**Тема 2. Захист інформації на рівні прикладного та системного програмного**

**забезпечення**

План

1. Розмежування доступу до інформації

2. Системи ідентифікації та автентифікації

3. Системи аудиту та моніторингу

4. Системи антивірусного захисту

Важливим елементом забезпечення цілісності та конфіденційної інформації є захист від несанкціонованого доступу до ресурсів інформаційних систем, що викликає необхідність створення надійних і зручних систем контролю доступу.

Контроль доступу – функція системи захисту інформації (СЗІ), яка дозволяє або забороняє доступ до певних типів даних.

Контроль доступу є одним із найбільш важливих елементів СЗІ в інформаційно-телекомунікаційних системах. Доступ до захищеної інформації повинен бути обмежений, щоб тільки люди, які мають право доступу, могли отримувати цю інформацію. Комп’ютерні програми і в багатьох випадках сторонні комп’ютери за допомогою локальної мережі, Інтернету, бездротової мережі можуть отримати секретну інформацію, яка не призначена їм. Це може завдати як фінансові, так і інформаційні втрати. У зв’язку з цим необхідний механізм контролю доступу до захищеної інформації. Складність механізмів контролю доступу, як зазначалось на попередньому занятті, має бути в паритеті з цінністю інформації, тобто чим більш важливою або цінною є інформація, тим більш складними повинні бути механізми контролю доступу. Основними механізмами контролю доступу є ідентифікація та аутентифікація.

Кожний користувач сучасних інформаційно-телекомунікаційних систем декілька разів на день стикається з процедурами ідентифікації та аутентифікації. Ці процедури виконуються кожного разу, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або при запуску прикладної програми. Таким чином ідентифікація та аутентифікація це перша лінія оборони, «прохідна» інформаційного простору організації. В результаті їх виконання користувач або отримує допуск до роботи в інформаційній системі, або ні.

Під ідентифікацією (від лат. Іdentifico – ототожнювати) розуміють процедуру розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. Ідентифікація використовується для отримання інформації про суб’єкт системи на основі наданого ним ідентифікатора. Є початковою процедурою надання доступу до системи. Після неї здійснюється аутентифікація та авторизація.

В свою чергу аутентифікація (з грец. αυθεντικός – реальний або істинний) особи в інформаційній системі – це перевірка приналежності суб’єкту доступу пред’явленого ним ідентифікатора та підтвердження його достовірності, за допомогою деякої унікальної інформації (паролю, відбитка пальця, голосу тощо). З позицій інформаційної безпеки аутентифікація є частиною процедури надання доступу до інформаційної системи, наступною після ідентифікації, та передує авторизації.

Таким чином, ідентифікація дозволяє суб’єкту (користувачеві, процесу, що діє від імені певного користувача, або іншого апаратно-програмного компоненту) назвати себе (повідомити своє ім’я). За допомогою аутентифікації друга сторона переконується, що суб’єкт дійсно той, за кого він себе видає. Як синонім слова «аутентифікація» іноді використовують словосполучення «перевірка справжності»

Стійкість підсистеми ідентифікації та аутентифікації користувача в СЗІ багато в чому визначає стійкість до злому самої СЗІ. Дана стійкість визначається гарантією того, що зловмисник не зможе пройти аутентифікацію, привласнивши чужий ідентифікатор або вкравши його. В зв’язку з цим існують різні методи ідентифікації та аутентифікації користувачів інформаційної системи, які відрізняються своєю складністю, надійністю, вартістю та іншими показниками. Кожний з цих методів має як позитивні, так і негативні сторони, тому далі проведемо їх короткий аналіз.

На сьогоднішній день, в інформаційних технологіях використовуються наступні види аутентифікації:

одностороння аутентифікація – полягає в тому, що кожен клієнт системи для доступу до інформації обов’язково повинен доводити свою аутентичність;

двостороння – полягає в тому, що окрім клієнта, свою аутентичність повинна підтверджувати і сама система;

тристороння – полягає у використанні, так званої, нотаріальної служби аутентифікації для підтвердження достовірності кожного з партнерів при обміні інформацією.

Методи аутентифікації умовно можна поділити (рис. 9.2) на однофакторні (слабкі, з точки зору безпеки) та багатофакторні (сильні)

Парольна система аутентифікації є одним із основних, простих та найбільш поширених методів. У цьому випадку при введенні суб’єктом свого пароля підсистема аутентифікації порівнює його з даними, які зберігаються в спеціальній захищеній базі еталонних даних в зашифрованому вигляді. У випадку успішної аутентифікації проводиться авторизація з подальшим отриманням певних повноважень і наданням доступ до конкретних ресурсів інформаційної системи.

