УДК 004.056.5

Я. В. Корпань
Черкаський державний технологічний університет
бул. Шевченка, 460, 18006 Черкаси, Україна

Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних

Наведено визначення основних термінів, які стосуються питань інформаційної безпеки, перераховано умови безпеки комп'ютерної системи, надано загальну класифікацію загроз інформаційної безпеки. В представленій класифікації загрози інформаційній безпеці розділено на три категорії: загрози, що характерні для програмного забезпечення; загрози, які спрямовано на комп'ютерну мережу; загрози, що стосуються апаратної частини інформаційної системи. Загрози, що відносяться до кожної із перерахованих категорій, розділено на групи за характерними ознаками, визначено їхній вплив на систему та методи захисту.

Ключові слова: *безпека інформації, цілісність, доступність, конфіденційність, загроза атаки.*

Вступ

На сьогоднішній день використання інформаційних технологій в усіх сферах людської діяльності робить закономірною та актуальною проблему захисту інформації, проблему забезпечення інформаційної безпеки.

З будь-яким об'єктом інформаційної безпеки пов'язано існування тієї чи іншої загрози, під якою розуміється сукупність умов і факторів, що виникають у процесі взаємодії даного об'єкта з іншими, або складових його компонентів між собою та здатних негативно на нього впливати [1, 2]. Загрози можуть бути як випадкові, так і навмисні. Найбільш небезпечними, з точки зору наслідків впливу, є навмисні загрози.

Відомо, що віддалена обробка різних за своєю природою даних в інформаційній системі заснована на використанні комп'ютерів, архітектура яких включає апаратну, програмну та комунікаційну складові. У зв'язку з цим, одним із найбільш актуальних питань безперебійного функціонування комп'ютерної системи, є питання забезпечення безпеки даних цієї системи.

Мета та об'єкт дослідження

Сучасні потреби інформатизації суспільства вимагають від комп'ютерних систем (незалежно від їхньої масштабності) високої стійкості до зовнішніх і внутрішніх загроз, доступності, цілісності та конфіденційності інформації (яка зберігається, обробляється, передається каналами зв'язку). Тому метою даної роботи є класифікація та порівняльний аналіз загроз безпеці інформації і методів протидії, а також систем виявлення загроз на початковому етапі атаки.

Для досягнення поставленої мети вирішувалися наступні задачі:

— аналіз основних властивостей загроз;

— визначення результатів впливу загроз;

— системний аналіз методів захисту від загроз;

— дослідження систем виявлення вторгнень на початкових етапах загроз.

Об'єкт дослідження — процеси обробки та захисту інформації у комп'ютерних системах.

Класифікація загроз безпеці інформації у комп`ютерних системах і мережах

Прийнято вважати [1, 3, 4], що незалежно від конкретних видів загроз або їхньої проблемно-орієнтованої класифікації, комп'ютерна система задовольняє вимогам безперебійної експлуатації, якщо забезпечуються наступні важливі властивості інформації та систем її обробки: доступність, цілісність і конфіденційність. Тобто інформаційна безпека комп'ютерної системи забезпечується у випадку, якщо для інформаційних ресурсів у системі підтримуються певні рівні:

— доступності (можливості за малий час отримати необхідну інформацію);

— цілісності (неможливості несанкціонованої або випадкової модифікації інформації);

— конфіденційності (неможливості несанкціонованого отримання інформації).

З точки зору безпеки, розподілені системи характеризуються перш за все наявністю віддалених атак, оскільки компоненти розподілених систем зазвичай використовують відкриті канали передачі даних, тому зловмисник може проводити не лише пасивне відстеження інформації, яка передається, але й активно впливати. І якщо активний вплив на трафік можна зафіксувати, то пасивний вплив практично не піддається виявленню.

У таблиці представлена класифікація основних загроз атаки на комп'ютерні системи, які характерні для їхнього програмного забезпечення, системи комунікацій і апаратної частини [1–7].

Складність розпізнання факту проведення віддаленої атаки виводить цю загрозу на перше місце за ступенем небезпеки. Проводячи аналіз характерних особливостей загроз (див. таблицю), їхній вплив на інформаційну систему, слід відзначити, що основний внесок у запобігання порушення доступності, цілісності та конфіденційності інформації відіграють системи виявлення вторгнень.

