ПРОБЛЕМИ БЕЗПЕКИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Як відомо, інформаційна система Державної податкової служби (ІС ДПС) є корпоративною розподіленою інформаційною системою. Отже, розглянемо найбільш важливі проблеми інформаційної безпеки таких систем.

Нагадаємо, що під інформаційною безпекою розуміють стан захищеності оброблюваних даних та даних що зберігаються та передаються від незаконного ознайомлення, перетворення і знищення, а також стан захищеності інформаційних ресурсів від дій, спрямованих на порушення їх працездатності.

Природа цих дій може бути найрізноманітнішою. Це і спроби проникнення зловмисників, і помилки персоналу, і вихід з ладу апаратних і програмних засобів, стихійні лиха (землетрус, ураган, пожежа і т.д.).

Інформаційна безпека комп'ютерних систем і мереж досягається ухваленням комплексу заходів по забезпеченню конфіденційності, цілісності, достовірності, юридичної значущості інформації, оперативності доступу до неї, а також по забезпеченню цілісності і доступності інформаційних ресурсів і компонентів системи або мережі.

Перераховані вище базові властивості інформації потребують більш повного тлумачення. Деякі з наведених нижче термінів були визначені раніше з посиланням на нормативні документи, проте їх тлумачення суттєво полегшує їх розуміння та сенс.

Конфіденційність інформації – це її властивість бути доступною тільки обмеженому колу користувачів інформаційної системи, в якій циркулює дана інформація. По суті, конфіденційність інформації – це її властивість бути відомою тільки допущеним суб'єктам системи і тим хто пройшов перевірку (користувачам, процесам, програмам). Для решти суб'єктів системи інформація повинна бути невідомою.

Під **цілісністю інформації** розуміється її властивість зберігати свою структуру та/або зміст в процесі передачі і зберігання. Цілісність інформації забезпечується в тому випадку, якщо дані в системі не відрізняються в

семантичному відношенні від даних в початкових документах, тобто якщо не відбулося їх випадкового або навмисного спотворення або руйнування.

Достовірність інформації – властивість, яка виражається в строгій приналежності інформації суб'єкту, що є її джерелом, або тому суб'єкту, від якого вона прийнята.

Критична інформація (sensitive information) – інформація, що вимагає захисту; будь-яка інформація, втрата або неправильне використання якої (модифікація, ознайомлення) може нанести шкоду власникові інформації або ІС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб.

Юридична значущість інформації означає, що документ, який є носієм інформації, володіє юридичною силою.

Оперативність доступу до інформації– це здатність інформації або деякого інформаційного ресурсу бути доступними кінцевому користувачу відповідно до його оперативних потреб.

Цілісність ресурсу або компоненту системи – це його властивість бути незмінним в семантичному значенні при функціонуванні системи в умовах випадкових або навмисних спотворень або руйнуючих дій.

Доступність ресурсу або компоненту системи – це його властивість бути доступним законним користувачам системи.

З допуском до інформації і ресурсів системи зв'язана група таких понять, як ідентифікація, автентифікація, авторизація, які були визначені раніше.

Після ідентифікації і автентифікації об'єкту виконують авторизацію.

Авторизація об'єкту – це процедура надання законному об'єкту, що успішно пройшов ідентифікацію і автентифікацію, відповідних повноважень і доступних ресурсів системи (мережі).

Збиток безпеки має на увазі порушення стану захищеності інформації, що міститься і обробляється в системі (мережі).

З поняттям загрози безпеки тісно зв'язане поняття уразливості комп'ютерних систем системи (мережі).

Уразливість системи (мережі) – це будь-яка характеристика комп'ютерних систем, використовування якої може привести до реалізації загрози.

Атака на комп'ютерну систему (мережу) – це дія, що робиться зловмисником з метою пошуку і використовування тієї або іншої уразливості системи. Таким чином, атака – це реалізація загрози безпеки.