Авторизація (Authorization) – процедура надання суб’єкту певних повноважень і ресурсів у даній системі, на основі введеного ним ідентифікатора та аутентифікатора (пароля). Іншими словами, авторизація встановлює сферу діяльності суб’єкта і доступні йому ресурси. Якщо система не може надійно відрізнити авторизовану особу від неавторизованої, в ній можуть бути порушені конфіденційність і цілісність інформації. Саме тому організації необхідно чітко визначити свої вимоги до безпеки та обрати відповідну модель безпеки, які будуть розглянуті на наступному занятті.

Парольні методи аутентифікації також можна розділити за ступенем змінності паролів:

* методи, що використовують постійні паролі (багаторазового використання);
* методи, що використовують одноразові паролі (динамічно змінюються).
* Введення пароля, як правило, виконують з клавіатури або за допомогою сенсорного екрану.

Розглядаючи ідентифікаційну аутентифікацію потрібно відзначити, що у більшості випадків вона відбувається за допомогою унікальних предметів, які забезпечують більш надійний захист, ніж звична парольна аутентифікація. Ці предмети умовно поділяють на дві групи:

* пасивні предмети, які містять аутентифікаційну інформацію (наприклад, якийсь випадково згенерований пароль) і за вимогою передають її в модуль аутентифікації. При цьому, дана інформація може зберігатися як у захищеному вигляді (смарт-картки з захищеною пам’яттю, USB-токени) так і в відкритому (магнітні карти, смарт-карти з відкритою пам’яттю, електронні таблетки Touch Memory);
* активні предмети, які володіють достатніми обчислювальними ресурсами і беруть активну участь в процесі аутентифікації (мікропроцесорні смарт-карти і USB-токени).

Основний недолік вище зазначених методів ідентифікації та аутентифікації зумовлений неоднозначністю ідентифікованої особи. Передусім це пов’язано з тим, що для встановлення аутентичності особи застосовують атрибутивні й основані на певних відомостях розпізнавальні характеристики. Іншим важливим недоліком традиційних методів ідентифікації та аутентифікації, який випливає з вищезазначеного, є відсутність можливості виявлення підміни ідентифікованого користувача, що дає змогу зловмисникові отримати доступ до ресурсів системи, який обмежений тільки правами ідентифікованого користувача. Однак дані недоліки можна виправити, доповнивши систему захисту методами біометричної аутентифікації.

Біометричні методи аутентифікації працюють на основі використання устаткування для вимірювання і порівняння з еталоном заданих індивідуальних характеристик користувача. Біометрія – сукупність автоматизованих методів аутентифікації людей на основі їх фізіологічних (статичних), тобто унікальних, вроджених та невід’ємних від неї, і поведінкових характеристик (динамічних). До фізіологічних характеристик належать особливості відбитків пальців, сітківки та рогівки очей, геометрія руки й обличчя та ін. До поведінкових характеристик відносяться динаміка підпису, клавіатурний почерк, розпізнавання голосу. Такі засоби дозволяють з високою точністю розпізнати власника за конкретною біометричною ознакою, а підробити такі параметри практично неможливо.

При всьому різноманітті існуючих механізмів аутентифікації, найбільш поширеним з них залишається парольний захист. Для цього є кілька причин, з яких ми відзначимо наступні:

* відносна простота реалізації, так як механізми захисту паролем зазвичай не вимагають залучення додаткових апаратних засобів;
* традиційність, оскільки механізми парольного захисту є звичними для більшості користувачів автоматизованих систем і не викликають психологічного відторгнення – на відміну, наприклад, від сканерів малюнка сітківки ока.

У той же час для парольних систем захисту характерний парадокс, що ускладнює їх ефективну реалізацію: стійкі паролі мало придатні для використання людиною. Дійсно, стійкість пароля виникає в міру його ускладнення; але чим складніший пароль, тим важче його запам’ятати, і в користувача з’являється спокуса записати незручний пароль, що створює додаткові канали для його дискредитації.

