Лекція 12. Програмні та програмно-апаратні комплекси засобів захисту інформації (ЗЗІ)

12.1. Антивіруси
12.2. Міжмережеві екрани.
12.3. IDS, IPS.
12.4. Системи контролю та управління доступом у мережі (Active Directory, ACL)
12.5. Системи контролю та управління фізичним доступом (СКУД)

12.1. Антивіруси

Антивірусна програма (антивірус) – спеціалізована програма для знаходження комп'ютерних вірусів, а також небажаних (шкідливих) програм загалом, та відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики – запобігання зараженню (модифікації) файлів чи операційної системи шкідливим кодом.

Основні завдання

- Сканування файлів і програм в режимі реального часу.
- Сканування комп'ютера за потребою.
- Сканування інтернет-трафіку.
- Сканування електронної пошти.
- Захист від атак ворожих вебвузлів.
- Відновлення пошкоджених файлів.

Класифікація антивірусних продуктів

Класифікувати антивірусні продукти можна відразу за кількома ознаками, таким, як: використовувані технології антивірусного захисту, функціонал продуктів, цільові платформи.

По використовуваних технологіях антивірусного захисту:

- Класичні антивірусні продукти (продукти, які застосовують тільки сигнатурний метод детектування).
- Продукти проактивного антивірусного захисту (продукти, які застосовують тільки проактивні технології антивірусного захисту).
- Комбіновані продукти (продукти, які застосовують як класичні, сигнатурні методи захисту, так і проактивні).

За функціоналом продуктів:

- Антивірусні продукти (продукти, що забезпечують тільки антивірусний захист).
- Комбіновані продукти (продукти, що забезпечують не тільки захист від шкідливих програм, але і фільтрацію спаму, шифрування та резервне копіювання даних та інші функції).

За цільовими платформами: Windows, * NIX (до даного сімейства відносяться ОС BSD, Linux, etc), MacOS, для мобільних платформ (iOS, Android та ін.)

Антивірусні продукти для корпоративних користувачів можна також класифікувати по об'єктах захисту:

- для захисту робочих станцій;
- для захисту файлових і термінальних серверів;
- для захисту поштових та Інтернет-шлюзів;
- для захисту серверів віртуалізації.

Склад антивірусного програмного забезпечення

Антивірусне програмне забезпечення складається з комп'ютерних програм, які намагаються знайти, запобігти розмноженню і видалити комп'ютерні віруси та інші шкідливі програми.

Методи знаходження вірусів

Антивірусне програмне забезпечення зазвичай використовує два різних методи для виконання своїх задач:

- Перегляд (сканування) файлів для пошуку відомих вірусів, що відповідають визначенню в словнику вірусів.
- Знаходження підозрілої поведінки будь-якої з програм, що схожа на поведінку зараженої програми.

Відповідність визначенню вірусів в словнику

При цьому методі антивірусна програма під час перегляду файлу звертається до словника з відомими вірусами, що складений авторами програми-антивірусу. У разі відповідності якоїсь ділянки коду програми, що проглядається, відомому коду (сигнатурі) вірусу в словнику, програма-антивірус може виконувати одну з наступних дій:

- Видалити інфікований файл.
- Відправити файл у карантин (тобто зробити його недоступним для виконання, з метою недопущення подальшого розповсюдження вірусу).
- Намагатися відтворити файл, видаливши сам вірус з тіла файлу.

Хоча антивірусні програми створені на основі пошуку відповідності визначенню вірусу в словнику, за звичайних обставин, вони можуть досить ефективно перешкоджати збільшенню випадків зараження комп'ютерів, автори вірусів намагаються триматися на півкроку попереду таких програм-антивірусів, створюючи «олігоморфні», «поліморфні» і, найновіші, «метаморфічні» віруси, у яких деякі частини шифруються або спотворюються так, щоб неможливо було знайти спільне з визначенням в словнику вірусів.

Підозріла поведінка програмних забезпечень

Антивіруси, що використовують метод знаходження підозрілої поведінки програм, не намагаються ідентифікувати відомі віруси, замість цього вони стежать за поведінкою всіх програм. Якщо програма намагається записати якісь дані в файл, що виконується (exe-файл), програма-антивірус може зробити помітку цього файлу, попередити користувача і спитати, що треба зробити.

На відміну від методу відповідності визначенню вірусів в словнику, метод знаходження підозрілої поведінки дає захист від абсолютно нових вірусів, яких ще немає в жодному словнику вірусів. Однак треба враховувати, що програми, побудовані на цьому методі, видають також велику кількість помилкових попереджень. Програми класу Firewall давно мали в своєму складі модуль знаходження підозрілої поведінки програм.

Методи захисту від вірусів

Для захисту від вірусів використовують три групи методів:

1. Методи, засновані на *аналізі вмісту файлів* (як файлів даних, і файлів з кодами команд). До цієї групи належать сканування сигнатур вірусів, а також перевірка цілісності та сканування підозрілих команд.

2. Методи, що ґрунтуються на *відстеженні поведінки програм* при їх виконанні. Ці методи полягають у протоколюванні всіх подій, що загрожують безпеці системи та відбуваються або при реальному виконанні коду, що перевіряється, бо при його програмній емуляції.

3. Методи *регламентації порядку роботи* з файлами та програмами. Ці методи належать до адміністративних заходів забезпечення безпеки.

Метод сканування сигнатур (сигнатурний аналіз, сигнатурний метод) заснований на пошуку у файлах унікальної послідовності байтів – **сигнатури**, характерною для певного вірусу До кожного нововиявленого вірусу фахівцями антивірусної лабораторії виконується аналіз коду, виходячи з якого визначається його сигнатура. Отриманий кодовий фрагмент поміщають у спеціальну базу даних вірусних сигнатур, з якою працює антивірусна програма. Перевагою даного методу є відносно низька частка хибних спрацьовувань, а головним недоліком – принципова неможливість виявлення в системі нового вірусу, для якого відсутня сигнатура в базі даних антивірусної програми, тому потрібна своєчасна актуалізація бази сигнатур.

Метод контролю цілісності ґрунтується на тому, що будь-яка несподівана та безпричинна зміна даних на диску є підозрілою подією, яка потребує особливої уваги антивірусної системи. Вірус обов'язково залишає свідчення свого перебування (зміна даних існуючих (особливо системних або виконуваних) файлів, поява нових файлів, що виконуються і т. д.). Факт зміни даних – *порушення цілісності* – легко встановлюється шляхом порівняння контрольної суми(дайджесту), заздалегідь підрахованої для вихідного стану коду, що тестується, і контрольної суми (дайджесту) поточного стану тестованого коду. Якщо вони не збігаються, значить цілісність порушена і є всі підстави провести для цього коду додаткову перевірку, наприклад, шляхом сканування вірусних сигнатур. Зазначений метод працює швидше методу сканування сигнатур, оскільки підрахунок контрольних сум вимагає менше обчислень, ніж операції побайтового порівняння кодових фрагментів, крім того, він дозволяє виявляти сліди діяльності будь-яких, у тому числі невідомих, вірусів, для яких у базі даних ще немає сигнатур.

Метод сканування підозрілих команд (евристичне сканування, евристичний метод) заснований на виявленні в файлі, що сканується, деякого числа підозрілих команд і (або) ознак підозрілих кодових послідовностей (наприклад, команда форматування жорсткого диска або функція впровадження у виконуваний процес або виконуваний код). Після цього робиться припущення про шкідливу сутність файлу і робляться додаткові дії щодо його перевірки. Цей метод має гарну швидкодію, але досить часто він не здатний виявляти нові віруси.

Метод відстеження поведінки програм суттєво відрізняється від способів сканування вмісту файлів, згаданих раніше. Цей метод заснований на аналізі поведінки запущених програм, який можна порівняти з упійманням злочинця «за руку» на місці злочину. Антивірусні засоби даного типу часто вимагають активної участі користувача, покликаного приймати рішення у відповідь на численні попередження системи, значна частина яких може бути згодом помилковими тривогами. Частота помилкових спрацьовувань (підозра на вірус для нешкідливого файлу або пропуск шкідливого файлу) при перевищенні певного порога робить цей метод неефективним, а користувач може перестати реагувати на попередження або вибрати оптимістичну стратегію (дозволяти всі дії всім програмам, що запускаються) або відключити цю функцію. При використанні антивірусних систем, що аналізують поведінку програм, завжди існує ризик виконання команд вірусного коду, здатних завдати шкоди комп'ютеру або мережі, що захищається. Для усунення такого недоліку пізніше було розроблено метод емуляції (імітації), що дозволяє запускати тестовану програму в штучно створеному (віртуальному) середовищі, яку часто називають пісочницею (sandbox), без небезпеки пошкодження інформаційного оточення. Використання методів аналізу поведінки програм показало їхню високу ефективність при виявленні як відомих, так і невідомих шкідливих програм.

Емуляція

Деякі програми-антивіруси намагаються імітувати початок виконання коду кожної нової програми, що викликається для виконання, перед тим, як передати їй керування. Якщо програма використовує код, що змінюється самостійно, або проявляє себе як вірус (тобто починає шукати інші exe-файли, наприклад), – така програма буде вважатися шкідливою (здатною нашкодити іншим файлам). Однак цей метод також має велику кількість помилкових попереджень.

Основні види антивірусних програм

– **Програми-детектори** забезпечують пошук та виявлення вірусів в оперативній пам'яті та на зовнішніх носіях, і при виявленні видають відповідне повідомлення. Розрізняють детектори *універсальні* та *спеціалізовані*.