Класифікація загроз в інформаційних системах

№№	Загрози безпеці інформації	Основні властивості	Результати атаки	Методи захисту
		Загрози для програмного забезпечення		
1.	Загрози, які спрямовані на інформацію, що знаходиться в пам'яті.			
1.1.	Переповнення буфера [5]	Переповнення буфера у зв'язку з неправильною роботою з даними, отриманими ззовні, та з пам'яттю, за відсутності жорсткого захисту з боку підсистеми програмування або операційної системи	Порушення умов цілісності, доступності, конфіденційності інформації	Використання спеціальних «безпечних» аналогів небезпечних функцій, заборона на виконання коду в області стека, перевірка меж змінних при кожному доступі до них та ін.
1.2.	«Висячі покажчики»	Представляє собою посилання на об'єкт, який був видалений	Порушення умов цілісності, доступності	Коректність видалення об'єктів посилання на них. Видалення «сміття»
2.	Коректність вхідних даних			
2.1.	Помилка форматуючого рядка [5]	Помилка в програмах, що використовують вивід за допомогою форматуючих рядків, формованих користувачем за відсутності перевірки введених параметрів	Відмова системи або її некоректна робота	Використання методики Майка Франтцена. Обмеження на довжину рядків, які використовуються [5]
2.2.	Маніпулювання метасимволами командної оболонки	Загроза характерна для систем, в яких не фільтровані вхідні дані служать параметрами команди, що призначена для виконання командною оболонкою	Залежить від можливостей командної оболонки	Використання функцій запуску програм, що дозволяють екранувати будь-які символи, які можуть бути використані для обману шелл-команд
2.3.	Проникнення в запити	Впровадження в запит довільних команд	Порушення умов конфіденційності і цілісності	Перевірка введеного запиту на коректність.
2.4.	Відкритий доступ до системних областей	Загроза характерна для систем з недостатнім контролем прав доступу до системних областей для додатків	Можливе порушення умов доступності, цілісності системного програмного забезпечення	Обмеження прав доступу до системних областей для додатків та програм, які встановлюються
2.5.	Маніпуляція з користувацькими скриптами	Системи, в яких є можливість установки на сервері скриптів користувача, що виконуються в клієнтських програмах інших користувачів, підключених до даного сервера	Залежить від можливостей, закладених в клієнтську програму	Заборона на спеціальні символи в полі введення даних

Продовження таблиці

3.	Нестійкі стани системи			
3.1.	Помилки часу перевірки до часу виконання	Характерні для систем, в яких перевірки контролю доступу не є атомарними з захищеними діями, що дозволяє обійти контроль доступу	Можливе порушення цілісності, доступності, конфіденційності (залежно від типу шкідливого коду)	Налагодження перевірок часу виконання машинного коду
3.2.	Гонки файлів	Характерні для багатозадачних систем, що виконують синхронізацію по створенню спеціальних файлів-семафорів у тимчасових каталогах	Порушення умов цілісності та доступності	Коректність функції ресурсу семафора
4.	Зміна рівня доступу			
4.1.	Ескалація привілеїв	Отримання доступу до ресурсів, зазвичай недоступних для користувача і додатків	Загроза умов цілісності, конфіденційності, доступності	Використання: вбудованої функції DEP; ASLR технології; антивірусних програм. Запуск додатків з мінімальними привілеями
4.2.	Атака за допомогою символічних посилань	Використання можливості звернення до файлу через символьне посилання	Порушення умов цілісності та доступності	Використання окремого каталогу для тимчасових файлів. Використання стандартних засобів для створення тимчасових файлів
	Загрози для системи комунікації			
5.	Можливість проведення атак на відмову в обслуговуванні			
5.1.	Проста атака на відмову (DoS-атака) [4, 5]	Системі, яка атакується, відправляються запити, число яких перевищує її здатність до обробки або є критичною для даної пропускної здатності каналу	Порушується умова доступності	Правильна конфігурація функцій антиспуфінга та анти-DoS на маршрутизаторах і міжмережних екранах. Обмеження об’єму трафіка
5.2.	Розподілена атака на відмову (DDoS-атака)	Цільова система атакується великою кількістю робочих станцій з використанням ботнету	Порушення умови доступності інформаційної системи	Використання спеціальних команд на вхідному інтерфейсі маршрутизатора. Фільтрувати усі RFC-1918 підмережі, використовуючи ACL. Застосовувати ingress- та egress-фільтрацію, використовуючи ACL. Використання CAR для обмеження ICMP пакетів

