УДК 004.725.5
DOI: 10.31673/2409-7292.2021.046469

Котенко А.М., Ясько М.С.

ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Описано шляхи несанкціонованого отримання інформації у комп'ютерних мережах та загрози кібернетичній безпеці у них. Показано, що для забезпечення надійного захисту інформації у комп'ютерних системах необхідно окрім забезпечення безпеки інформації у мережі забезпечити безпеку фізичного середовища комп'ютерній мережі. Для забезпечення безпеки інформації у комп'ютерній мережі пропонується використовувати рекомендації стандарту Х.805.

Ключові слова: кібербезпека, компьютерна мережа, загрози інформації, інформація з обмеженим доступом, об'єкт інформаційної діяльності, конфіденційність, матеріально-речовий канал витоку інформації.

Вступ

Наш час характеризується бурхливим розвитком інформаційних технологій. Інформаційні технології застосовуються майже у всіх сферах людської діяльності. Технічною підтримкою інформаційних технологій є комп'ютерні системи і невідмінна їх складова - комп'ютерні мережі призначені для інформаційного обміну. Необхідність використання комп'ютерних мереж породжує ряд питань обумовлених особливостями їх функціонування. Одне з цих питань – інформаційна безпека у мережі. При цьому питання інформаційної безпеки розглядається не тільки в площині забезпечення цілісності та доступності інформації у мережі, а й у деяких випадках забезпечення конфіденційності інформації.

Основна частина.

Можливості порушників інформаційної безпеки у локальних компьютерних мережах стають дедалі більш досконалішими. Як свідчить статистика злочинних дій, шляхів для несанкціонованого доступу (НСД) до інформації у мережі існує багато. Найбільш поширені шляхи НСД до інформації у комп'ютерній мережі наведені на рис. 1 [1].

Рис. 1. Найбільш поширені шляхи НСД до інформації у комп'ютерній мережі

Загрози інформаційній безпеці у комп'ютерних мережах на ОІД не обмежуються представленими на рис. 1. Не слід забувати також про різного роду закладні пристрої,

перехоплення побічних електромагнітних випромінювань основних технічних засобів, крадіжку матеріальних носіїв таємної інформації. Також часто застосовуються приховування під зареєстрованого користувача, методи подолання парольного захисту, нав'язування небезпечної передачі; неправильно настроєна система контролю доступу до певних баз даних, збереження логіну та інших відомостей у загальнодоступному місці, використання застарілого програмного забезпечення та ін.

Методику протидії негативним наслідкам небезпекам у комп'ютерній мережі можна представити наступним чином:

ідентифікація загроз безпеці інформації у обчислювальній системі;

визначення шляхів захисту від цих загроз;

вибір технології захисту.

По класифікації загроз.

Опис загроз безпеці комп'ютерних мереж можливо здійснювати у наведеному нижче порядку.

За характером впливу:

а) пасивні;

б) активні.

Пасивний вплив на комп'ютерну мережу це такий, що впливає на роботу мережі не безпосередньо. Але він може порушувати її політику безпеки.

Активний вплив на комп'ютерну мережу безпосередньо впливає на роботу мережі і порушує політику безпеки в ній. Всі типи віддалених атак являються активними впливами. Характерною відмінністю активного впливу від пасивного - можливість виявлення, оскільки у його здійснення у системі відбуваються характерні зміни.

За метою впливу:

а) порушення конфіденційності інформації;

б) порушення цілісності інформації;

в) порушення доступності (працездатності) системи.

За умовою початку здійснення впливу

Віддалений вплив починає здійснюватись лише за визначених умов. Взагалі наявні три види таких умов:

а) атака після запиту від об'єкта, який атакується;

б) атака після здійснення очікуваної події на об'єкті, що атакується;

в) безперечна атака.

За наявності зворотного зв'язку з об'єктом, що атакується

а) із зворотним зв'язком;

б) без зворотного зв'язку або односпрямована атака.

Відрізняються наявністю або відсутністю зворотного зв'язку між зловмисником та об'єктом впливу. Це необхідно для адекватного реагування при зміні ситуації.

За розташуванням суб'єкта атаки відносно об'єкта, що атакується

а) внутрішньосегментне;

б) міжсегментне.

Під сегментом мається на увазі сегмент мережі як фізичне об'єднання хостів.

Для здійснення віддаленого впливу необхідно знати як один до одного розташовані суб'єкт і об'єкт атаки. В одному або в різних сегментах вони знаходяться.

