ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Збірник тез доповідей семінару кафедри Систем інформаційного та кібернетичного захисту від 07 травня 2019 року

Київ – 2019

«Актуальні проблеми кібербезпеки та захисту інформації»: тези доповідей семінару кафедри Систем інформаційного та кібернетичного захисту від 07 травня 2019 року – Київ: - ДУТ, 2019 – 31с.

Збірник містить тези доповідей семінару кафедри Систем інформаційного та кібернетичного захисту від 07 травня 2019 року навчально-наукового інституту захисту інформації Державного університету телекомунікацій. Пропонує тези студентів, що висвітлюють перспективи розвитку інформаційної та кібернетичної безпеки в світі.

ЗМІСТ

АНАЛІЗ ВІБРОАКУСТИЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Бичківський Р. В., СЗЗМ-71
Державний Університет Телекомунікацій

Теза присвячена захисту акустичної інформації на об’єктах інформаційної діяльності. Проаналізовано засоби віброакустичного захисту інформації. Для захисту інформації від витоку віброакустичним каналом застосовуються система віброакустичного захистуяка складається з генератора шуму, акустичних випромінювачів та віброперетворювачів.

Захист мовної інформації від можливого витоку по технічних каналах є однією з приорітетних задач забезпечення інформаційної безпеки. Для перехвату мовної інформації використовується велика кількість засобів, які дозволяють знімати інформацію з наступних каналів: акустичних, віброакустичних, акусто-оптичних та інших. Насамперед, основну увагу слід приділяти активним методам захисту інформації до яких належать віброакустичні системи захисту.

Зазвичай системи активного віброакустичного захисту складаються з генератора шуму, акустичних випромінювачів та сукупності віброперетворювачів.

Провівши аналіз генераторів віброакустичних завад можливо виділити проблеми, які виникають підчас їх використання. До них належать: висока споживча потужність, виникнення паразитних акустичних шумів, незадовільні масо-габаритні показники, невисокі ККД. Окрім цього рівень паразитних акустичних перешкод, що створюється системою віброакустичних зашумлень є також важливою характеристикою систем віброакустичного захисту, тому при роботі даної системи постає задача зменшення зазначеного рівня шумів при збережені високої вібровіддачі.

Високі вимоги висуваються також і до джерела електричного сигналу захисного зашумлення, яке використовується в системах віброакустичного захисту інформації.

Так, усі канали кожного з генераторів повинні бути цілком незалежними, тобто до складу кожного каналу повинні входити – вихідний підсилювач, задаючий генератор білого шуму та коректор спектру. Це важливо, як для підвищення надійності пристрою в цілому, так і для покращення якості захисту, адже підвищення ефективності системи віброакустичного захисту потребує вдосконалення технічних рішень стосовно складових частин (вихідних блоків генератора шуму).

Отже, підвищення ефективності систем віброакустичного захисту інформації можливе за рахунок вдосконалення генератора шуму, вихідного підсилювача потужності та засобів корекції.

Література:

1. Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації НД ТЗІ 1.6-003-04. [Чинний від 2004-04-01]. – К. : Департамент спеціальних телекомунікаційних систем захисту

інформації Служби безпеки України, 2004. – 20 с. – (Нормативний документ системи технічного захисту інформації).

2. Захист інформації на об’єкті інформаційної діяльності. Норми протидії технічній розвідці в акустичному і віброакустичному каналах витоку мовної інформації НД ТЗІ 2.2-006-08. [Чинний від 2008-08-26]. – К. : Державна служба спеціального зв'язку та захисту інформації України, 2008. – 6 с. – (Нормативний документ системи технічного захисту інформації).

3. Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами [Текст]: НД ТЗІ 2.3-017-08. [Чинний від 2008-08-26]. – К. : Державна служба спеціального зв'язку та захисту інформації України, 2008. – 18 с. – (Нормативний документ системи технічного захисту інформації).

КОНТРОЛЬ ЯКОСТІ ЗАВАД В СУЧАСНИХ СИСТЕМАХ ВІБРОАКУСТИЧНОГО ЗАШУМЛЕННЯ

Кнауб С.Е., СЗЗМ-71
Державний Університет Телекомунікацій

Здобування конфіденційної мовленнєвої інформації завжди було, є й буде одним із головних завдань військового, політичного, промислового, комерційного та інших видів шпигунства, оскільки вона містить оперативні дані щодо діяльності організацій чи осіб і надає можливість оцінити відношення співрозмовників до предмету розмови. Важливою задачею при захищенні мовленнєвої інформації від витоку технічними каналами є об’єктивна оцінка ефективності заходів захисту та рівня захищеності, яка проводиться при атестаційних випробуваннях та в процесі оперативного контролю.

Акустичні хвилі, поширюючись від джерела, впливають і на огороджувальні елементи конструкцій приміщень. Вібрації, поширюючись по конструкціях будівель, створюють канали витоку мовленнєвої інформації. При цьому, як експериментально встановлено, звукопоглинаючі покриття майже не впливають на поширення віброколивань в жорстких конструкціях. Вібраційні коливання можуть мати значну амплітуду та поширюватись по жорстким комунікаціям на значні відстані і можуть бути перехоплені стетоскопами, лазерними засобами акустичної розвідки тощо.

Особливості мовленнєвих сигналів, що визначають дальність їх поширення, полягають у наступному:

- мовленнєвий сигнал являє собою процес сплескового характеру з частотним діапазоном від 50 Гц до 10 кГц;
- тривалість сплесків - від 15 до 150 мс;
- сплески згруповані в пачки по 2-8 штук в кожній з проміжками між пачками від 10 мс до 1 с;
- наявність в спектрі сигналу основного тону з частотою 75-800 Гц;

- наявність в спектрі сигналу формант, частоти яких найчастіше лежать в діапазонах f1 = (300 ... 1000) Гц, f2 = (1000 ... 2000) Гц, f3 = (2000 ... 3000) Гц, f4 = (3000 ... 4000) Гц, f5 = (4000 ... 5000) Гц.

Експериментальними дослідженнями встановлено, що мовленнєві сигнали, поширюючись по елементах огороджувальних конструкцій приміщення, загасають з різними швидкостями. Більш високочастотні складові спектра загасають швидше, і мовленнєвий сигнал спотворюється. Для забезпечення захисту мовленнєвої інформації у виділеному приміщенні можуть застосовуватися, в першу чергу, пасивні методи, які реалізуються при будівництві будівель, і активні методи, засновані на створенні в елементах конструкцій маскувальних сигналів зі спектром частот, що перекриває частоти мовленнєвих сигналів [1].

Оцінка ступеня захищеності мовленнєвої інформації у виділеному приміщенні здійснюється на базі методів оцінки звукоізоляції приміщень з подальшим визначенням розбірливості мовленнєвих сигналів, що поширюються по огороджувальних елементах конструкцій приміщень, в місцях її можливого перехоплення.

Акустичні хвилі, які утворюються в виділеному приміщенні в результаті мовленнєвої діяльності, впливають на огороджувальні елементи конструкцій приміщень з рівнями звукового тиску порядку 70 дБ в частотному діапазоні від

50 Гц до 10 кГц. При цьому акустичні хвилі впливають на огороджувальні елементи конструкцій приміщень під різними кутами і має місце наявність багаторазово відбитих акустичних хвиль.

Оскільки суттєвий вплив на погіршення сприйняття мовленнєвої та іншої акустичної інформації мають різного роду шумові завади, і методи захисту акустичної інформації ґрунтуються на забезпеченні такого співвідношення між корисним сигналом і шумом, при якому сприйняття інформації певною мірою було б неможливим, то в якості критерію захищеності використовують відповідність нормам відношення сигнал/шум, виміряного в контрольних точках можливого перехоплення інформації.

Захист мовленнєвої інформації від витоку акустичними каналами з використанням як пасивних, так і активних методів захисту може виявитися або недостатньою, або надлишковою через неадекватність застосованих моделей можливих каналів витоку мовленнєвої інформації, моделей джерела мовленнєвого сигналу та моделей оцінки ступеня захищеності.

