Тема: Контроль цілісності програмних і інформаційних ресурсів. Виявлення атак. Захист периметра комп'ютерних мереж. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки.

Цілісність є однією з властивостей безпеки інформації. Цілісність забезпечується або механізмами розмежування доступу, або механізмами контролю цілісності.

Під *контролем цілісності інформації* розуміють процес перевірки наявності викривлень цієї інформації, незалежно від причин їх походження (навмисні чи ненавмисні)

Під *контролем та поновленням цілісності інформації* розуміють процес перевірки наявності викривлень цієї інформації, незалежно від причин їх походження (навмисні чи ненавмисні), з наступною корекцією викривленої інформації.

Порушення цілісності може статись внаслідок наступних причин:

1) помилок користувачів, які викликають викривлення чи втрату інформації;
2) навмисних дій осіб, які не мають прав доступу до автоматизованої системи;
3) збоїв обладнання, які викликають викривлення чи втрату інформації;
4) фізичних впливів на носії інформації;
5) вірусних впливів.

Цілісність програмних засобів та інформації, що обробляється досягається використанням двох груп механізмів захисту - без перетворення інформації та механізмів захисту з її перетворенням.

До механізмів забезпечення цілісності без перетворення інформації слід віднести використання резервних копій програмних засобів та баз даних. Такий спосіб, безумовно, є найнадійнішим, оскільки завжди дозволяє не тільки установити факт порушення цілісності, але й поновити порушену інформацію, правда це є і першою вадою. Іншими словами, цей спосіб не дає змоги оперативно установити наявність порушення цілісності інформації, що змінюється.

До другої групи механізмів захисту відносяться такі відомі механізми з використанням: сигнатур важливих об’єктів, хеш – функції важливих об’єктів, забезпечення цілісності архівної інформації в тому числі і резервних копій програмних засобів та баз даних.

При передачі інформації по каналах зв’язку контроль цілісності (контроль наявності будь – яких викривлень інформації) та усунення цих викривлень покладаються на комунікаційне обладнання та протоколи зв’язку. Проблема поновлення цілісності вирішується за рахунок повторної передачі повідомлень Таким чином, механізми захисту з використанням сигнатур важливих об’єктів ґрунтуються на застосуванні швидко діючих процедур виявлення порушення цілісності та подальшому поновленні викривленої інформації за рахунок повторної передачі непошкодженої інформації чи повторного запису непошкодженої інформації з її резервної копії.

Механізми захисту з використанням хеш: контроль цілісності інформації носія забезпечується шляхом порівняння хеш функції відповідного носія, яка обчислюється під час контролю цілісності інформації, з хеш-функцією, яка була обчислена для того ж самого носія під час запису інформації. Якщо ці функції співпадають, то цілісність даного носія не порушена.

Виявлення атак. Захист периметра комп’ютерних мереж

Процес виявлення атак є процесом оцінки підозрілих дій, які відбуваються в корпоративній мережі. Інакше кажучи, виявлення атак (intrusion detection) це процес ідентифікації й реагування на підозрілу діяльність, спрямовану на обчислювальні або мережні ресурси.

Основні підходи до виявлення атак практично не змінилися за останню чверть століття, і, незважаючи на гучні заяви розробників, можна з упевненістю стверджувати, що виявлення атак базується або на методах *сигнатурного аналізу*, або на методах *виявлення аномалій*. Можливо також спільне використання зазначених вище методів.

Існує кілька способів класифікації систем виявлення атак, кожен з яких заснований на різних характеристиках:

- *Спосіб контролю за системою* (поділяються на network-based, host-based і applicationbased).

- *Спосіб аналізу.* (частина системи визначення проникнення, яка аналізує події, отримані з джерела інформації, і приймає рішення, чи відбувається проникнення). Способами аналізу є виявлення зловживань (misuse detection) та виявлення аномалій (anomaly detection).
- *Затримка в часі між отриманням інформації з джерела та її аналізом і прийняттям рішення*. Залежно від затримки в часі, системи виявлення атак діляться на interval-based (або пакетний режим) і real-time.

Механізми виявлення атак, застосовувані в сучасних системах виявлення атак IDS (Intrusion Detection System), засновані на декількох загальних методах.

