Захищена система передачі даних в корпоративній мережі приватного підприємства

УДК 004.056.53

Ірина Грищенко

Національний авіаційний університет, irinka260196.95@icloud.com

Мета роботи: розглянути деякі принципи побудови системи захисту, проблеми забезпечення захисту інформації, вимоги до процесу інформаційного обміну системи захисту інформації та деякі проблеми захисту інформації в автоматизованих системах.

Сучасний етап розвитку інформатизації характеризується необхідністю переходу до створення глобальних територіально розподілених автоматизованих інформаційно-аналітичних систем. Аналіз систем передачі даних в корпоративних мережах приватного підприємства показав, що на даний момент ці системи є не досить захищеними. Тому актуальним є розробка принципів побудови системи захисту, яка є більш захищеною від несанкціонованого проникнення зловмисника.

Одним із найважливіших показників надійності автоматизованої системи є забезпечення доступності,цілісності та конфіденційності інформації.

Для здійснення управління доступом і захистом інформації в різнорідних автоматизованих системах обрана доменна організація системи захисту інформації. Домен системи захисту інформації від несанкціонованого доступу – це програмно-апаратний комплекс, що здійснює захист територіально відокремленої частини автоматизованої системи. Взаємодія між доменами полягає в передачі команд віддаленого управління від одних доменів до інших і поверненні інформації про результати виконання цих команд.

Нормальна передача інформації у мережах з гарантованою якістю обслуговування користувачів має на увазі виконання трьох етапів : 1) у площині менеджменту - формування й коректування баз даних (БД) про стан елементів мережі. 2) у площині керування - організацію маршруту між вузлом - джерелом (ВД) і вузлом - одержувачем (ВО) у вигляді віртуального що комутирує або постійного з'єднання. 3) у площині користувача - безпосередня передача користувальницької інформації.

Під порушенням передачі інформації будемо розуміти одну із ситуацій, які можуть бути організовані порушником: 1) переривання або роз'єднання. Інформація знищується або стає недоступною або непридатною для використання. 2) перехват. До інформації відкривається несанкціонований доступ. 3) модифікація. До інформації відкривається несанкціонований доступ з метою зміни інформації. 4) фальсифікація. Порушник видає себе за джерело інформації.

Сервісні служби захисту інформації є відповідальними за забезпечення основних вимог користувачів, пропонованих до телекомунікаційних систем (з погляду її надійності). Причому дані служби повинні функціонувати у всіх трьох площинах.

За установку й припинення дії тієї або іншої служби відповідають агенти захисту (Security Agent , SA). Узгодження служб захисту між агентами

відбувається через з'єднання захисту. По цих з'єднаннях виробляється обмін інформацією захисту.

Найпростіший варіант організації з'єднання захисту - агенти захисту розміщені в межах кінцевих систем користувачів. У цьому випадку кінцеві системи й агенти захисту взаємодіють із мережею через інтерфейс «користувач - мережа + захист» (UNI+Sec).

Агенти захисту для віртуального з'єднання (каналу або тракту), що встановлений між кінцевими системами користувачів, послідовно виконують наступні дії: визначають вид сервісних служб захисту, які повинні бути застосовані до даного віртуального з'єднання; погоджують служби захисту між собою; застосовують необхідні служби захисту до даного віртуального з'єднання.

Інший варіант організації з'єднання захисту: один агент захисту розміщається на кінцевій системі користувача, а іншої на комутаторі віртуальних каналів. Відповідно, користувачі й агенти захисту взаємодіють із мережею зв'язку через інтерфейси «користувач – мережа» (UNI) або UNI+Sec; комутатор віртуальних каналів через інтерфейс «вузол – мережа + захист» (NNI+Sec).

У цьому випадку агент захисту, розміщений у межах комутатора віртуальних каналів, має можливість забезпечувати служби захисту не тільки для користувача П2, але й для інших вузлів і мереж, які приєднуються до даного комутатора віртуальних каналів.

Установлення й підтримка з'єднань захисту на мережах АТМ досить складний і відповідальний процес, що складається із двох етапів і базується на протоколі обміну повідомленнями захисту (Security Message Exchange, SME) і передачі спеціальних осередків захисту OAM . Тобто спочатку проходить аутентифікація агентів захисту між собою, потім узгоджуються служби захисту між агентами захисту, встановлюється зєднання захисту і вже потім йде передача спеціальних осередків захисту OAM. Протокол може реалізовуватися у площині користувача і у площині керування.

Щодо площини користувача, то тут аутентифікація забезпечується через обмін інформацією між агентами безпеки, які обмінюються між собою повідомленнями безпеки. Конфіденційність площини користувача забезпечується криптографічними механізмами, які захищають дані користувача у віртуальних каналах від несанкціонованого розкриття.

Щодо площини контролю, то це механізм, що дозволяє пристроям конфігурувати мережу, щоб домогтися певних цілей (наприклад, установити віртуальний канал, що комутує). Так як повідомлення площини керування можуть впливати на стан і працездатність мережі, їх захист дуже важливий.

Науковий керівник – д.т.н., професор, Хорошко В.О.