Моделювання джерела мовленнєвого сигналу у вигляді "білого" шуму із заданим діапазоном частот і заданим рівнем звукового тиску в 70 дБ не враховує сплескового характеру мовленнєвого сигналу. Розрахунок ступеня захищеності мовленнєвої інформації в виділеному приміщенні на базі методу оцінки розбірливості мови (в його різних варіантах) вимагає оцінки достовірності та визначення довірчих інтервалів.

Отже, однією з актуальних проблем в подальшому розвитку систем акустичного та віброакустичного зашумлення розмов у захищеному приміщенні є забезпечення ефективного та безперервного контролю за якістю завадових коливань.

У всіх сучасних системах активного зашумлення у тій чи іншій мірі впроваджено елементи (пристрої, системи), що дозволяють контролювати та регулювати параметри завад.

В доповіді розглядається система контролю, побудована за модульним принципом, яка дозволяє забезпечити всеосяжний постійний контроль працездатності всіх елементів системи захисту і безперервний моніторинг стану акустичних і віброакустичних каналів витоку мовленнєвої інформації.

Загальні модулі системи:

- модуль збору та обробки інформації з винесених датчиків акустичного та віброакустичного контролю (дистанційний комунікатор);
- модуль дистанційного групового управління генераторами завад;
- модуль активного захисту (генератори завад та віброакустичні випромінювачі).

Література:

1. В. К. Железняк, И. Б. Бураченок, Д. С. Рябенко. Критерии оценки защищенности от утечки речевых сигналов / Весці Нацыянальнай акадэміі навук Беларусі. Серыя фізіка-тэхнічных навук. 2017. №1. С. 122–128.

ШВИДКІСНИЙ МЕТОД ЗАХИСТУ ВІДЕОДАНИХ В СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

Кривенко В. І., СЗЗМ-71
Державний Університет Телекомунікацій

Відеозображення є невід'ємною складовою мультимедійної інформації, що створюється, накопичується і зберігається на цифрових носіях та передається каналами зв'язку. З широким поширенням цифрового медіаконтенту гостро постало питання його захисту від перехоплення, спотворення і незаконного використання.

Особливо актуальним є застосування шифрування відеоінформації у військовій техніці. За повідомленням газети «The Wall Street Journal» [1], бойовики, що протистояли силам НАТО в Іраку і Афганістані, використовували просту програму SkyGrabber для перехоплення відеоінформації розвідувально-ударних безпілотних літальних апаратів (БПЛА) MQ-1 Predator. Реалізація шифрування даних на етапі розробки в цих БПЛА була згорнута через складнощі шифрування відео в реальному часі [2]. Розробка велася в кінці 80-х – на початку 90-х років, коли була відсутня елементна база для забезпечення шифрування таких потоків даних в малогабаритному варіанті з прийнятним енергоспоживанням.

Окреме занепокоєння викликає можливе порушення функцій дистанційного керування БПЛА через збільшення часу на доставку даних оператору, який здійснює управління.

Ще однією проблемою є обсяг передаваної інформації. При використанні цифрового відеозв'язку загальна затримка в каналі зв'язку не повинна перевищувати 150 мс, причому це сумарна затримка, яка враховує не тільки шифрування/дешифрування конфіденційних даних, а й компресію - передачу - приймання - декомпресію - відображення. І чим менші витрати часу на шифрування/дешифрування, тим краще.

Можна виділити кілька важливих обставин, пов'язаних з реалізацією доставки відеоданих.

По-перше, в даний час в більшості бездротових мереж використовуються, як правило, протоколи передачі, які не передбачають наявність QoS (Quality of Service) механізмів.

По-друге, обмежена смуга частот в каналі обумовлює необхідність передачі відеоданих в стисненому вигляді.

По-третє, стиснені відеодані дуже чутливі до канальних помилок. Навіть одиночна помилка в стисненому бітовому потоці може призвести до появи послідовності, яку відеодекодер не здатен відновити, що в свою чергу може викликати зупинку декодування.

Існуючі технології захисту відеоінформаційних ресурсів забезпечують необхідну конфіденційність. Однак вони мають істотний недолік: їх робота заснована на закритті усього потоку інформації, що передається, незалежно від типу та змісту відеосцени. Такий підхід до закриття інформації називається повним. Його використання для відкритих відеоінформаційних ресурсів в інфокомунікаційних системах реального часу є непрактичним. Це обумовлено такими причинами: уся структура відеоданих руйнується у разі виникнення помилки в каналі передачі даних, збільшується час обробки. Для вирішення цієї проблеми застосовується селективний підхід шифрування, сутність якого полягає в приховуванні найбільш значущих компонент відеопотоку.

Аналіз існуючих технологій стиснення відеозображень показав, що методи кодування без втрати інформації забезпечують низькі коефіцієнти стиснення. Тому існує важлива науково-прикладна задача підвищення рівня стиснення відеозображень без втрати інформації і забезпечення захищеності відеоінформації в системах відеоспостереження.

В доповіді розглядається швидкісний метод захисту відеоданих в системах відеоспостереження.

З метою забезпечення безпеки відеоінформації розглянуто два методи її досягнення: селективний і повний. Вони відрізняються різними вимогами до обчислювальних ресурсів, виконуються на різних етапах їх обробки і надають різний рівень безпеки.

Внутрішній формат відеоінформації після стиснення зберігає складні взаємозв'язки між своїми елементами, тому на основі селективних методів створити гарантовано стійкий захист неможливо. Ці взаємозв'язки полегшують зловмисникові криптоаналіз захищеного відеоконтенту. При істотному порушенні даних взаємозв'язків (для підвищення стійкості), падає ступінь стиснення відеоінформації, збільшується кількість даних, які підлягають шифруванню, знижує переваги застосування селективного шифрування.

Комбінований алгоритм формування псевдовипадкових чисел на базі методу Фібоначчі з запізнюваннями та блочного шифру в режимі лічильника забезпечує захист від відновлення послідовності за її частиною а, отже, отримання таблиці перестановок і відновлення всього відеокадра.

Окремі відеозображення можна захистити за допомогою перестановки блоків перед стисненням.

Перспективною для захисту відеоданих є перестановка блоків перед ентропійним кодуванням. Це дозволяє відеокодеру працювати з природною послідовністю блоків зображення. Після перестановки статистичні властивості змінюються неістотно, тому ентропійне кодування дає майже такий же результат, як і при обробці оригінальної послідовності блоків в кадрі.

Запропонований швидкісний метод захисту відеоданих в системах відеоспостереження, враховує неоднорідність інформації в відеопотоці і дозволяє знизити ризики розкриття, спотворення і підміни при передачі відеоінформації.

Література:

1. Siobhan Gorman. Insurgents Hack U.S. Drones, $26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected / Siobhan Gorman, Yochi J.Dreazen, August Cole // The Wall Street Journal. -2009. - December 17. - https://www.wsj.com/articles/SB126102247889095011

2. Pauline Jelinek. Pentagon; Insurgents intercepted UAV videos / Pauline Jelinek // The Associated Press. -2009. -December, 17. - http://www.armytimes.com/news/2009/12/ap_uav_insurgents_hacked_l 21709/

МОНІТОРИНГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП`ЮТЕРНИХ МЕРЕЖ

Курлов Є.О., СЗЗМ -71,
Державний Університет Телекомунікацій

Моніторинг інформаційної безпеки комп`ютерних мереж багатогранний процес, який включає: сучасні методики управління ризиками, , правила доступу користувачів до різних сервісів проектування і супроводу корпоративних систем захисту інформації, конфігурацію міжмережевого екрану з екрануючою під мережею.

Актуальність досліджень.

Будь-яке державне та комерційне підприємство зацікавлене в збереженні інформації, яка може йому нашкодити, якщо потрапить до рук зловмисників або буде знищена, або викривленя. Щоб не стати жертвою хакерів, необхідно захищати комп'ютери і всю мережу організації від різного роду загроз, в тому числі, від інтернет-загроз.

Коли виникає необхідність забезпечити інформаційну безпеку компанії, керівництво, як правило, звертається до системних інтеграторів. Вони проводять

комплексний аналіз і розробляють проект із захисту інформації. В остаточному підсумку все це обертається придбанням дорогих програмних і апаратних засобів, таких як Cisco PIX, Checkpoint, Microsoft ISA. Такі великі комплексні проекти коштують більше 15 тис. дол., вимагають постійного супроводу і доцільні тільки для великих підприємств. Отже, актуальність досліджень моніторингу інформаційної безпеки комп`ютерних мереж потребує подальших досліджень.