Протидія загрозам безпеки – мета, яку покликані виконати засоби захисту комп'ютерних систем і мереж.

Безпечна або захищена система – це система із засобами захисту, які успішно і ефективно можуть протистояти загрозам безпеки.

Підходи щодо вирішення проблеми забезпечення безпеки.

Корпоративні системи (КС) відносяться до розподілених комп'ютерних систем, що здійснюють автоматизовану обробку інформації. Проблема забезпечення інформаційної безпеки є центральною для таких комп'ютерних систем. Забезпечення безпеки КС передбачає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування КС, а також спробам модифікації, викрадення, виходу з ладу або руйнування її компонентів, тобто захист всіх компонентів КС – апаратних засобів, програмного забезпечення, даних і персоналу.

Існують два підходи до проблеми забезпечення безпеки КС: фрагментарний і комплексний.

Фрагментарний підхід направлений на протидію чітко певним загрозам в заданих умовах. Як приклади реалізації такого підходу можна вказати окремі засоби управління доступом, автономні засоби шифрування, спеціалізовані антивірусні програми і т.п.

Достоїнство цього підходу полягає у високій вибірковості до конкретної загрози. Істотним недоліком його є відсутність єдиного захищеного середовища обробки інформації. Фрагментарні заходи захисту інформації забезпечують захист конкретних об'єктів КС тільки від конкретної загрози. Навіть невелика видозміна загрози веде до втрати ефективності захисту.

Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в КС, що зводить воєдино різнорідні заходи протидії загрозам. Організація захищеного середовища обробки інформації дозволяє гарантувати певний рівень безпеки КС, що можна віднести до безперечних достоїнств комплексного підходу. До його недоліків відносяться обмеження на свободу дій користувачів КС, чутливість до помилок установки і настройки засобів захисту, складність управління.

Комплексний підхід до проблеми забезпечення безпеки заснований на розробленій для конкретної КС ПБ.

Оскільки ПБ є набором норм, правил і практичних рекомендацій, на яких будуються управління, захист і розподіл інформації в КС, саме вона регламентує ефективну роботу засобів захисту КС. Вона охоплює всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях.

ПБ реалізується за допомогою комплексного застосування адміністративно-організаційних заходів, фізичних заходів і програмно-апаратних засобів і визначає архітектуру системи захисту. Для конкретної організації ПБ повинна носити індивідуальний характер і залежати від конкретної технології обробки інформації і використовуваних програмних і технічних засобів.

Крім управління доступом суб'єктів до об'єктів системи проблема захисту інформації має ще один аспект. Для отримання інформації про який-небудь об'єкт системи зовсім необов'язково шукати шляхи НСД до нього. Необхідні відомості можна зібрати, спостерігаючи за обробкою необхідного об'єкту, тобто використовуючи канали просочування інформації. У системі завжди існують інформаційні потоки. Тому адміністратору необхідно визначити, які інформаційні потоки в системі є «легальними», тобто не ведуть до просочування інформації, а які ведуть. Як наслідок, виникає необхідність розробки правил, що регламентують управління інформаційними потоками в системі. Звичайно воно застосовується в рамках виборчої або повноважної ПБ, доповнюючи її та сприяючи підвищенню надійності системи захисту.

Комплексний підхід до вирішення проблеми забезпечення безпеки при раціональному поєднанні виборчого і повноважного управління доступом, а також управління інформаційними потоками служить тим фундаментом, на якому будується вся система захисту.

Недоліки у сфері захищеності служб і протоколів Internet

Ряд служб Internet дуже ефективно використовуються для обробки інформації в КС, зокрема, і в системах ДПС. Однак для них слід зазначити певні «природжені слабкості», що створює проблеми з інформаційної безпеки. Спочатку розглянемо основні причини уразливості Internet.

Як відомо, до служб Internet відносяться:

- простий протокол передачі електронної пошти SMTP (Simple Mail Transfer Protocol);
- програма електронної пошти Sendmail;
- служба мережевих імен DNS;
- служба емуляції видаленого терміналу Telnet;
- всесвітня павутина WWW;
- протокол передачі файлів FTP;
- графічна віконна система Windows і ін.

