УДК 004.638.2

Хохлачова Ю.Є.

УРАЗЛИВІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ

У даній статті проведені класифікація та аналіз загроз безпеці інформаційних систем. Також розглянуті основні уразливості систем.

Ключові слова: інформаційна система, безпека інформаційної системи, уразливість інформаційної системи, загрози безпеці інформаційної системи.

Вступ. У процесі функціонування інформаційних систем (ІС) відбуваються різноманітні події, які змінюють їх стани. Дані події можуть бути представлені з точки зору безпеки за допомогою двох складових: дії та адресату.

Під дією будемо розуміти кроки, які здійснюються суб'єктами системи для досягнення деякого результату, а до поняття дії віднесемо: читання, копіювання, модифікацію, видалення тощо.

Поняття адресат визначає логічний або фізичний об'єкт системи.

Подія - це мінімальна одиниця, якою оперує сучасна теорія захисту. Прикладом події може бути несанкціонований доступ до файлів зловмисником. На основі роздумів, також можливий розгляд третього параметру – джерела події, яке виноситься за межі опису моделі події безпеки, так як цей параметр стає значним тільки у випадку реального здійснення атаки та нанесення збитку. При цьому події вважаються рядовими, якщо вони виконуються у відповідності з політикою безпеки [1]. Як тільки події порушують політику безпеки, вони вже кваліфікуються як елемент атаки на ІС.

Для того щоб виявити в інформаційному просторі та просторі, що контролюється, порушення політики безпеки, необхідно визначити ознаки їх ідентифікації та відмінності від рядових подій безпеки. Таким чином, актуальність визначення уразливості ІС у теперішній час дуже висока та створення методики її оцінки представляє собою складну задачу.

Мета роботи. Метою роботи є класифікація та аналіз загроз безпеці ІС.

Основна частина. Для визначення загроз безпеці ІС сформулюємо ознаки атак на ІС. До них можна віднести наступні:

- повтор визначених подій;
- аномалії мережевого трафіку;
- непередбачені атрибути;
- непояснені проблеми;
- загрози ІС.

Розглянемо більш детально усі перелічені ознаки.

До повтору визначених подій можна віднести, коли зловмисник, який не отримав несанкціонований доступ до інформації з першої спроби, намагається це зробити вдруге, втретє тощо. Алгоритми визначення несанкціонованої діяльності повинні визначати такі повторні спроби та вирішувати: по завершенні деяких спроб можна зробити висновок про наявність атаки. Необхідно відмітити, що якщо зловмисник знає наперед шляхи доступу до інформаційних ресурсів та не здійснив ніяких помилок, то виявити такий несанкціонований доступ практично неможливо.

До аномалії мережевого трафіку відносяться будь-які відхилення показників ІС від еталонних значень. Такими показниками можуть бути: коефіцієнт завантаження, типовий розмір інформаційного пакету, середнє число фрагментованих пакетів тощо. Однак слід мати на увазі, що будь-яке відхилення може характеризувати собою як атаку, так і просто проблему, що виникла у мережі ІС.

Запити будь-якої системи, мережі або користувача характеризуються деякими атрибутами, які описують так званий профіль системи захисту, мережі або користувача. Такі профілі застосовуються для нагляду та аналізу об'єкту, що контролюється [2].

До непередбачених атрибутів відносяться:

- модифікація часу та дати, оскільки час та дата – це характерні атрибути, які використовуються при виявленні порушень політики безпеки;
- аномалії у роботі системних ресурсів.

Характеристики багатьох системних ресурсів можуть виступати індикатором такої атаки.

З інших характеристик інформаційних ресурсів, які часто використовуються для ідентифікації атаки, можна назвати інтенсивне звернення до оперативної та дискової пам'яті, файлам, телекомунікаційним портам тощо.

Несподівані запити серверів та послуг.

Цей спосіб ідентифікації атаки полягає в аналізі тих серверів та послуг, які найбільш часто запитуються суб'єктом у своїй повсякденній діяльності.

Аномалії у роботі профілів системи.

Аналіз профілів системи сам по собі включає аналіз запитів сервісів, послуг або системних ресурсів. Він також доповнюється і новими параметрами, які враховують специфіку конкретного користувача, процесу або ІС. Відхилення роботи параметрів елементів системи, що контролюється, за час поточного сеансу від параметрів, які задані в профілі, можуть свідчити про його аномальну поведінку.