Виклад основного матеріалу дослідження.

На перших порах захисту мереж постає питання управління ризиками.

Сучасні методики управління ризиками, проектування і супроводу корпоративних систем захисту інформації повинні дозволяти вирішити ряд завдань перспективного стратегічного розвитку компанії:

По-перше, кількісно оцінити поточний рівень інформаційної безпеки компанії, що потребують виявлення ризиків на правовому, організаційно-управлінському, технологічному, а також технічному рівнях забезпечення захисту інформації.

По-друге розробити і реалізувати комплексний план вдосконалення корпоративної системи захисту інформації для досягнення прийнятного рівня захищеності інформаційних активів компанії.

При формуванні політики доступу до мережевих сервісів повинні бути сформульовані правила доступу користувачів до різних сервісів, що використовуються в організації. Цей аспект, таким чином складається з двох компонент:

-набір правил для користувачів описує коли, який користувач (група користувачів) яким сервісом і на якому комп'ютері може скористатися. Окремо визначаються умови роботи користувачів поза локальної мережі організації так само як і умови їх аутентифікації;

-набір правил для сервісів описує набір сервісів, що проходять через мережевий екран, а також допустимі адреси клієнтів серверів для кожного сервісу (групи сервісів).

У політиці, яка регламентує роботу брандмауера, рішення можуть бути прийняті як на користь безпеки на шкоду легкості використання, так і навпаки. Є два основних:

-все, що не дозволено, то заборонено;

-все, що не заборонено, то дозволено.

Конфігурація міжмережевого екрану з екрануючою підмережею є однією з найбільш надійних на сьогоднішній день. Причиною цього є наявність принаймні трьох рівнів захисту:

-зовнішній екрануючий маршрутизатор;

-екрануючий шлюз;

-внутрішній екрануючий маршрутизатор.

Екрануюча підмережа також дозволяє легко включати комутаційні канали зв'язку в загальний цикл безпеки.

Для об’єктивної оцінки стану мережі з точки зору її захищеності необхідне використання скануючи пристроїв та програм

На сьогоднішній день перспективним напрямком захисту мереж компаній являється використання екрануючих під мереж, яка включає, в тому числі, шлюзи, їх здатність ефективно обробляти інформацію. Це, у свою чергу, вимагає установки ПЗ з невеликими втратами в продуктивності системи на на екрануючий комп'ютер-шлюз, який сам по собі досить надійно захищений вбудованою ОС - наприклад, комп'ютером фірми SUN з ОС Solaris с програмою Firewall-1 і т.п..

Висновки. Таким чином, моніторинг інформаційної безпеки комп`ютерних мереж є комплексне поняття, яке включає ряд організаційних, технічних, програмних та інших видів заходів, з метою комплексного захисту інформації в них.

Список використаних джерел:

1. Ахрамович. В.М. Адміністративний рівень інформаційної безпеки. Сучасний захист інформації. К. ДУТ:-2017 .-№1.- с. 10-14

2. Ахрамович, В.М. Чегренець. Інформаційна безпека. Практикум/ В.М. Ахрамович, В.М. Чегренець.-К.: ДУТ, 2017.-396с.

3. Ахрамович В.М., Котенко А.М. Мережеві сніфери. Тези доповідей IV Міжнародної науково-практичної конференції. «Актуальні проблеми забезпечення інформаційної та кібернетичної безпеки» 27 жовтня 2017 року с. 58-59

4. Баутов А. Стандарты и оценка эффективности защиты информации. Доклад на Третьей Всероссийской практической конференции "Стандарты в проектах современных информационных систем".- Москва, 23-24 апреля 2008 г.

УЯЗВИМОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ КАК ОСНОВНОЙ ЭЛЕМЕНТ МОДЕЛИРОВАНИЯ СХЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лаптев А. А.,к.т.н., снс
Государственный университет телекоммуникаций

Отличительной особенностью предлагаемого математического моделирования (аппарата) является использование в качестве элемента информационной безопасности не угрозы несанкционированого съема информаци - атаки, а угрозы - возможности съема информации уязвимости, что позволяет выбирать схему информационной безопасности на начальном этапе построения системы информационной безопасности

Большинство известных подходов изложенных в литературе по моделированию информационной безопасности, отличающихся тем, какие параметры при моделировании используются в качестве входной информации и какие характеристики моделируемой системы рассчитываются и поступают на выход модели.

Отличительной особенностью предлагаемого мною математического моделирования (аппарата) является использование в качестве элемента информационной безопасности не угрозы несанкционированого съема информаци - атаки, а угрозы - возможности съема информации уязвимости.

При моделировании, основанном на использовании в качестве простейшего элемента безопасности угрозы атаки, возникновение различных угроз атак рассматривается в качестве независимых событий, исходя из чего используются соответствующие расчетные формулы. Однако такой подход с моей точки зрения некорректен, т.к.реальные угрозы атак создаются выявляемыми в системе уязвимостями, при этом события возникновения угроз атак, как правило, зависимы по уязвимостям, поскольку многими атаками используются одни и те же уязвимости.

Для случая одного объекта обследования искомая характеристика безопасности – стационарный коэффициент готовности (в данном случае готовности к безопасной эксплуатации в отношении угрозы уязвимости)определяется следующим образом: PОу $= 1 - \rho$, где $\rho = \lambda/\mu$ (λ-интенсивность возникновения угрозы,μ-интенсивность устранения угрозы, а вероятность наличия в системе одновременно R не устраненных уязвимостей (реальных угроз уязвимостей): $P_{Ry} = \rho^R (1 - \rho)$.[1,с.131]

На практике одновременно может устраняться несколько уязвимостей, т.е. для такой модели искомая характеристика определяется следующим образом: $P_{оу}=(1+\rho+\frac{\rho^2}{2!}+\cdots+\frac{\rho^C}{C!})^{-1}$, а вероятность наличия в системе одновременно R не устраненных уязвимостей: $\_P_{Ry} = \frac{\rho^C}{C!}\ P_{оу}$. Отметим, что угроза уязвимости в данном случае моделируется в качестве простейшего или базового элемента безопасности информационной системы.[2,с.57]

Таким образом используя приведенный подход - использование в качестве элемента информационной безопасности не угрозы несанкционированого съема информаци - атаки, а угрозы - возможности съема информации уязвимости, с применяемыми нами допущениями позволяет опираясь на теорию «гибели и размножения», определить структуру системы информационной безопасности которая при использовании приведеной методики моделирования угрозы (проведя расчеты по указанной методики для различных значений ρ получили практический результат, что для обеспечения безопасности информации при ρ <2 моделирование угрозы может использоваться одноканальная схема, а для ρ >2 уже двухканальная с хема) позволяет выбрать схему обеспечения требуемой информационной безопасности.

Литература:

1. Эксплуатационные характеристики риска нарушений безопасности информационной системы // Щеглов К.А., Щеглов А.Ю. Научно-технический вестник информационных технологий, механики и оптики.-СПб - 2014. - №1(89). - С.129-139.

2. Математические модели эксплуатационной информационной безопасности // Щеглов К.А., Щеглов А.Ю. Вопросы защиты информации-М. - 2014. - Вып. 106. - № 3. - С. 52-65.

3. Исследование операций: задачи, принципы, методология //Вентцель Е.С.. - М.: Наука, 1988.-С.288.

ЗАХИСТ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Люлько Т.В., СЗЗМ - 71
Державний університет телекомунікацій

Теза присвячена захисту акустичної інформації на об’єктах інформаційної діяльності. Розглянуто поняття мовного сигналу. Розглянуто причини появи акустичного каналу витоку інформації. Приводиться класифікація акустичних каналів витоку інформації. Для захисту інформації від витоку акустичним каналом використовується комплекс технічного захисту інформації від витоку технічними каналами.

Захист мовної інформації – діяльність, спрямована на запобігання витоку інформації, яка циркулює у вигляді акустичних хвиль (голосу людини).

