в RSA – функции генерации модуля преобразования N, функции генерации ключей X и Y, функции прямого и обратного преобразований;

в ГОСТ 28.147 – операции шифрования и дешифрования;

в ГОСТ 34.310-95 – функции генерации общесетевых параметров P, Q, A, функции генерации ключей X и Y, функции наложения и проверки подписи;

в ГОСТ 34.311-95 – функции формирования хеш.

Далее необходимо проверить работу центров сертификации и всей системы в комплексе. Для этого необходимо проверять сначала простейшие функции, выполняемые центром. Сначала нужно установить только центр верхнего уровня и полностью протестировать его работу. Затем наращивают и постепенно усложняют функции, реализуемые центрами сертификации. Далее создается подчиненный центр и тестируется их совместная работа. После дальнейшего создания и тестирования центра третьего уровня можно утверждать о правильности работы системы с неограниченным количеством уровней. Тестируются также удаленные генераторы ключей и их работа совместно с одним из центров. После тестирования работы генератора ключей с одним из центров можно утверждать о правильности работы генератора ключей с любым из центров. Создаются рабочие места в центре и у клиентов, тестируется работа рабочих мест друг с другом. На основании прохождения всех этапов тестирования можно делать вывод о правильности работы системы в целом.

Выводы

Задача создания многоуровневого центра сертификации является актуальной на сегодняшний день, поскольку существуют предприятия и организации с многоуровневой структурой управления. Рассмотрены основные принципы построения многоуровневого центра сертификации. Рассмотрена модель проектирования программного обеспечения Microsoft Solutions Frames, согласно которой была проведена разработка многоуровневого центра управления и сертификации. Описаны цели и задачи создания такого центра, обоснована необходимость его создания. Определены сферы применения центра сертификации. Определены основные функции, которые должен выполнять центр сертификации. На этапе планирования определены стандарты и криптоалгоритмы, которые должны быть использованы в программном обеспечении, обоснованы причины применения именно этих алгоритмов.

Рассмотрена структура ключей в многоуровневом центре сертификации, которая состоит из главных ключей, рабочих ключей, сеансовых ключей. Описано функциональное назначение ключей каждого типа. Рассмотрена работа многоуровнего центра сертификации, построенная на критериях выбора ключевых параметров и оценки качества ключевых данных. Выполнен анализ протоколов импортирования, экспортирования ключей. Приведен состоятельный протокол направленной передачи сертификатов и сообщений по открытому каналу связи.

На этапе реализации и тестирования обоснован выбор программных средств для создания пакета инсталляции системы. Описаны принципы тестирования программного продукта на соответствие его стандартам и корректной его работы.

УДК 681.3

МОДЕЛЮВАННЯ ДОСТУПУ ТА КАНАЛІВ ВИТОКУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Анатолій Антонюк, Віктор Жора*

Інститут програмних систем Національної Академії наук України

**Фізико-технічний інститут НТУУ «КПІ»*

Анотація: **Розглянуто множину можливих доступів до інформації в автоматизованих системах. За допомогою поняття каналів витоку подано формальні визначення загроз інформації.**

Summary: **The report deals with the multitude of possible accesses to information in automated systems. The formal definitions of information threats are proposed using the concept of leakage channels.**

Ключові слова: **Інформація, конфіденційність, цілісність, доступність, спостереженість, захист, доступ, канал витоку, послуга.**

І Вступ

В [1–4] сформульовано фундаментальні властивості захищеної інформації (ФВЗІ), що визначають її цінність: конфіденційність, цілісність, доступність і спостереженість.

Якщо розглядати загрози інформації з точки зору їх будь-якої небажаної дії на будь-яку з цих властивостей і можливого їх порушення, то в автоматизованих системах (АС) можна розрізняти наступні класи загроз інформації:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності або відмова в обслуговуванні;
- порушення спостереженості або керованості.

Аналіз загроз є одним з найбільш важливих питань при побудові захищених АС. Розвиток теорії та практики захисту інформації (ЗІ) показує, що на сьогоднішній день визначаються наступні основні шляхи здійснення наведених загроз в АС [5]:

- втрата контролю над системою захисту інформації (СЗІ);
- канали витоку інформації.

Всі інші способи реалізації загроз так чи інакше зводяться до них. Захист АС від наведених загроз забезпечується за допомогою цілого ряду послуг [3], принципи реалізації яких визначаються політикою безпеки.

Якщо СЗІ перестає адекватно функціонувати, то, звичайно, може реалізуватися несанкціонований доступ (НСД) до інформації. Втрата керування СЗІ може бути реалізована внаслідок будь-яких порушень безпеки. Зрозуміло, що в реальному житті можливі їх комбінації. Вони можуть бути також причиною виникнення прихованих каналів витоку інформації. Прихований канал витоку інформації або просто канал витоку – це спосіб отримання інформації за рахунок використання шляхів передачі інформації, які присутні в АС, але не керуються або не спостерігаються СЗІ. Канали витоку характеризують ситуацію, коли або проектувальники не змогли попередити НСД, або СЗІ не в змозі розглядати такий доступ як заборонений.

