визначає трирівневу методологію оцінювання безпеки, описує декілька методів оцінювання та надає посилання на подальшу літературу та підходи. Цей документ може стати основою для оцінки кібербезпеки в інформаційних системах «інтелектуальної мережі» та її компонентів.

1. Енергетична стратегія України на період до 2030 року [Електронний ресурс] – http://www.niss.gov.ua/public/File/2014_nauk_an_rozrobku/ Energy%20Strategy%202035.pdf.
2. Аналіз зарубіжної практики впровадження автоматизованих систем управління технологічними процесами в електроенергетиці [Електронний ресурс] – https://ua.energy/wp-content/uploads/2018/01/2.-SMART-GRID.pdf.
3. European Smar tGrids Technology Platform [Електронний ресурс] – http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf.
4. Estimating the Costs and Benefits of the Smart Grid [Електронний ресурс] – http://www.rmi.org/Content/Files/EstimatingCostsSmartGRid.pdf.
5. IEC / TS 62351-1: Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security Introduction to security issues.
6. NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations.
7. DHS (2009). Catalog of Control Systems Security: Recommendations for Standards Developers. Technical report.
8. NIST SP 800-115: Technical Guide to Information Security Testing and Assessment.

http://doi.org/10.5281/zenodo.3860750

Поступила 30.09.2019р.

УДК 519.7-004.65

М.Ю. Комаров, Київ

КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЇ, ЯКА ЦИРКУЛЮЄ В АВТОМАТИЗОВАНИХ ТА АВТОМАТИЧНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Abstract. Threats, automatic systems, Sniffing, Hijacking, Denial-of-Service, DoS, Man-in-the-Middle.

Актуальність

На сьогоднішній день відомий достатньо широкий перелік загроз інформаційної безпеки, який містить сотні позицій. Перелік загроз, оцінки імовірності їх реалізації, а також модель порушника є основою для аналізу

ризику реалізації загроз та формулювання вимог до системи захисту автоматизованих систем (АС). Крім виявлення можливих загроз, доречно проведення аналізу цих загроз на основі їх класифікації за рядом ознак. Кожна із ознак класифікації відображає одну із узагальнених вимог до системи захисту. Загрози, що відповідають кожній ознаці класифікації, дозволяють деталізувати вимогу, що відображається цією ознакою.

Постановка задачі

В даній статті пропонується провести аналіз та класифікацію кіберзагроз інформаційній безпеці.

Вирішення задачі

Необхідність класифікації загроз інформаційної безпеки обумовлена тим, що інформація, яка зберігається та обробляється в АС, схильна до впливу надзвичайно великої кількості чинників, завдяки чому стає неможливим формалізувати задачу опису повної множини загроз. Тому для АС, що підлягає захисту, визначається не повний перелік загроз, а перелік класів загроз.

Згідно з нормативними документами технічного захисту інформації (ТЗІ) (НД ТЗІ 1.1-002-99 [1], ТЗІ 2.5-004-99 [2]) за результатом впливу на інформацію та систему її обробки загрози поділяються на чотири класи:

1. Порушення конфіденційності («К») інформації (отримання доступу до інформації з обмеженим доступом). При реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступу. В термінах комп'ютерної безпеки загроза порушення конфіденційності має місце усякий раз, коли отриманий несанкціонований доступ до певної закритої інформації, що зберігається у комп'ютерній системі або передається між ними.

2. Порушення цілісності («Ц») інформації (повне або часткове знищення, викривлення, модифікація, нав'язування хибної інформації). Цілісність інформації може бути порушена навмисно, а також в результаті об'єктивних впливів з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передавання інформації – комп'ютерних систем та мереж передачі даних.

3. Порушення доступності («Д») інформації (часткова або повна втрата працездатності системи, блокування доступу до інформації). Блокування доступу до ресурсів може бути постійним або тимчасовим.

4. Втрата спостереженості («С») або керованості системи обробки (порушення процедур ідентифікації та автентифікації користувачів та процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

Беручи до уваги проведений аналіз реалізованих кіберзагроз на об'єкти критичної інфраструктури [3] можна зробити висновок, що вищенаведені види загроз є первинними, або безпосередніми, оскільки їх реалізація веде до

безпосереднього впливу на інформацію, що підлягає захисту.