Простий протокол передачі електронної пошти SMTP дозволяє здійснювати поштову транспортну службу Internet. Одна з проблем безпеки, пов'язана з цим протоколом, полягає у тому, що користувач не може перевірити адресу відправника в заголовку електронного листу. В результаті хакер здатний направити у внутрішню мережу велику кількість поштових повідомлень, що приведе до перевантаження і блокування роботи поштового серверу.

Популярна в Internet програма електронної пошти Sendmail використовує для роботи деяку мережеву інформацію – IP-адресу відправника. Перехоплюючи повідомлення, що відправляються за допомогою Sendmail, хакер може застосувати цю інформацію для нападів, наприклад для спуфінгу (підміни адрес).

Протокол передачі файлів FTP забезпечує передачу текстових і двійкових файлів, тому його часто використовують в Internet для організації сумісного доступу до інформації. Його звичайно розглядають як один з методів роботи з

видаленими мережами. На FTP-серверах зберігаються документи, програми, графіки і інші види інформації. До даних цих файлів на FTP-серверах не можна звернутися напряму. Це можна зробити, тільки переписавши їх цілком з FTP-серверу на локальний сервер. Деякі FTP-сервери обмежують доступ користувачів до своїх архівів даних за допомогою пароля, інші ж надають вільний доступ (так званий анонімний FTP-сервер).

Служба мережевих імен DNS є розподіленою базою даних, яка перетворює імена користувачів і хостів в IP-адреси, що вказуються в заголовках пакетів, і навпаки. DNS також зберігає інформацію про структуру мережі компанії, наприклад, про кількість комп'ютерів з IP-адресами в кожному домені.

Одна з проблем DNS полягає у тому, що цю базу даних дуже важко «приховати» від неавторизованих користувачів. В результаті DNS часто використовується хакерами як джерело інформації про імена довірених хостів.

Служба емуляції видаленого терміналу Telnet використовується для підключення до видалених систем, приєднаних до мережі; вона застосовує базові можливості емуляції терміналу. При використовуванні цього сервісу Internet користувачі повинні реєструватися на сервері Telnet, вводячи свої ім'я і пароль. Після автентифікації користувача його робоча станція функціонує в режимі терміналу, підключеного до зовнішнього хосту. З цього терміналу користувач може вводити команди, які забезпечують йому доступ до файлів і запуск програм. Підключившись до серверу Telnet, хакер може конфігурувати його програму так, щоб вона записувала імена і паролі користувачів.

Всесвітня павутина WWW – це система, заснована на мережевих додатках, які дозволяють користувачам проглядати вміст різних серверів в Internet або інтра мережах. Найкорисніша властивість WWW – використовування гіпертекстових документів, в які вбудовані посилання на інші документи і Web-вузли, що дає відвідувачам сайтів можливість легко переходити від одного вузла до іншого. Проте ця ж властивість є і найслабкішим місцем системи WWW, оскільки посилання на Web-вузли, що зберігаються в гіпертекстових документах, містять інформацію про те, як здійснюється доступ до відповідних

вузлів. Використовуючи цю інформацію, хакери можуть зруйнувати Web-вузол або дістати доступ до конфіденційної інформації, що зберігається в ньому.