Класифікація систем виявлення атак може бути виконана за декількома ознаками:

- *за способом реагування*; розрізняють пасивні й активні IDS. **Пасивні** IDS просто фіксують факт атаки, записують дані у файл журналу й видають попередження. **Активні** IDS намагаються протидіяти атаці.
- за способом виявлення атаки; За способом виявлення атаки системи IDS прийнято ділити на дві категорії: *виявлення аномального поводження* (anomaly-based); *виявлення зловживань* (misuse detection або signature-based). Аномальне поводження користувача (тобто атака або яка-небудь ворожа дія) часте проявляється як відхилення від нормального поводження. Прикладом аномального поводження може служити велика кількість з'єднань за короткий проміжок часу, високе завантаження центрального процесора й т.ін. Однак аномальне поводження не завжди є атакою. Наприклад, одночасну посилку великої кількості запитів від адміністратора мережі система виявлення атак може ідентифікувати як атаку типу "відмова в обслуговуванні" (denial of service).
- *за способом збору інформації про атаку*.

Аналіз активності

Статичні і динамічні IDS

- Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе ПО, 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.

Хостові IDS

- IDS, які встановлюються на хості і виявляють зловмисні дії на ньому називаються хостовими або системними IDS.

Експертні системи.

- Експертна система складається з набору правил, які охоплюють знання людини-експерта. Використання експертних систем являє собою розповсюджений метод виявлення атак, при якому інформація про атаки формулюється у вигляді правил. Ці правила можуть бути записані, наприклад, у вигляді послідовності дій або сигнатури. При виконанні кожного із цих правил приймається рішення про наявність несанкціонованої діяльності. Важливим достоїнством такого підходу є практично повна відсутність фіктивних тривог.

Сигнатурний аналіз заснований на припущенні, що сценарій атаки відомий і спроба її реалізації може бути виявлена в журналах реєстрації подій або шляхом аналізу мережевого трафіку

Стандарти кібербезпеки

Стандарти кібербезпеки – це методи, що зазвичай викладені в опублікованих матеріалах, які намагаються захистити кібернетичне середовище користувача чи організації.

Це середовище включає в себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, інформацію в режимі зберігання або транзиту, програми, служби та системи, які можуть бути безпосередньо або опосередковано підключені до мереж.

Основна мета — знизити ризики, включаючи попередження або пом'якшення кібер-атак. Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології.

Міжнародні стандарти

BS 7799-1: 2005 — Британський стандарт BS 7799 перша частина. BS 7799 Частина 1 — Кодекс практики управління інформаційною безпекою (Практичні правила управління інформаційної безпеки) описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду в цій області . Цей документ служить практичним керівництвом по створенню СУІБ

BS 7799-2: 2005 — Британський стандарт BS 7799 друга частина стандарту. BS 7799 Частина 2 — Управління інформаційною безпекою — специфікація систем управління інформаційною безпекою (Специфікація системи управління інформаційної безпеки) визначає специфікацію СУИБ. Втора частина стандарту використовується як критерії при проведенні офіційної процедури сертифікації СУІБ організації.

BS 7799-3: 2006 — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт в області управління ризиками інформаційної безпеки

ISO/IEC 17799: 2005 — «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005.

ISO/IEC 27000 — Словарь і визначення.

ISO/IEC 27001 — «Інформаційні технології — Методи забезпечення безпеки — Системы управління інформаційної безпеки — Требования». Міжнародний стандарт, базувався на BS 7799-2: 2005.

ISO/IEC 27002 — Зараз**: ISO/IEC 17799: 2005**. «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Дата выхода — 2007 год.

ISO/IEC 27005 — Зараз: **BS 7799-3: 2006** — Руководство по управлению рисками ИБ.

Німецьке агентство з інформаційної безпеки. Інструкція з захисту базової лінії — стандартні гарантії безпеки (керівництво по базовому рівню захисту інформаційних технологій).

Тема: Проблеми забезпечення безпеки в комп'ютерних системах і мережах. Типова корпоративна мережа. Рівні інформаційної інфраструктури корпоративної мережі. Мережеві загрози, вразливості і атаки. Засоби захисту мереж.

1. Проблеми забезпечення безпеки в комп'ютерних системах і мережах

Захист інформації в комп'ютерних системах володіє рядом специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаної з носієм, може легко і швидко копіюватись та передаватися по каналах зв'язку. Виникнення глобальних інформаційних мереж типу Internet є важливим досягненням комп'ютерних технологій, однак, з Internet пов'язано безліч комп'ютерних злочинів.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи:

1) перехоплення інформації – при перехоплені порушується конфіденційність інформації;

2) модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і надсилається адресату;

3) підміна авторства інформації.

