УДК 004.056.53

Комаров М.Ю.
Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України

Гончар С.Ф.
Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України

АНАЛІЗ І ДОСЛІДЖЕННЯ ЗАГРОЗ ДЛЯ ЗАХИЩЕНОГО ВУЗЛА ІНТЕРНЕТ ДОСТУПУ

У роботі здійснено аналіз і дослідження основних загроз безпеці інформації для захищеного вузла Інтернет доступу. Приведені загрози для інформації, яка циркулює в захищеному вузлі Інтернет доступу. Показано, що навіть загрози, які на перший погляд не є суттєвими, насправді можуть завдати значної шкоди захищеному вузлу Інтернет доступу. Розробка адекватної та максимально всеохоплюючої моделі загроз під час побудови ЗВІД є обов'язковим етапом захисту інформації. Розглянуто модель основних загроз безпеці інформації, яка циркулює в захищеному вузлі Інтернет доступу.

Ключові слова: *загроза, модель, безпека інформації, програмне забезпечення, захищений вузол Інтернет доступу.*

Постановка проблеми. Захищені вузли Інтернет доступу (далі – ЗВІД) призначені для надання органам державної влади та органам місцевого самоврядування, державним підприємствам, установам, організаціям, іншим юридичним і фізичним особам (далі – споживачам) послуг зв'язку, послуг захищеного доступу споживача до ресурсів і сервісів мережі Інтернет.

ЗВІД будується на базі інформаційно-телекомунікаційної системи (далі – ІТС). ІТС ЗВІД є складною гетерогенною мережею, яка здійснює обмін інформацією та її обробку з метою забезпечення функціональної діяльності захищеного вузла Інтернет доступу й обміну інформацією з іншими організаціями та установами.

ІТС ЗВІД використовує технології побудови локальних обчислювальних мереж (Ethernet) і глобальних обчислювальних мереж (TCP/IP). Як фізичне середовище передачі інформаційних сигналів (горизонтальна підсистема структурованої кабельної системи) в обчислювальній мережі ІТС ЗВІД використовують симетричний кабель типу «звита пара» та волоконно-оптичні лінії зв'язку.

Аналіз останніх досліджень і публікацій. Згідно з нормативними документами системи технічного захисту інформації (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) [1; 2], загрози поділяються за результатом впливу на інформацію та систему її обробки; за джерелом впливу загрози; за характером впливу на ЗВІД; за способом впливу на об'єкт атаки; за використовуваним для атаки компонентом ЗВІД; за засобами атаки; за станом об'єкта атаки. Разом із тим відсутня узагальнена модель загроз для інформації, яка циркулює у ЗВІД.

Постановка завдання. Необхідно розробити модель загроз для інформації, яка циркулює у ЗВІД. Під розробкою моделі загроз будемо розуміти класифікацію загроз, їх перелік, наслідки, об'єкти та суб'єкти загроз.

Виклад основного матеріалу дослідження. Згідно з нормативними документами, системи технічного захисту інформації 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).

2. Порушення цілісності («Ц») інформації (повне або часткове знищення, викривлення, модифікація, нав'язування хибної інформації).

3. Порушення доступності («Д») інформації (часткова або повна втрата працездатності системи, блокування доступу до інформації).

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

За джерелом впливу загрози поділяються на:

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

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

– загрози, зумовлені стихійними факторами (пожежа, землетрус, повінь тощо).

За характером впливу на ЗВІД загрози поділяються на:

– активні;

– пасивні.

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.

За використовуваним для атаки компонентом ЗВІД загрози поділяються на:

– загрози, які використовують технічні засоби ЗВІД;

– загрози, які використовують технологічну інформацію ЗВІД;

– загрози, які використовують програмні засоби ЗВІД.

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.

За станом об'єкта атаки загрози поділяються на:

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

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

Розглянемо загрози загального характеру, що можуть виникнути в ЗВІД, і можливі наслідки їх реалізації:

– пожежа – виникнення полум'я та розповсюдження пожежі в приміщеннях, де знаходяться технічні засоби ЗВІД. Можуть бути пошкоджені об'єкти захисту, структурні компоненти ЗВІД, канали передачі даних, утрачена інформація;

– руйнування – руйнування приміщень і їх умісту внаслідок вибуху, зсуву, урагану тощо. Можуть бути пошкоджені об'єкти захисту, структурні компоненти ЗВІД, канали передачі даних, утрачена інформація;

– затоплення – заливання приміщень унаслідок аварій, стихійних лих у вигляді дощів, танення снігу, гасіння полум'я водою. Можуть бути пошкоджені об'єкти захисту, структурні компоненти ЗВІД;