Мовний сигнал – складний фізичний процес, пов'язаний зі зміною акустичних параметрів, які містять інформацію про зміст повідомлення. Мовний сигнал створюється голосовим апаратом людини і являє собою обурення повітряного середовища у вигляді хвиль стиснення і розтягнення (акустичні коливання). Енергія мовного сигналу зосереджена в діапазоні 300 - 4000 Гц. У своєму первісному вигляді мовний сигнал в приміщенні присутній у вигляді акустичних і вібраційних коливань [1].

Залежно від середовища поширення сигналів і способів їх перехоплення технічні канали витоку мовної інформації можна розділити на [2]:

- акустичні- за рахунок поширення акустичних коливань у вільному повітряному просторі (переговори на відкритому просторі, відкриті двері, вікна, вентиляційні канали);
- вібраційні (віброакутсичні) - за рахунок впливу звукових коливань на елементи і конструкції будівель, викликаючи вібрації (огороджувальні конструкції (стіни, стелі, підлоги, вікна, двері, короба вентиляційних систем тощо), інженерні комунікації (труби водопостачання, опалення, кондиціонування тощо));
- акустоелектричні- за рахунок впливу звукових коливань на ДТЗС (за рахунок зміни параметрів (ємність, індуктивність, опір) під дією акустичного поля,створюваного джерелом мовного сигналу та виникнення електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цимелементам, за рахунок «мікрофонного ефекту», за рахунок використання «високочастотного електромагнітного нав'язування»);

- оптико-електронні (лазерні канали) канали - за рахунок приймання та демодуляції відбитого від вібруючих під дією акустичного сигналу поверхонь приміщень (шибок, дзеркал тощо) випромінювання;

- параметричні - за рахунок впливу звукових коливань на ОТЗ і ДТЗС (за рахунок паразитної модуляції інформаційним сигналом випромінювань гетеродинів радіоприймальних і телевізійних пристроїв, які перебувають у приміщеннях, де ведуться конфіденційні переговори, за рахунок утворення вторинних радіохвиль, при «при високочастотному опроміненні» приміщення, де встановлені закладні пристрої, що мають елементи, параметри яких змінюються під дією мовного сигналу);

При проведенні робіт із технічного захисту інформації одночасно, з використанням одних і тих же приладів, методик та спеціалістів можуть здійснюватися заходи із захисту декількох каналів витоку інформації. Так, при проведенні робіт із захисту інформації від витоку акустичним каналом можуть проводитися роботи із захисту інформації від витоку віброакустичним і оптоелектронним каналами. Аналогічним чином здійснюються роботи із захисту інформації від витоку акустоелектричним та параметричним каналами побічних електромагнітних випромінювань та наводок (канали побічних електромагнітних випромінювань та наводок).

Виходячи з цього види роботи з технічного захисту інформації доцільно проводити за наступними напрямками [2]:

- захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами;

- захист інформації від витоку акустоелектричними та параметричними каналами;

- захист інформації від витоку через закладні пристрої.

Для захисту мовної інформації з обмеженим доступом від витоку технічними каналами на об’єктах інформаційної діяльності створюється комплекс ТЗІ [3,4,5].

Результатом проведення всіх вище перерахованих заходів є випробування та атестація. КТЗІ [5].

Література:

1. Системи та пристрої інформаційної безпеки. Навчальний посібник / під ред. проф. В.А.Хорошко / Співавтори: А.П.Провозин, О.В.Рыбальский, В.А.Хорошко, Д.В.Чирков. – К.: ДУИКТ, 2007 р.

2. Методи та засоби захисту інформації. В 2-х томах / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко, Під ред. В.А.Хорошко. – К.: Арий, 2008.– Том II. Інформаційна безпека. – 344 с.

3. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

4. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи.

5. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

АНАЛІЗ ЕФЕКТИВНОСТІ ЗАХИСТУ ERP- СИСТЕМ

Мартиненко О.О., СЗЗМ-71
Державний університет телекомунікацій

В даний час вдосконалення корпоративного управління стає ключовою стратегічним завданням розвитку і життєдіяльності будь-якого підприємства. В силу того, що практично всі екстенсивні способи вдосконалення управління вичерпані, єдиним способом виживання в конкурентній боротьбі залишаються інтенсивні способи поліпшення управління. Одним з таких способів є інформатизація корпоративного управління за рахунок впровадження інформаційних технологій, в тому числі систем класу ERP.

Зростання систем обробки, зберігання інформації, а також величезна кількість впроваджуваних нових технологій з якими доводиться стикатися при забезпеченні інформаційної безпеки породжує велику кількість проблем.

У зв'язку з цим важливу роль починає грати інформаційна безпека, так як вся інформація компанії знаходиться в цифровому вигляді [1]. Тому життєво важливо захищати інформацію компанії як від зовнішніх, так і від внутрішніх порушників.

Основну роль в IT-інфраструктурі компанії грає ERP система, яка практично допомагає керувати всіма бізнес процесами компанії, так що вона містить саму важливу бізнес ін-формацію. Головним механізмом захисту є розмежування пів-номочій користувачів в ERP системі. Даний механізм дозволяє відповідно до бізнес ролями кожного співробітника дати йому відпо-ціалу повноваження по роботі з тією чи іншою інформацією. Це необхідно, оскільки на ринку величезна кількість конкурентів і від того, як працює фірма, як налаштовані її ролі в системі буде залежати її конкурентоспроможність.

Інформаційну безпеку необхідно забезпечити для всіх компонентів ERP-системи, тому розглянемо її архітектуру.

Сучасна ERP-система складається з трьох компонентів, пов'язаних через клієнт-серверну архітектури.

Виділяють такі рівні ERP-системи:

- рівень бази даних (БД);
- рівень додатків;
- рівень представлення (призначений для користувача).

Забезпечення тій чи іншій мірі захищеності інформації можливо на кожному з цих рівнів. Вибір механізмів захисту інформації на вищевказаних рівнях ERP-системи залежить від специфіки конкретного проекту [2].

Сполучною середовищем для компонентів, що знаходяться на різних архітектурних рівнях ERP, є мережева інфраструктура. У підсумку, можна виділити наступні основні аспекти безпеки:

- мережева безпека;
- безпека БД;
- безпека на рівні сервера додатків;
- захист інформації на клієнтському комп'ютері.

Виконавши аналіз побудови, можна зробити наступний основний висновок: складність ERP-системи веде до виникнення її вразливостей. ERP-системи обробляють велику кількість різних транзакцій і реалізують складні механізми, які надають різні рівні доступу різним користувачам. Практично для будь-якої ERP крім штатних засобів захисту інформації, як правило, потрібні додаткові програмні засоби, в тому числі криптографічні, і залучення сторонніх постачальників для виконання всіх вимог з інформаційної безпеки.

Саме тому дослідження можливих рішень захисту ERP-системи на сьогоднішній день є актуальним питанням.

Перелік використаної літератури:

1. О'Лири Д. ERP-системы. Современное планирование и управление ресурсами предприятия. Выбор, внедрение, эксплуатация. М.: Вершина, 2014. 272с.

2. Егорова Г.В., Шляпкин А.В. Информационная безопасность ERP-систем// Информационные системы и технологии: управление и безопасность. 2013. №2. С.202-211.

ШЛЯХИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ

Новік А.М., СЗЗМ – 71
Державний університет телекомунікацій

Проводиться аналітичний огляд шляхів несанкціонованого доступу до інформації. У якості шляхів розглядаються WEB технології, та фізичні канали доступу. Розглядається можливість несанкціонованого доступу через технологію WiFi, WEB камери, мобільні телефони.

Крадіжка інформації зазвичай є останньою стадією цільової атаки на організацію. Існує безліч прекрасних статей і інструментів для реалізації різної техніки, і в цій публікації ми спробувано зібрати все воєдино. Цей документ також може використовуватися як чек-листа для пентестера, якого попросили провести аналіз на предмет присутності каналів просочування інформації.

Веб-технології [1].

1) Якщо в організації відсутнє що-небудь схоже на проксі-сервер, ваше тестування на предмет витоків з високою мірою вірогідності завершиться результативно.

2) Сайти на кшталт pastebin, призначені для обміну інформацією, або навіть GitHub є очевидним каналом витоку. GitHub часто дозволений у багатьох технологічних компаніях.