Ця проблема може мати серйозні наслідки. Наприклад, хтось може надіслати листа від вашого імені (цей вид обману прийнято називати спуфінга) або Web-сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

2. Корпоративна мережа.

Корпоративна мережа — це мережа, головним призначенням якої є підтримка роботи конкретного підприємства, що володіє даною мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства.

Корпоративна мережа - це складний комплекс взаємозалежних і узгоджено функціонуючих програмних і апаратних компонентів, який забезпечує передачу інформації між різними віддаленими додатками й системами, що використовуються на підприємстві.

Основними елементами мережі є робочі станції, сервери і комутатори. Основну частину мережі складають робочі станції, які підключені до комутаторів. Комутатори пересилають пакети даних з одного порту в іншій за потрібною адресою. Також в мережі є сервери, що забезпечують роботу робочих станцій в складі мережі.

Наявність мережі приводить до ***вдосконалення комунікацій*** між співробітниками підприємства, а також його клієнтами і постачальниками. Мережі знижують потребу підприємств в інших формах передачі інформації, таких як телефон або звичайна пошта.

Безпе́ка мере́жі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу.

Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів.

3. Мережеві загрози вразливості і атаки

Дії, які так або інакше загрожують збереженню, що допускають нанесення збитків інформаційній безпеці підрозділяються на певні категорії.

1. *Дії, які здійснюють користувачі, авторизовані в системі*. Ця категорія включає:
   - зловмисні дії користувача з метою крадіжки або повного або часткового знищення даних, що є на сервері або робочій станції компанії
   - пошкодження наявних даних як результат прояву необережності, халатності у діях користувача.

2. *"Електронне" втручання - дії хакерів*:
   - здійснення DOS та dDOS-атак
   - незаконе проникнення в захищені комп'ютерні мережі;

Несанкціоноване проникнення ззовні в захищену мережу тієї або іншої компанії може здійснюватися з метою нанесення збитку (знищення, підміна наявних даних), крадіжка інформації, що відноситься до розряду конфіденційною з подальшим її незаконним використанням, розпорядження мережевою інфраструктурою компанії як методом для здійснення атак на інші мережеві вузли, крадіжка грошових коштів з рахунків компанії або окремих користувачів і т.д.

Атаки категорії DOS ("Denial of Service") здійснюються ззовні і направлені на мережеві вузли тієї або іншої компанії, які відповідають за її безпечне, ефективне і стабільне функціонування (поштовий, файловий сервер). Зловмисниками організовується масова відправка яких-небудь даних на вибрані вузли, що викликає їх перевантаження, тим самим, виводячи з працездатного стану на деякий час. Подібні атаки можуть обернутися для постраждалої компанії різними порушеннями в здійсненні безперервних бізнес-процесів, втратою клієнтів, а також втратою репутації.

3. *Комп'ютерні віруси*. Комп'ютерні віруси, так само, як і деякі інші шкідливі програми відносяться до окремої категорії способів електронної дії з подальшим нанесенням збитку. Дані засоби дії є реальною загрозою для ведення сучасного бізнесу, що має на увазі широке використання комп'ютерних мереж, електронної пошти і Інтернету в цілому. Так, "вдале" проникнення шкідливої програми (вірусу) в корпоративні мережеві вузли тягне за собою не тільки виведенням їх із стану стабільного функціонування, але і велику втрату часу, втрату наявних даних, зокрема не виключена можливість крадіжки конфіденційної інформації і прямих розкрадань грошових коштів з рахунків. Програма-вірус, яка проникла і залишилася непоміченою в корпоративній мережі дає можливість здійснення зловмисниками повного або ж часткового контролю над всією діяльністю компанії, що ведеться в електронному основним каналом для ефективного і швидкого розповсюдження спаму і вигляді.