У загальному випадку пароль може бути отриманий зловмисником одним з трьох основних джерел:

1. *за рахунок використання слабкостей людського фактору*. В даному випадку методи отримання паролів можуть бути достатньо різноманітними: соціальна інженерія, підслуховування, підглядання, погрози, шантаж, і навіть, використання чужих облікових записів з дозволу їх законних власників;
2. *шляхом підбору*. Дана технологія народилася досить давно, але до цих пір використовується і дуже успішно. При цьому виділяють наступні методи:
	* *повний перебір*. Даний метод дозволяє підібрати будь-який пароль в незалежності від його складності, проте для стійкого пароля час, необхідний для даної атаки, має значно перевищувати допустимі часові ресурси зловмисника;
	* *підбір за словником*. Значна частина використовуваних на практиці паролів являє собою певні осмислені слова або вирази, на основі цього створюються словники найбільш поширених паролів, які в багатьох випадках дозволяють обійтися без повного перебору. Для того щоб досягти успіху в 60% випадків зазвичай досить словника розміром 50000 іменників. Величезне число інцидентів зі зломами систем змусило користувачів додавати до слів 1-2 цифри з кінця, записувати першу та/або останню букву у верхньому регістрі, використовувати «трансліт». Але як показали дослідження, навіть складання двох абсолютно не пов’язаних осмислених слів поспіль не дає достатньо реальної надійності пароля;
	* *підбір з використанням відомостей про конкретного користувача*. Даний інтелектуальний метод підбору паролів ґрунтується на тому факті, що якщо політика безпеки системи передбачає самостійне призначення паролів користувачами, то в переважній більшості випадків в якості пароля буде обрана якась персональна інформація, пов’язана з користувачем АС. І хоча в якості такої інформації може бути вибрано що завгодно, від дня народження дружини і до прізвиська улюбленої домашньої тварини, наявність інформації про користувача дозволяє перевірити найбільш поширені варіанти (дні народження, імена дітей тощо);
3. *за рахунок використання недоліків реалізації самої парольної системи*. До таких недоліків реалізації відносяться критичні уразливості мережевих сервісів, які реалізуються в тих чи інших компонентах парольної системи захисту, несанкціонований доступ до носія інформації, на якому вони містяться, або ж використання недокументованих можливостей відповідного програмного або апаратного забезпечення.

Аудит (audit) – систематичний, незалежний і документований процес отримання даних аудиту та їх об'єктивне оцінювання з метою встановлення відповідності критеріям аудиту.

Внутрішні аудити, які іноді називають «аудити першої сторони», проводяться самою організацією або від її імені з метою аналізу з боку керівництва та для інших внутрішніх цілей (наприклад, для підтвердження результативності системи менеджменту або для отримання інформації про підвищення ефективності системи менеджменту).

Внутрішні аудити можуть створювати основу для самодекларування організацією своєї відповідності критеріям безпеки. У багатьох випадках, особливо в маленьких організаціях, незалежність аудиторів може бути продемонстрована відсутністю відповідальності за діяльність, що підлягає аудиту, або свободою від упередженості і конфлікту інтересів.

Зовнішні аудити – це аудити, які проводяться другою і третьою сторонами. Аудити другої сторони проводяться сторонами, що мають інтерес до організації (наприклад, споживачами), або іншими особами від їх імені. Аудити третьої сторони проводяться незалежними аудиторськими організаціями (наглядовими органами або організаціями, що здійснюють сертифікацію).

Якщо дві системи менеджменту якості різного типу або більше (наприклад, система менеджменту якості, система екологічного менеджменту, СМІБ і забезпечення безпеки праці) піддаються аудиту спільно, це називається комбінованим аудитом.

Якщо дві аудиторські організації або більше об’єднуються, щоб провести аудит однієї аудиторської організації, це називається спільним аудитом.

Одним з найпоширеніших видів аудиту інформаційних систем є активний аудит. Він полягає у дослідженні стану захищеності ІС з точки зору зловмисника (або зловмисника, що володіє високою кваліфікацією в галузі ІТ).

Найчастіше компанії-постачальники послуг активного аудиту іменують його **інструментальним аналізом захищеності**, щоб відокремити даний вид аудиту від інших.

Сутність активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів, здійснюється збір інформації про стан системи мережевого захисту. Під станом системи мережевого захисту розуміють лише ті параметри і налаштування, використання яких допомагає зловмисникові проникнути в мережі і нанести збитки компанії.

При здійсненні даного виду аудиту система мережевого захисту піддається якомога більшій кількості мережевих атак, які може виконати зловмисник. При цьому аудитор штучно ставиться саме в ті умови, в яких працює зловмисник. Йому надається мінімум інформації, тільки та, яку можна здобути у відкритих джерелах.

Атаки тільки моделюються і не завдають будь-якого деструктивного впливу ІС. Їх різноманітність залежить від використовуваних систем аналізу захищеності і кваліфікації аудитора.

Активний аудит умовно можна розділити на два види – зовнішній і внутрішній.