3) Якщо в організації використовується проксі і фільтрація даних, потрібно буде попрацювати трохи інтенсивніше, проте багато сервісів для зберігання файлів, як, наприклад, Dropbox, GoogleDrive або Box дозволені, особливо в організаціях, які користуються сторонніми хмарними сервісами.

4)Зазвичай перехоплення TLS (атаки типу "людина посередині) не доступні. Один з варіантів - розгорнути окремий домен з прив'язаним сертифікатом Lets Encrypt.

5) Навіть якщо використовується щось схоже на Websense, багато типів сайтів, наприклад, фінансові або медичні, не піддаються повній TLS- інспекції в цілях безпеки співробітників. Багато систем категоризації дозволяють додати сайт в потрібну категорію. Таким чином, трохи підготувавшись, зловмисник може створити власним медичний сайт і обійти фільтри.

6) Flickr і YouTube доступні? У цих сервісах можна зберігати великі файли і використати стеганографію.

7) Можливо в організації є веб-сервера, доступні через інтернет, один з яких можна спробувати скомпрометувати в якості проміжної стадії

Файлові архіви

У організації може бути дозволена передача інформації, наприклад, за допомогою електронної пошти, проте в DLP можуть бути правила блокування окремих сигнатур [2]. Для обходу фільтрів в DLP спробуйте упакувати файли в архів

- Звичайний zip.
- Zip з паролем.
- Багаторазово вкладений zip (багато систем зупиняють сканування, якщо рівень вкладеності перевищує 10-100, з метою уникнення файлових бомб).
- 7zip.
- Rar
- Cab. Tar (+/ - gzip) Образ WIM.

Фізичні канали [3].

Якщо у зловмисника або неохайного інсайдера є фізичний доступ до системи, можливі наступні варіанти витоків.

1) Через USB- порти ноутбука і робочої станції, включаючи MP3 плеєри, смартфони і зашифровані USB- флешки.

2) Хоча в наші дні оптичні драйвера рідко використовуються в організаціях, але все таки нелишним буде перевірити, чи дозволений запис на CD і DVD. З іншого боку, скопіювати великі томи набагато складніше, ніж на USB.

3) Чи виносяться за межі офісу ідентифікаційні наклейки ноутбуків? Чи використовуються портативні пристрої з повним шифруванням диска? Продаються або викидаються застарілі комп'ютери?

4) З високою мірою вірогідності в організації використовуються принтери, багато хто з яких має безліч функцій і може експлуатувати для отримання списку попередніх завдань на друк або навіть для передачі інформації факсом.

5) Чи може зловмисник, знаходячись неподалік, скомпрометувати корпоративний Wi - Fi (особливо, якщо використовується WPA - PSK)? Наскільки добре чи відокремлені гостьові Wi - Fi мережі від головної корпоративної мережі? У разі ненадійної ізоляції, чи вирішено питання із забороною підключення корпоративних систем до гостьовій Wi - Fi мережі?

6) Може зловмисник скористатися незахищеністю портів для впровадження пристрою в мережу, як, наприклад, RaspberryPi з можливістю виконання команд через власне стільникове позасмугове підключення?

7) Веб-камери.

8) Мобільні телефони.

9) Паперові копії документів.

Література:

1. Хорошко В.А., Чекатков А.А. Методи та засоби захисту інформації. – К.: ЮНІОР, 2003. – 504 с.

2. Каторин Ю.Ф., Куренков Е.В., Лисов А.В., Остапенко А.Н. Велика енциклопедія промислового шпіонажу. – СПб.: Полігон, 2000. – 896 с.

3. Методи та засоби захисту інформації. В 2-х томах / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко, Під ред. В.А.Хорошко. – К.: Арий, 2008.– Том II. Інформаційна безпека. – 344 с.

ВИКОРИСТАННЯ КОМП'ЮТЕРНОГО ЗОРУ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

Орленко І.П., СЗЗМ – 71
Державний університет телекомунікацій

Розглянуто принципово нові технології, які дозволять зіставляти поведінку людини і обставини, аналізувати наскільки адекватні її дії в конкретній ситуації. Наведено приклади використання системи відеоспостереження які на сьогоднішній день розрізняють в транспортних потоках номерні знаки транспортних засобів, за допомогою розпізнання обличь здійснюється пошук осіб що перебувають у базах розшуку. Показано перспективні напрямки системи відеоспостереження.

Сучасне суспільство прагне зменшити рівень злочинності, для цього використовують певні форми і методи боротьби зі злочинністю, профілактики та попередження правопорушень.

Таким чином використання систем відеоспостереження в галузі охорони громадського порядку – є допоміжними чинником, який підвищить рівень інформаційно-аналітичного забезпечення прийняття управлінських рішень та організації ефективної взаємодії між територіальними органами виконавчої влади, органами внутрішніх справ та адміністраціями об'єктів із масовим скупченням людей, антитерористичними комісіями й оперативними штабами в інтересах

попередження, припинення й ліквідації кризових ситуацій криміногенного, терористичного, природного й техногенного характеру, антитерористичної захищеності й антикримінального захисту, забезпечення правопорядку.

Пріоритетним напрямком у сфері відеоспостереження слід вважати інтелектуальне відеоспостереження що допоможе автоматизувати широкий спектр завдань, які щодня виконують працівники правоохоронних органів. Окремий напрямок відеоаналізу, який стає все більш затребуваним, це біометричне розпізнавання осіб. Ця технологія дуже ефективна в якості інструменту забезпечення превентивної безпеки. Найбільшою перевагою систем біометричного розпізнавання осіб перед звичайним відеоспостереженням або співробітником правоохоронних органів є їх швидкість і майже 100% вірогідність розпізнавання.

Література:

1. Економічна та інформаційна безпека: проблеми та перспективи: матеріали Міжнародної науково-практичної конференції м. Дніпро, 27 квітня 2018 р. С. 144–146.

2. Мирошниченко В.О. Аналіз біометричних систем ідентифікації особи. Матеріали науковопрактичного семінару 1 грудня 2016 р. Львів: ЛьвДУВС, 2016. С.82-93.

3. Мирошниченко В.О., 2018 © Гавриш О.С., 2018 Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2018. № 2 ISSN 2078-3566 61.

АЛГОРИТМИ ВИЯВЛЕННЯ ТРИВОЖНИХ ПОДІЙ ДЛЯ СИСТЕМ ІНТЕЛЕКТУАЛЬНОГО ВІДЕОСПОСТЕРЕЖЕННЯ

Петрушенко О.В., СЗЗМ-71
Державний університет телекомунікацій

Системи відеоспостереження стали невід'ємною частиною нашого повсякденного життя. В першу чергу відеоспостереження є превентивним заходом. Адже сама наявність відеокамер зупиняє більшість зловмисників.

Оператори систем відеоспостереження виконують монотонну роботу протягом тривалого часу, звідки виникає проблема стомленості і зниження концентрації уваги. Встановлено [1], що при безперервному спостереженні протягом 12 хвилин оператор починає пропускати 45% потенційно тривожних подій, а якщо час спостереження збільшити до 22 хвилин, то відсоток пропуску зростає до 95. Тому важливою задачею є аналіз відеоінформації без прямої участі людини.

Сучасні системи відеоспостереження стають все більш точними, "розумними" і багатофункціональними. Можливості їх застосування

розширюються з кожним роком, а темпи розвитку цифрових технологій обіцяють подальший прогрес у цій сфері.

Серед задач цифрової обробки зображень можна виділити дві, пов'язані з рухом об'єктів: розпізнавання рухомих об'єктів і побудова траєкторій їх руху. При вирішенні цих завдань виділяють два типи відеозображень: зняті нерухомою і рухомою камерою, для яких існують свої методи. У доповіді розглянуто алгоритми обробки даних, отриманих нерухомою камерою.

Традиційним методом виявлення руху на послідовності зображень є обчислення міжкадрової різниці – абсолютної різниці двох послідовних зображень з відеопотоку [2]. В результаті такого обчислення отримують зображення з виділеними областями руху. Найчастіше на такому зображенні складно виділити контури об'єкта, це вдається зробити, тільки якщо об'єкт однотонний і випуклий.