– **Програми-доктора (фаги)** як знаходять заражені вірусами файли, а й «лікують» їх, тобто видаляють з файлу тіло програми вірусу, повертаючи файли у вихідний стан. На початку своєї роботи фаги шукають віруси в оперативній пам'яті, знищуючи їх і лише потім переходять до «лікування» файлів. Серед фагів виділяють поліфаги, тобто програми-лікарі, призначені для пошуку та знищення великої кількості вірусів. Враховуючи, що постійно з'являються нові віруси, програми-детектори та програми-лікарі швидко застарівають, і потрібне регулярне оновлення їх версій.

– **Програми-ревізори** відносяться до найнадійніших засобів захисту від вірусів. Ревізори запам'ятовують вихідний стан програм, каталогів та системних областей диска тоді, коли комп'ютер не заражений вірусом, а потім періодично або за бажанням користувача порівнюють поточний стан з вихідним. Виявлені зміни відображаються на екрані монітора. Як правило, порівняння станів роблять

відразу після завантаження операційної системи. При порівнянні перевіряються довжина файлу, код циклічного контролю (контрольна сума файлу), дата та час модифікації та інші параметри.

– **Програми-фільтри (сторожі)** є невеликі резидентні програми, призначені виявлення підозрілих дій під час роботи комп'ютера, притаманних вірусів.

– **Програми-вакцини (імунізатори)** – це резидентні програми, що запобігають зараженню файлів. Вакцини застосовують, якщо відсутні програми-лікарі, які «лікують» цей вірус. Вакцинація можлива лише від відомих вірусів. Вакцина модифікує програму або диск таким чином, щоб це не відбивалося на їхній роботі, а вірус сприйматиме їх зараженими і тому не впровадиться. Істотним недоліком таких програм є їх обмежені можливості щодо запобігання зараженню від великої кількості різноманітних вірусів.

12.2. Міжмережеві екрани

Міжмережевий екран, **мережевий екран**, **брандмауер**, **фаєрво́л**, **файрво́л** (англ. *Firewall*, *вогняна стіна*) – узагальнювальна назва фізичних пристроїв чи програмних застосунків, зконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі згідно з бажаним набором безпеки.

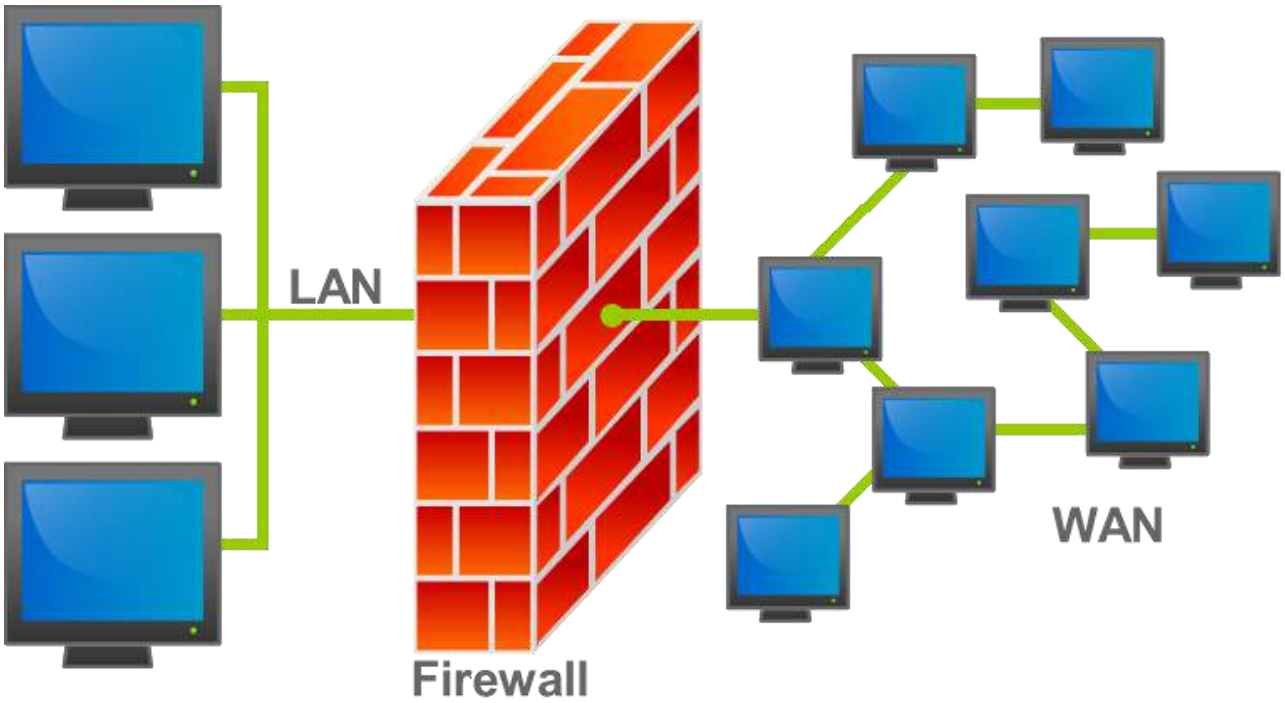

Рисунок 12.1 – Розташування фаєрвола у мережі

Функції

Фаєрвол може бути у вигляді окремого приладу (так званий *маршрутизатор* або *роутер*), або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі-сервер. Простий та дешевий фаєрвол може не мати такої гнучкої системи налаштувань правил фільтрації пакетів та *трансляції* адрес вхідного та вихідного трафіку (функція *переадресації*).

В залежності від активних з'єднань, що відслідковуються, фаєрволи розділяють на:

– *stateless* (проста фільтрація), які не відслідковують поточні з'єднання (наприклад TCP), а фільтрують потік даних виключно на основі статичних правил;

– *stateful* (фільтрація з урахуванням контексту), з відслідковуванням поточних з'єднань та пропуском тільки таких пакетів, що відповідають логіці й алгоритмам роботи відповідних протоколів та програм. Такі типи фаєрволів дозволяють ефективніше боротися з різноманітними DDoS-атаками та вразливістю деяких протоколів мереж.

Фільтрація трафіку

Фільтрація трафіку здійснюється на основі набору попередньо налаштованих правил, які називаються *ruleset*. Зручно представляти міжмережевий екран як послідовність фільтрів, які обробляють інформаційний потік. Кожен із фільтрів призначений для інтерпретації окремого правила. Послідовність правил набору істотно впливає на продуктивність міжмережевого екрану. Наприклад, багато міжмережевих екранів послідовно порівнюють трафік з правилами до тих пір, поки не буде знайдено відповідність. Для таких міжмережевих екранів правила, які відповідають найбільшій кількості трафіку, слід розташовувати якомога вище у списку, збільшуючи тим самим продуктивність.

Існує два принципи обробки трафіку, що надходить. Перший принцип говорить: "Що явно не заборонено, то дозволено". В даному випадку, якщо міжмережевий екран отримав пакет, що не потрапляє під жодне правило, то він передається далі. Протилежний принцип – "Що явно не дозволено, то заборонено" – гарантує набагато більшу захищеність, оскільки він забороняє весь трафік, який явно не дозволений правилами. Однак цей принцип обертається додатковим навантаженням на адміністратора.

У кінцевому рахунку міжмережні екрани виконують над трафіком, що надходить, одну з двох операцій: пропустити пакет далі (*allow*) або відкинути пакет (*deny*). Деякі міжмережові екрани мають ще одну операцію – *reject*, коли пакет відкидається, але відправнику повідомляється про недоступність сервісу, доступом до якого він намагався отримати. На противагу цьому, при операції *deny* відправник не інформується про недоступність сервісу, що є безпечнішим.

Типи фаєрволів

Для того щоб відповідати вимогам широкого кола користувачів, існує три типи фаєрволів: мережного рівня, прикладного рівня і рівня з'єднання. Кожен з цих трьох типів використовує свій, відмінний від інших підхід до захисту мережі:

– **Фаєрвол мережного рівня** представлений екрануючим маршрутизатором. Він контролює лише дані службової інформації пакетів мережевого і транспортного рівнів моделі OSI. Мінусом таких маршрутизаторів є те, що ще п'ять рівнів залишаються неконтрольованими. Нарешті, адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам'ятати, що у більшості приладів, що здійснюють фільтрацію пакетів, відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть проінформовані.

– **Фаєрвол прикладного рівня** також відомий як проксі-сервер (сервер-посередник). Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мережею і Internet, тому вони відповідають найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому як сервер-посередник використовуються швидші комп'ютери.

– **Фаєрвол рівня з'єднання** схожий на фаєрвол прикладного рівня тим, що обидва вони є серверами-посередниками. Відмінність полягає в тому, що фаєрволи прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, фаєрволи рівня з'єднання обслуговують велику кількість протоколів.

Класифікація міжмережевих екранів

Досі немає єдиної і загальновизнаної класифікації міжмережевих екранів. Однак у більшості випадків рівень мережевої моделі OSI, що підтримується, є основною характеристикою при їх класифікації. Враховуючи цю модель, розрізняють такі типи міжмережевих екранів:

1. Керовані комутатори.
2. Пакетні фільтри.
3. Шлюзи сеансового рівня.
4. Посередники прикладного рівня.
5. Інспектори стану.

Керовані комутатори

Керовані комутатори іноді відносять до класу міжмережевих екранів, оскільки вони здійснюють фільтрацію трафіку між мережами або вузлами мережі. Однак вони працюють на канальному рівні і поділяють трафік у рамках локальної мережі, а отже не можуть бути використані для обробки трафіку із зовнішніх мереж (наприклад, з Інтернету).