Міжсегментну дію здійснити набагато важче, ніж внутрішньо сегментну, оскільки об'єкт і суб'єкт атаки перебувають на великий відстані один від одного, а це суттєво ускладнює можливості по безпосередньому виявленню атакуючого та своєчасній реакції на атаку.

За рівнем еталонної моделі ISO/OSI, на якому здійснюється вплив:

а) фізичний;

б) канальний;

в) мережевий;

г) транспортний;
д) сеансовий;
е) представницький;
ж) прикладний.

Таблиця 1

Шляхи реалізації загроз мережі

Об'єкти впливу	**Втрата конфіденційності інформації**	**Втрата цілісності інформації**	**Втрата доступності**
Апаратні засоби	НСД – використання ресурсів; крадіжка носіїв	НСД – використання ресурсів; модифікація, зміна режимів	НСД – вивод з ладу; руйнування
Програмне забезпечення	НСД – копіювання; крадіжка; перехоплення	НСД, застосування "троянського коня", "вірусів", "хробаків"	НСД – спотворення; видалення; підміна
Дані	НСД – копіювання; крадіжка; перехоплення	НСД – спотворення; модифікація	НСД – спотворення; видалення; підміна
Персонал	Розголошення; передача відомостей про захист; халатність	"Маскарад"; підкуп персоналу	Уход з робочого місця; фізичне усунення

Для забезпечення безпеки комп'ютерної мережі ОІД пропонується застосовувати комплексний підхід. Його сутність полягатиме у застосуванні засобів захисту інформації безпосередньо у мережі та засобів фізичного захисту ОІД.

Для того щоб забезпечити безпеку інформації у мережі

Потрібно проаналізувати локальну мережу, що до неї підключено, яке програмне забезпечення використовується. Це необхідно для чіткого розуміння що необхідно захистити. І це допоможе переконатися в тому, що буде забезпечуватися потрібний рівень інформаційної безпеки. Також необхідно знати що за інформація підлягає захисту, де в автоматизованій системі зберігається найважливіша інформація, ступінь надійності паролів що використовують системні адміністратори і користувачі. Як відомо [2] окрім згаданих суб'єктивних загроз інформації ще є об'єктивні, тобто такі що не залежать від людського чинника (природного характеру).

Проаналізувавши усі ці чинники можна зробити наступні висновки. Захист інформації у комп'ютерній мережі ОІД треба розглядати у двох напрямах: власне забезпечення інформаційної безпеки від НСД у інформаційно-телекомунікаційній системі (ІТС) і забезпечення безпеки фізичного середовища функціонування ІТС.

Для забезпечення безпеки фізичного середовища необхідно застосовувати наступні технічні системи: технічна система охорони, система контролю та управління доступом на ОІД, система відео спостереження. Є ще не технічні засоби, як то організаційні заходи.

Спектр засобів захисту від НСД великий. Проте потрібен системний підхід до цього питання. Перспективним бачиться, під час створення системи захисту, керування стандартом Х.805. Цей документ розроблений на заміну застарілому стандарту Х.800. Х.805 визначає вимоги до архітектури безпеки для систем, що забезпечують зв'язок між кінцевими пристроями. Цей документ торкається трьох питань, які вище вже згадувались:

1) Який захист потрібен і від яких загроз.
2) Які типи мережевого обладнання та їх сукупність повинні бути захищені.
3) Які типи мережевої активності повинні бути захищені.

Ці питання відносяться до трьох компонентів архітектури: виміру захисту (комплекс мір захисту призначених для реалізації конкретного аспекту мережевого захисту), рівні захисту і площини захисту.

Такі принципи задаються архітектурою захисту та можуть застосовуватися до широкого кола мереж незалежно незалежно від їх технології. Згідно X.805 пропонується застосовувати наступний комплекс мір захисту:

1) управління доступом;
2) аутентифікація;
3) збереженість інформації;
4) конфіденційність інформації;
5) безпека зв'язку;
6) цілісність інформації;
7) доступність;
8) секретністть.

Кожен з цих критеріїв має своє визначення [3].

Для забезпечення надійного захисту виміри захисту, описані вище, повинні застосовуватися до ієрархії мережного обладнання та груп засобів, що визначаються як рівні захисту. У X.805 визначаються три рівні захисту:

рівень захисту інфраструктури;
рівень захисту послуг; і
рівень захисту програм.

Ці рівні у комплексі забезпечують мережеві рішення.

На рис. 1 показано, як вимірювання захисту застосовуються до рівнів захисту для зменшення вразливості, яка існує у кожному рівні, і таким чином пом'якшують наслідки атак на захист.

