1. *Петриашвили Г. Г.* Моделирование системы функционирования книжно-журнальных изданий с переменным информационным содержанием / *Г. Г. Петриашвили* // Моделювання та інформаційні технології. — К., 2007. — Вип. 41. — С. 188–194.
2. *Цаленко М. Ш.* Моделирование семантики в базах данных / *М. Ш. Цаленко*. — М. : Наука, 1989. — 288 с.
3. *Гладкий А. В.* Формальные грамматики и языки / *А. В. Гладкий*. — М. : Наука, 1973. — 383 с.
4. *Гуйванюк Н. В.* Семантична структура тексту / *Н. В. Гуйванюк, О. С. Гнатчук, М. В. Нечипорук* // Навч.-метод. посіб. (Чернів. нац. ун-т ім. Ю. Федьковича). — Чернівці : Рута, 2000. — 131 с.
5. *Дурняк Б. В.* Моделі семантичного аналізу з використанням формальних граматик / *Б. В. Дурняк, В. І. Сабат* // Зб. наук. праць (ІПМЕ ім. Г. Є. Пухова НАН України). — К., 2003. — Вип. 21. — С. 173–180.
6. *Соломатин Н. М.* Информационные семантические системы / *Н. М. Соломатин*. — М., 1989. — 127 с.

Поступила 6.09.2010р.

УДК 004.921

Б. В. Дурняк, Л.Є.Шведова

ЗАСОБИ СИСТЕМ ЗАХИСТУ ДОСТУПОМ ТА МОДЕЛІ КЛАСИФІКАЦІЇ РІВНІВ ЗАХИСТУ

Підставою для використання тих чи інших засобів захисту доступу до інформаційних систем є наявність інформації про існуючі небезпеки для цих систем, про поточний стан рівня безпеки системи та про загрози, що характеризують стан можливості виникнення атак на систему.

Одним з внутрішніх механізмів визначення стану безпеки є аудит безпеки. Основною задачею аудиту є поточне моніторування активності користувачів і реєстрація подій, що відбуваються в системі. Кожна подія, що відбувається в системі, записується в контрольний реєстр. В такому аудиторському записі знаходиться інформація про суб'єкти та об'єкти, які приймали участь у події. Прикладами подій, що записуються в контрольні реєстри можуть бути такі події:

— реєстрація користувача;
— читання;
— запис;
— зміна параметру системи захисту (наприклад, зміна пароля користувача) тощо.

Інформація з контрольного реєстру використовується для відслідкову-

вання інцидентів, пов'язаних із забезпеченням або реконструкцією даних, що виявились у результаті інциденту знищеними чи пошкодженими.

Для викривання спроб порушення безпеки системи та з метою впровадження до помилки потенційного інтруза використовуються засоби для створення так званих щілин в системі, що захищається, які легко виявити ззовні і які, насправді є добре моніторованими слабими місцями, що називаються загрозами. Такі засоби прийнято називати пастками для користувачів [1]. Інформація, яку збирає така пастка, використовується для вдосконалення системи захисту. Існують наступні методи створення системи пасток:

— комп'ютер зі стандартною операційною системою, який під'єднують до мережі Інтернет з ціллю притягування до себе інтрузів;
— програмні системи, які емулюють функції різних реальних систем;
— системи, які створюють ілюзію існування в інформаційних системах великої кількості загроз для безпеки.

Дві базові вимоги відносно таких систем полягають у вбудовуванні можливості відслідковування всіх дій інтрузів та гарантія не виявлення реальних цілей для яких такі системи створені.

Щораз частіше стандартні механізми аудиту в операційних системах є доповнені спеціальними програмами, які відслідковують активність користувачів. Такі програми виконують цілий ряд функцій, до яких відносяться:

— реєстрація інформації про сторінки WWW, які відвідуються користувачами та реєстрація часу, який користувачі затрачують на це;
— виконують аналіз суті електронної пошти, що висилається та відбирається користувачем;
— блокування доступу до вибраних місць в Інтернеті;
— реєстрація різних форм активності користувачів (використання комп'ютерних ігор, використання програмних засобів фірми для тривалих потреб).