Серед каналів витоку інформації небезпечними слід вважати ті, що виникають внаслідок реалізації легального або нелегального доступу користувачів і/або процесів до об'єктів АС із захищеною інформацією. Канали такого типу можуть виникнути, якщо доступ реалізується суб'єктами, які не мають на це повноважень. В [5] розглянуто формальну модель таких доступів, що дозволяє в подальшому моделювати наведені вище загрози інформації. Однак детальний аналіз моделі показує, що для більш точного формального опису наведених каналів слід враховувати структуру множини можливих доступів.

Отже, спочатку наведемо деякі відомості з моделювання систем, що розглядаються нижче.

Модель АС розглядається у вигляді скінченої множини елементів. Далі використовуються такі основні поняття як об'єкт, суб'єкт, загроза, визначення яких вважаються відомими [6]. Для визначення поняття доступу введемо поняття потоку інформації між двома об'єктами [7].

Визначення 1. Потоком інформації між об'єктами O_i і O_j назвемо довільну операцію над об'єктом O_j, що реалізується суб'єктом S_k, пов'язаним з об'єктом O_i.

Визначення 2. Доступом суб'єкта S_i до об'єкта O_j називається породження потоку інформації між деяким об'єктом O_i і об'єктом O_j.

Враховуючи наведені вище загрози інформації, зручно множину всіх потоків поділити на декілька підмножин: підмножина, що пов'язана з несанкціонованим доступом для ознайомлення з інформацією, підмножина, що пов'язана з можливістю несанкціонованої модифікації інформації, підмножина потоків спостереження за процесами обробки інформації, підмножина, що характеризує всі легальні доступи. Тоді на основі такого поділу можна визначити аналогічний поділ множини всіх можливих доступів до інформації. Позначимо множину всіх видів доступів через R і вважаємо, що $|R|<\infty$.

Отже, в АС множина доступів R представляється у вигляді

$$R = R_1 \cup R_2 \cup R_3,$$

де R_1 – множина доступів, за якими можливе ознайомлення з інформацією;
R_2 – множина доступів, за якими можлива модифікація інформації;
R_3 – множина доступів, за якими можливе спостереження за обробкою інформації, тобто спостереження за об'єктами.

Така структуризація множини всіх доступів дозволяє досить точно визначити основні загрози інформації в АС.

Вважається далі, що час є дискретним і приймає значення з множини N={1, 2,... }, тобто $t \in N$. Якщо p – деякий доступ і $p \subseteq R$, то доступ p активізованого (тобто такого, що може перетворювати інформацію)

суб'єкта S до об'єкта O позначимо через $S \xrightarrow{p} O$. Якщо в деякий проміжок часу реалізована послідовність доступів

$$U \xrightarrow{a} S_1 \xrightarrow{a} S_2 \xrightarrow{a} \ldots \xrightarrow{a} S_k \xrightarrow{p} O,$$

то вважається, що здійснено доступ $S \xrightarrow{p} {}^{*}O$ від імені суб'єкта S до об'єкта O (через a тут позначено процес активізації). Позначимо також через O_t множину об'єктів системи в момент t, $|O_t|<\infty$, а через $O_t(U)$ – множину об'єктів з O_t, які породив користувач U.

II Загрози інформації

Звичайно, вважаємо, що $U \in O_t(U)$. Отже, за наведеними вище позначеннями для i-го та j-го користувачів запишемо наступний вираз для визначення загрози *конфіденційності*: ця загроза полягає у тому, що користувач, який не має відповідних повноважень, отримує доступ з R_1 до інформації:

$$\exists t \in N, \quad \exists p \in R_1, \quad R_1 \subset R \neq \varnothing, \quad \exists U_i, \exists O \in O_t, \quad U_i \xrightarrow{p} {}^{*}O, \quad O \in O_t(U_j), \quad i \neq j,$$

який змістовно означає, що в певний момент часу існує деякий (непорожній) вид доступу, можливий для певного користувача, до об'єкта, який створив інший користувач. Такі доступи вважаються небезпечними, оскільки завдяки ним можуть реалізуватися загрози. Саме вони називаються каналами витоку.