Завдання відстеження об'єктів полягає в тому, щоб на основі послідовності зображень побудувати траєкторії руху заданих об'єктів. При цьому послідовність зображень може бути доповнена різною інформацією: об'єктами, виявленими на попередніх кадрах, швидкістю і напрямом їх руху.

В доповіді розглядаються алгоритми виявлення тривожних подій для систем інтелектуального відеоспостереження, що являють собою набір пов'язаних між собою модулів. В процесі функціонування модуль очікує появи вхідних даних, після чого виконує обчислення і формує дані, які в подальшому будуть передані іншим модулям. Набір модулів може бути конфігурований окремо для кожної з камер або групи камер в залежності від розв'язуваних завдань. Застосування зазначеного підходу дозволяє створити легко масштабовану і розподілену систему.

Алгоритм відстеження рухомих об'єктів складається з двох модулів: детектора рухомих об'єктів і модуля відстеження об'єктів. Окремий модуль аналізує переміщення об'єктів і генерує повідомлення про тривожну подію, яке пересилається оператору системи відеоспостереження.

Детектор рухомих об'єктів послідовно приймає на вхід по одному кадру, який представляє собою матрицю F=(f x,y) розміром W x H , і базується на методі вирахування фону. Елемент матриці – значення інтенсивності зображення в точці (x, y). На виході детектор видає список виявлених об'єктів – структуру, яка містить координати об'єкта на зображенні, його розмір і набір ознак, необхідних для ідентифікації об'єкта на наступних кадрах.

Модуль відстеження об'єктів приймає виявлені об'єкти, а на виході видає інформацію про їх переміщення: час початку і закінчення відстеження, розмір об'єкта, місце розташування й напрямок руху. Модуль працює зі структурою, що носить назву трек. Трек t – це список об'єктів (o1,…, on), виявлених на послідовних кадрах, що містить одну і ту ж множину фізичних об'єктів.

Запропоновано методи виявлення чотирьох типів тривожних подій: рух в забороненому напрямку, перебування в стерильній зоні, залишення предмета і перекидання предмета.

Перші три події розпізнаються за допомогою модуля відстеження рухомих об'єктів, який використовує покращений нами метод вирахування фону для

виявлення об'єктів і аналіз відстаней і гістограм зображень для зіставлення об'єктів, виявлених на різних кадрах.

Для розпізнавання події «перекидання предмета» використовується окремий модуль, який використовує метод міжкадрової різниці для виділення областей руху об’єкта і алгоритм RANSAC (RANdom SAmple Consensus) [3] для пошуку траєкторій кинутого предмета.

Перспективними напрямками подальших досліджень є:

- удосконалення методів виявлення та відстеження об'єктів для підвищення чутливості і швидкості роботи розглянутих алгоритмів шляхом оптимізації та паралелізації обчислень, зокрема перенесення операцій обробки зображень на обчислювальні потужності графічних прискорювачів;
- розробка алгоритмів відстеження об'єкта на відеозображеннях, отриманих за допомогою поворотних камер;
- розробка алгоритмів відстеження об'єктів декількома камерами, що спостерігають за однією сценою з різних ракурсів;
- розробка модулів класифікації об'єкта (людина, машина, тварина) і ідентифікації об'єкта (розпізнавання осіб для ідентифікації людей і автомобільних номерів для ідентифікації транспортних засобів) та їх інтеграція з існуючими модулями.

Література:

1. Ainsworth T.Buyer Beware // Security Oz. 2002. Vol. 19. P. 18–26.
2. Singla M.Motion Detection Based on Frame Difference Method International // Journal of Information & Computation Technology. 2014. Vol. 4. No. 15. P. 1559–1565.
3. Fischler M. A., Bolles R. C. Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography // Communications of the ACM 24. 1981. P. 381–395.

ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Прокопенко А.А., СЗЗМ - 71
Державний університет телекомунікації

У тезы розглядаються питання управління інформаційною безпекою підприємства. Розглянуто заходи, спрямовані на формування та підтримання режиму інформаційної безпеки. Розглянуто основні положення концепції інформаційної безпеки підприємства.

Система забезпечення інформаційної безпеки (СЗІБ) підприємства являє собою сукупність заходів організаційного та програмно-технічного рівня, спрямованих на захист інформаційних ресурсів (ІР) підприємства від загроз інформаційної безпеки (ІБ). Заходи захисту організаційного рівня реалізуються

шляхом проведення відповідних заходів, передбачених документованої політикою ІБ. Заходи захисту програмно-технічного рівня реалізуються за допомогою відповідних програмно-технічних засобів і методів захисту інформації (ЗІ) [1].

Економічний ефект від впровадження СЗІБ повинен проявлятися у вигляді зниження величини можливого матеріальної, репутаційної та інших видів шкоди, що завдається підприємству, за рахунок використання заходів, спрямованих на формування та підтримання режиму ІБ [2]. Ці заходи покликані забезпечити:

- доступність інформації (можливість за прийнятний час отримати необхідну інформаційну послугу);
- цілісність інформації (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни);
- конфіденційність інформації (захист від несанкціонованого ознайомлення);
- неспростовності (неможливість заперечення скоєних дій);
- автентичність (підтвердження автентичності і достовірності електронних документів).

Концепція ІБ підприємства визначає склад критичних ІР і основні принципи їх захисту. Принципи забезпечення ІБ обумовлюють необхідність застосування певних методів і технологій захисту. Визначення способів реалізації цих принципів шляхом застосування конкретних програмно-технічних засобів захисту інформації (ЗЗІ) та системи організаційних заходів що є предметом конкретних проектів і політик ІБ, що розробляються на основі цієї концепції.

Концепція забезпечення ІБ підприємства визначає [3]:

- Основні принципи формування переліку критичних ресурсів, які потребують захисту, який формується в процесі проведення аудиту безпеки і аналізу ризиків. Даний перелік повинен включати в себе опис фізичних, програмних і ІР з визначенням вартості ресурсів і ступеня їх критичності для підприємства;
- Основні принципи захисту, що визначають стратегію забезпечення ІБ і перелік правил, якими необхідно керуватися при побудові СЗІБ підприємства;
- Модель порушника безпеки, яка визначається на основі обстеження ресурсів системи і способів їх використання;
- Модель загроз безпеки і оцінку ризиків, пов’язаних з їх здійсненням, що формується на основі переліку критичних ресурсів і моделі порушника, яка включає визначення ймовірностей загроз і способів їх здійснення, а також оцінка можливих збитків;
- Вимоги безпеки, які визначаються за результатами аналізу ризиків;
- Заходи забезпечення безпеки організаційного і програмно-технічного рівня, що вживаються для реалізації перерахованих вимог;
- Відповідальність співробітників підприємства за дотримання встановлених вимог ІБ при експлуатації інформаційної системи (ІС) підприємства.

Концепція має переглядатися в міру виявлення нових методів і технологій здійснення атак на ІР. Подібний перегляд також повинен проводитися в міру

розвитку ІС підприємства. Рекомендований термін перегляду концепції становить три роки (за умови відсутності корінних змін в структурі системи, в технологіях управління і передачі інформації).

Підготовка цього документу, внесення в нього змін і загальний контроль виконання вимог щодо забезпечення ІБ підприємства здійснюється співробітниками відділу ІБ підприємства.

Відповідальність за виконання вимог ІБ, які визначаються концепцією та іншими організаційно-розпорядчими документами підприємства, покладається на користувачів і адміністраторів корпоративної мережі передачі даних підприємства, а також їх керівників.

Література:

1. Методи та засоби захисту інформації. В 2-х томах / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко, Під ред. В.А.Хорошко. – К.: Арий, 2008.– Том II. Інформаційна безпека. – 344 с.

2. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

3. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 8 жовтня 1997 р. N 1126 // Урядовий кур’єр,1997.

МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ

Синьова А.Д., СЗЗМ-71
Державний університет телекомунікацій

У зв’язку із зростанням ролі інформаційних технологій у житті сучасного суспільства, а також через реальності численних загроз з точки зору їх захищеності проблема ІБ вимагає до себе все більшої уваги. В останні роки багато компаній добре усвідомили необхідність управління інформаційною безпекою ,подбали про захист інформації, а саме діяльність щодо запобігання витоку, розкрадання, втрати, модифікації (підробки), несанкціонованих і ненавмисних) впливів на захищену інформацію. Розробили метод управління питаннями інформаційної безпеки,що набуває все більшого значення для компаній підприємств та організацій.