Багато виробників мережного обладнання, такі як Cisco, Nortel, 3Com, ZyXEL, надають у своїх комутаторах можливість фільтрації трафіку на основі MAC-адрес, що містяться в заголовках кадрів. Наприклад, у комутаторах

сімейства Cisco Catalyst ця можливість реалізована за допомогою механізму Port Security. Однак даний метод фільтрації не є ефективним, оскільки апаратно встановлена в мережній карті MAC-адреса легко змінюється програмним шляхом, оскільки значення, вказане через драйвер, має більш високий пріоритет, ніж зашите в плату. Тому багато сучасних комутаторів дозволяють використовувати інші параметри як ознаку фільтрації – наприклад, VLAN ID. Технологія віртуальних локальних мереж (англ. *Virtual Local Area Network*) дозволяє створювати групи хостів, трафік яких повністю ізольований від інших вузлів мережі.

При реалізації політики безпеки в рамках корпоративної мережі, основу яких становлять керовані комутатори, вони можуть бути потужним та досить дешевим рішенням. Взаємодіючи лише з протоколами канального рівня, такі міжмережові екрани фільтрують трафік із дуже високою швидкістю. Основним недоліком такого рішення є неможливість аналізу протоколів вищих рівнів.

Пакетні фільтри

Пакетні фільтри функціонують на мережному рівні та контролюють проходження трафіку на основі інформації, що міститься в заголовку пакетів. Багато міжмережевих екранів цього типу можуть оперувати заголовками протоколів і вищого, транспортного, рівня (наприклад, TCP чи UDP). Пакетні фільтри одними з перших з'явилися на ринку міжмережевих екранів і досі залишаються найпоширенішим їх типом. Ця технологія реалізована в переважній більшості маршрутизаторів і навіть у деяких комутаторах.

При аналізі заголовка мережного пакета можна використовувати такі параметри:

– IP-адреси джерела та одержувача;

– тип транспортного протоколу;

– поля службових заголовків протоколів мережного та транспортного рівнів;

– порт джерела та одержувача.

Досить часто доводиться фільтрувати фрагментовані пакети, що ускладнює визначення деяких атак. Багато атак мережі використовують дану вразливість міжмережевих екранів, видаючи пакети, що містять заборонені дані, за фрагменти іншого, довіреного пакета. Одним із способів боротьби з даним типом атак є конфігурування міжмережевого екрану таким чином, щоб блокувати фрагментовані пакети. Деякі міжмережеві екрани можуть дефрагментувати пакети перед пересиланням у внутрішню мережу, але це вимагає додаткових ресурсів самого міжмережевого екрану, особливо пам'яті. Дефрагментація повинна використовуватися дуже обґрунтовано, інакше такий міжмережевий екран легко може стати жертвою DoS-атаки.

Пакетні фільтри можуть бути реалізовані в наступних компонентах мережної інфраструктури:

- прикордонні маршрутизатори;
- операційні системи;
- персональні міжмережеві екрани.

Так як пакетні фільтри зазвичай перевіряють дані тільки в заголовках мережного та транспортного рівнів, вони можуть виконувати це досить швидко. Тому пакетні фільтри, вбудовані в прикордонні маршрутизатори, є ідеальними для розміщення на кордоні з мережею з низьким ступенем довіри. Однак у пакетних фільтрах відсутня можливість аналізу протоколів вищих рівнів мережевої моделі OSI. Крім того, фільтри пакетів зазвичай уразливі до атак, які використовують підміну мережевих адрес. Такі атаки зазвичай виконуються для обходу управління доступом, що здійснюється міжмережевим екраном.

Шлюзи сеансового рівня

Міжмережевий екран сеансового рівня виключає пряму взаємодію зовнішніх хостів з вузлом, розташованим у локальній мережі, виступаючи як посередник (англ. *proxy*), який реагує на всі вхідні пакети та перевіряє їх допустимість на підставі поточної фази з'єднання. Шлюз сеансового рівня гарантує, що жоден мережний пакет не буде пропущений, якщо він не належить раніше встановленому з'єднанню. Як тільки надходить запит на встановлення з'єднання, в спеціальну таблицю міститься відповідна інформація (адреси відправника та одержувача, які використовуються протоколи мережного та транспортного рівня, стан з'єднання тощо). У випадку, якщо з'єднання встановлено, пакети, що передаються в рамках цієї сесії, просто копіюватимуться в локальну мережу без додаткової фільтрації. Коли сеанс зв'язку завершується, відомості про нього видаляються з таблиці. Тому всі наступні пакети, що «прикидаються» пакетами вже завершеного з'єднання, відкидаються.

Так як міжмережевий екран даного типу виключає пряму взаємодію між двома вузлами, шлюз сеансового рівня є єдиним елементом між зовнішньою мережею і внутрішніми ресурсами. Це створює видимість того, що на всі запити із зовнішньої мережі відповідає шлюз, і робить практично неможливим визначення топології мережі, що захищається. Крім того, оскільки контакт між вузлами встановлюється лише за умови його допустимості, шлюз сеансового рівня запобігає можливості реалізації DoS-атаки, властивої пакетним фільтрам.

Незважаючи на ефективність цієї технології, вона має серйозний недолік: як і у всіх вищезгаданих класів міжмережевих екранів, у шлюзів сеансового рівня відсутня можливість перевірки змісту поля даних, що дозволяє зловмиснику передавати «троянських коней» в мережу, що захищається.

Посередники прикладного рівня

Міжмережеві екрани прикладного рівня, до яких, зокрема, відноситься файл веб-додатків, як і шлюзи сеансового рівня, виключають пряму взаємодію двох вузлів. Однак, функціонуючи на прикладному рівні, вони здатні «розуміти» контекст трафіку, що передається. Міжмережні екрани, що реалізують цю технологію, містять кілька додатків-посередників (англ. *application proxy*), кожна з яких обслуговує свій прикладний протокол. Такий міжмережевий екран здатний виявляти в повідомленнях, що передаються, і блокувати неіснуючі або небажані послідовності команд, що часто означає DoS-атаку, або забороняти

використання деяких команд (наприклад, FTPPUT, яка дає можливість користувачеві записувати інформацію на сервер FTP).

Посередник прикладного рівня може визначати тип інформації, що передається. Наприклад, це дозволяє заблокувати поштове повідомлення, що містить файл, що виконується. Іншою можливістю міжмережевого екрану цього типу є перевірка аргументів вхідних даних. Наприклад, аргумент імені користувача довжиною 100 символів або містить бінарні дані є, принаймні, підозрілим.

Посередники прикладного рівня здатні виконувати автентифікацію користувача, а також перевіряти, що сертифікати SSL підписані конкретним центром. Міжмережні екрани прикладного рівня доступні для багатьох протоколів, включаючи HTTP, FTP, поштові (SMTP, POP, IMAP), Telnet та інші.

Недоліками даного типу міжмережевих екранів є великі витрати часу та ресурсів для аналізу кожного пакета. Тому вони зазвичай не підходять для додатків реального часу. Іншим недоліком є неможливість автоматичного підключення підтримки нових мережевих додатків та протоколів, так як для кожного з них потрібний свій агент.

Інспектори стану

Кожен із вищеперелічених типів міжмережевих екранів використовується для захисту корпоративних мереж і має ряд переваг. Однак, куди ефективніше було б зібрати всі ці переваги в одному пристрої і отримати міжмережевий екран, що здійснює фільтрацію трафіку з мережевого прикладного рівня. Ця ідея була реалізована в інспекторах станів, що поєднують у собі високу продуктивність та захищеність. Даний клас міжмережевих екранів дозволяє контролювати:

- кожен переданий пакет – на основі таблиці правил;
- кожну сесію – на основі таблиці станів;
- кожен додаток – на основі розроблених посередників.

Здійснюючи фільтрацію трафіку за принципом шлюзу сеансового рівня, цей клас міжмережевих екранів не втручається у процес встановлення з'єднання між вузлами. Тому продуктивність інспектора станів помітно вище, ніж у посередника прикладного рівня та шлюзу сеансового рівня, і можна порівняти з продуктивністю пакетних фільтрів. Ще одна перевага інспекторів стану – прозорість для користувача: для клієнтського програмного забезпечення не потрібно додаткове налаштування. Дані міжмережевих екранів мають великі можливості розширення. При появі нової служби або нового протоколу прикладного рівня для підтримки достатньо додати кілька шаблонів. Проте інспекторам станів порівняно з посередниками прикладного рівня властива нижча захищеність.

Термін інспектор стану (англ. *stateful inspection*), впроваджений компанією Check Point Software, полюбився виробникам мережного обладнання настільки, що зараз практично кожен міжмережевий екран зараховують до цієї технології, навіть якщо він і не реалізує її повністю.

Реалізація

Існує два варіанти виконання міжмережевих екранів – програмний та програмно-апаратний. У свою чергу програмно-апаратний варіант має два різновиди – у вигляді окремого модуля в комутаторі або маршрутизаторі і у вигляді спеціалізованого пристрою.

В даний час найчастіше використовується програмне рішення, яке на перший погляд виглядає більш привабливим. Це викликано тим, що для його застосування достатньо, здавалося б, лише придбати програмне забезпечення міжмережевого екрану і встановити на будь-який наявний в організації комп'ютер. Однак, як показує практика, в організації далеко не завжди знаходиться вільний комп'ютер та ще й задовольняє досить високим вимогам щодо системних ресурсів. Після того, як комп'ютер все-таки знайдений (найчастіше – куплений), слідує процес встановлення та налаштування операційної системи, а також, безпосередньо, програмного забезпечення міжмережевого екрану. Неважко помітити, що використання звичайного персонального комп'ютера далеко не так просто, як здається. *Security appliance*, на основі, як правило, FreeBSD або Linux, «урізані» для виконання лише необхідних функцій. Перевагами даних рішень є:

- Простота впровадження: дані пристрої мають встановлену та налаштовану операційну систему та вимагають мінімум налаштувань після впровадження в мережу.
- Простота управління: цими пристроями можна керувати звідки завгодно за стандартними протоколами, такими як SNMP або Telnet, або за допомогою захищених протоколів, таких як SSH або SSL.
- Продуктивність: дані пристрої працюють ефективніше, оскільки з їхньої операційної системи виключені всі сервіси, що не використовуються.
- Відмовостійкість та висока доступність: дані пристрою створені для виконання конкретних завдань з високою доступністю.