Кожна проблема, яка виникає в ІС і яку неможливо пояснити, у будь-якому випадку потребує проведення спеціального розслідування. Якщо з'ясовується, що дана проблема не обумовлена атакою на ІС, то слід мати на увазі, що вже сам факт виявлення проблеми буде у подальшому позитивно впливати на функціонування та працездатність цієї ІС. До проблем, які неможливо пояснити, можна віднести:

- проблеми, пов'язані з системними ресурсами, коли раптова недостача дискового простору може свідчити про появу у системі "бомби", що являє собою упакований файл невеликого розміру, який при розархівуванні розкривається у файл розміром в сотні мегабайтів;
- проблеми, пов'язані з продуктивністю системи, коли віддалені за часом відповіді від сервера застосовувань можуть маскувати атаку типу "відмова в обслуговуванні";
- поведінка користувача, яку неможливо пояснити, коли несподіване звернення до ресурсу, що раніше не мав запитів, може бути викликано тим, що зловмисник перехопив або підібрав пароль авторизованого користувача та намагається у рамках його повноважень отримати доступ до інформаційних ресурсів ІС.

Під загрозою ІС розуміється потенційно можлива подія, дія, процес або явище, яке може викликати нанесення збитку інформаційним ресурсам ІС. Так безпеці ІС можуть загрожувати:

- стихійні лиха та аварії;
- збої та відмови обладнання;
- помилки проектування та розробки компонентів ІС;
- помилки експлуатації;
- навмисні дії порушників та зловмисників.

Джерела загроз по відношенню до ІС можуть бути зовнішніми та внутрішніми. Вся множина потенційних загроз за природою їх виникнення поділяється на два класи: природні (об'єктивні) та штучні (суб'єктивні).

Природні загрози - це загрози, викликані впливами на ІС та її елементи в результаті об'єктивних фізичних процесів або стихійних природних явищ, які не залежать від користувача.

До штучних загроз ІС, які обумовлені діяльністю людини, відносяться:

- непередбачені (ненавмисні, випадкові) загрози, викликані помилками в проектуванні ІС та її елементів, помилками в програмному забезпеченні, в діях персоналу тощо;
- умисні (навмисні) загрози, пов'язані з корисливими спрямуваннями людей (зловмисників).

До основних ненавмисних штучних загроз безпеці ІС (діям, що здійснюються людьми випадково, за незнанням, неуважністю або халатністю, з цікавості, але без лихого наміру) можна віднести:

- ненавмисні дії, що приводять до часткової або повної відмови системи або зруйнування апаратних, програмних, інформаційних ресурсів системи (ненавмисне псування обладнання, видалення, викривлення файлів з важливою інформацією або програм, у тому числі системних тощо), а також неправомірне включення обладнання або зміна режимів роботи пристроїв та програм;
- ненавмисне псування носіїв інформації;
- запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання або зациклювання) або здійснювати незворотні зміни в системі (форматування або реструктуризація носіїв інформації, видалення даних тощо);
- нелегальне впровадження та використання неврахованих програм (ігрових, навчальних, технологічних та ін., які не є необхідними для виконання порушником своїх службових обов'язків) з наступним необґрунтованим розкодуванням ресурсів (завантаження процесора, захват оперативної пам'яті та пам'яті на зовнішніх носіях);
- зараження ІС вірусами;
- необачні дії, що приводять до розголошення конфіденційної інформації або роблять цю інформацію загальнодоступною;
- розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, pin-кодів, перепусток тощо);
- проектування архітектури системи, технології обробки даних та розробка прикладних програм з можливостями, що представляють небезпеку для працездатності системи та безпеки інформації;
- ігнорування організаційних обмежень (встановлених правил) при роботі в системі;
- вхід в систему в обхід засобів захисту (завантаження сторонньої операційної системи зі змінних магнітних носіїв тощо);
- пересилка інформації за помилковим адресом абонента;
- ненавмисне пошкодження каналів зв'язку;
- некомпетентне використання, настройка або неправомірне відключення засобів захисту персоналом служби безпеки;
- ввід помилкових даних (синтаксичні та логічні помилки – набір невірного сполучення алфавітно-цифрових символів у коді, номері, адресі, прізвищі тощо).

Основні можливі навмисні загрози безпеці ІС, що приводять до порушення її працездатності, виводу системи зі строю, проникненню в систему та організації несанкціонованого доступу до інформації, що обробляється в ІС, представляються як:

- фізичне руйнування системи або вивід зі строю всіх або окремих найбільш важливих компонентів ІС;
- відключення або вивід зі строю підсистем забезпечення функціонування ІС;
- дії по дезорганізації функціонування системи;
- впровадження агентів в число персоналу системи;
- вербування персоналу або окремих користувачів, що мають певні повноваження;
- застосування радіоелектронних підслуховуючих систем, дистанційна фото- та відеозйомка тощо;
- перехват побічних електромагнітних, акустичних та інших випромінювань пристроїв та ліній зв'язку, а також наводок активних випромінювань на допоміжні технічні засоби, що безпосередньо не приймають участь в обробці інформації;
- перехват інформації, що передається по каналах зв'язку, та їх аналіз з метою з'ясування протоколів обміну, правил входження у канали зв'язку, авторизації користувача для наступних спроб їх імітації для проникнення в систему;
- розкрадання носіїв інформації різних типів;