Черговим класом засобів захисту даних є антивірусні системи. Найбільш успішна методика боротьби з комп'ютерними вірусами є відповідна профілактика. Вона полягає у тому, щоб не допустити віруси до системи. Очевидно, що таким способом забезпечити безпеку є неможливо, але це дозволяє відгородити велику кількість вірусів, які могли б досягнути до системи. Базовим елементом такої профілактики є запуск програмного забезпечення в комп'ютері, яке є безпечним, протестованим антивірусними програмами. Антивірусне тестування повинно проводитись з усіма цифровими носіями даних та файлами, що передаються по комп'ютерній мережі [2]. Антивірусні програми використовують цілий ряд методів виявлення вірусів до яких можна віднести такі методи та підходи:

— методи, що полягають у відшукуванні сигнатур, що являє собою відшукування в файлі, який тестується послідовностей кодів програми, які відповідають кодам програм, що реалізують віруси (відшукування специфічних послідовностей байтів), у більш розвинутих антивірусних програмах для виявлення вірусів у тестованих файлах

використовуються експертні системи та нейронні мережі;

— метод, що полягає у перевірці інтегральності програми, яка перевіряється, при цьому перевіряються актуальні параметри відповідної програми, наприклад, довжина програми, контрольна сума коду програми, ці дані порівнюються з величинами параметрів, які знаходяться в базі даних про цю програму, визначені в період, коли відповідна програма була чиста від вірусів;
— на основі використання евристичного аналізу, який полягає у аналізі поведінки програми і виявлені спроб інфікування системи, наприклад, шляхом ініціації системних переривань.

Більшість антивірусних систем поєднує в собі кілька різних методів виявлення вірусів з ціллю збільшення ефективності їх дії. Антивірусні програми можуть працювати в режимі резидента, або при їх ініціації. Програми, що працюють в режимі резидента запускають файли, що завантажуються на диски комп'ютера. Програми, що запускаються, перевіряють пам'ять і актуальні записані на диску файли.

Розвиток технології генерування вірусів та технологій захисту відбувається в однаковому темпі. Віруси, як і антивірусні програми, стають все більш складними. кількість нових вірусів систематично зростає. Тим не менше, відчувається недостатність антивірусних систем, які могли б викривати нові віруси, що тільки з'являються в інформаційних системах. Це зумовлюється тим, що антивірусні засоби з'являються в наслідок появи нових вірусів. Тому, при реалізації антивірусного захисту надзвичайно актуальною є задача регулярного поповнення баз даних, які використовують антивірусні системи у своїй роботі.

Наступна проблема захисту, що існує і потребує розв'язку при побудові систем захисту є проникаюче електромагнітне випромінювання, яке може приводити до уявлення даних, що передаються по системах зв'язку в комп'ютерних мережах. Для захисту інформації перед такою небезпекою виконуються такі процедури та створюються наступні засоби:

— інсталюється та використовується обладнання, яке характеризується низькими рівнями електромагнітного випромінювання, прикладом одного з стандартів, що передбачає подібні вимоги стандарт TEMPEST;
— екранування електромагнітного випромінювання створеного інстальованими пристроями, наприклад, комп'ютерами, друкарками, спеціальними захисними корпусами або екранованими приміщеннями, використанням екранованих кабелів і з'єднань, або використанням світловодів;
— обмеженням до мінімально можливих довжин кабелів, що використовуються для передачі даних в інформаційних системах;
— фільтрування живлення;
— необхідним заземленням пристроїв;
— використанням спеціальних комбінацій знаків для виводу на екрани

дисплеїв тексту;
— електромагнітне маскування, яке полягає у впроваджені сигналів, які спотворюють сигнали, або впровадження сигналів, що мають структуру подібну до структури вторинної емісії.

Важливим елементом захисту такого типу небезпек є дослідження реальних відстаней, на яких інформація, яка знаходиться у випромінювальному сигналі може бути відібрана. Дані про такі дослідження повинні являти таємницю у рамках системи захисту.