– забруднення – запиленість і забрудненість приміщень і технічних засобів. Наслідком можуть стати відмови та збої компонентів ЗВІД та окремих технічних засобів, пошкодження носіїв інформації;

– перегрів – зміна температури повітря внаслідок погодних аномалій, порушення в роботі систем опалення й вентиляції. Наслідком можуть стати відмови та збої компонентів ЗВІД та окремих технічних засобів;

– вологість – зміна вологості повітря внаслідок погодних аномалій, порушення систем вентиляції. Можуть бути пошкоджені носії інформації, електроконтакти, що спричинятиме відмови та збої компонентів ЗВІД та окремих технічних засобів;

– електромагнітні випромінювання – магнітні наводки від потужних електроприладів (трансформатори, електродвигуни, динаміки), електромагнітні бурі. Можливе пошкодження носіїв інформації, відмови технічних засобів;

– поламки, відмови апаратури – відмова в роботі технічних засобів ЗВІД, вихід з ладу апаратного забезпечення внаслідок техногенних аварій, порушення умов експлуатації, несвоєчасного діагностування проблеми. Наслідком може стати непрацездатність компонентів ЗВІД та окремих технічних засобів, утрата й перекручення інформації в процесі запису/зчитування;

– нестача ресурсів – нестача ресурсів центрального процесору, оперативної пам'яті, місця на жорстких дисках, перепускної здатності каналів передачі даних. Може призводити до втрати й перекручення інформації, доступності ресурсів ЗВІД, непрацездатності компонентів ЗВІД та окремих технічних засобів;

– навмисне пошкодження або крадіжка обладнання – навмисний вивід з ладу обладнання, що може призвести до тимчасової або повної непрацездатності компонентів ЗВІД, крадіжка технічних засобів ЗВІД, що може мати як наслідок простій ЗВІД, розголошення технологічної інформації захисту (далі – ТІЗ). Може проявлятися за можливості безпосереднього доступу до обладнання;

– випадкове пошкодження обладнання – ненавмисний вивід з ладу обладнання, що може призвести до тимчасової або повної непрацездатності компонентів ЗВІД. Може проявлятися за можливості безпосереднього доступу до обладнання.

Розглянемо мережеві загрози, що можуть виникнути в ЗВІД, і можливі наслідки їх реалізації:

– відсутність фізичного з'єднання – створення з'єднань, що не відповідають проектній докумен-

тації й/або призводять до порушення функціонування мережі;

– помилки та непрацездатність активного мережевого обладнання (далі – АМО) – помилкове функціонування мережі внаслідок помилок програмної або апаратної конфігурації АМО чи помилок програмного забезпечення АМО. Загроза може мати місце під час проектування, експлуатації та модернізації ЗВІД;

– розголошення даних про мережу – розголошення ТІЗ мережі, що є наслідком мережевої розвідки – збирання інформації про мережу за допомогою загальнодоступних і спеціальних застосувань. На рівні мережі збирається інформація про структуру мережі, наявні сегменти мережі, хости. На рівні АМО збирається інформація про мережеві конфігурації та протоколи (зокрема схему IP-адресації);

– перехоплення (сніферинг) пакетів – розголошення технологічної інформації, що є наслідком перехоплення мережевих пакетів (сніферингу). Сніфер пакетів являє собою прикладну програму, яка використовує мережеву карту, що працює в режимі promiscuous mode (у цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє застосуванню для обробки);

– підміна отримувача (спуфінг пакетів) – утрата даних унаслідок спуфінгу. Це відбувається, коли зловмисник, що знаходиться всередині ЗВІД або поза нею, видає себе за іншого користувача;

– відмова в обслуговуванні (DoS) – атака Denial of Services (DoS) робить мережу або окремі сервіси мережі недоступними для звичайного використання за рахунок перевищення припустимих параметрів функціонування мережі, ОС або застосування;

– дзеркалювання трафіку – для дзеркалювання трафіку (атаки типу Man-in-the-Middle) зловмиснику потрібний доступ до пакетів, переданих по мережі;

– непрацездатність мережевих застосувань – атаки на рівні застосувань можуть проводитися декількома способами. Найпоширеніший із них полягає у використанні добре відомих уразливостей серверного ПЗ;

– створення альтернативних несанкціонованих точок доступу до мережі – існує можливість додзвонювання на модеми, які несанкціоновано підключені користувачами до робочих станцій.