Метод управління інформаційною безпекою — це комплекс заходів, які ґрунтуються на підході, що враховує бізнес-ризики, призначені для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення інформаційної безпеки. Сьогодні втрати інформації носять, як фінансові, так і репутаційні складові, а крадіжки інформації привертають величезну увагу з боку підприємців і суспільства в цілому. Перших лякають можливі втрати, які здатні привести до банкрутства, других — цікавить

професійний аспект, треті занепокоєні можливостями згадування їх в пресі. Витоки особистої інформації клієнтів різноманітних компаній зростають і це спричиняє фінансові і моральні втрати для них, обсяги цих втрат зростають кожен рік. Найбільш складними для розрахунків є витоки інформації як інтелектуальної власності, та тих, що шкодять безпеці та репутації країни.Для підвищення ефективності захисту інформації необхідно побудувати систему управління інформаційною безпекою,а саме описати процеси діяльності ,визначити найбільш незахищені системи, види порушень,та використати технічний захист цієї інформації,як діяльність що спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Клієнтам важливо знати, що дотримується конфіденційність їхніх персональних і ділових даних. Інвесторам необхідна впевненість в тому, що бізнес та інформаційні активи компанії захищені. Ділові партнери очікують, що компанія буде функціонувати без збоїв, які можуть бути викликані помилками в роботі інформаційних систем, навмисними або ненавмисними діями персоналу, шкідливим програмним забезпеченням та іншими факторами.

Ґрунтуючись на даних проведеного аналізу та використаних джерел, можна зробити висновок що застосування систем технічного захисту інформації дозволяє знаходити та ліквідовувати велику кількість усіх спроб їх несанкціонованого отримання.

Список використаних джерел:

1. Додонов О.Г., Горбачик О.С., Кузнєцова М.Г. Глобалізація інформаційних систем та безпека // Інформаційні технології та безпека. Зб. наук. праць. — К.: ІПРІ НАН України, 2002.

2. Домрачев В.М. Система підтримки прийняття рішення з інформаційної безпеки організації / В.М. Домрачев // Збірник тез доповідей VII Міжнародної науково-технічної конференції «Сучасні інформаційно — комунікаційні технології» — К.: ДУІКТ. –2011. — С. 126.

РЕКОМЕНДАЦІЇ ПО ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ У МЕРЕЖІ IP-ВІДЕОСПОСТЕРЕЖЕННЯ

Сіренко Є.В., СЗЗМ - 71
Державний університет телекомунікацій

Розглядаєтьсяпередача інформації у IP – системі відеоспостереження. Розроблені рекомендації для захисту: інформації архівів та баз даних, ліній зв’язку, обладнання.

При розробці рекомендацій треба починати перш за все - зі структури та характеру системи IP-відеоспостереження, тому що цим визначається список

можливих загроз та, відповідно, список заходів захисту [1]. Розглянемо розподільну систему на базі зовнішніх неконтрольованих мереж зв'язку.

Рис. 1. IP система відеоспостереження

Оснащення: кілька мережевих сегментів тільки для задач відеоспостереження, сервери, камери, сховища, ВРМ. Для зв'язку між сегментами використовується Інтернет та/або корпоративна мережа організації [2].

Захист архівів та баз даних:

-вибір топології «сервер без відображення ВРМ для персоналу»;

-вибір ПЗ з можливістю створення резервних БД;

-наявність антивірусного ПЗ на відеосерверах, мережевих сховищах, ВРМ;

-створення резервних копій БД;

-обмеження доступу користувачів до налаштувань ПЗ;

Захист ліній зв'язку:

-вибір керуючого комутатора з можливістю фільтрації по MAC-відеоспостереженняадресам та відключення невикористовуваємих портів;

-відеоспостереженняорганізація підключення до корпоративної мережі через виділений комутатор з функціями «білого списку», VLAN, VPN, маршрутизації портів, шифрування трафіку;

-налаштування «білого списку» MAC-відеоспостереження адрес

-відключення невикористовуваних портів комутатора

-налаштування безпечного з'єднання через мережу Інтернет або корпоративну мережу між окремими сегментами системи відеоспостереження згідно з вимогами проекту.

Захист обладнання:

-вибір станційного устаткування з обмеженням доступу до ОС;

-вибір ПЗ відеоспостереження з захистом від підбору паролів;

-наявність антивірусного ПЗ у складі відеосервера;

-створення резервних копій БД;

-зміна усіх паролів доступу до налаштувань комутаторів, IP-відеоспостереженнякамер та інших IP-відеоспостереження пристроїв «за замовчуванням»;

-налаштування та перевірка роботи функції захисту від підбору паролів;

-відмова від використовування стандартних мережевих-відеоспостереженняпортів (тих, які за замовчуванням використовують виробники камер, комутаторів, Windows та ін.).

Для ефективного впровадження захисту та експлуатації систем відеонагляду необхідно: слідкувати за новинами, підписатися на розсилки виробників обладнання, не забувати встановлювати рекомендовані виробниками «апдейти», запрошувати фахівців на аудит, регулярно задавати нові паролі та робити резервні копії БД відеоспостереження тільки тоді систему відеоспостереження можна буде вважати відносно захищеною.

Література:

1. IP-видеонаблюдение: наглядное пособие, Александр Лыткин 2011.
2. Бабаш А.В., Шанкин Г.П. Криптография. М.: СОЛОН – ПРЕСС, 2007.–512 с.
3. Смарт Н. криптография / Пер. с англ. С.А. Кулишова. М.: техносфера, 2005.–528с.

ВПЛИВ СУЧАСНИХ ТЕХНОЛОГІЙ ВІДЕОСПОСТЕРЕЖЕННЯ НА ЕФЕКТИВНІСТЬ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Стукало М.О., СЗЗМ-71
Державний університет телекомунікацій

У тезы розглядається питання побудови комплексної системи захисту інформації у автоматизованій системі класу 2. Наведено класифікацію автоматизованих систем. Розглянуто вплив сучасних технологій відеоспостереження на ефективність комплексної системи захисту інформації.

Комплексна система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу.

Одним з напрямків захисту інформації в комп'ютерних системах є технічний захист інформації (ТЗІ). В свою чергу, питання ТЗІ розбиваються на два великих класи задач [1]:

- захист інформації від несанкціонованого доступу (НСД)
- захист інформації від витоку технічними каналами.

Для забезпечення ТЗІ створюється комплекс технічного захисту інформації, що є складовою КСЗІ.

Під НСД звичайно розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали побічних електромагнітних випромінювань і наводок (ПЕМВН), акустичні канали, оптичні канали та інші.

Криптографі́чний захист інформації — вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних

даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Складові комплексної системи захисту інформації наступні [2].

Організаційні заходи захисту інформації — комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціювання засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ.

Автоматизована система – це організаційно-технічна система, що реалізує інформаційну технологію та поєднує в собі: обчислювальну систему, фізичне середовище, персонал та інформацію, що обробляється. Існує три класи АС.

Клас «1» — одно машинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності.

Істотні особливості:

- в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється;
- технічні засоби (носії інформації і засоби У/В) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження і/або У/В всієї інформації.Приклад — автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.

Клас «2» — локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності. Приклад — ЛОМ.

Клас «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Приклад — глобальна мережа.

В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю і доступністю.

Підвищення ефективності всієї КСЗІ за рахунок використання сучасних технологій відеоспостереження полягає у наступному: система відеоспостереження може виконувати функції системи контролю та управління доступом, функції технічної системи охорони, у свою чергу це веде до зменшення штату служби захисту інформації та як наслідок до здешевлення всієї комплексної системи захисту інформації.

Література:
1. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
2. Гребенніков В.А. Комплексні системи захисту інформації. Проектування, впровадження, супровід/— «Издательские решения»,2018. – 249 с.