Обмеженість аналізу міжмережевого екрану

Міжмережевий екран дозволяє здійснювати фільтрацію тільки трафіку, який він здатний «розуміти». В іншому випадку, він втрачає свою ефективність, тому що не здатний свідомо прийняти рішення про те, що робити з нерозпізнаним трафіком. Існують протоколи, такі як TLS, SSH, IPsec і SRTP, що використовують криптографію для того, щоб приховати вміст, через що їх трафік не може бути проінтерпретований. Також деякі протоколи, такі як OpenPGP та S/MIME, шифрують дані прикладного рівня, через що фільтрувати трафік на підставі інформації, що міститься на даному мережному рівні, стає неможливо. Ще одним прикладом обмеженості аналізу міжмережевих екранів є тунельований трафік, так як його фільтрація є неможливою, якщо міжмережевий екран «не розуміє» механізм тунелювання. У всіх цих випадках правила, налаштовані на міжмережевому екрані, повинні визначати, що робити з трафіком, який вони не можуть інтерпретувати.

12.3. IDS, IPS

Система виявлення атак (вторгнень) (IDS)

Система виявлення атак (вторгнень) (англ. *Intrusion Detection System, IDS*) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет. Про будь-яку активність шкідливого ПЗ або про порушення типової роботи централізовано збирається інформація SIEM-системою (англ. *Security information and event management*). SIEM-система обробляє дані отримані від багатьох джерел і використовує методи фільтрування тривог для розрізнення несанкціонованої активності від хибного спрацювання тривоги. Про що оповіщається або адміністратор або операційний центр безпеки.

Деякі системи виявлення вторгнень можуть виявити початок атаки на мережу, причому деякі з них здатні виявляти раніше не відомі атаки. Такі системи називають системами запобігання вторгненням (англ. *Intrusion Prevention System, IPS*). IPS не обмежуються лише оповіщенням, але й здійснюють різні заходи, спрямовані на блокування атаки (наприклад, розрив з'єднання або виконання скрипту, заданого адміністратором). На практиці досить часто програмно-апаратні рішення поєднують у собі функціональність двох типів систем. Їх об'єднання називають **IDPS** (**IDS і IPS**).

Хоч існує декілька типів IDS, які за розміром варіюються від окремих комп'ютерів до великих мереж, найпоширенішими класифікаціями є системи виявлення вторгнень у мережу (англ. *network intrusion detection systems, NIDS*) та системи виявлення вторгнень засновані на аналізі хостів (англ. *host-based intrusion detection systems, HIDS*). Прикладом HIDS буде система, яка відслідковує важливі файли операційної системи, прикладом NIDS буде система, яка аналізує вхідний мережевий трафік. Також можна класифікувати IDS відповідно до методів виявлення загроз: найбільш відомим є виявлення на основі сигнатур (розпізнавання поганих шаблонів, таких як шкідливе ПЗ) та виявлення аномалій (виявлення відхилень від «правильного» трафіку, часто за допомогою машинного навчання).

Порівняння IDS і файрвола

Хоча й IDS, і мережевий екран відносяться до засобів забезпечення інформаційної безпеки, мережевий екран відрізняється тим, що обмежує надходження на хост або підмережу певних видів трафіку для запобігання вторгнень і не відслідковує вторгнення, які відбуваються всередині мережі. IDS, навпаки, пропускає трафік, аналізуючи його і сигналізуючи при виявленні підозрілої активності. Виявлення порушення безпеки проводиться звичайно з використанням евристичних правил та аналізу сигнатур відомих комп'ютерних атак. Система яка розриває з'єднання називається системою запобігання вторгненням (англ. *Intrusion Prevention System, IPS*) і є однією з видів мережевого екрану на рівні застосунку.

Класифікація IDS

IDS можна класифікувати за місцем виявлення вторгнення (мережа або хост) та методу виявлення, який використовується.

Аналіз активності

Статичні і динамічні IDS

– Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе ПЗ, помилки в конфігураціях і т. д. Статичні IDS перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів. Статичні IDS виявляють сліди вторгнення.

– Динамічні IDS здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Динамічні IDS реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

Мережеві IDS

– Мережеві IDS (англ. *Network-based IDS, NIDS*) розташовуються в стратегічному місці або у таких місцях мережі, де можливий контроль трафіку всіх пристроїв у мережі. Вони здійснюють контроль усього трафіку даних всієї підмережі та порівнюють трафік, який передається у підмережі з бібліотекою відомих атак. Як тільки розпізнана атака або визначено відхилення у поведінці, відразу відсилається попередження адміністратору. Наприклад, NIDS встановлюють у підмережі, де розташовані мережеві екрани, щоб побачити, чи намагається хтось втрутитися в брандмауер.

Ще один приклад, коли NIDS-система, контролює велике число TPC-запитів на з'єднання (SYN) з багатьма портами на обраному комп'ютері, виявляючи, таким чином, що хтось намагається здійснити сканування TCP – портів. Мережева IDS може запускатися або на окремому комп'ютері, який контролює свій власний трафік, або на виділеному комп'ютері, прозоро переглядають весь трафік у мережі (концентратор, маршрутизатор). Мережеві IDS контролюють багато комп'ютерів, тоді як інші IDS контролюють тільки один. Прикладом мережевої IDS є Snort.

Хостові IDS

– IDS, які встановлюються на хості і виявляють зловмисні дії на ньому називаються хостовими або системними IDS. Прикладами хостових IDS можуть бути системи контролю цілісності файлів, які перевіряють системні файли з метою визначення, коли в них були внесені зміни. Монітори реєстраційних файлів (Log – file monitors, LFM), контролюють реєстраційні файли, створювані мережевими сервісами і службами. Обманні системи, що працюють з псевдосервісами, мета яких полягає у відтворенні добре відомих вразливостей для обману зловмисників.

Методи виявлення

Аналіз сигнатур і протоколів

– Аналіз сигнатур був першим методом, застосованим для виявлення вторгнень. Він базується на простому понятті збігу послідовності зі зразком. У вхідному пакеті проглядається байт за байтом і порівнюється з сигнатурою (підписом) – характерним рядком програми, що вказує на характеристику шкідливого трафіку. Такий підпис може містити ключову фразу або команду, яка пов'язана з нападом. Якщо збіг знайдено, оголошується тривога.

– Другий метод аналізу полягає в розгляді строго форматованих даних трафіку мережі, відомих як протоколи. Кожен пакет супроводжується різними протоколами. Кожен протокол має кілька полів з очікуваними або нормальними значеннями. Якщо що-небудь порушує ці стандарти, то ймовірна зловмисність. IDS переглядає кожне поле всіх протоколів вхідних пакетів: IP, TCP, і UDP. Якщо є порушення протоколу, наприклад, якщо він містить несподівані значення в одному з полів, оголошується тривога.

PIDS (Protocol – based IDS) являє собою систему (або агента), яка відстежує і аналізує комунікаційні протоколи з пов'язаними системами або користувачами. Для вебсервера подібна IDS зазвичай веде спостереження за HTTP і HTTPS протоколами. При використанні HTTPS IDS повинна розташовуватися на такому інтерфейсі, щоб переглядати HTTPS пакети ще до їх шифрування і відправки в мережу.

APIDS (Application Protocol – based IDS) – це система (або агент), яка веде спостереження та аналіз даних, переданих з використанням специфічних для певних програм протоколів. Наприклад, на вебсервері з SQL базою даних IDS буде відслідковувати вміст SQL команд, що передаються на сервер.

Виявлення аномалій

Системи виявлення вторгнень на основі аномалій були здебільшого введені для виявлення невідомих атак, почасти через стрімкий розвиток шкідливих програм. Основний підхід полягає у використанні машинного навчання, щоб створити модель правдоподібної діяльності, з якою потім порівняється нова поведінку. Хоча такий підхід і дозволяє виявити невідомі види атак, але з недоліків є наявність хибно позитивних спрацювань: невідома раніше законна діяльність може бути також класифікована як шкідлива.

Система запобігання вторгненням (IPS)

Система запобігання вторгненням (англ. *Intrusion Prevention System*, IPS) – програмна або апаратна система мережевої та комп'ютерної безпеки, яка виявляє вторгнення або порушення безпеки і автоматично захищає від них.

Системи IPS можна розглядати як розширення систем виявлення вторгнень (IDS), так як завдання відстеження атак залишається однаковою. Однак, вони відрізняються в тому, що IPS повинна відслідковувати активність в реальному часі і швидко реалізовувати дії щодо запобігання атак.

Класифікація IPS

– **Мережеві IPS (Network – based Intrusion Prevention, NIPS):** відстежують трафік в комп'ютерній мережі і блокують підозрілі потоки даних.

– **IPS для бездротових мереж (Wireless Intrusion Prevention Systems, WIPS):** перевіряє активність в бездротових мережах. Зокрема, виявляє невірно сконфігуровані точки бездротового доступу до мережі, атаки людина посередині, спуфинг MAC-адрес.

– **Поведінковий аналіз мережі (Network Behavior Analysis, NBA):** аналізує мережевий трафік, ідентифікує нетипові потоки (виявляє аномалії), наприклад DoS і DDoS атаки.