При зовнішньому активному аудиті фахівці моделюють дії зовнішнього зловмисника. У даному випадку проводяться наступні процедури:

* визначення доступних із зовнішніх мереж IP-адрес підприємства;
* сканування даних адрес з метою визначення працюючих сервісів і служб, а також призначення відсканованих хостів;
* визначення версій сервісів і служб хостів, що скануються;
* вивчення маршрутів проходження трафіку до хостів замовника;
* збір інформації про ІС замовника з відкритих джерел;
* аналіз отриманих даних з метою виявлення уразливостей.

Внутрішній активний аудит за складом робіт аналогічний зовнішньому, однак при його проведенні за допомогою спеціальних програмних засобів моделюються дії «внутрішнього» зловмисника.

Даний розподіл активного аудиту на «зовнішній» і «внутрішній» актуальний для підприємства в таких випадках:

* існують фінансові обмеження на придбання послуг і продуктів ЗІ;
* модель зловмисника, яка існує, не містить «внутрішніх» зловмисників;
* розслідується факт обходу системи мережевого захисту.

Найчастіше організація у своїй ІС використовує спеціалізоване програмне забезпечення (ПЗ) власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, різні бухгалтерські системи або системи документообігу). Подібні ПЗ унікальні, тому яких-небудь готових засобів і технологій для аналізу їх захищеності та відмовостійкості не існує. У даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного ПЗ.

Також під час активного аудиту здійснюється дослідження виробленості і стабільності системи, або стрес-тестування. Воно спрямоване на визначення критичних точок навантаження, при якій система внаслідок атаки на відмову в обслуговуванні або підвищеної завантаженості перестає адекватно реагувати на легітимні (визначені політикою безпеки) запити користувачів.

Стрес-тест дозволить виявити «вузькі» місця у процесі формування та передачі інформації і визначити ті умови, за яких нормальна робота системи неможлива. Таке тестування передбачає моделювання атак на відмову в обслуговуванні запитів користувача до системи і загальний аналіз її продуктивності.

Результатом активного аудиту є інформація про всі уразливості, ступені їх критичності і методи усунення, відомості про загальнодоступну інформацію (інформацію, доступну будь-якому потенційному порушнику) мережі замовника.

За результатами активного аудиту надаються рекомендації з модернізації системи мережевого захисту, які дозволяють усунути небезпечні уразливості, і таким чином підвищити рівень захищеності ІС від дій «зовнішнього» зловмисника при мінімальних витратах на ІБ.

Однак без проведення інших видів аудиту ці рекомендації можуть виявитися недостатніми для створення «ідеальної» системи мережевого захисту. Наприклад, за результатами даного виду аудиту неможливо зробити висновок про коректність, з точки зору безпеки, проекту ІС.

Експертний аудит можна умовно представити як порівняння стану ІБ з «ідеальним» описом, що передбачає:

* вимоги, які були висунуті керівництвом у процесі проведення аудиту;
* опис «ідеальної» системи безпеки, заснованої на акумульованому у компанії-аудитора загальновідомому та власному досвіді.

При виконанні експертного аудиту проводяться наступні види робіт:

* збір первинних даних про систему ІБ, про її функції й особливості, використовувані технології автоматизованої обробки та передачі даних (з урахуванням найближчих перспектив розвитку);
* збір інформації про наявні організаційно-розпорядчі документи щодо забезпечення ІБ і їх аналіз;
* визначення точок відповідальності систем, пристроїв і серверів ІС;
* формування переліку підсистем кожного підрозділу компанії з категоруванням критичної інформації та схемами інформаційних потоків.

Одним із найбільших за обсягом видом робіт серед тих, які проводяться при експертному аудиті, є збір даних про ІС шляхом інтерв'ювання представників замовника і заповнення ними спеціальних анкет.

Основна мета інтерв'ювання технічних фахівців – збір інформації про функціонування мережі, а керівного складу компанії – з’ясування вимог, які висуваються до системи ІБ.

Основні складові системи аудиту інформаційної безпеки

У загальному вигляді під час проведення аудиту ІБ вирішуються такі *завдання*:

* + - збір та аналіз первинних даних про організаційну та функціональну структури ІТС організації, необхідних для оцінки стану ІБ;
		- аналіз існуючої політики забезпечення ІБ на предмет повноти та ефективності;
		- аналіз інформаційних і технологічних ризиків, пов'язаних із реалізацією загроз ІБ;
		- тестові спроби несанкціонованого доступу до критично важливих вузлів ІТС та визначення уразливості в налаштуваннях захисту цих вузлів;
		- формування рекомендацій з розробки (або доопрацювання) політики забезпечення інформаційної безпеки на підставі аналізу існуючого режиму інформаційної безпеки;
		- формування пропозицій щодо використання існуючих та встановлення додаткових засобів захисту інформації для підвищення рівня надійності та безпеки ІТС організації.