4. *Спам*. Якщо ще кілька років тому спам був всього лише незначним по масштабах, дратівливим чинником, то в даний час технології спаму представляють достатньо серйозну загрозу для забезпечення інформаційної безпеки:

- основним каналом для ефективного і швидкого розповсюдження спаму і інших шкідливих програм стала електронна пошта;
- на перегляд спаму йде достатньо велика кількість часу, а подальше видалення численних повідомлень може викликати відчуття дискомфорту співробітників на психологічному рівні
- спам може виступати одним з основних методів реалізації різних шахрайських схем, жертвами яких можуть ставати як приватні, так і юридичні особи;
- великий ризик видалення потрібної кореспонденції разом із спамом, що може привести до різного роду неприємним наслідкам; при цьому така небезпека зростає, якщо удаватися до використання недосконалих поштових фільтрів для виявлення і відсіювання спаму;

5. *"Природні" загрози*. В категорію "природних" загроз відносять різні зовнішні чинники. Так, причиною втрати інформаційної безпеки може виступити крадіжка інформаційних носіїв, форс-мажорні обставини, неправильний спосіб зберігання інформації

Засоби захисту мереж. Політика безпеки при доступі до мереж загального значення

Для безпеки в комп'ютерних мереж використовують таке програмне забезпечення:

● Secure Shell, SSH (англ. Secure SHell — «безпечна оболонка» — мережевий протокол рівня додатків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів).

● Міжмережевий екран (брандмауер, файрвол англ. Firewall, буквально «вогняна стіна») — пристрій або набір пристроїв, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік між областями різної безпеки згідно з набором правил та інших критеріїв. Фаєрвол може бути у вигляді окремого приладу (так званий маршрутизатор або роутер), або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі- сервер.

● Антівірусна програма (антивірус) — програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом. Антивірусне програмне забезпечення складається з комп'ютерних програм, які намагаються знайти, запобігти розмноженню і видалити комп'ютерні віруси та інші шкідливі програми.

Тема. **Призначення, можливості, і основні захисні механізми міжмережевих екранів (брандмауерів). Основні захисні механізми мереж. Політика безпеки при доступі до мережі загального користування.**

Якщо комп'ютер підключений до Інтернету, то будь-який користувач, також підключений до Інтернету, може отримати доступ до інформаційних ресурсів цього комп'ютера.

Є різні механізми проникнення з Інтернету на локальний комп'ютер і в локальну мережу:

- веб-сторінки, що завантажуються в браузер, можуть містити активні елементи, здатні виконувати *деструктивні дії* на локальному комп'ютері;
- деякі веб-сервери розміщують на локальному комп'ютері текстові файли cookie, використовуючи які, можна отримати конфіденційну інформацію про користувача локального комп'ютера; електронні листи або дописи в соціальних мережах можуть містити *шкідливі посилання*;
- за допомогою спеціальних програм можна отримати доступ до дисків і файлів локального комп'ютера тощо.

Що таке "cookie-файл"?

"Cookie-файл" (**HTTP-cookie**, «**Ку́кі**» або «**реп'яшки**» (англ. *Cookies*- тістечка, печиво)) - це невеликий файл, який містить ряд символів, що надсилається до вашого комп'ютера при перегляді веб-сайта. Застосовується для збереження даних, специфічних для даного користувача.

Таким чином веб-сервер помічає браузер користувача при відвідуванні. Куки створюються за ініціативою скриптового сценарію на стороні веб-браузера. При наступному візиті сервер буде знати, що користувач вже тут був. За допомогою кукі-технології можна вивчити вподобання відвідувача. Кукі є одним із найточніших засобів визначення унікального користувача.

Google використовує cookie-файли, щоб покращити якість надання послуг і краще розпізнавати бажання користувачів до взаємодії. Увімкнення cookie-файлів необхідне для користування обліковим записом Google.

В комп'ютерних системах використовуються такі засоби мережевого захисту інформації:

1) Брандмауери (або ***міжмережеві екрани*** *(Firewall)*) — для блокування атак, це окремі пристрої чи спеціальні програми, які створюють бар'єр між комп'ютером і мережею, між внутрішньою локальною мережею організації та Інтернетом.

Термін брандмауер походить від нім. brand — пожежа та mauer — стіна; його англійський еквівалент — firewall, асоціюється з вогнестійкою капітальною стіною, що перешкоджає поширенню пожежі. Термін виник приблизно в 1995 р.

Мережеві екрани керують проходженням мережевого трафіку відповідно до правил (*policies*) захисту, контролюють трафік, що входить в мережу і що виходить з неї.