– **Система попередження вторгнень для окремих комп'ютерів (Host – based Intrusion Prevention, HIPS):** резидентні програми, які виявляють підозрілу активність на комп'ютері.

Історія розробок

Історія розвитку сучасних IPS включає в себе історії розвитку декількох незалежних рішень, проактивних методів захисту, які розроблялися в різний час для різного роду загроз. Під проактивними методами захисту, пропонованими сьогодні ринком, розуміється наступне:

1. Поведінковий аналізатор процесів для аналізу поведінки запущених в системі процесів і виявлення підозрілих дій, тобто невідомих шкідливих програм.

2. Усунення можливостей попадання інфекції на комп'ютер, блокування портів, які використовуються вже відомими вірусами, і тих, які можуть використовуватися їх новими модифікаціями.

3. Недопущення переповнення буфера у найбільш поширених програм і сервісів, що найбільш часто використовується зловмисниками для здійснення атаки.

4. Мінімізація шкоди, завданої інфекцією, запобігання подальшого її розмноження, обмеження доступу до файлів та директорій; виявлення і блокування джерела інфекції в мережі.

Аналіз мережевих пакетів

Зазвичай в якості першої загрози, яка спонукала до протидії вторгненням, називають хробака Морріса, що вразив підключені до мережі Unix-комп'ютери в листопаді 1988 року.

Згідно іншої теорії, стимулом для створення нової фортифікаційної споруди стали дії групи хакерів спільно зі спецслужбами СРСР і НДР. У період з 1986-го по 1989 рік група, ідейним керівником якої був Маркус Гесс, передавала своїм національним спецслужбам інформацію, здобуту ними шляхом вторгнення в комп'ютери. Все почалося з невідомого рахунку всього на 75 центів в Національній лабораторії ім. Е. Лоуренса в Берклі. Аналіз його походження в кінцевому підсумку вивів на Гесса, який працював програмістом в невеликій західнонімецькій компанії і одночасно належав до екстремістської групи Chaos Computer Club, яка базувалася в Гамбурзі.

Організоване ним вторгнення починалося з дзвінка з дому через найпростіший модем, що забезпечував йому зв'язок з європейською мережею Datex-P і далі проникнення в комп'ютер бібліотеки Бременського університету, де хакер отримував необхідні привілеї і вже з ними пробивався в Національну лабораторію ім. Е. Лоуренса в Берклі.

Перший лог був зареєстрований 27 липня 1987 року, і з 400 доступних комп'ютерів він зміг влізти приблизно в 30 і після цього спокійно пересуватись в закритій мережі Milnet, використовуючи, зокрема, пастку у вигляді файлу під назвою Strategic Defense Initiative Network Project (його цікавило все, що було пов'язано зі Стратегічною оборонною ініціативою президента Рейгана). Негайною реакцією на появу зовнішніх мережевих загроз виявилося створення міжмережевих екранів, як перших систем виявлення та фільтрації загроз.

Аналіз програм і файлів

Поведінковий блокувальник

З появою нових видів загроз згадали про поведінкові блокувальники.

Перше покоління поведінкових блокаторів з'явилося ще в середині 90-х років. Принцип їх роботи – при виявленні потенційно небезпечних дій користувачеві ставилося питання, дозволити або заборонити дію. Теоретично блокіратор здатний запобігти розповсюдженню будь-яких відомих, так і невідомих вірусів. Основним недоліком перших поведінкових блокувальників було надмірна кількість запитів до користувача. Причина цього – нездатність поведінкового блокувальника судити про шкідливості тої чи іншої дії. Однак, в програмах, написаних на VBA, можна з дуже великою ймовірністю відрізнити шкідливі дії від корисних.

Друге покоління поведінкових блокувальників відрізняється тим, що вони не аналізують окремі дії, а послідовність дій і вже на підставі цього роблять висновок про шкідливості того чи іншого ПЗ.

Методи реагування на атаки

Після початку атаки

Методи реалізуються вже після того, як була виявлена інформаційна атака. Це означає, що навіть у разі успішного виконання системі, що захищається може бути завдано шкоди.

Блокування з'єднання

Якщо для атаки використовується TCP-з'єднання, то реалізується його закриття за допомогою посилки кожному або одному з учасників TCP-пакета з встановленим прапором RST. У результаті зловмисник позбавляється можливості продовжувати атаку, використовуючи мережеве з'єднання. Даний метод найчастіше реалізується з допомогою наявних мережевих датчиків.

Метод характеризується двома основними недоліками:

1. Не підтримує протоколи, відмінні від TCP, для яких не вимагається попереднього встановлення з'єднання (наприклад, UDP і ICMP).

2. Метод може бути використаний тільки після того, як зловмисник вже отримав несанкціоноване з'єднання.

Блокування записів користувачів

Якщо кілька облікових записів користувачів були скомпрометовані в результаті атаки або виявилися їх джерелами, то здійснюється їх блокування хостовими датчиками системи. Для блокування датчики повинні бути запущені від імені облікового запису, який має права адміністратора.

Також блокування може відбуватися на заданий строк, який визначається налаштуваннями Системи запобігання вторгнень.

Блокування хоста комп'ютерної мережі

Якщо з одного з хостів була зафіксована атака, то може бути проведене його блокування хостовими датчиками або блокування мережевих інтерфейсів або на нього, або на маршрутизаторі або комутаторі, за допомогою яких хост підключений до мережі. Розблокування може відбуватися через заданий проміжок часу або за допомогою активації адміністратора безпеки. Блокування не скасовується після перезапуску або відключення від мережі хоста. Так само для нейтралізації атаки можна блокувати ціль атаки, хост комп'ютерної мережі.

Блокування атаки за допомогою мережевого екрану

IPS формує і надсилає нові конфігурації в мережевому екрані (ME), за якими екран буде фільтрувати трафік від порушника. Така реконфігурація може відбуватися в автоматичному режимі з допомогою стандартів OPSEC (наприклад SAMP, CPMI).

Для ME, які не підтримують протоколи OPSEC, для взаємодії із Системою запобігання вторгнення може бути використаний модуль-адаптер:

- на який будуть надходити команди про зміну конфігурації ME;
- який буде редагувати конфігурації ME для модифікації його параметрів.

Зміна конфігурації комунікаційного обладнання

Для протоколу SNMP, IPS аналізує і змінює параметри з бази даних MIB (такі як таблиць маршрутизації, налаштування портів) з допомогою агента пристрою, щоб блокувати атаку. Також можуть бути використані протоколи TFTP, Telnet та ін.

Активне придушення джерела атаки

Метод теоретично може бути використаний, якщо інші методи виявляться марними. IPS виявляє і блокує пакети порушника, та здійснює атаку на його сайт, за умови, що його адресу однозначно визначено і в результаті таких дій не буде завдано шкоди іншим легальним вузлам.

Такий метод реалізовано в декількох некомерційних ПЗ:

– NetBuster запобігає проникненню в комп'ютер «Троянського коня». Він може також використовуватися як засіб «fool-the-one-trying to NetBus-you» ("обдури того, хто намагається проникнути до тебе на «Троянському коні»). У цьому випадку він розшукує шкідливу програму і визначає комп'ютер який запустив її, а потім повертає цю програму адресанту.

– Tambu UDP Scrambler працює з портами UDP. Продукт діє не тільки як фіктивний UDP-порт, він може використовуватися для «паралізації» апаратури хакерів за допомогою невеликої програмки UDP flooder.

Так як гарантувати виконання всіх умов неможливо, широке застосування методу на практиці поки що неможливо.

На початку атаки

Методи реалізують заходи, які запобігають виявлені атаки до того, як вони досягають мети.

З допомогою мережевих датчиків

Мережеві датчики встановлюються в розрив каналу зв'язку так, щоб аналізувати всі пакети які проходять. Для цього вони оснащуються двома мережевими адаптерами, які функціонують у «змішаному режимі», на прийом і на передачу, записуючи всі пакети в буферну пам'ять, звідки вони зчитуються модулем виявлення атак IPS. У разі виявлення атаки ці пакети можуть бути видалені.

Аналіз пакетів проводиться на основі сигнатурного або поведінкового методів.

За допомогою хостових датчиків

- **Віддалені атаки**, які реалізуються відправкою від зловмисника серією пакетів. Захист реалізується з допомогою компоненти IPS за аналогією з мережевими датчиками, але на відміну від останніх мережева компонента перехоплює і аналізує пакети на різних рівнях взаємодії, що дає запобігати атакам по криптозахищеним IPsec і SSL/TLS з'єднанням.
- **Локальні атаки** при несанкціонованому запуску зловмисником програм або інших діях, що порушують інформаційну безпеку. Перехоплюючи системні виклики всіх додатків і аналізуючи їх, датчики блокують ті виклики, які становлять небезпеку.

12.4. Системи контролю та управління доступом (Active Directory, ACL)

Список контролю доступу (ACL)

Access Control List або ACL (*список контролю доступу*) – список прав доступу до об’єкта, який визначає, хто або що може отримувати доступ до нього, і які саме операції дозволено або заборонено цьому суб'єкту проводити над об'єктом.

Списки контролю доступу є основою систем з вибірковим управлінням доступом. У типових ACL кожен запис визначає суб'єкт впливу і операцію: наприклад, запис (Taras, delete) в ACL для файлу XYZ дає можливість користувачеві Taras видалити файл XYZ.

В системі з моделлю безпеки, заснованої на ACL, коли суб'єкт запитує виконання операції над об'єктом, система спочатку перевіряє список дозволених для цього суб'єкта операцій, і тільки після цього дає (або не дає) доступ до запитуваної дії.