Основна *мета* аудиту ІС – об'єктивно оцінити, наскільки поточний стан ІБ компанії відповідає висунутим вимогам і стандартам ІБ, а також завданням бізнесу щодо підвищення ефективності і рентабельності економічної діяльності компанії. Таким чином, завдання, які вирішуються при проведенні аудиту, можна розбити на дві групи:

1. Завдання, пов'язані з бізнес-процесами компанії.
2. Технічні завдання, пов'язані з особливостями функціонування мережі зв'язку, які відображають самі бізнес процеси.

У першій групі завдань аудиту піддаються бізнес-процеси, а в другій – технологічні процеси обміну інформацією, які відображають бізнес-процеси компанії. Деталізуючи завдання аудиту ІБ, можна виділити такі три важливі цілі, які реалізуються в процесі його проведення:

* Оцінка поточної безпеки функціонування мережі зв'язку та корпоративної інформаційної системи;
* прогноз ризиків, а також створення системи управління їх впливом на бізнес-процеси компанії;
* технічно коректний і економічно обґрунтований підхід до питання забезпечення безпеки інформаційних активів компанії.

Процедура аудиту ІБ складається з:

* ініціювання та планування;
* обстеження, документування та збору інформації;
* аналізу отриманих даних і уразливостей;
* вироблення рекомендацій;
* підготовки звітних документів і здавання робіт. В якості критеріїв аудиту ІБ використовуються:
* міжнародні, національні та галузеві стандарти;
* законодавча та нормативна база;
* внутрішні організаційно-розпорядчі документи організації;
* вимоги, сформульовані за результатами оцінки ризиків. Методика проведення аудиту ІБ включає:
* методи аналізу захищеності, включаючи тестування на вторгнення (penetration testing), аналіз конфігурації засобів захисту інформації, аналіз сценаріїв здійснення атак і використання списків перевірки (checklists);
* інтерв'ю зі співробітниками організації з використанням заздалегідь підготовлених і стандартизованих опитувальників;
* документування системи та аналізу ризиків з використанням спеціалізованого програмного забезпечення і шаблонів звітів;
* аналіз організаційно-розпорядчих документів з організації захисту інформації;
* оцінку процесів забезпечення інформаційної безпеки в організації, кваліфікації співробітників, знання ними своїх посадових обов'язків та ступеня їх обізнаності в питаннях інформаційної безпеки;
* оцінку достатності фізичних механізмів безпеки.

Аудит може бути внутрішнім і зовнішнім. Внутрішні аудити проводяться самою організацією або від її імені для різних внутрішніх цілей, наприклад для оцінки відповідності системи забезпечення ІБ встановленим вимогам. Зовнішні аудити проводяться сторонами, зацікавленими у діяльності організації, наприклад споживачами або іншими особами від їх імені, а також зовнішніми незалежними організаціями.

Не зважаючи на важливість забезпечення ІБ, аудит ІБ далеко не у всіх організаціях визнається критично необхідним процесом менеджменту ІБ. Усвідомлення необхідності аудиту ІБ формується в результаті аналізу проблем ІБ організації та подальшого визначення потреб організації в оцінці відповідності політик, процесів, процедур забезпечення відповідності рівня ІБ організації встановленим критеріям. Основні елементи процесу усвідомлення аудиту ІБ представлені на рис. 1.

До заходів процесу усвідомлення аудиту ІБ відносяться:

* формування потреби в розробці та менеджменті програми аудиту ІБ;
* формування вимог до програми аудиту ІБ;
* визначення ролей для розробки та менеджменту програми аудиту ІБ;
* визначення і виділення фінансових, кадрових та інфраструктурних ресурсів для розробки та менеджменту програми аудиту ІБ.

Під програмою аудиту ІБ розуміють сукупність кількох аудитів ІБ та інших перевірок ІБ (наприклад, самооцінок ІБ), запланованих на конкретний період часу і спрямованих на досягнення конкретної мети.

Потреба в розробці та менеджменті програми аудиту ІБ організації формується залежно від цілей вимірювань ІБ, які стосуються аудиту ІБ. Цілі аудиту ІБ визначаються керівництвом організації на основі бізнес-цілей і результатів діяльності організації, а також на основі інформації про внутрішнє і зовнішнє середовище організації, яка враховує оцінку ризиків ІБ. Такими цілями можуть бути: ідентифікація уразливостей системи забезпечення ІБ організації, оцінка відповідності ІБ організації встановленим критеріям ІБ, підвищення довіри до організації. При формуванні рішень щодо програми аудиту ІБ аналізуються вартість програми аудиту ІБ і вигода від її реалізації. Потреба в розробці та менеджменті програми аудиту ІБ документується у вигляді рішення керівництва організації та затверджується ним.