Продовження таблиці

6.	Підробка пакетів керуючих мережних пристроїв			
6.1.	Підміна довіреного об'єкта мережі [4, 5]	Полягає в підробці ідентифікаційних даних і передачі каналом зв'язку повідомлень від довільного об'єкта розподіленої системи	Порушує умови цілісності, доступності конфіденційності	Використання міжмережних екранів, криптографічних методів різних рівнів ідентифікації
6.2.	Нав'язування помилкового маршруту	Полягає в несанкціонованому використанні протоколів керування мережею для зміни початкових таблиць маршрутизації	Порушує умови цілісності та конфіденційності	Використання надійних моделей довіри. Використання HIDS
6.3.	Загроза атаки «людина посередині» (Man-in-the-Middle) [4]	Для реалізації даного типу атаки повинні бути відомі параметри сеансу зв'язку та адреси абонентів	Порушує умови цілісності та конфіденційності інформації	Використання шифрування даних
7.	Аналіз трафіка і конфігурації мережі			
7.1.	Аналіз мережного трафіка [4]	Перехоплення і аналіз зловмисником інформації, призначеної іншим абонентам	Порушення умов конфіденційності інформації	Контроль доступу. Фільтрація RFC 2827. Використання криптографічної аутентифікації
7.2.	Сканування	Реалізована шляхом спроб послідовного підключення до мережних порталів атакованої системи, що дозволяє виявити активні сервіси	Формально не порушує умов безпеки інформаційної системи, однак може бути підготовчим етапом для подальшої атаки	Відключення ICMP Echo-Request та ICMP Echo-Reply на периферійних маршрутизаторах (однак це може призвести до втрати даних, які необхідні для діагностики мережних збоїв). Використовувати системи виявлення вторгнень (IDS)
	Загрози для апаратної частини			
8.	Неправильне конфігурування апаратних засобів	Недостатня захищеність засобів конфігурації і відсутність перевірок на встановлення некоректних параметрів	Може викликати відмову апаратних засобів або їхнє фізичне пошкодження	Коректне налагодження апаратних засобів
9.	Несанкціоноване використання закладок розробників	Характерна для апаратних пристроїв, у низькорівневе програмне забезпечення яких закладена можливість обходу процедури аутентифікації для отримання доступу до інженерних функцій	Порушення умови цілісності, доступності та конфіденційності інформації	Дотримання адекватної політики безпеки, як на локальному ПК, так і в локальній мережі

Продовження таблиці

10.	Апаратне прослуховування середовища передачі даних [5]	Загроза характерна для розподілених систем, що не використовують криптографічного захисту переданої інформації або використовують алгоритми шифрування з недостатньою криптостійкістю	Витік інформації технічними каналами. Порушення умови цілісності і конфіденційності	Використання шифрування даних на основі складних алгоритмів. Застосування програм пошуку аналізаторів
11.	Фізичний доступ до носіїв інформації	Загроза можлива в тому випадку, коли інформація зберігається на носіях у незашифрованому вигляді	Порушення умови цілісності, доступності і конфіденційності	Використання шифрування інформації. Розмежування прав доступу до інформації

Аналіз систем виявлення загроз

Системи виявлення загроз можна поділити на системи, які орієнтовані на пошук:

— аномалій взаємодій об'єктів контролю;

— сигнатур усіх відомих атак;

— зміни еталонної профільної інформації.

На сьогоднішній день майже відсутні схеми гібридного типу, а також такі, які використовують інформацію розподіленого у часі та просторі характеру. Під час роботи переважної більшості сучасних систем використовується тільки сигнатурний метод розпізнавання атакуючого впливу або тільки зміни поведінки контрольованої системи.

Відомо, що сигнатурні методи дозволяють описати атаку набором правил або за допомогою формальної моделі, в якості якої може використовуватися символьний рядок, семантичний вираз на спеціальній мові та ін. Отже сигнатурний метод може захистити від вірусного або хакерського впливу на систему в тому випадку, коли вже відома сигнатура атаки.