При централізованому зберіганні списків контролю доступу можна говорити про матрицю доступу, в якій по осях розміщені об'єкти і суб'єкти, а в клітинках – відповідні права. Однак у великій кількості систем списки контролю

доступу до об'єктів зберігаються окремо для кожного об'єкта, найчастіше безпосередньо з самим об'єктом.

Традиційні ACL системи призначають права індивідуальним користувачам, і з часом і зростанням числа користувачів в системі списки доступу можуть стати громіздкими. Варіантом вирішення цієї проблеми є призначення прав групам користувачів, а не персонально. Іншим варіантом вирішення цієї проблеми є керування доступом на основі ролей, де функціональні підмножини прав до ряду об'єктів об'єднуються в «ролі», і ці ролі призначаються користувачам. Однак, у першому варіанті групи користувачів також часто називаються ролями.

Список контролю доступу (ACL) містить правила, які надають або забороняють доступ до певних цифрових середовищ. Є два типи ACL:

– **ACL файлової системи** – фільтрує доступ до файлів і/або каталогів. ACL файлової системи повідомляє операційним системам, які користувачі можуть отримати доступ до системи та які привілеї надані користувачам.

– **Мережні ACL** – фільтрує доступ до мережі. Мережні ACL повідомляють маршрутизаторам і комутаторам, який тип трафіку може отримати доступ до мережі та яка діяльність дозволена.

Файлові системи з ACL

У файлових системах для реалізації ACL використовується ідентифікатор користувача процесу (UID в термінах POSIX).

Список доступу являє собою структуру даних (зазвичай таблицю), що містить записи, які визначають права індивідуального користувача або групи на спеціальні системні об'єкти, такі як програми, процеси або файли. Ці записи також відомі як ACE (англ. *Access Control Entries*) в операційних системах Microsoft Windows і OpenVMS.

В операційній системі Linux і Mac OS X більшість файлових систем мають розширені атрибути, що виконують роль ACL. Кожен об'єкт в системі містить покажчик на свій ACL. Привілеї (або повноваження) визначають спеціальні права доступу, що дозволяють користувачеві читати з (англ. *read*), писати в (англ. *write*), або виконувати (англ. *execute*) об'єкт. У деяких реалізаціях ACE можуть визначати право користувача або групи на зміну ACL об'єкта.

Концепції ACL в різних операційних системах різняться, незважаючи на існуючий «стандарт» POSIX. (Проекти безпеки POSIX,.1e і.2c, були відкликані, коли стало ясно що вони зачіпають занадто велику область і робота не може бути завершена, але добре опрацьовані частини, що визначають ACL, були широко реалізовані і відомі як «POSIX ACLs».)

Мережеві ACL

У мережах ACL представляють список правил, що визначають порти служб або імена доменів, доступних на вузлі або іншому пристрої третього рівня OSI, кожен зі списком вузлів та/або мереж, яким дозволений доступ до сервісу. Мережеві ACL можуть бути налаштовані як на звичайному сервері, так і на маршрутизаторі і можуть керувати як вхідним, так і вихідним трафіком, як брандмауер.

Спочатку ACL були єдиним способом захисту брандмауерів (фаєрволів, міжмережевих екранів). Сьогодні існує багато типів брандмауерів і альтернатив ACL. Однак організації продовжують використовувати списки керування доступом у поєднанні з такими технологіями, як віртуальні приватні мережі (VPN), які визначають, який трафік слід шифрувати та передавати через тунель VPN.

Причини використання ACL:

– Контроль транспортного потоку.

– Обмежений мережевий трафік для кращої продуктивності мережі.

– Рівень безпеки доступу до мережі, який визначає, до яких областей сервера/мережі/служби може отримати доступ користувач, а до яких ні.

– Детальний моніторинг трафіку, що виходить і входить в систему.

Як працює ACL

ACL файлової системи – це таблиця, яка інформує операційну систему комп'ютера про привілеї доступу, які має користувач до системного об'єкта, включаючи один файл або файловий каталог. Кожен об'єкт має властивість безпеки, яка пов'язує його зі списком керування доступом. У списку є запис для кожного користувача з правами доступу до системи.

Типові привілеї включають право читати один файл (або всі файли) у каталозі, виконувати файл або записувати файл або файли. Операційні системи, які використовують ACL, включають, наприклад, Microsoft Windows, Digital OpenVMS і системи на базі UNIX.

Коли користувач запитує об'єкт у моделі безпеки на основі ACL, операційна система вивчає ACL на предмет відповідного запису та перевіряє, чи допустима запитана операція.

Мережеві ACL встановлюються в маршрутизаторах або комутаторах, де вони діють як фільтри трафіку. Кожен мережевий ACL містить попередньо визначені правила, які контролюють, яким пакетам або оновленням маршрутизації дозволено чи заборонено доступ до мережі.

Маршрутизатори та комутатори з ACL працюють як фільтри пакетів, які передають або відхиляють пакети на основі критеріїв фільтрації. Будучи пристроєм рівня 3, маршрутизатор із фільтрацією пакетів використовує правила, щоб визначити, чи слід дозволити або заборонити доступ до трафіку. Він вирішує це на основі IP-адрес джерела та призначення, порту призначення та вихідного порту та офіційної процедури пакета.

Типи списків контролю доступу

Списки контролю доступу можна розділити на дві основні категорії:

Стандартний ACL

Список доступу, розроблений виключно з використанням вихідної IP-адреси. Ці списки контролю доступу дозволяють або блокують увесь набір протоколів. Вони не розрізняють IP-трафік, наприклад UDP, TCP і HTTPS. Вони використовують номери 1-99 або 1300-1999, щоб маршрутизатор міг розпізнати адресу як вихідну IP-адресу.

Розширений ACL

Список доступу, який широко використовується, оскільки він може диференціювати IP-трафік. Він використовує IP-адреси джерела та призначення та номери портів, щоб зрозуміти IP-трафік. Ви також можете вказати, який IP-трафік має бути дозволений або заборонений. Вони використовують числа 100-199 і 2000-2699.

Порівняння Linux ACL та Windows ACL

Linux забезпечує гнучкість для внесення змін до ядра, що неможливо зробити з Windows. Однак, оскільки ви можете вносити зміни до ядра Linux, вам можуть знадобитися спеціальні знання для підтримки робочого середовища.

Windows пропонує перевагу стабільної платформи, але вона не така гнучка, як Linux. Що стосується інтеграції додатків, Windows легше, ніж Linux.

Користувач може налаштувати механізми контролю доступу в системі Windows без додавання програмного забезпечення.

З точки зору виправлень, Microsoft є єдиним джерелом для випуску виправлень Windows. З Linux ви можете зачекати, доки комерційний постачальник Linux випустить виправлення, або ви можете скористатися організацією з відкритим кодом для виправлень.

У Windows кожен дескриптор безпеки містить два види ACL – системні (system, SACL) та вибіркові (Discretionary, DACL)

Яка різниця між ACL, ACE, DACL і SACL?

Дескриптор безпеки містить два **списки керування доступом (ACL)**, які використовуються для призначення та відстеження інформації про безпеку для кожного об’єкта: **дискреційний список контролю доступу (DACL)** і **список контролю доступу до системи (SACL)**.

Дискреційні списки контролю доступу (DACL). DACL ідентифікують користувачів і групи, яким призначено або заборонено доступ до об’єкта. Якщо DACL явно не ідентифікує користувача або будь-які групи, членом яких є користувач, користувачеві буде відмовлено в доступі до цього об’єкта. За замовчуванням DACL контролюється власником об’єкта або особою, яка створила об’єкт, і містить **записи керування доступом (ACE)**, які визначають доступ користувача до об’єкта.

Списки контролю доступу до системи (SACL). SACL ідентифікують користувачів і групи, які потрібно перевірити, коли вони успішно отримують або не можуть отримати доступ до об’єкта. Аудит використовується для моніторингу подій, пов’язаних із системною або мережевою безпекою, для виявлення порушень безпеки, а також для визначення ступеня та місця будь-яких пошкоджень. За замовчуванням SACL контролюється власником об’єкта або особою, яка створила об’єкт. SACL містить **записи керування доступом (ACE)**, які визначають, чи реєструвати успішну чи невдалу спробу користувача отримати доступ до об’єкта за допомогою наданого дозволу, наприклад, Повний доступ і Читання.

Найкращі практики ACL

Налаштовуючи списки керування доступом, слід дотримуватися кількох найкращих практик, щоб переконатися, що безпека є жорсткою, а підозрілий трафік блокується:

1. Наскрізний ACL

ACL застосовуються на кожному інтерфейсі, майже в усіх засобах безпеки та маршрутизації. Це доречно, оскільки ви не можете мати однакові правила для зовнішніх інтерфейсів та інтерфейсів, які формують мережу вашого кампусу. Однак інтерфейси схожі, і ви не хочете, щоб деякі були захищені списками керування доступом, а інші – відкритими.

Практика ACL на всіх інтерфейсах є важливою для вхідних ACL, зокрема правил, які визначають, яка адреса може передавати дані у вашу мережу. Це правила, які роблять значну різницю.

2. ACL за порядком

Майже у всіх випадках механізм, що забезпечує дотримання ACL, починається зверху та рухається вниз у списку. Це має наслідки для розробки того, що ACL робитиме з певним потоком даних.

Одна з причин, чому організації використовують ACL, полягає в тому, що вони мають менші обчислювальні витрати, ніж брандмауери з підтримкою стану, і вони працюють на високій швидкості. Це важливо, коли ви намагаєтесь реалізувати безпеку для швидких мережевих інтерфейсів. Однак, чим довше пакет залишається в системі, поки він перевіряється на відповідність правилам у ACL, тим нижча продуктивність.