Вимоги до програми аудиту повинні містити: вимоги до обсягу програми аудиту ІБ, методології проведення аудиту, компетентності аудиторів, обізнаності співробітників організації щодо програми аудиту ІБ і вимоги до перегляду і коригування програми аудиту ІБ.

Комп’ютерний “вірус” – це програма, здатна створювати власні копії, необов’язково збіжні з оригіналом, та впроваджувати їх у файли, системні області комп’ютера, комп’ютерних мереж, а також чинити інші деструктивні дії. При цьому копії зберігають здатність подальшого розповсюдження. Такий паразитуючий програмний код зумовлює виконання несанкціонованих команд/програм на ураженому комп’ютері. Вірус розповсюджується у вигляді програм, файлів та макросів. Він впливає на цілісність інформації, програмне забезпечення та/або режим роботи обчислювальної техніки, що може призвести до відмови комп’ютера, виконання ним дій, прихованих від користувача, й відповідно, до порушування цілісності та доступності інформації або її витікання.

В сфері комп’ютерної вірусології застосовують наведені нижче терміни.

Захист програмних засобів – організаційні, правові, технічні та технологічні засоби, спрямовані на попередження можливих несанкціонованих дій по відношенню до програмних засобів та усунення наслідків цих дій.

“Профілактика” – систематичні дії експлуатаційного персоналу, мета яких – виявляти та усувати несприятливі зміни у властивостях та характеристиках використовуваних програмних засобів, зокрема перевіряти експлуатовані, збережувані й нові отримувані програмні засоби на наявність комп’ютерних вірусів.

Аудит – перевіряння нових отриманих програм спеціальними засобами, яке проводиться шляхом їхнього запускання у контрольованому середовищі.

“Вакцинування” – опрацьовування файлів, дисків, каталогів, що проводиться із застосовуванням спеціальних програм, які створюють умови, подібні до тих, що створюються певним комп’ютерним вірусом, і утруднює повторну його появу.

Несанкціонований доступ до програмних засобів – доступ до програм, записаних у пам’яті комп’ютера або на певному носії, а також до відображених даних у документації на ці програми, здійснений з порушуванням встановлених правил.

Найбільш критичним до впливу вірусів чинником є працездатність автоматизованих робочих місць користувачів комп’ютерних мереж та серверного комплексу: серверів електронної пошти, серверів доменів, DNS серверів, WINS серверів, DHCP серверів, а також серверів забезпечування безпеки даних.

Ймовірними вірусними загрозами працездатності автоматизованого робочого місця можуть бути:

* ушкодження комп’ютерним вірусом файлової структури операційної системи та прикладного програмного забезпечення автоматизованого робочого місця, наприклад ушкодження файлів Microsoft Office;
* ушкодження локальної системи роботи з електронною поштою або несанкціоноване її використання;
* знищення даних в енергонезалежній пам’яті комп’ютера (Flash BIOS, CMOS), що може призвести до відмови роботи комп’ютера.

Загрозами працездатності серверного комплексу мереж можуть бути:

* ушкодження комп’ютерним вірусом файлової структури операційної системи, прикладного та сервісного програмного забезпечення;
* порушування комп’ютерним вірусом цілісності та доступності інформації, яка зберігається та опрацьовується на серверах;
* несанкціоноване витікання інформації з комп’ютерної мережі;
* перенавантаження комп’ютера або заблокування обчислювальних ресурсів, спричинювані діями комп’ютерного вірусу.

Практика свідчить, що комп’ютерні віруси наносять значних фінансових збитків. Для протистояння загрозам зараження в галузі телекомунікацій створюють системи антивірусного захисту.

Мета створення системи антивірусного захисту – забезпечення захисту робочих станцій та серверів локальних обчислювальних мереж від деструктивного впливу комп’ютерних вірусів за мінімальних видатків на адміністрування, ресурси обчислювальної техніки та телекомунікаційне устаткування.

Система антивірусного захисту має гарантувати достатній рівень захищеності від комп’ютерних вірусів, необхідний для забезпечування цілісності, доступності та спостережуваності опрацьовуваної в інформаційно- обчислювальній мережі інформації, потрібної для забезпечування життєдіяльності галузі.