За допомогою програм-брандмауерів відслідковуються всі під'єднання й за необхідності дозволяється чи блокується доступ до комп'ютера. Використовуючи інтерфейс налаштувань профілю доступу міжмережевого екрану, є можливість для кожного користувача створити свій профіль, який буде визначати не тільки права доступу цього користувача до мережі Інтернет, але і права доступу до цього користувача з Інтернет. Міжмережевий екран може блокувати спроби хакерів, вірусів і черв'яків отримати доступ до вашого комп'ютера через Інтернет. Добре сконфігурований міжмережевий екран спроможний зупинити більшість відомих комп'ютерних атак.

Як правило, міжмережеві екрани встановлюються на вході мережі і розділяють внутрішні (приватні) та зовнішні (загального доступу) мережі.

2) Іншим пристроєм ефективного захисту в комп'ютерних мережах є ***маршрутизатор***. Він здійснює фільтрацію пакетів даних для передачі і, тим самим, з'являється можливість заборонити доступ деяким користувачам до певного "хосту", програмно здійснювати детальний контроль адрес відправників та одержувачів та ін

   Міжмережеві екрани працюють з програмами маршрутизації та фільтрами всіх мережевих пакетів, щоб визначити, чи можна пропустити інформаційний пакет, а якщо можна, то відправити його до певної комп'ютерної служби за призначенням. Для того щоб міжмережевий екран міг зробити це, необхідно визначити правила фільтрації. Отже, міжмережевий екран є немовби віртуальним кордоном, на якому перевіряється цілісність фрагментованих пакетів даних, що передаються, їх відповідність стандарту тощо.
3) ***системи виявлення втручань*** — для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні». Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі.
4) ***засоби аналізу захищеності*** — для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації. Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.
5) ***засоби створення віртуальних приватних мереж*** (*Virtual Private Network*) — для організації захищених каналів передачі даних через незахищене середовище.

Віртуальні приватні мережі (virtualprivatenetworks, VPN) - територіально розподілені корпоративні мережі, які використовують для зв'язку між окремими сегментами Інтернет.
Часто корпоративні мережі зв'язують офіси, розкидані в місті, регіоні, країні або всьому світі. Провідні постачальники міжмережевих екранів і маршрутизаторів запропонували ***технологію S/WAN***. Протоколи S/WAN допомагають досягти сумісності між маршрутизаторами і брандмауерами різноманітних виробників. Іншими словами, компанії зможуть створювати власні віртуальні приватні мережі (virtualprivatenetworks, VPN) і використовувати Інтернет як альтернативу традиційним каналам зв'язку, які орендуються за високу плату .

Віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування.

Засоби захисту VPN - це інтегровані з віртуальними мережами засоби захисту мережі, в цілому, її сегментів та кожного клієнта мережі окремо (захист TCP/IP трафіку, створюваного будь-якими додатками і програмами; захист робочих станцій, серверів WWW, баз даних і додатків; автопроцесингу, трансакцій для фінансових та банківських додатків і платіжних систем). Вони реалізуються в рамках програмно-апаратних рішень VVPN-шлюзів. Серед основних функцій VPN-шлюзів: автентифікація (MD5, SHA1), шифрування (DES, 3DES, AES), тунелювання пакетів даних через IP. Певні шлюзи підтримують також функції firewall.

Однак міжмережеві екрани не є універсальним вирішенням усіх проблем безпеки в Інтернет. Брандмауер може блокувати доступ до комп’ютера вірусів і хробаків, але він не здійснює перевірку на віруси і не здатен забезпечити цілісність даних.

6) Використання антивірусних засобів вважається необхідною умовою при підключенні до Internet, дозволяє значно знизити втрати інформації в наслідок зараження шкідливими програмами.

Антивірус - програма, що виявляє або виявляє та знищує комп'ютерні віруси. *Мережеві антивіруси* - використовують для захисту від вірусів однієї або кількох OS, протоколів та команди комп'ютерних мереж і електронної пошти. Використання автоматизованих засобів перевірки мережі на можливі уразливості в системі захисту та аудиту безпеки корпоративних серверів дозволяє встановити джерела загроз та значно понизити вірогідність ефективних атак на корпоративну мережу або персональний комп'ютер.