Для уникнення загроз конфіденційності в АС реалізуються певні послуги. Нагадаємо, згідно з [3], про послуги з забезпечення конфіденційності та їх зміст:

* довірча конфіденційність – коли реалізується таке керування доступом, при якому засоби захисту дозволяють звичайним користувачам керувати (довіряють керування) потоками інформації між іншими користувачами і об'єктами свого домену (наприклад, на підставі права володіння об'єктами), тобто призначення і передача повноважень не вимагають адміністративного втручання;
* адміністративна конфіденційність – таке керування, при якому засоби захисту дозволяють керувати потоками інформації між користувачами і об'єктами тільки спеціально авторизованим користувачам;
* повторне використання об'єктів – якщо перед наданням об'єкта користувачеві або процесу в ньому не залишається інформації, яку він містив, і скасовуються попередні права доступу до об'єкта;
* аналіз прихованих каналів – виконується з метою виявлення і вилучення потоків інформації, що існують, але не контролюються іншими послугами;
* конфіденційність при обміні – дозволяє забезпечити безпеку обміну інформацією між захищеними об'єктами через незахищене середовище.

Далі, скориставшись наведеним вище формалізмом, подамо вираз для визначення каналу дії на цілісність. Отже, загроза цілісності полягає у тому, що користувач, який не має відповідних повноважень, отримує доступ з R_2 до інформації. Запишемо математичний вираз:

$$\exists t \in N, \quad \exists p \in R_2, \quad R_2 \subset R \neq \varnothing, \quad \exists U_i, \exists O \in O_t, \quad U_i \xrightarrow{p} {}^{*}O, \quad O \in O_t(U_j), \quad i \neq j,$$

Прикладом виникнення каналу дії на цілісність є використання програми «троянський кінь». Така програма, крім документованих функцій, може здійснювати приховані дії від того, хто її активізує, на користь розробника програми (зловмисника). Як правило, «троянський кінь» використовується для модифікації захищеної інформації.

Послуги, за допомогою яких забезпечується цілісність, наступні [3]:

* довірча цілісність – аналогічна довірчій конфіденційності;
* адміністративна цілісність – аналогічна адміністративній конфіденційності;
* відкат – дозволяє відновлюватися після помилок користувача, збоїв програмного забезпечення або апаратури і підтримувати цілісність баз даних, додатків, побудованих на транзакціях і т. ін.; вона забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану;
* цілісність при обміні – дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище; найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис.

Загроза *доступності* полягає у тому, що користувач, який має відповідні повноваження, не може отримати доступ з R_1 або R_2. Оскільки результатом дії будь-якої загрози доступності є її відсутність або відсутність будь-яких каналів доступу, то формально це можна виразити наступним чином:

$$\exists t \in N, \quad \neg\exists p \in R_1 \cup R_2, \quad \exists U_i, \exists O \in O_t, \exists i \quad U_i \xrightarrow{p} {}^{*}O, \quad O \in O_t(U_i),$$

$$\exists t \in N, \quad (\neg\exists p \in R_1)\,\&\,(\neg\exists p \in R_2), \quad \exists U_i, \exists O \in O_t, \exists i \quad U_i \xrightarrow{p} {}^{*}O, \quad O \notin O_t(U_i),$$
$$R_1 \cap R_2 = \varnothing.$$

На відміну від конфіденційності або цілісності, де наявність каналів витоку є негативною обставиною, спостереженість повинна мати канали спостереження, тобто канали, за допомогою яких можна контролювати процес обробки інформації. Графічно це можна зобразити наступним чином

$$U_1 \xrightarrow{(r,exe)} S \xrightarrow{r} \{S_c, O_c\},$$

тобто користувач U_1 активізує процес S, який може отримати доступ, наприклад на читання (*r*), до певної множини процесів та об'єктів $\{S_c, O_c\}$. Термін «певна множина» має на увазі обраний і фіксований перелік подій, які мають відношення до безпеки інформації в АС. Слід також звернути увагу на те, що спосіб контролю процесу обробки інформації «на читання» є досить сильною вимогою, оскільки для спостереженості достатньо більш слабкого доступу (який, наприклад, дозволяв би тільки визначати – була подія чи ні).

Послуги доступності наступні [3]:

* використання ресурсів – дозволяє керувати використанням послуг і ресурсів користувачами;
* стійкість до відмов – має гарантувати доступність комп'ютерної системи (КС) (можливість використання інформації, окремих функцій чи КС в цілому) після відмови її компоненту;
* гаряча заміна – дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів; основна мета реалізації даної послуги полягає в тому, що встановлення нової версії системи, відмова або заміна захищеного компонента не повинні призводити до того, що система потрапить до стану, коли політика безпеки, яка реалізується нею, стане скомпрометованою;
* відновлення після збоїв – послуга забезпечує повернення КС до відомого захищеного стану після відмови або переривання обслуговування; відновлення може вимагати втручання оператора, а для її більш високих рівнів реалізації СЗІ може продукувати відновлення працездатності автоматично; якщо ж відновлення неможливе, то СЗІ повинна переводити систему до стану, з якого її може повернути до нормального функціонування тільки адміністратор.