Система антивірусного захисту призначена для організації та проведення обстежування, виявляння й усування комп’ютерних вірусів у програмних засобах та їхніх компонентах силами служби захисту інформації на головних етапах життєвого циклу програм: придбання та здачі до експлуатації, архівування та власне технічної експлуатації обчислювальних мереж. Комплексна система антивірусного захисту використовується службою захистуінформації для забезпечування інформаційної безпеки в сегментах корпоративної мережі передавання інформації, локальних обчислювальних мережах, автоматизованих робочих місцях (АРМ).

Випробування програмного забезпечення на наявність комп’ютерних вірусів проводять на спеціально устаткованому програмно-апаратному випробувальному стенді, в складі якого мають бути необхідні технічні та програмні засоби, у тому числі антивірусні програми.

Служба захисту інформації, яка проводить перевірку програмного забезпечення на наявність вірусів, визначає мету та обсяг випробувань, підтримує випробувальний стенд у працездатному стані і має не припускати проникнення вірусів до програм та даних до початку проведення випробувань.

Служба захисту інформації має забезпечувати весь процес перевірки необхідними обчислювальними технічними та програмними засобами, а також призначати спеціально навчених співробітників для проведення випробування. Служба захисту інформації призначає постійного представника, який отримує певні повноваження і несе постійну відповідальність за виконання вимог цих рекомендацій.

При дослідженні програмного забезпечення на наявність комп’ютерних вірусів використовують дві основні групи методів виявлення вірусів і захисту програм від них: програмні та апаратно-програмні. *До програмних методів* належать сканування; виявлення змін; евристичне аналізування; резидентна «сторожа»; вакцинування програмного забезпечення. *Апаратно-програмні методи* базуються на здійсненні будь-яких із зазначених вище програмних методів захисту від вірусів за допомогою спеціальних технічних пристроїв. У конкретних дослідженнях можуть бути використані способи та засоби виявлення комп’ютерних вірусів, які реалізовують один із розглянутих методів або їхні комбінації.

Метод *сканування* полягає в тому, що спеціальна антивірусна програма, яка називається с к а н е р о м, послідовно переглядає перевірювані файли в пошуках так званих “сигнатур” відомих вірусів. Під с и г н а т у р о ю розуміють унікальну послідовність байтів, яка належить конкретному відомому вірусові і не зустрічається в інших програмах. Сканування є найпростішим програмним методом пошуку вірусів. Антивірусні програми-сканери можуть гарантовано виявити лише вже відомі віруси, які були вивчені і для яких була визначена сигнатуру. Антивірусні програми-сканери, які можуть вилучати виявлені віруси, називають п о л і ф а г а м и. Для ефективного використання антивірусних програм, які реалізовують метод сканування, слід постійно оновлювати їх, отримуючи найостанніші версії.

Метод *виявлення змін* полягає в тому, що антивірусна програма спочатку запам’ятовує характеристики всіх областей диска, які можуть бути піддані нападові вірусів, а потім періодично перевіряє їх. Якщо зміни цих характеристик будуть виявлені, то така програма повідомляє користовачеві, що, можливо до комп’ютера потрапив вірус. Метод виявлення змін базується на використанні антивірусних програм-ревізорів, які запам’ятовують у спеціальних файлах образи головного завантажувального запису, завантажувальних секторів логічних дисків, параметри усіх контрольованих файлів, інформацію щодо структури каталогів та номери поганих кластерів диска. Можуть бути перевірені інші характеристики комп’ютера, обсяг встановленої оперативної пам’яті, кількість підімкнених дисків та їхні параметри.

Програми-ревізори потенційно можуть виявляти які завгодно віруси, навіть раніше невідомі. Але слід враховувати, що не всі зміни спричиняються вторгненням вірусів. Завантажувальний запис може змінюватись при оновленні операційної системи, певні програми записують змінювані дані всередині свого виконавчого файла. Файл AUTOEXEC.BAT може змінюватись при встановленні нового програмного забезпечення. Програми-ревізори не виявляють випадків, коли користувач записує до комп’ютера новий файл, заражений вірусом. Але якщо вірус заразить і інші програми, вже враховані ревізором, то він буде виявлений. Є додаткова можливість програм-ревізорів щодо здатності відновлювати змінені (заражені) файли та завантажувальні сектори на підставі раніш запам’ятованої інформації. Антивірусні програми- ревізори неможливо використовувати для виявлення вірусів у файлах документів, тому що ці файли повсякчас змінюються. Для контролю таких файлів слід використовувати програми-сканери або евристичне аналізування.