Наступним засобом захисту, що використовуються для захисту доступу є шлюз безпеки, який являє собою систему proxi і firewall. Такий шлюз безпеки часто вміщає і реалізує функції NAT та функції VPN. Шлюз безпеки являє собою засіб блокування, який охороняє приватну внутрішню комп'ютерну мережу від прослуховування, аналізу та моніторингу, а також від атак з мережі Інтернет. Переважно шлюз безпеки є невід'ємною частиною інформаційної системи, що з'єднується з мережею Інтернет. Такий шлюз також використовується для відокремлення різних підмереж у рамках однієї внутрішньої корпоративної мережі. Власні шлюзи безпеки захищають приватні комп'ютери користувачів, що використовують Інтернет [3]. До базових функцій шлюза захисту відносяться:

— перехоплення всієї інформації, що передається між приватною мережею та мережею Інтернет і прийняття рішення чи пакет даних, або з'єднання, може бути пропущений;
— аутентифікація користувачів;
— укриття IP-адрес комп'ютерів з приватної мережі, або реалізація функції NAT;
— перетворення електронної пошти;
— відслідковування та реєстрація всіх подій;
— створення віртуальних приватних мереж з шифруванням трансмісії між вузлами, або реалізація функції VPN;
— генерування сигналів тривоги для мережі, що охороняється та мереж, з якими є відповідні узгодження.

Функції перехоплення пакетів реалізує firewall. На основі визначеної політикою безпеки послідовності правил фільтрування, firewall затримує, або пропускає певні пакети. Правила фільтрування складаються з критеріїв та опису дій, які у рамках правил являють опис умов, при яких може бути виконана відповідна дія. Функції, основними з яких є блокування чи пропускання пакетів, описують дії, які реалізуються у випадку виконання критеріїв та умов вибору. Критеріями вибору можуть бути адреси джерела та адреси приймача пакетів, тип протоколу, номери портів джерел і приймачів, напрямок трансмісії [4].

Для кожного пакету реалізується аналіз послідовності чергових правил фільтрування. Якщо пакет виконує умови правила, або відповідає його критеріям, то виконується функція, яка записана у відповідному правилі. Якщо пакет не виконує умови правила і не відповідає критеріям, то

перевіряється наступне за списком правило. Останнє правило у послідовності всіх правил firewall повинно полягати у блокуванні усіх пакетів. Прийнято розрізняти пасивні та активні фільтри. Пасивні фільтри аналізують кожен пакет незалежно від інших пакетів. Активні фільтри зберігають контекст сесії, завдяки чому стає можливим фільтрування пакетів, що пересилаються за допомогою безадресних протоколів UDP.

Аутентифікація користувачів з двох сторін шлюзу безпеки виконується так званими брамами прикладних частин програмних засобів, які прийнято називати аплікаціями, з серверами proxi. Для кожного типу аплікації необхідно використовувати окремий сервер. Proxi-сервер контролює обмін даними між двома мережами, обмінюється пакетами від імені користувача мережі із серверами зовнішньої мережі.

Користувач, який хоче скористатися Інтернет-послугою з другого боку шлюзу, відносно мережі Інтернет, повинен зареєструватись не proxi-сервері. Після аутентифікації і підтвердження відповідних повноважень, користувач отримує доступ до аплікації з другого боку шлюзу.

Шлюз безпеки не гарантує повного захисту приватної мережі. Безпека приватної мережі може бути порушена користувачем внутрішньої мережі при з'єднанні з мережею Інтернет, що реалізується поза відповідний шлюз. Крім того, у зв'язку із необхідністю захисту від вірусів, необхідно у шлюзи включити додаткове програмне антивірусне забезпечення.

Шлюз безпеки охороняє доступ до даних, але не захищає від операцій на тих даних.