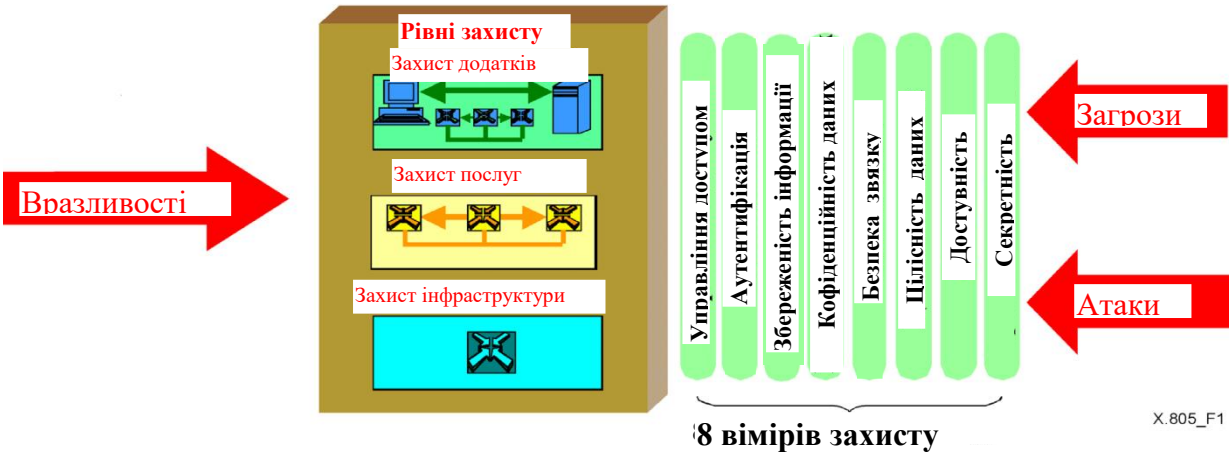

Рис. 1. Застосування вимірювань захисту до рівнів захисту

Площина захисту управління [3].

Площина захисту – це конкретний тип мережевої операції яка захищена вимірами захисту. У X.805 визначається три площини захисту для представлення трьох типів захищених мережевих операцій. Визначаються наступні площини захисту:

1) площина управління;
2) площина контролю;
3) площина кінцевого користувача.

Вони відносяться до конкретних потреб у захисті, пов'язаних з управлінням мережею, контролем за мережею або сигнальними операціями, а також операціями кінцевого користувача відповідно.

Мережі необхідно проектувати так, щоб події в одній площині захисту були повністю ізольовані з інших площин захисту. Наприклад, приплив пошуків DNS у площині кінцевого користувача, ініційований запитами кінцевого користувача, не повинен блокувати інтерфейс OAM&P у площині управління, який дозволить адміністратору вирішити цю проблему.

Перетин кожного рівня захисту з кожною площиною захисту представляє собою область захисту, в якій вимірювання захисту застосовуються для протидії загрозам. У таблиці 2 показано схематичне співвідношення вимірювань захисту до загроз безпеці.

Таблиця 2

Співвідношення вимірювань захисту до загроз безпеці

Вимір захисту	**Загроза безпеці**				
	Знищення інформації або інших ресурсів	**Спотворення або зміна інформації**	**Крадіжка, видалення або втрата інформації інших ресурсів**	**Розкриття інформації**	**Переривання обслуговування**
Управління доступом	ТАК	ТАК	ТАК	ТАК	
Аутентифікація			ТАК	ТАК	
Збереженність інформації	ТАК	ТАК	ТАК	ТАК	ТАК
Конфіденційність даних			ТАК	ТАК	
Безпека зв'язку			ТАК	ТАК	
Цілісність даних	ТАК	ТАК			
Доступність	ТАК				ТАК
Секретність				ТАК	

Висновок.

У статті зроблено огляд поширених загроз інформаційній безпеці у комп'ютерних мережах. Зроблено висновок, що для забезпечення безпеки інформації потрібні чіткі розуміння що за інформація підлягає захисту, де в автоматизованій системі зберігається найважливіша інформація, ступінь надійності паролів що використовують системні адміністратори і користувачі розуміння і т. ін. Для забезпечення надійної безпеки інформації у локальній мережі необхідне комплексне використання апаратних, програмних та фізичних засобів.

Перелік посилань

1. Бондарев В.В. Введення в інформаційну безпеку автоматизованих систем. / – М: МГТУ ім. Баумана, 2016. –252 с.

2. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

3. https://lib.itsec.ru/articles2/networks/x_805_vsestoronniy_podhod

Надійшла: 17.11.2021 Рецензент: д.т.н., професор Вишнівський В.В.