Метод *евристичного аналізування* реалізовується за допомогою антивірусних програм, які перевіряють інші програми та завантажувальні сектори дисків та дискет, намагаючись виявити в них код, притаманний комп’ютерним вірусам. Приміром, евристичний аналізатор може виявити, що у перевірюваній програмі є наявний код, який встановлює резидентний модуль у пам’яті. Евристичне аналізування дозволяє виявляти раніше невідомі віруси. До головних недоліків евристичного методу належать:

* принципово не може бути виявлено всі віруси;
* можливі хибні сигнали щодо виявлення вірусів у програмах, які використовують вірусоподібні технології (приміром антивіруси).

У методі *резидентної сторожі* використовуються антивірусні програми, які постійно перебувають в оперативній пам’яті комп’ютера й відстежують усі підозрілі дії, виконувані іншими програмами. Резидентна сторожа повідомляє користувачеві про те, що певна програма намагається змінити завантажувальний сектор твердого диска або дискети, а також виконуваний файл. Резидентна сторожа дозволяє автоматично перевіряти всі задіювані програми на зараження відомими вірусами. Процес завантаження програми при цьому уповільнюється. Резидентна сторожа має багато недоліків, які роблять її малопридатною до використання. Резидентна сторожа постійно перериває роботу користувача – і він кожного разу вимушений з’ясовувати, чим це спричинено: комп’ютерним вірусом, легальною командою чи програмою. Багато програм, не заражених комп’ютерними вірусами, можуть виконувати дії, на які реагує резидентна сторожа. Окрім того, вони зменшують обсяг пам’яті, доступний для інших програм.

*Вакцинування* встановлює спосіб захисту будь-якої конкретної програми від вірусів, за якого до цієї програми долучається спеціальний модуль контролю, що стежить за її цілісністю. При цьому перевіряються контрольна сума програми або певні інші її характеристики. Якщо вірус заражає вакцинований файл, модуль контролю виявляє зміну контрольної суми файла і повідомляє про це користувача. Метод вакцинування має той недолік, що є можливість оминання такого захисту за використання віруса так званої “стелс- технології”. Певні програми після вакцинації можуть працювати некоректно.

*Апаратно-програмні* методи захисту програмного забезпечення від комп’ютерних вірусів реалізовуються за допомогою спеціалізованого пристрою – контролера, котрий вставляється в один із портів розширення комп’ютера, і спеціального програмного забезпечення, яке керує роботою цього контролера і здійснює один або декілька програмних методів, зазначених вище.

Апаратно-програмні методи є найбільш надійним способом захисту від зараження вірусами.

Система антивірусного захисту виконує функції із захисту серверів та робочих станцій від атак комп’ютерних вірусів та перекриває найбільш імовірні варіанти проникнення вірусів до мережі. Система антивірусного захисту забезпечує:

* можливість невпинного захисту об’єктів інформаційно- обчислювальної мережі відповідно до встановлених вимог та політики безпеки;
* можливість автоматизованого блокування проникнення комп’ютерних вірусів з усіх можливих джерел;
* принципи мінімальної достатності, автоматичного функціонування та централізованого захищеного віддаленого керування антивірусним програмним забезпеченням і має доповнюватися адміністративними заходами. Також система антивірусного захисту не повинна істотно знижувати продуктивність об’єктів інформаційно-обчислювальної мережі;
* роботу з повним набором існуючих операційних систем для серверів та робочих станцій інформаційно-обчислювальної мережі;
* “лікування” усіх відомих комп’ютерних вірусів із занесенням інформації про це у відповідні протоколи роботи для забезпечування моніторингу роботи. В разі підозри на зараження невідомими комп’ютерними вірусами та неможливості лікування забезпечується блокування доступу користувачів до цієї інформації;
* можливість оперативного повідомлення відповідальних осіб щодо виникнення критичних або особливих ситуацій у мережі, тобто: виявлення вірусу, збої у системі оновлень, змінення налаштовувань системи антивірусного захисту. Також передбачено генерацію керувальних SNMP-послідовностей з метою візуалізації контрольованих подій у системі мережного керування;
* автоматизоване централізоване оновлення антивірусного програмного забезпечення;
* гнучке масштабування за появи нових об’єктів антивірусного захисту;
* ліцензійність та підтримування постачальниками застосовуваного антивірусного програмного забезпечення.

Структурно систему антивірусного захисту зорганізовано за ієрархічним рівневим принципом. Ефективний захист від комп’ютерних вірусів забезпечується комплексною системою антивірусного захисту, котра складається з чотирьох антивірусних рівнів і передбачає встановлення антивірусного програмного забезпечення на об’єкти, які є найбільш піддавані вірусному зараженню.

Використані джерела:

1. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. – К.: КУБГ, 2019. – 218 с.

2. Аудит та управління інцидентами інформаційної безпеки: навч.посіб./ [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.