Для проведення повноцінної політики безпеки в широкому значенні цього терміну, необхідне також використання системи виявлення вторгнень в систему, що охороняється (IDS). Система викривання вторгнень використовується для виявлення спроб атак інформаційної системи ззовні а також для виявлення спроб виходу за встановлені обмеження, при використанні засобів мережі вповноваженим на це користувачем, які, у відповідності з прийнятою термінологією, будемо називати «надвикористанням» засобів. Система детекції інтрузів (IDS) функціонує, на фоні роботи інформаційної системи, безперервно у відповідності з вибраними дисциплінами сумісного функціонування. Система IDS інформує адміністратора про різні події, які визначаються як підрозділи з точки зору можливості їх негативної дії на систему, яка захищається. Значна частина цих систем функціонує на основі аналізу записів в аудиторських документах, які заповнюються операційною системою. Крім того, такі системи можуть реалізовувати власні додаткові процедури аудиту. Залежно від обсягу аналізу реєстрів аудиторських документів, можна виділити такі системи IDS:

— одномісні, що проводять аналіз аудиторських документів з реєстрів одного хосту;
— багатомісні, що проводять аналіз аудиторських документів з великої кількості хостів;
— мережні, що аналізують інформацію про рух в мережі а також

аналізують реєстри аудиту з окремих хостів, або з багатьох хостів.

Існує дві моделі викривання вторгнень:

— модель з викриванням аномалій;
— модель з викриванням надвикористань.

В системах, що використовують модель викривання вторгнень на основі виявлення аномалій, вторгнення викривається на основі пошуку окремих подій і послідовностей подій, які виходять за рамки нормального профілю користувача системи. Нормальний профіль визначається на основі використання статистичного аналізу особливостей проявів в рамках системи користувача, на основі аналізу реєстрів аудиту, а також на основі іншої інформації до якої можна віднести наступне:

— завантаження процесора;
— завантаження дисків;
— завантаження оперативної пам’яті;
— активності користувача;
— кількості сесій, які відкривались користувачем.

Нормальний профіль споживача повинен постійно обновлятися, щоб він не втрачав своєї актуальності.

В системах IDS, які використовують модель виявлення надвикористань, проводиться порівняння послідовностей подій з множиною сигнатур, що знаходяться в пам’яті і описують відомі техніки реалізації атаки на інформаційну систему. Успішність цього типу систем обмежується влаштуванням, що виконуються за допомогою відомих атак.

Важливими засобами є засоби, що використовуються для тестування систем безпеки та виявлення незахищених проходів до інформаційної системи у системі захисту. Засоби цього типу складають досить велику групу різних інструментів. До засобів цього типу можна віднести:

— прості аналізатори версій програм і пакетів, що орієнтовані на проведення ремонтних робіт;
— універсальні сканери забезпечувальних засобів;
— сканери портів;
— сканери модемних каналів;
— аналізатори системних реєстрів;
— аналізатори списків контролю доступу;
— аналізатори засобів безпеки баз даних;
— аналізатори рівня безпеки паролів користувачів;
— сканери безпеки для вихідних, або початкових версій програмних систем;
— генератори пакетів для тестування забезпечувальних засобів.

Інформаційні системи піддаються безперервним змінам. Наприклад, додаються нові користувачі, які використовують віддалений доступ, що призводить до появи нової небезпеки зумовленої можливістю допущення помилок, при конфігурації системи.

При використанні засобів для тестування необхідно пам’ятати, що тести

забезпечень безпеки, або просто забезпечень, повинні проводитись систематично. Недостатньо у таких випадках проводити тести після інсталяції системи, або тільки після переконфігурації. З іншого боку , часте виконання тестів забезпечень є досить важке (наприклад, якщо його проводити раз на один день роботи системи).

База даних сканера вміщає систематично обновлюваний список потенційних загроз. Сканери забезпечень відшуковують в системі проходи, які являють собою загрози. Деякі сканери автоматично аналізують безпеку, або міру захисту на межі між системою, що охороняється, та зовнішнім середовищем, а також — міру захисту, або міру безпеки внутрішньої мережі.

Тести можуть охоплювати загрози у таких типів програм:

— операційних систем;
— мережевих систем;
— навігаторів WWW;
— шлюзів безпеки;
— ремонтних пакетів.