Розглянемо загрози для операційних систем, що можуть виникнути у ЗВІД, і можливі наслідки їх реалізації:

– помилка, збій і відмова системного ПЗ – помилки та відмови системного ПЗ, що можуть виникати внаслідок неправильних налаштувань ОС, помилок розробників ОС, невідповідності системним вимогам тощо (ненавмисна загроза);

– перехоплення ТІЗ – підглядання атрибутів доступу, автоматичний підбір паролів за допомогою спеціалізованих програмних засобів (закладки типу «троянський кінь»), перехоплення логінів і паролів за допомогою перехоплювачів клавіатури (keyloggers);

– пошкодження файлів ОС – порушення цілісності файлів системного ПЗ (в т. ч. системних журналів) унаслідок необережності або навмисних дій;

– збирання «сміття» – відновлення знищеної користувачем або сеансової інформації (так званого «сміття») шляхом аналізу тимчасових каталогів ОС, оперативної пам'яті тощо;

– втручання в роботу ОС з мережі – зовнішнє втручання в роботу з боку інших користувачів ОС, що спричиняє загрози спостереженості (керованості), цілісності, доступності, а також конфіденційності ТІЗ. Зловмисник може використовувати як відомі вразливості ОС, так і штатні засоби комунікацій.

Розглянемо загрози для прикладного програмного забезпечення, що можуть виникнути у ЗВІД, і можливі наслідки їх реалізації:

– помилка, збій і відмова прикладного ПЗ – помилки та відмови прикладного ПЗ, що можуть виникати внаслідок неправильних налаштувань ПЗ, помилок розробників ПЗ, невідповідності системним вимогам тощо (ненавмисна загроза);

– виконання недокументованих функцій – маскування всередині коду модулів прикладного ПЗ програмних закладок, що здатні перехоплювати технологічну інформацію та здійснювати низку несанкціонованих операцій. Зазвичай закладка слугує відправною точкою для реалізації інших загроз;

– розповсюдження вірусів – ураження й/або пошкодження файлів прикладного ПЗ (в т. ч. файлів журналів) комп'ютерними вірусами. Може здійснюватися як навмисно, так і ненавмисно;

– несумісність версій ПЗ – несумісність різних версій/типів ПЗ, що може спричинити збої в роботі прикладних АС, загрози цілісності й доступності інформації;

– перехоплення ТІЗ – підглядання атрибутів доступу, автоматичний підбір паролів за допомогою спеціалізованих програмних засобів (закладки типу «троянський кінь»), перехоплення логінів і паролів за допомогою перехоплювачів клавіатури (keyloggers);

– підміна або дезорганізація – порушення цілісності ПЗ внаслідок підміни елементів програм, динамічних бібліотек, модулів ПЗ, даних аудиту або дезорганізації структури ПЗ. Може викликати непрацездатність ЗВІД або її компонентів, перекручення даних;

– прикладне ПЗ – обхід чи злам механізмів захисту шляхом аналізу програмного коду за допомогою спеціалізованих програмних засобів з подальшим несанкціонованим отриманням доступу до даних і конфігурацій.

Висновки. Приведені вище загрози для інформації, яка циркулює в ЗВІД, наявно демонструють, що навіть загрози, які на перший погляд не є суттєвими, насправді можуть завдати значної шкоди ЗВІД зокрема й інформаційно-телекомунікаційній системі загалом. Розробка адекватної та максимально всеохоплюючої моделі загроз під час побудови ЗВІД є обов'язковим етапом, реалізація якого дасть змогу убезпечити його ресурси, в тому числі інформаційні, від деструктивного впливу загроз будь-якого типу.

Список літератури:

1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

2. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

АНАЛИЗ И ИССЛЕДОВАНИЕ УГРОЗ ДЛЯ ЗАЩИЩЕННОГО УЗЛА ИНТЕРНЕТ ДОСТУПА

В работе осуществлены анализ и исследование основных угроз безопасности информации для защищенного узла Интернет доступа. Приведены угрозы для информации, которая циркулирует в защищенном узле Интернет доступа. Показано, что даже угрозы, которые на первый взгляд не являются существенными, на самом деле могут нанести значительный ущерб защищенному узлу Интернет доступа. Показано, что разработка адекватной модели угроз при построении защищенного узла Интернет доступа является обязательным этапом защиты информации. Рассмотрена модель основных угроз безопасности информации, которая циркулирует в защищенном узле Интернет доступа.

Ключевые слова: *угроза, модель, безопасность информации, программное обеспечение, защищенный узел Интернет доступа.*

ANALYSIS AND RESEARCHES OF THREATS FOR A PROTECTED INTERNET ACCESS NODE

Analysis and researches of threats for a protected internet access node is given in the work. Threats to information circulating in the protected internet access node are presented. It is shown that even threats that, at first glance, are not significant, can in fact cause significant damage to the protected internet access node. It is shown that the development of an adequate model of threats in the building of the protected internet access node is a mandatory step for the protection of information. The model of basic information security threats, which circulates in protected internet access node, is considered.

Key words: *threat, model, information security, Software, protected internet access node.*