Фокус полягає в тому, щоб розмістити правила, які, як ви очікуєте, будуть активовані у верхній частині ACL. Працюйте від загального до конкретного, забезпечуючи логічне згрупування правил. Ви повинні знати, що на кожен пакет діятиме початкове правило, яке він запускає, ви можете в кінцевому підсумку передати пакет через одне правило, коли ви збираєтеся заблокувати його через інше. Подумайте, як ви хочете, щоб відбувався ланцюг подій, зокрема, додаючи нові правила.

3. Задокументуйте свою роботу

Коли ви додаєте правила ACL, задокументуйте, чому ви їх додаєте, для чого вони призначені та коли ви їх додали.

Вам не потрібно мати один коментар до правила. Ви можете зробити один коментар для блоку правил, складне пояснення для окремого правила або поєднати обидва підходи.

Розробники повинні переконатися, що поточні правила задокументовані, щоб нікому не доводилося здогадуватися, чому існує правило.

Порівняння RBAC й ACL

Розробники можуть використовувати системи **списків доступу на основі ролей (RBAC)** для контролю безпеки на детальному рівні. Замість того, щоб підкреслювати особу користувача та визначати, чи має він мати дозвіл переглядати щось у програмі, RBAC керує безпекою на основі ролі користувача в організації.

Наприклад, замість того, щоб надати дозвіл Джону Сміту, архітектору з Нью-Йорка, RBAC надасть дозвіл на роль для архітекторів США. Джон Сміт може бути одним із багатьох користувачів із цією роллю. Таким чином, RBAC гарантує контролюючим особам, що лише певні користувачі мають доступ до конфіденційної інформації, оскільки дає всі дозволи на основі ролей.

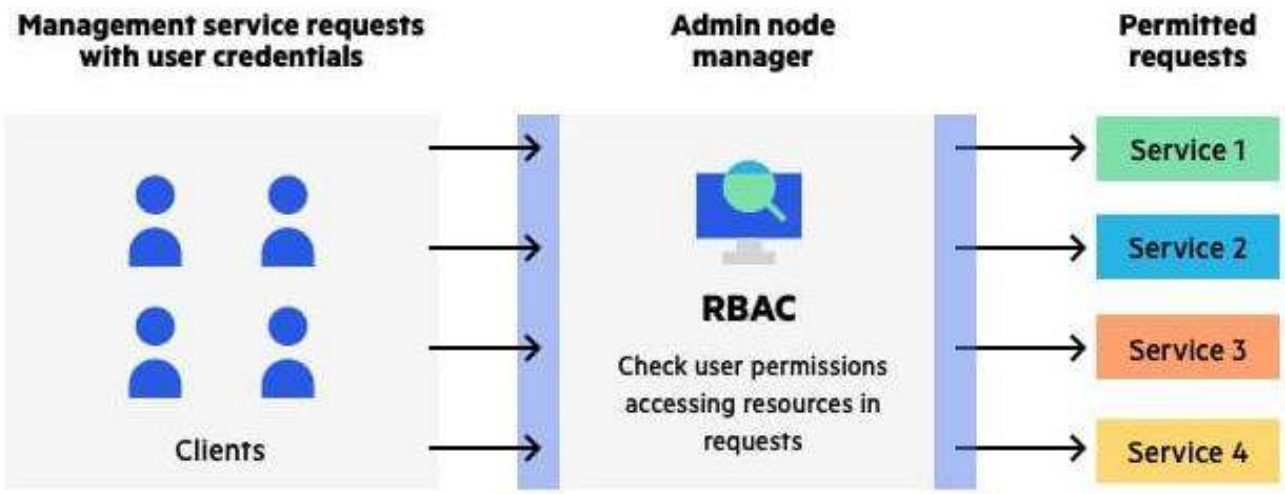

Рисунок 12.2 – Приклад системи керування доступом на основі ролей (RBAC)

RBAC зазвичай вважається кращим методом для бізнес-додатків. RBAC є більш ефективним, ніж ACL, щодо адміністративних витрат і безпеки. ACL найкраще використовувати для застосування безпеки на рівні окремого користувача. Ви можете використовувати RBAC для обслуговування системи безпеки всієї компанії, яку контролює адміністратор. Наприклад, ACL може надати доступ для запису до певного файлу, але він не може визначити, як користувач може змінювати файл.

12.5. Система контролю та управління доступом (СКУД)

Система контролю та управління доступом, **СКУД** (англ. *Physical Access Control System, PACS*) – сукупність програмно-апаратних технічних засобів контролю та засобів управління, що мають на меті обмеження та реєстрацію входу-виходу об'єктів (людей, транспорту) на заданій території через «точки проходу»: двері, ворота, КПП.

Основне завдання – управління доступом на задану територію (кого пускати, в який час і яку територію), включаючи:

– обмеження доступу на задану територію;
– ідентифікацію особи, яка має доступ на задану територію.

Додаткові завдання:

– облік робочого часу;

– розрахунок заробітної плати (при інтеграції із системами бухгалтерського обліку);

– ведення бази персоналу/відвідувачів;

– інтеграція із системою безпеки, наприклад:

- із системою відеоспостереження для поєднання архівів подій систем, передачі системі відеоспостереження сповіщень про необхідність стартувати запис, повернути камеру для запису наслідків зафіксованої підозрілої події;
- з системою охоронної сигналізації (СОС), наприклад, для обмеження доступу до приміщень, що стоять на охороні, або для автоматичного зняття та постановки приміщень на охорону.
- з системою пожежної сигналізації (СПС) для отримання інформації про стан пожежних сповіщувачів, автоматичне розблокування евакуаційних виходів та закриття протипожежних дверей у разі пожежної тривоги.

На особливо відповідальних об'єктах мережа пристроїв СКУД виконується фізично не пов'язаною з іншими інформаційними мережами.

Запобіжні пристрої

Встановлюються на двері:

– Електрозасувки – їх зазвичай встановлюють на внутрішні двері (внутрішньоофісні і т. п.) Електрозащілки, як і інші типи замків, бувають напругою, що відкриваються (тобто двері відкриваються при подачі напруги живлення на замок), і напругою, що закриваються (відчиняються, як тільки з них знімається напруга живлення, тому рекомендовано для використання пожежною інспекцією).

– Електромагнітні замки – практично всі замикаються напругою, тобто придатні для встановлення на шляхах евакуації під час пожежі.

– Електромеханічні замки – досить стійкі до злому (якщо міцний замок механічно), багато хто має механічний перевзвод (це означає, що якщо на замок подали відкриваючий імпульс, він буде розблокований до тих пір, поки двері не відчинять).

Встановлюються на проходах/проїздах:

Турнікет-трипод поясний із зчитувачем системи контролю доступу

– Турнікети використовуються на прохідних підприємствах, суспільно значущих об'єктах (стадіони, вокзали, метро, деякі держустанови) скрізь, де потрібно організувати контрольований прохід великої кількості людей. Турнікети поділяються на два основні типи: поясні та повноростові. Якщо поряд з турнікетом немає вільного проходу, що швидко відкривається (на випадок пожежі), поясний турнікет повинен бути обладнаний т.з. планками «антипаніка» – планками, що зламуються зусиллям нормальної людини (вимога пожежної інспекції).

– Шлюзові кабіни – використовуються в банках, на режимних об'єктах (на підприємствах із підвищеними вимогами до безпеки).

– Ворота та шлагбауми – переважно встановлюються на в'їздах на територію підприємства, на автомобільних парковках та автостоянках, на в'їздах на прибудинкову територію, у двори житлових будівель. Основна вимога – стійкість до кліматичних умов та можливість автоматизованого керування (за допомогою системи контролю доступу). Коли йдеться про організацію контролю доступу до проїзду, до системи пред'являються додаткові вимоги – підвищена дальність зчитування міток, розпізнавання автомобільних номерів (у разі інтеграції із системою відеоспостереження).

– Автоматичні дорожні бар'єри – використовуються для гарантованого запобігання несанкціонованому проїзду автотранспорту на територію, що захищається. Є заходами антитерористичного захисту, оскільки проїзд через піднятий бар'єр призводить до руйнування підвіски автомобіля.

Ідентифікатор

Основні типи виконання – картка, брелок, мітка. Є базовим елементом системи контролю доступу, оскільки зберігає код, який служить визначення прав («ідентифікації») власника. Це може бути Touch memory, безконтактна карта (наприклад, RFID-мітка), або застаріваючий тип карток з магнітною смугою. Як ідентифікатор можуть виступати також коди, що вводяться на клавіатурі, або окремі біометричні ознаки людини – відбиток пальця, малюнок сітківки або райдужної оболонки ока, тривимірне зображення обличчя.

Надійність (стійкість до злому) системи контролю доступу значною мірою визначається типом ідентифікатора, що використовується: наприклад, найбільш поширені безконтактні карти proximity можуть підроблятися в майстернях з виготовлення ключів на устаткуванні, наявному у вільному продажу. Тому для об'єктів, які потребують вищого рівня захисту, такі ідентифікатори не підходять. Принципово вищий рівень захищеності забезпечують RFID-мітки, у яких код карти зберігається у захищеній області й шифрується.

Крім безпосереднього використання в системах контролю доступу, RFID-мітки широко застосовуються і в інших областях. Наприклад, у локальних розрахункових системах (оплата обідів у їдальні та інших послуг), системах лояльності тощо.

Контролер

Автономний контролер – це «мозок» системи: саме контролер визначає, чи пропустити власника ідентифікатора у двері, оскільки зберігає коди ідентифікаторів зі списком прав доступу кожного з них у власній енергонезалежній пам'яті. Коли людина пред'являє (підносить до пристрою, що зчитує) ідентифікатор, лічений з нього код порівнюється з зберігається в базі, на підставі чого приймається рішення про відкриття дверей.