- несанкціоноване копіювання носіїв інформації;
- розкрадання виробничих відходів;
- читання залишкової інформації з оперативної пам'яті та з зовнішніх запам'ятовуючих пристроїв;
- читання інформації з областей оперативної пам'яті, що використовуються операційною системою (у тому числі й підсистемою захисту) або іншими користувачами, в асинхронному режимі, використовуючи недоліки мультизадачних операційних систем та систем програмування;
- незаконне отримання паролів та інших реквізитів розмежування доступу з послідуючим маскуванням під зареєстрованого користувача;
- несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції у мережі, фізична адреса, адреса в системі зв'язку, апаратний блок кодування тощо;
- розкривання кодів та шифрів крипто захисту інформації;
- впровадження апаратних спец укладань, програмних закладок та вірусів, тобто таких ділянок програм, які не потрібні для здійснення заявлених функцій, але дозволяють подолати систему захисту;
- незаконне підключення до мереж зв'язку для роботи "між строк" з використанням пауз в діях законного користувача від його імені з подальшим вводом хибних повідомлень або модифікацією повідомлень, що передаються.

Як правило для досягнення поставленої мети зловмисник реалізує не одну, а деяку сукупність з перелічених загроз, використовуючи так звані уразливості ІС. До уразливостей ІС можна віднести будь-які характеристики ІС, використовуючи які зловмисник (порушник) може досягти реалізації конкретних загроз. Уразливості ІС можуть класифікуватися наступним чином:

- уразливості, які реалізовані або створені розробником програмного або апаратного забезпечення;
- уразливості, які добавлені адміністратором в процесі керування компонентами системи;
- уразливості, які внесені користувачем в процесі експлуатації системи.

Уразливості, створені розробником, містять помилки, представлені поновлення операційної системи, уразливі сервіси та незахищені конфігурації за замовчуванням. Уразливості, пов'язані з діями адміністратора, представляються собою доступні, але не вірно використані настройки та параметри інформаційної системи, що не відповідають політиці безпеки. Уразливості, що відносяться до діяльності користувача, включають відхилення від приписань прийнятої політики безпеки.

Класифікація уразливостей, що відображує етапи життєвого циклу ІС, приведена в таблиці 1.

Життєвий цикл ІС — Таблиця 1

Етапи життєвого циклу ІС	Категорії вразливостей ІС
Проектування ІС	Уразливості проектування
Реалізація ІС	Уразливості реалізації
Експлуатація ІС	Уразливості конфігурації

Розглянемо більш детально уразливості ІС.

Уразливості проектування найбільш небезпечний тип уразливостей, оскільки виявляється та усувається дуже складно. У цьому випадку уразливість притаманна проекту або алгоритму та, відповідно, навіть цілковита його реалізація не позбавить від слабкості, яка закладена у ньому.

Смисл уразливостей реалізації полягає в появі помилки на етапі реалізації в програмному або апаратному забезпеченні коректного з точки зору безпеки проекту або алгоритму.

Виявляються та усуваються такого роду уразливості відносно легко. Якщо немає вихідного коду програмного забезпечення, в якому виявлена уразливість, то усунення останньої полягає або в поновленні версії цього програмного забезпечення, або в повній його заміні, або у відмові від нього.

До уразливостей конфігурації відносяться помилки конфігурації програмного або апаратного забезпечення. Поряд з уразливостями реалізації це самий розповсюджений вид уразливостей.

Можливості по виявленню та усуненню уразливостей в ІС відображені в таблиці 2.

Можливості по виявленню та усуненню уразливостей в ІС Таблиця 2.

Категорія уразливостей	Виявлення	Усунення
Уразливості проектування	Складно та довго	Складно та довго, іноді неможливо
Уразливості реалізації	Відносно складно та довго	Легко, але відносно довго
Уразливості конфігурації	Легко та швидко	Легко та швидко

Висновки. Таким чином, актуальність визначення уразливості ІС у теперішній час дуже висока та створення методики її оцінки представляє собою складну задачу. У статті було сформулювано ознаки атак на ІС для визначення загроз безпеці ІС та детально розглянуто всі перелічені ознаки. Приведено та детально розглянуто атрибути, які описують так званий профіль системи захисту, мережі або користувача. Приведені визначення основним поняттям, які стосуються ІС.

Відображені можливості по виявленню та усуненню уразливостей в ІС.

Проведені детальна класифікація та аналіз загроз безпеці інформаційних систем.

Також розглянуті та проаналізовані основні уразливості систем.

ЛІТЕРАТУРА

1. Голубенко О.Л. Політика інформаційної безпеки / Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є. – Луганськ: Вид. СНУ ім. В. Даля, 2009. – 300 с.

2. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу.

3. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

Надійшла: 08.09.2012р.

Рецензент: д.т.н., проф. Дівізінюк М.М.