Результатом аналізу, реалізованого тестовими системами, є запам'ятовування висновків тестування у базі даних, приготування звітів, оцінка ризику та рекомендації з реалізації способів усунення виявлених неполадок у забезпеченні. Виявлені неполадки можуть бути автоматично усуненими шляхом переінсталювання відповідного ремонтного пакету. Більш сучасні засоби цього типу можуть тестувати велику кількість систем одночасно з ціллю виявлення потенційних загроз, що не становлять небезпеки, але разом із великою кількістю інших потенційних загроз, можуть викликати суттєві проблеми.

Виконуючи детальний аналіз, сканер генерує велику кількість даних (список потенційних загроз може вміщати сотні чи тисячі елементів), тому важливим аспектом його функціонування є спосіб представлення результатів відповідного аналізу. Оскільки не можна приймати, що результати тестування будуть завжди аналізуватися спеціалістом з безпеки, важливим є те, щоб рапорт мав зрозумілу форму, яка б помогла адміністратору інформаційної системи легко його інтерпретувати. Окрім того виявлені загрози повинні бути впорядкованими у рапорті таким чином, щоб найнебезпечніші із них були представленими в першу чергу.

Використання засобів захисту повинно відповідати певним принципам, які необхідно виконувати, щоб їх використання було найбільш ефективним. Важливим фактором, який впливає на безпеку, є виконання принципів використання засобів захисту. До таких принципів можна віднести:

— визначення функцій захисту у цілому процесі створення, впровадження та експлуатації інформаційної безпеки;
— використання систем і механізмів, які є перевіреними та сертифікованими незалежними установами;
— стандартизація рішень;
— неперервність використання;

— правильне впровадження;
— правильна конфігурація з постійним контролем;
— узгодження з користувачем, оскільки відсутність узгодженості може призвести до виникнення неполадок у процесі використання;
— максимально можлива автоматизація, що дозволяє звільнити користувачів та адміністраторів від необхідності виконання додаткових процедур, що пов'язані з охороною, оскільки участь людей у виконанні тих чи інших процедур у найбільшій мірі зумовлює можливість виникнення помилок і неполадок;
— інтегрування функцій безпеки з іншими елементами інформаційної системи (ініціація антивірусних програм, криптографічних механізмів в операційних системах);
— узгоджена співпраця між різними механізмами безпеки, наприклад, система виявлення вторгнень після викриття атаки, повинна зв'язатись із шлюзом безпеки, що блокує джерело атаки;
— нагляд над способами використання засобів захисту, наприклад, контроль складності використання паролів для користувачів;
— актуалізація засобів охорони, що дозволяє забезпечити попередження нових загроз, зміну обмежень;
— кожне неправильне, неочікуване відхилення від норми функціонування інформаційної системи повинно бути піддане аналізу з ціллю виявлення причин відповідних відхилень;
— розробка документації системи безпеки;
— систематичний контроль стану безпеки, який реалізується шляхом виконання тестів, моделювання вторгнень та інших негативних дій на систему;
— розроблення та використання політики безпеки, яка передбачає певну поведінку користувачів та їх відповідальність за допущені помилки та неуважність при роботі з інформаційною системою.

Вищенаведені принципи можуть бути розширені та уточнені. Вони повинні у тій, чи іншій мірі мати своє відображення у проекті політики безпеки, який є базовим документом і відображає всі особливості реалізації функцій захисту в інформаційній системі.

1. *Piotrowski M.* Ochrona sieci komputerowych za pomoca technolofii honeypot. — Warszawa : MIKOM, 2007/
2. *Козлов Д. А.* Энциклопедия компьютерных вирусов / *Д. А. Козлов, А. А. Парандовский, А. К. Парандовский.* — М. : СОЛОН-Р, 2001.
3. *Cheswick W. R.* Firewall and Internet Security. Respelling the Wily Hacker / *W. R. Cheswick, S. M. Bellavin, A. Rubin,* 2003.
4. *Польман Н.* Архитектура брандмаэров для сетей предприятий / *Н. Польман, Т. Кразес.* — М. : Изд. дом «Вильямс», 2003.

Поступила 15.09.2010р.