SKIPBridge - система, яка встановлюється на інтерфейсі внутрішня / зовнішня мережа (локальна мережа або комунікаційний провайдер), забезпечує захист (шифрування) трафіка,

що направляється з внутрішньої мережі у зовнішню на основі протоколу SKIP, а також фільтрацію і дешифрування трафіка, який поступає із зовнішньої мережі у внутрішню. IP-пакети, що приймаються із зовнішньої мережі, обробляються протоколом SKIP (розшифровуються, фільтруються відкриті пакети в режимі тільки захищеного трафіка, контролюється і забезпечується імітозахист). Пакети, які пройшли фільтрацію SKIP, за допомогою протоколу IP передаються програмному забезпеченню SKIP-Bridge. Програмне забезпечення вирішує завдання адміністративної безпеки (забезпечуючи пакетну фільтрацію), і потім системи SKIPBridge, який маршрутизує пакети на адаптер локальної мережі.

Використання Proxy та анонімних серверів дозволяє залишатись умовно анонімним при діях в мережі Internet та знизити ризики, пов'язані із збиранням та моніторингом мережевої інформації на користь третіх осіб, потоком непотрібної та шкідливої інформації у системі.

Використання систем обмеження доступу до мережевих ресурсів Internet, використання маршрутизаторів та надійних постачальників мережевих послуг, короткочасного каналу зв'язку дозволяє скоротити збір та моніторинг мережевої інформації на користь третіх осіб, потік непотрібної та шкідливої інформації.

Захист даних в Інтернеті.

Для захисту даних під час роботи в Інтернеті доцільно використовувати підключення, захищене шифруванням. Наприклад, за замовчуванням Google шифрує з’єднання з Gmail, а також при виборі інших сервісів Google, наприклад Google Диск, активується протокол шифрування SSL, який використовується до завершення сеансу роботи.

Щоб визначити, що сайти захищені, слід звернути увагу на їхню URL-адресу — вона починається з https://. Це, на відміну від протоколу http, — протокол зашифрованого підключення, що забезпечує більш ефективний захист даних. У деяких браузерах поруч із назвою протоколу відображається значок замка, це означає, що з’єднання захищене й більш безпечне.

HTTPS (від англ. HyperText Transfer Protocol Secure) — розширення протоколу http для підтримки шифрування з метою підвищення безпеки.

Браундмаєр

Перш ніж під’єднати комп’ютер до Інтернету, бажано підключити брандмауер. Наприклад, щоб підключити брандмауер в операційній системі Windows 7, треба виконати вказівку Пуск/Панель керування та обрати Брандмауер Windows.

У вікні, що відкрилося, слід встановити режим Підключено та за необхідності задати додаткові параметри.

Після встановлення міжмережевого екрана при кожному першому запуску мережевих програм брандмауер видаватиме вікно з попередженням, що деяка програма намагається одержати доступ до мережевого ресурсу.

Користувачеві пропонується на вибір: одноразово чи назавжди дозволити або заборонити доступ до комп’ютера для обраної програми.

Крім брандмауера, вбудованого у Windows 7, є багато інших засобів, що мають гнучкі параметри налагодження.

Поради:

- Якщо у вас будинку до Інтернету підключено кілька комп'ютерів, або вони з'єднані в мережу, важливо захистити кожен з них. Для захисту мережі слід використовувати апаратний брандмауер (наприклад, маршрутизатор), однак, щоб запобігти поширенню вірусу в самій мережі в разі зараження одного з комп'ютерів, на кожному з них необхідно включити програмний брандмауер.
- Якщо ваш комп'ютер підключений до корпоративної, шкільної або мережі іншої організації, дотримуйтесь політиці, встановленої адміністратором даної мережі .
- При використанні комп'ютера вдома, найперший крок, який слід зробити для його захисту , - включити брандмауер.

За допомогою брандмауера можна запобігти проникненню на комп'ютер хакерів або зловмисних програм (наприклад, хробаків) через мережу або Інтернет. Крім того, брандмауер запобігатиме надсиланню зловмисних програм із вашого комп'ютера на інші.

У брандмауер Windows вбудований журнал безпеки, який дозволяє фіксувати ip-адреси і інші дані, що відносяться до з'єднань в домашніх і офісною мережах або в Інтернеті. Можна записувати як успішні підключення, так і пропущені пакети. Це дозволяє відстежувати, коли комп'ютер в мережі підключається, наприклад, до web-сайту. Дана можливість за умовчанням відключена (її може включити системний адміністратор).