Мережевий контролер об'єднується в єдину систему з іншими контролерами та комп'ютером для можливості централізованого контролю та управління. У такому разі рішення про надання доступу може прийматись як

контролером, так і програмним забезпеченням головного комп'ютера. Найчастіше об'єднання контролерів мережу здійснюється за допомогою промислового інтерфейсу RS-485 або локальної мережі Ethernet.

У випадках, коли необхідно забезпечити роботу контролера при аваріях електромережі, блок контролера забезпечується власним акумулятором або зовнішнім блоком резервного живлення. Час роботи від акумулятора може становити від кількох годин до кількох діб.

Зчитувач

Це пристрій, який отримує («зчитує») код ідентифікатора та передає його в контролер. Варіанти виконання зчитувача залежать від типу ідентифікатора: для «таблетки» – це два електричні контакти (у вигляді «лузи»), для proximity-карти – це електронна плата з антеною в корпусі, а для зчитування, наприклад, малюнку райдужної оболонки ока до складу зчитувача має входити камера. Якщо зчитувач встановлюється на вулиці (ворота, зовнішні двері будівлі, проїзд на територію автостоянки), то він повинен витримувати кліматичні навантаження – перепади температур, опади – особливо якщо йдеться про об'єкти в районах із суворими кліматичними умовами. А якщо існує загроза вандалізму, потрібна ще й механічна міцність (сталевий корпус). Окремо можна виділити зчитувачі для дальньої ідентифікації об'єктів (з відстанню ідентифікації до 50 м). Такі системи зручні на автомобільних проїздах, парковках, на в'їздах на платні дороги тощо. Ідентифікатори для таких зчитувачів, як правило, активні (містять вбудовану батарейку).

Конвертери середовища

Служать для підключення апаратних модулів СКУД один до одного та до ПК. Наприклад, є популярними конвертори RS-485 ↔ RS-232 та RS-485 ↔ Ethernet. Деякі контролери СКУД вже мають інтегрований інтерфейс Ethernet, що дозволяє без використання будь-яких додаткових пристроїв підключатися до ПК і зв'язуватися один з одним.

Допоміжне обладнання

Блоки безперебійного живлення, дверні доводчики, датчики відчинення дверей, кнопки, дроти, відеоспостереження і т.д.

Програмне забезпечення

Не є обов'язковим елементом системи контролю доступу, використовується у разі, коли потрібна обробка інформації про проходи, побудова звітів, або коли для початкового програмування, управління та збору інформації в процесі роботи системи необхідне мережне програмне забезпечення, яке встановлюється на один або кілька ПК, з'єднаних у мережа.

Усі СКУД можна віднести до двох великих класів або категорій: мережеві системи та автономні системи.

Популярні компанії виробники програмного забезпечення систем контролю та управління доступу: ITV Group, ZkTeco, PERCo, ControlGate, Hikvision, Bosh, Parsec, Bolid, RusGuard, HID Global, IronLogic, OVISION.

Мережеві системи

У мережі всі контролери з'єднані з комп'ютером, що дає безліч переваг для великих підприємств, але зовсім не потрібно для «однодверної» СКУД. Мережеві системи зручні для великих об'єктів (офіси, виробничі підприємства), оскільки керувати навіть десятком дверей, на яких встановлені автономні системи, стає надзвичайно важко. Незамінні мережеві системи у таких випадках:

– якщо необхідно реалізувати складні алгоритми допуску груп співробітників з різними привілеями до різних зон підприємства та мати можливість оперативно їх змінювати;

– якщо необхідно вибірково видаляти або створювати перепустки (мітки) для великої кількості точок проходу або для великої кількості співробітників (велика текучка та втрати пропусків);

– якщо необхідна інформація про події (архів подій), що відбулися раніше, або потрібен додатковий контроль у реальному часі. Наприклад, у мережній системі існує функція фотоверифікації: на прохідній при піднесенні вхідною людиною ідентифікатора до зчитувача, службовець (вахтер, охоронець) може на екрані монітора бачити фотографію людини, якій у базі даних присвоєно даний ідентифікатор, і порівняти із зовнішністю проходить, що під передачі карток іншим;

– якщо необхідно організувати облік робочого дня та контроль трудової дисципліни;

– якщо необхідно забезпечити взаємодію (інтеграцію) з іншими підсистемами безпеки, наприклад, відеоспостереженням або пожежною сигналізацією).

У мережній системі з одного місця можна не тільки контролювати події на всій території, що охороняється, але і централізовано управляти правами користувачів, вести базу даних. Мережеві системи дозволяють організувати кілька робочих місць, розділивши функції управління між різними співробітниками та службами підприємства.

У мережевих системах контролю доступу можуть застосовуватися бездротові технології, звані радіоканали. Використання бездротових мереж часто визначається конкретними ситуаціями: складно чи неможливо прокласти провідні комунікації між об'єктами, скорочення фінансових витрат на монтаж точки проходу тощо. Існує велика кількість варіантів радіоканалів, однак у СКУД використовуються лише деякі з них.

– Bluetooth. Даний вид бездротового пристрою передачі даних є аналогом Ethernet. Його особливість полягає в тому, що відпадає необхідність прокладати паралельні комунікації для об'єднання компонентів під час використання інтерфейсу RS-485.

– Wi-Fi. Основна перевага даного радіоканалу полягає у великій дальності зв'язку, здатного досягати кількох сотень метрів. Це особливо необхідно для

з'єднання між собою об'єктів на великих відстанях (?). При цьому скорочуються як тимчасові, і фінансові витрати на прокладання вуличних комунікацій.

– ZigBee. Спочатку сферою застосування даного радіоканалу була система охоронної та пожежної сигналізації. Технології не стоять на місці та активно розвиваються, тому ZigBee може використовуватись і в системах контролю доступу. Ця бездротова технологія працює в діапазоні 2,45 ГГц, що не ліцензується.

– GSM. Перевага використання бездротового каналу зв'язку – практично суцільне покриття. До основних методів передачі інформації в мережі, що розглядається, відносяться GPRS, SMS і голосовий канал.

Непоодинокі ситуації, коли встановлення повноцінної системи безпеки може виявитися невиправдано дорогою для вирішення поставленого завдання. У таких ситуаціях оптимальним рішенням буде встановлення автономного контролера на кожну точку проходу, які необхідно обладнати доступом.

Автономні системи

Автономні системи дешевші, простіше в експлуатації, не вимагають прокладання сотень метрів кабелю, використання пристроїв сполучення з комп'ютером, самого комп'ютера. При цьому до мінусів таких систем відноситься неможливість створювати звіти, вести облік робочого часу, передавати та узагальнювати інформацію про події, керуватися дистанційно. При виборі автономної системи з високими вимогами безпеки рекомендується звернути увагу на наступне:

– Зчитувач повинен бути відокремлений від контролера, щоб дроти, якими можливе відкривання замка, були недоступні зовні.

– Контролер повинен мати резервне джерело живлення у разі відключення електроживлення.

– Переважно використовувати зчитувач у вандалозахищеному корпусі.

У складі автономної системи контролю доступу використовуються також електронні замки, що передають інформацію бездротовими каналами зв'язку: у двері встановлюється механічний замок з електронним управлінням і вбудованим зчитувачем. Замок по радіоканалу пов'язаний з хабом, який вже по дротах обмінюється інформацією з робочою станцією, де встановлено програмне забезпечення.

Для автономної системи можна використовувати «зворотний метод», коли на контрольних точках встановлюються ідентифікатори, а співробітники відзначаються зчитувачем-контролером, згодом дані передаються при першій нагоді – поява зв'язку у зчитувача. Цей метод зручно використовувати, наприклад, у місцях, де відсутня зв'язок, можливість прокладання електроживлення або інших комунікацій. Також «зворотний метод» може використовуватися для контролю патрулювання великих периметрів: після обходу території або після закінчення зміни охоронець здає на перевірку контролер, в якому записані всі контрольні точки, що пройшли, із зазначенням послідовності проходу і часу проходу кожної точки.

Додаткові можливості

– GSM модуль, який дозволяє надсилати SMS з інформацією про прохід (використовується, наприклад, у школах).

– для мережевий СКУД (також деякі автономні системи) – можливість віддаленого управління мережею Інтернет (наприклад, управління системою контролю доступу з центрального офісу, якщо підприємство має безліч філій).

– комплекс для персоналізації пластикових карток (принтер для друку на пластиковій картці даних власника, у тому числі фотографії).

– режим «антипасбек» – якщо людина вже пройшла на територію, що охороняється, то повторне пред'явлення її ідентифікатора на вхід буде заборонено (поки карта не буде пред'явлена на вихід), що виключить можливість проходу по одній карті двох і більше осіб. При цьому мережний СКУД дозволяє організувати такий режим на всіх точках проходу, об'єднаних у мережу, що забезпечує повнофункціональний захист по всьому периметру контрольованої території.

Застосування СКУД

Сфери застосування СКУД різноманітні:

– офіси компаній; бізнес-центри;
– банки;
– заклади освіти (школи, технікуми, виші);
– промислове підприємство;
– охоронювані території;
– автостоянки, паркування;
– місця проїзду автотранспорту;
– приватні будинки, житлові комплекси, котеджі;
– готелі;
– громадські установи (спорткомплекси, музеї, метрополітен та ін.).

Основні типи компаній на ринку

– Виробники.
– Дистриб'ютори.
– Проектувальники.
– Інтегратори.
– Торгові будинки.
– Монтажні організації.
– Кінцеві замовники.
– Великі кінцеві замовники (мають власну службу безпеки).