1. За природою виникнення загрози поділяються на:

– природні загрози, що викликані впливами на АС об'єктивних фізичних процесів або стихійних природних явищ;

– штучні загрози, викликані діяльністю людини.

2. За ступенем навмисності прояву загрози поділяються на:

– загрози, викликані посилками або халатністю персоналу (некомпетентне використання засобів захисту; введення помилкових даних тощо);

– загрози навмисної дії (наприклад дії зловмисників).

3. За джерелом впливу загрози поділяються на:

– загрози, обумовлені діями людини (викрадення, підміна, пошкодження інформації, паролів і атрибутів доступу, технічних та програмних засобів її обробки);

– загрози, обумовлені технічними засобами (неякісні технічні та програмні засоби обробки інформації);

– загрози, обумовлені стихійними факторами (пожежа, землетрус, повінь та ін.).

4. За положенням джерела загрози. Джерело загрози може бути розташовано:

– поза межами контрольованої зони (наприклад перехоплення даних, що передаються каналами зв'язку, перехоплення електромагнітних, акустичних та інших випромінювань пристроїв);

– в межах контрольованої зони (наприклад використання прослуховуючи пристроїв, викрадення роздруківок, записів, носіїв інформації тощо);

– безпосередньо в АС (некоректне використання ресурсів АС).

5. За ступенем залежності від активності АС загрози проявляються:

– незалежно від активності АС (наприклад розкриття шифрів крипто захисту інформації);

– тільки в процесі обробки даних (наприклад загрози виконання та розповсюдження програмних вірусів).

6. За характером впливу на АС загрози поділяються на:

– активні загрози, які при впливі вносять зміни у структуру та зміст АС (наприклад впровадження троянських коней та вірусів);

– пасивні загрози, які при реалізації нічого не змінюють у структурі та змісті АС (наприклад загроза копіювання конфіденційної інформації).

7. За етапами доступу користувачів або програм до ресурсів АС загрози поділяються на:

– загрози, які проявляються на етапі доступу до ресурсів АС (наприклад загрози несанкціонованого доступу до АС);

– загрози, які проявляються після дозволу доступу до ресурсів АС (наприклад загрози несанкціонованого або некоректного використання ресурсів АС).

8. За способом доступу до ресурсів АС загрози поділяються на:

– загрози з використанням стандартного шляху доступу до ресурсів АС (наприклад незаконне отримання паролів та інших атрибутів розмежування доступу з наступним маскуванням під зареєстрованого користувача);

– загрози з використанням скритого нестандартного шляху доступу до ресурсів АС (наприклад несанкціонований доступ до ресурсів АС шляхом використання недокументованих можливостей операційної системи (ОС)).

9. За поточним місцем розташування інформації, що зберігається та обробляється в АС, загрози поділяються на:

– загрози доступу до інформації на зовнішніх запам'ятовуючих пристроях (наприклад несанкціоноване копіювання конфіденційної інформації з жорсткого диску);

– загрози доступу до інформації в оперативній пам'яті (наприклад читання остаточної інформації із оперативної пам'яті, доступ до системної області оперативної пам'яті з боку прикладних програм);

– загрози доступу до інформації, що циркулює у лініях зв'язку (наприклад незаконне підключення до ліній зв'язку з наступним введенням хибних повідомлень або модифікацією повідомлень, що передаються; незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача з наступним введенням дезінформації та нав'язуванням хибних повідомлень);

– загрози доступу до інформації, що відображається на терміналі або друкується на принтері (наприклад запис інформації, що відображається, на скриту відеокамеру).

10. За способом впливу на об'єкт атаки загрози поділяються на:

– загрози з безпосереднім впливом на об'єкт атаки;

– загрози з впливом на систему прав доступу;

– загрози з опосередкованим впливом.

11. За використовуваним для атаки компонентом АС загрози поділяються на:

– загрози, які використовують технічні засоби АС;

– загрози, які використовують технологічну інформацію АС;

– загрози, які використовують програмні засоби АС.

12. За засобами атаки загрози поділяються на:

– загрози з використанням стандартного програмного забезпечення або технічних засобів;

– загрози з використанням спеціально розробленого програмного забезпечення або технічних засобів.