Системи пошуку аномалій виявляють незвичайну поведінку (аномалію) у функціонуванні об'єкта контролю. Як об'єкт контролю може бути система в цілому, окремий комп'ютер, мережева служба, користувач та ін. Основний недолік такого підходу полягає в необхідності навчання системи «стандартній» поведінці.

Найбільш простими і дешевими є адміністративні методи захисту, а саме: використання в мережі стійкої криптографії, статичних ARP-таблиць, hosts-файлів замість виділених DNS-серверів, використання або невикористання певних операційних систем та інші методи [6, 7].

Наступна група методів захисту від віддалених атак — програмно-апаратні. До них відносяться:

— методика Firewall (тобто багаторівнева фільтрація мережевого трафіка, Proxy-схема з додатковою ідентифікацією і аутентифікацією користувачів на Firewall-хості, та створення приватних мереж з «віртуальними2 IP-адресами);

— захищені мережеві криптопротоколи;

— програмні засоби виявлення атак;
— програмні засоби аналізу захищеності;
— захищені мережні операційні системи.

Також слід виділити підгрупу методів захисту — програмні методи. До них відносяться, перш за все, захищені криптопротоколи, використовуючи які можна підвищити надійність захисту з'єднання.

Існуючі підходи до рішення задач виявлення вторгнень найчастіше відрізняються не лише реалізацією методів виявлення, але і своєю архітектурою, рівнем деталізації та типами виявлення вторгнень.

Таким чином, вимоги та особливості сучасних комп'ютерних мереж, такі як підвищення надійності та мобільності мереж, ієрархічна структура мереж, різні вимоги до безпеки, — все це накладає відбиток на технології та підходи, які повинні бути вже сьогодні реалізовані в системах виявлення атак.

Висновки

Проведений аналіз загроз інформаційній безпеці комп'ютерних систем при віддаленій обробці даних, класифікацію яких представлено в таблиці, дає можливість сформулювати шляхи подальшого вдосконалення комплексу заходів щодо забезпечення безперебійної роботи інформаційної системи за рахунок розробки архітектури та програмного коду на різних рівнях програмного і апаратного забезпечення.

Проаналізовані основні мережні атаки та способи протидії показали, що не дивлячись на можливість використання комплексних мір по захисту інформаційних систем, тобто цілеспрямованого застосування різних методів і засобів [1–7], найбільш надійним способом захисту комп'ютера є використання перевірених електронних ресурсів і дотримання жорстких умов розмежування привілеїв.

Сучасний підхід до побудови систем виявлення мережних вторгнень і виявлення ознак комп'ютерних атак на інформаційні системи сповнений недоліків і вразливостей. Перехід від пошуку сигнатур атак до виявлення передумов виникнення загроз інформаційній безпеці повинен сприяти тому, щоб докорінно змінити дану ситуацію, скоротивши дистанцію відставання в розвитку систем захисту від систем їхнього подолання. Крім того, такий перехід має сприяти підвищенню ефективності управління інформаційною безпекою.

1. *Семененко В.А.* Информационная безопасность: учебн. пособ. — [2-е изд., стереот.] / В.А. Семененко. — М.: МГИУ. — 2005. — 215 с.

2. *Корпань Я.В.* Комплекс методів та засобів захисту інформації в комп'ютерних системах / Я.В. Корпань // Мир науки и инноваций. — Иваново: Научный мир, 2015. — Вып. 1(1). — Т. 3. — С. 31–35.

3. *Скляров Д.* Искусство защиты и взлома информации / Д. Скляров. — СПб.: БХВ-Петербург. — 2004. — 288 с.

4. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. — М.: ДМК Пресс, 2012. — 592 с.

5. *Райан Р.* Защита от хакеров корпоративных сетей / Р. Рассел. — Компания АйТи, ДМК Пресс. — 2005. — 864 с.

6. *Гладких А.А.* Базовые принципы информационной безопасности вычислительных сетей: учебн. пособ. / А.А. Гладких, В.Е. Дементьев. — Ульяновск: УлГТУ. — 2009. — 156 с.

7. *Безбогов, А.А.* Методы и средства защиты компьютерной информации / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. — Тамбов: Изд-во Тамб. гос. техн. ун-та. — 2006. — 196 с.

Надійшла до редакції 12.05.2015