Серед основних причини уразливості мережі Internet можна відзначити наступні:

- мережа Internet розроблялася як відкрита і децентралізована мережа з початковою відсутністю ПБ. При цьому основні зусилля були направлені на досягнення зручності обміну інформацією в Internet. Крім того, багато мереж спроектовано без механізмів контролю доступу з боку Internet;
- для Internet характерні велика протяжність ліній зв'язку і уразливість основних служб. Сервісні програми базового набору протоколів TCP/IP мережі Internet не гарантують безпеки;
- модель «клієнт-сервер», на якій заснована робота в Internet, не позбавлена певних слабкостей і лазівок в продуктах окремих виробників. Дана модель об'єднує різноманітне програмне і апаратне забезпечення, в якому можуть бути “діри” для проникнення зловмисників;
- при створенні Web-сторінок ряд компаній використовує власний дизайн, який може не відповідати вимогам забезпечення певного класу безпеки для Web-вузла компанії і пов'язаної з ним локальної або корпоративної мережі;
- інформація про існуючі і використовувані засоби захисту доступна користувачам. Крім того, можливий витік технологій безпеки високого рівня з секретних джерел при розкритті представлених в мережі Web-вузлів і мереж організацій, що займаються розробкою цих технологій;
- існує можливість спостереження за каналами передачі даних, оскільки значна частина інформації передається через Internet у відкритій незахищеній формі. Зокрема, електронна пошта, паролі і вкладені в листи файли можуть бути легко перехоплені зловмисником за допомогою доступних програм;
- засоби управління доступом часто складно конфігурувати, настроювати і контролювати. Це приводить до неправильної конфігурації засобів захисту і, як наслідок, до несанкціонованого доступу;

- істотну роль виконує і людський чинник. Окремі користувачі, не визначені високими моральними принципами, можуть за відповідну платню надати зловмисникам доступ в мережу своєї фірми. Є користувачі-дилетанти, які, не володіючи необхідними знаннями, вважають, що засоби захисту їм взагалі не потрібні, або неправильно конфігурують ці засоби;
- для обслуговування роботи в Internet використовується велике число сервісів, інформаційних служб і мережевих протоколів. Знання правильності і тонкості використовування хоча б більшості цих сервісів, служб і протоколів одній людині в особі адміністратора мережі практично недоступно;
- фахівці із захисту інформації в Internet готуються поки в недостатньому об'ємі; часто в ролі адміністраторів мережі працюють люди, що не мають глибокої професійної підготовки;
- для роботи в Internet характерна лише уявна анонімність. Існує потенційна можливість обійти засоби виявлення відправника тієї або іншої інформації або відвідувача того або іншого Web-вузла за допомогою використовування віртуальних IP-адрес і проміжних вузлів електронної пошти,

Виникає природне питання: скільки потенційно вразливих місць в принципі може бути у мереж, підключених до Internet? Фахівці компанії Internet Security Systems вважають, що в будь-якій мережі, заснованій на протоколі TCP/IP, існує близько 135 потенційних каналів для НСД.

Перші засоби захисту даних, які передаються, з'явилися практично відразу після того, як уразливість IP-мереж дала про себе знати з практики. Характерними прикладами розробок в цій області можуть служити PGP/Web-of-Trust для шифрування повідомлень електронної пошти, SSL для захисту Web-трафіку, SSH (Secure SHell) для захисту сеансів Telnet і процедур передачі файлів.

Загальним недоліком подібних широко поширених рішень є їх «прихильність» до певного типу додатків, а значить, нездатність задовольнити

тим різноманітним вимогам до систем мережевого захисту, які пред'являють крупні корпорації або Internet-провайдери.

Найрадикальніший спосіб подолати вказане обмеження зводиться до того, щоб будувати систему захисту не для окремих класів додатків (хай і дуже популярних), а для мережі в цілому. Стосовно IP-мереж це означає, що системи захисту повинні діяти на мережевому рівні моделі OSI.

Перевага такого вибору полягає в тому очевидному факті, що в IP-мережах саме даний рівень відрізняється найбільшою гомогенністю: незалежно від вище розміщених протоколів, фізичного середовища передачі і технології канального рівня транспортування даних по мережі не може бути здійснено в обхід протоколу IP. Тому реалізація захисту мережі на третьому рівні автоматично гарантує як мінімум такий же ступінь захисту всіх мережевих додатків. При цьому не потрібна яка-небудь модифікація останніх. Для користувачів процедури захисту виявляться такими ж прозорими, як і сам протокол IP.