші експлойти, які використовують уразливості ПЗ на боці користувача. Усі ці дії, як правило, виконують для встановлення на ПЕОМ користувача злоякісного ПЗ

7	**Атаки на адміністративні інтерфейси**	Більшість великих корпоративних систем, таких як комплекси забезпечення безпеки кінцевих точок, засобів мережного адміністрування, ERP-системи тощо налаштовуються через адміністративні web-інтерфейси. Виконуючи атаки перехоплення браузера або експлуатуючи уразливості ПЗ на боці користувача, зловмисники все частіше полюють на адміністративні інтерфейси, які можуть забезпечити контроль відповідної системи або інфраструктури
8	**Атаки «передача хешу» (pass the hash) у Windows інтегровано в пакети для проведення атак**	Зловмисники замість паролів використовують техніку «передачі хешу» відносно Windows-систем, аби отримати доступ до корпоративного домена. Нині ці можливості включено в широко використовувані інструменти комп'ютерних атак, такі як Metasploit та Nmap, що значно спрощує проведення широкомасштабних атак із використанням відповідної техніки
9	**Зламування обладнання**	Оскільки захист ПЗ останнім часом значно поліпшився й водночас набули значного поширення «розумні» пристрої (*embedder device*), такі як стільникові телефони, безпроводові маршрутизатори тощо, то кіберзлочинці частіше почали зламувати обладнання. Через перехоплення інформації, що передається шинами даних (*bus sniffing*), зламування прошивок, змінювання системного часу (*clock glitching*) та інші витончені атаки на обладнання зловмисники обминають захисні механізми й отримують ключі шифрування, що допомагає їм при подальших атаках на інфраструктуру компанії-жертви


МЕТА АТАКИ
Інформаційна складова
Соціальна складова
Порушення доступності інформаційних ресурсів
Із метою проникнення (злому) системи:
– отримання доступу;
– виконання засобів управління;
– копіювання (модифікація) ІР
Із метою блокування системи захисту:
– знищення засобів захисту;
– подавлення засобів захисту
Порушення конфіденційності інформації
Із метою розвідки:
– сканування;
– аналіз мережного трафіку;
– запит на обслуговування тощо
Із метою розголошення
Порушення цілісності інформації
Із метою впровадження та отримання контролю
Із метою порушення функціонування системи
ОБ'ЄКТ АТАКИ:
акаунт, процес, інформація (файл), сервіс, хост, мережа (LAN, MAN, WAN), мережна служба тощо
Тип системи
– керуючі системи;
– сховища даних;
– фінансові установи;
– телекомунікації;
– військові частини тощо
Фізичні носії
– обчислювальний пристрій;
– комп'ютер;
– кластер;
– локальна мережа;
– розподілена система (конгломерат мереж, комунікаційне обладнання)
Тип і ступінь захисту
– брандмауер;
– IDS;
– антивірус;
– засоби перевірки та верифікації програмно-апаратного забезпечення (типи, характеристики, налашування)
Зовнішні комунікації
Тип зовнішніх каналів зв'язку
Характер інформаційного обміну
Спосіб контролю та захисту зовнішніх каналів
Зв'язок з іншими критичними об'єктами
СУБ'ЄКТ АТАКИ:
користувач, процес (програма), компонент, хост, ID тощо
Розташування
– локальне;
– внутрішньосегментне;
– зовнішнє;
– мішане
Початкові привілеї та права доступу
Кількість атакувальників
Наявність координації між ними
ТИП ТА ВЛАСТИВОСТІ АТАКИ
Типи атак:
– сканування хосту (групи хостів);
– сканування портів хосту;
– підбір пароля;
– установлення прослуховувального пристрою (sniffer);
– використання програмних уразливостей (exploit);
– використання уразливостей БД (SQL-injection);
– методи соціальної інженерії;
– запуск (використання) засобів віддаленого управління (backdoors);
– дезінформація (poisoning);
– підміна ідентифікатора (spoofing);
– перехоплення сесії (session hijacking);
– використання web-уразливостей тощо.
Властивості атак:
– темпоритмічність;
– спостережуваність;
– відстежуваність тощо