13. За станом об'єкту атаки загрози поділяються на:

– загрози на об'єкт атаки, який знаходиться в стані зберігання;

– загрози на об'єкт атаки, який знаходиться в стані обробки.

Існує чотири основні категорії мережевих атак [4]:

– атаки доступу;
– атаки модифікації;
– атаки на відмову в обслуговуванні;
– комбіновані атаки.

Атака доступу – це спроба отримання зловмисником інформації, для ознайомлення з якою у нього немає дозволу. Атака доступу направлена на порушення конфіденційності інформації, що підлягає захисту. До найвідоміших атак доступу відносяться:

– прослуховування (Sniffing);
– перехоплення (Hijacking);
– перехоплення сеансу (Session Hijacking).

Атака модифікації – це спроба неправомірної зміни інформації. Така атака можлива всюди, де існує або передається інформація. Атака направлена на порушення цілісності інформації. До найвідоміших атак модифікації відносяться:

– зміна даних;
– додавання даних;
– знищення даних.

Атака на відмову в обслуговуванні (Denial-of-Service, DoS) відрізняється від атак інших типів. Вона не націлена на отримання доступу до мережі або на отримання із мережі будь-якої інформації. Атака DoS робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або додатків. Ця атака позбуває користувачів доступу до ресурсів або комп'ютерів мережі організації.

Більшість атак DoS спираються на загальні слабкості системної архітектури. У випадку використання деяких серверних додатків (таких як веб- або FTP-сервер) атаки DoS можуть полягати в тому, щоби зайняти всі з'єднання, що доступні для цих додатків, та тримати їх у зайнятому стані, не допускаючи обслуговування звичайних користувачів. В ході атак DoS можуть використовуватись звичайні Інтернет-протоколи, такі як TCP та ICMP (Internet Control Message Protocol).

Атаки DoS важко попередити, так як для цього необхідна координація дій з провайдером. Якщо трафік, призначений для переповнення мережі, не зупинити у провайдера, то на вході у мережу зробити це вже неможливо, тому що вся смуга пропускання буде зайнята.

Якщо атака даного типу проводиться одночасно через множину пристроїв, то можна казати про розподілену атаку відмови в обслуговуванні DDoS (Distributed DoS).

Простота реалізації атак DoS та велика шкода, що завдається ними організаціям та користувачам, приваблюють до цих атак пильну увагу адміністраторів мережевої безпеки. До найвідоміших та найнебезпечніших

атак відмови у доступі належать такі:

– відмова у доступі до інформації;
– відмова у доступі до додатків;
– відмова у доступі до системи;
– відмова у доступі до засобів зв'язку.

Комбіновані атаки полягають у застосуванні зловмисниками декількох взаємно пов'язаних дій для досягнення своєї мети. Серед найвідоміших комбінованих атак можна виділити такі:

– підміна довіреного суб'єкту;
– посередництво;
– посередництво в обміні незашифрованими ключами (атака Man-in-the-Middle – «людина в середині»);
– атака експлойту;
– парольні атаки;
– вгадування ключа;
– атаки на рівні додатків.

Висновки

Проведено класифікацію типів загроз за різними ознаками. Проведено аналіз мережевих атак за основними категоріями.

За результатами проведеного аналізу встановлено, що:

– на сьогоднішній день існує велика кількість типів та категорій мережевих загроз та атак;

– враховуючи стрімкий розвиток новітніх технологій фахівцям з кібербезпеки необхідно постійно вдосконалювати свій професійний рівень підготовки, а організаціям, що потребують захисту від кібератак, своєчасно поліпшувати матеріально-технічну базу засобів кіберзахисту.

1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
2. ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
3. *Комаров М.Ю.* Огляд кібератак на об'єкти критичної інфраструктури // Національна академія наук України. Інститут проблем моделювання в енергетиці. Електронне моделювання. Т 41 № 6, 2019.
4. *Шаньгін В.Ф.* Информационная безопасность и защита информации – М.: ДМК-Пресс, 2017. – 702 с.

http://doi.org/10.5281/zenodo.3860752

Поступила 26.09.2019р.