Отже, загроза *спостереженості* полягає в тому, що користувач, який має відповідні повноваження, не може отримати доступ з R_3 до інформації. Запишемо математичний вираз:

$$\exists t \in N, \quad \neg\exists p \in R_3, \quad \exists U_i, \exists O \in O_t, \exists i \quad U_i \xrightarrow{p} {}^{*}O, \quad O \in O_t(U_j), \forall j.$$

Отже, загрози спостереженості зводяться до ушкодження або навіть знищення каналів спостереження, а головна задача спостереженості в АС – їх підтримувати. Вона реалізується за допомогою наступних послуг [3]:

* реєстрація (аудит) – дозволяє контролювати небезпечні для КС дії;
* ідентифікація і автентифікація – дозволяють СЗІ визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до КС; хоча поняття ідентифікація і автентифікація відрізняються, на практиці обидва ці процеси важко буває поділити, тому важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем; за результатами ідентифікації і автентифікації користувача приймається рішення про те, чи дозволено даному користувачеві ввійти в систему, а також здійснюється розмежування доступу на підставі атрибутів доступу користувача, що увійшов;
* достовірний канал – дозволяє гарантувати, що користувач взаємодіє безпосередньо з СЗІ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається);
* розподіл обов'язків – дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій;
* цілісність комплексу засобів захисту – визначає міру спроможності комплексу засобів захисту захищати себе і гарантувати свою спроможність керувати захищеними об'єктам; жодна КС не може вважатися захищеною, якщо самі засоби захисту є об'єктом для несанкціонованого впливу;
* самотестування – дозволяє перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС;
* ідентифікація і автентифікація при обміні – ця послуга дозволяє одному об'єкту ідентифікувати інший (встановити і перевірити його ідентичність) і забезпечити іншому можливість ідентифікувати перший, перш ніж почати взаємодію;

* автентифікація відправника – дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем;

* автентифікація отримувача – послуга дає можливість забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем.

Найбільш розповсюдженою і ефективною практикою реалізації спостереженості є реєстрація, яка включає протоколювання та аудит. Для АС з високим рівнем захищеності вони мають проводитися в реальному часі [3].

III Висновки

За допомогою поняття потоку інформації подано визначення доступу. Проведено аналіз множини доступу і визначені підмножини доступів, за допомогою яких уточнено формальне визначення основних загроз інформації. Отримані формальні визначення загроз інформації в подальшому дозволяють на різних класах політики безпеки аналізувати захищеність АС. Крім того, наведений формалізм дає можливість описати поняття профілю [3], а також проводити формальне дослідження інших політик (наприклад, рольової) безпеки в АС. Перелічуємо також основні послуги, за допомогою яких забезпечується захист від наведених загроз інформації.

Література: 1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-98, ДСТСЗІ СБ України, Київ, 1998. 2. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-001-98, ДСТСЗІ СБ України, Київ, 1998. 3. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 2.2-001-98, ДСТСЗІ СБ України, Київ, 1998. 4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – НД ТЗІ 2.2.-002 -98, ДСТСЗІ СБ України, Київ, 1998. 5. Антонюк А. О., Жора В. В. Загрози інформації і канали витоку // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – К.: НТУУ «КПІ». – К. 2001 – С. 42 – 46. 6. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М.: «Яхтсмен», 1996. 7. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С. В., 2001, 352 с., ил.

УДК 681.513

ОБНАРУЖЕНИЕ АНОМАЛИЙ ПОВЕДЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Алексей Новиков, Сергей Кащенко

Физико-технический институт НТУУ «КПИ»

Анотація: **Розглядається модель поведінки програмного забезпечення з точки зору безпеки у вигляді стохастичного автомата, що дозволить обраховувати ймовірність появи поточних даних моніторингу на основі попередніх спостережень.**

Summary: **In the report the software security behavior model based on stochastic automaton is considered, which will allow to calculate probability of current monitoring data appearance on the basis of previous observations.**

Ключевые слова: **Безопасность, системы обнаружения атак, стохастический автомат.**

I Введение

В последнее десятилетие появились и приобретают все большее распространение средства обеспечения безопасности компьютерных систем нового класса – средства мониторинга или системы обнаружения атак (СОА). Появление и развитие такого рода средств обусловлено недостаточностью в современных условиях, характеризующихся экспоненциальным ростом глобальных и корпоративных сетей, традиционных средств обеспечения безопасности, таких как криптографические системы, средства контроля доступа операционных систем и средства защиты периметра распределенных компьютерных систем (межсетевые экраны). Ряд источников (например, [1]) указывают на постоянный рост рынка СОА и количества нарушений, выявленных с их помощью, что говорит о высокой эффективности и признании роли СОА в задаче обеспечения безопасности компьютерных систем.