Основні типи кібернетичних атак згідно з класифікацією П. Неймана

Тип атак		Спосіб здійснення	Результат
Зовнішні		Візуальне спостереження	Спостереження за клавіатурою або монітором
		Омана	Уведення в оману операторів або користувачів
		Вилучення сміття	Вилучення інформації зі сміттєвих корзин
Апаратні		Логічне відновлення	Вилучення інформації з викрадених носіїв
		Прослуховування	Перехоплення даних
		Втручання	—
		Фізична атака	Руйнування або ушкодження обладнання, джерел живлення
		Фізичне видалення	Вилучення обладнання або сховищ даних
Маскувальні		Імітування	Використання хибних ідентифікаторів
		Узурпація ліній зв'язку або хостів	—
		Атака з підміною параметрів	—
		Заплутування мереж	Маскування фізичного місця розташування або маршруту
Зловмисні програмні коди		Троянські коні	Впровадження зловмисного коду
		Логічні бомби	Різновид троянських коней
		Черв'яки	Заволодіння розподіленими ресурсами
		Віруси	Прикріплення до програм та розповсюдження
		Обхід	Обхід механізмів безпеки
		Експлуатація уразливостей	—
		Злам паролів	—
Зловживання	активне	Інкрементальні атаки	Поступова ескалація привілеїв, повільне просування до мети
		Відмова в обслуговуванні	Здійснення масованих атак
	пасивне	Огляд	Випадковий або вибірковий пошук
		Збір та виведення даних	Використання баз даних та аналіз трафіку
		Приховані канали	Використання прихованих каналів або інших способів витоку інформації
	інертне	—	—
	побічне	—	—

Особливості найпоширеніших кібератак

№ з/п	Тип атаки	Опис впливу
1	Denial of service	Атака з поодинокого джерела. Блокує авторизованим користувачам доступ до того чи іншого комп'ютера-жертви через «переповнення» легального трафіку зовнішніми повідомленнями
2	Distributed denial of service	Скоординована атака відразу з багатьох комп'ютерів. Для її організації комп'ютери, що беруть у ній участь, часто попередньо заражаються спеціальними програмами — черв'яками
3	Exploit tools	Привселюдно доступні засоби проникнення в системи різного рівня складності з метою пошуку в тій чи іншій кіберсистемі уразливих місць і одержання доступу до комп'ютера-жертви
4	Logic bombs	Форма саботажу, коли програміст уводить спеціально сконструйований код, що викликає деструктивну роботу виконуваної програми, зокрема її повне припинення
5	Phishing	Створення та подальше використання спеціальних електронних повідомлень і web-сайтів, подібних до легальних і добре відомих користувачам. Має на меті дезорієнтувати користувачів, спонукати їх до розкриття своїх персональних даних
6	Sniffer	Програма, що перехоплює та фільтрує інформаційний трафік, вишукуючи в ньому спеціальну інформацію про користувача, наприклад передані паролі
7	Trojan horse	Комп'ютерна програма, що містить неявні шкідливі коди. Трояни, як правило, маскуються під звичайні програми, якими користувач зазвичай послуговується
8	Virus	Програма, що інфікує комп'ютерні файли включенням до них спеціальних команд. Ці команди виконуються, як правило, при завантаженні інфікованого файла в оперативну пам'ять комп'ютера. На відміну від комп'ютерних черв'яків, розмноження вірусів вимагає втручання (хоча найчастіше й неусвідомленого) людини-користувача
9	Vishing	Різновид фішингу, який використовує дешеві інтернет-технології для передавання звукових (у тому числі голосових) файлів. Дає змогу шахраям створювати власні телефонні «кол-центри» і звідти (від імені легальних користувачів) надсилати потенційним жертвам голосові або електронні повідомлення з проханням виконати певні деструктивні дії
10	War driving	Метод отримання несанкціонованого доступу до комп'ютерних мереж, що використовують ноутбуки. Для проникнення в мережу Інтернет застосовує антени та бездротові мережні адаптери, що містять контрольовані локатори
11	Worm	Незалежні комп'ютерні програми, поширювані в мережі Інтернет за допомогою копіювання самих себе з одного комп'ютера в інший. На відміну від комп'ютерних вірусів, черв'яки не вимагають для свого розмноження втручання людини
12	Zero-day exploit	Спосіб запобігання кіберзлочину. Загроза реалізується того самого дня, коли громадськість дізнається про наявність у системі безпеки уразливих місць

Дякую за увагу!