ЗАХИСТ ПК: ХМАРНІ ТЕХНОЛОГІЇ

Шаповаленко О.Д., СЗЗМ-71
Державний університет телекомунікацій

У світі щомісячно блокується більше 200 млн. мережевих атак, за рік у використовуваних програмах було виявлено більше 2000 уразливостей і щодняз'являються більше 35 тис. шкідливих програм. Природно, ніяка антивіруснапрограма, встановлена на локальному комп'ютері не в змозі впораться з цим руйнівним потоком. Щоб ефективно захистити інформацію, треба витрачати колосальні ресурси комп'ютера, щоб тільки оновлювати і зберігати антивіруснібази. Але тоді комп'ютер перестане виконувати свою головну функцію. Здавалося б, проблема нерозв'язна.

Виникають логічні питання: де зберігати інформацію про комп'ютерні погрози, як забезпечити миттєву реакцію на них, якщо навіть проактивні технології, використовувані в програмах-антивірусах, неефективні?

Тільки “хмарні” технології здатні забезпечити миттєву реакцію на погрози, позбавити від необхідності зберігати величезні за об'ємом антивірусні бази на персональних комп'ютерах. Цю функцію бере на себе потужний сервер,доступ до баз якого забезпечується через інтернет.

Але використання персональним комп'ютером захисних можливостей “хмари” не гарантує від локального зараження ПК. Ваш комп'ютер, не підключений до Інтернету, може стати уразливим перед новими вірусами, які не встигли увійти до вашої бази при оновленні. Оптимальним варіантом захисту від усіх погроз стає гібридний захист – об'єднує локальні можливості антивірусного захисту ПК і глобальні можливості “хмарного” захисту.

Зовсім нещодавно Лабораторія випустила нові продукти, в які вбудовані самі передові і ефективні засоби захисту від комп'ютерних погроз.

Для більше оперативної реакції на нові погрози ще в попередніх версіях був реалізований “хмарний” захист.

Але з виходом нових продуктів «хмарний» захист став ефективнішої у рамках системи Eset Nod. Сервіс KSN збирає і доставляє на централізовані сервери інформацію про усі спроби заражень шкідливими програмами, здійснюючи постійний моніторинг вірусної ситуації в Інтернеті. Варто тільки новому вірусуспробувати заразити який-небудь комп'ютер, як інформація про це відразу ж через Eset Nod потрапляє до експертів “Лабораторії”. Система негайно виробляє відповідні засоби захисту, і вашкомп'ютер автоматично отримує противовирус, незалежно від вашого графікуоновлення антивірусних баз.

Чим більше користувачів бере участь в сервісі Eset Nod Network, тим надійніше стає захист з “хмари” для усіх учасників.

Реакція на вірусні погрози при використанні такої «хмарної» технології незвичайно висока – усього лише декілька десятків секунд, при цьому не навантажуючи ресурси вашого комп'ютера.

Дуже часто користувачеві доводиться приймати нелегкі рішення, що стосуються безпеки комп'ютера і інформації, що зберігається на ньому.

У нових програмах з'явилася унікальна можливість перевірити репутацію підозрілого файлу або програми (отримати повну інформацію про об'єкт) одним кликом миші. У вікні Репутація програми буде зафіксована виробник програми, визначений рейтинг небезпеки від сервісу KSN (наприклад, довірена), міра довіри користувачів, які працювали з нею, дата її створення і останньої зміни, географія поширення у світі, цифровий підпис.

Основною гідністю цієї функції є те, що при оцінці репутації програми використовується інформація з “хмари”, а це означає, що отримані вами відомості про програму найактуальніші. Це дає можливість упевнитися у безпеці навіть програм, що нещодавно з'явилися, і файлів.

Ще одна новинка– це можливість збирати і на выдповыдны ресурси відправляти в “хмару” дану про шаблони поведінку усіх програм, що запускаються вами.

Дуже корисний інструмент при роботі в Інтернеті, що входить до складу KAV2012 і KIS2012, – Модуль перевірки посилань. Модуль автоматично позначає спеціальним колірним індикатором посилання, що ведуть на заражені або шахрайські ресурси. Інформація про небезпеки поступатиме на ПК з «хмари», а значить, майже миттєво. Захист від спаму піднятий на новий рівень.

Результати досліджень свідчать про значний розвиток технологій у сфері розробок итантивірусних хмарних рішень.

Тенденція така, що у технологій cloudcomputing досить перспективне майбутнє. І ймовірно, що незабаром модель “обчислювального хмари” стане однією з найбільш затребуваних і зручних.

Література:

1. http://www.softline.ua/news/13089/
2. http://www.softcom.ua/it/antivirus/pc_safe.php
3. http://www.zvit.net/archives/2755
4. http://www.headtechnology.com.ua/ru/products/?p=83&sup=4

МОДЕЛІ ЗАГРОЗ ТА ПАСИВНОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ ПІДПРИЄМСТВА

Шерстюк В.В., СЗЗМ-71
Державний університет телекомунікацій

Захист інформації в комп'ютерних мережах являє собою комплексну систему, що включає апаратно-програмні засоби і методи, а також організаційно-правові заходи, які дозволяють запобігти або максимально ускладнити можливість реалізації загроз інформації. Для оцінки ефективності такої системи необхідно мати інструмент її формального подання, у якості якого виступає модель захисту інформації [1].

Загальною моделлю формального опису систем захисту є модель системи безпеки з повним перекриттям, у якій визначаються повний перелік об'єктів захисту й загроз інформації, оцінюються засоби забезпечення безпеки з погляду їхньої ефективності й внеску в забезпечення безпеки всієї комп'ютерної мережі. З цією метою в модель вводяться набір об'єктів, що захищаються, O = {o} і набір загроз T = {ti}, кожна з яких спрямована на один або кілька захищених об'єктів. Множина зв'язків загроза-об'єкт утворюють дводольний граф, у якому ребро <t, o> існує тоді й тільки тоді, коли загроза t є засобом для одержання доступу до об'єкта o.

Слід зазначити, що одна загроза може бути спрямована на кілька об'єктів, і один об'єкт може піддаватися декільком загрозам. Мета системи захисту, що моделюється, полягає в тому, щоб перекрити всі можливі ребра в графі {<T,O>}, тобто домогтися, щоб до жодного об'єкту не було ні одного неперекритого шляху ні від однієї загрози. Це досягається введенням третього набору M = {тк}, що включає засоби забезпечення безпеки.

В ідеальній системі кожний засіб тк∈M повинен усувати, принаймні, одне ребро <t, o> із графа {<T,O>}. Введення набору M засобів забезпечення безпеки перетворить дводольний граф {<T,O>} у тридольний граф {<T, M, O>}, що містить дуги виду <t,m> і <т,o>. Таким чином, в «захищеній» системі будь-яке ребро у формі <t, o> визначає незахищений об'єкт. Один і той же засіб забезпечення безпеки може перекривати більше однієї погрози й захищати більше одного об'єкта. Описана модель задовольняє також загальній схемі взаємодій, що включає систему організаційного керування, зовнішні й внутрішні загрози, а також середовище взаємодії між ними. Із співставлення моделі з повним перекриттям і загальної схеми взаємодій очевидно, що модель не враховує можливостей одночасного співіснування різних типів загроз, можливостей їхньої взаємодії та, відповідно, можливостей захисних заходів. Отже, розвиток моделі формального опису систем захисту пов'язаний, насамперед, із введенням більш загального поняття загроз, а також з побудовою механізму для моделювання різних типів загроз та їх взаємодій.

В термінах задачі оцінки захищеності має бути не тільки опис зовнішніх об'єктів, але й опис передбачуваного порушника. В найпростішому випадку порушник описується більшістю зовнішніх впливів (загроз) T={ ti } з

відповідними характеристиками H(T)={h(t)}. В більш загальному випадку необхідно розгладати різноманітні типи зовнішніх взаємодій: T1, T2 ... . Це відповідає різноманітним цілям порушника: зняття інформації, проникнення, руйнуючі дії і так далі. Таким чином, у загальному випадку маємо список множин: T={Ti} при 1,…,N, який описується відповідним списком характеристик H(T).

Крім того, в моделі мають бути враховані так звані внутрішні «напіввзаємодії», які відповідають, з одного боку, можливій дії на об'єкт (елемент об'єкта), а з іншого – можливості елемента самому проводити дії, не передбачені технологією, які можуть мати небажані наслідки. Як складові опису об'єкта U та V для отримання оцінок повинні мати відповідні набори характеристик: H(U) та H(V). Передбачається, що загрози повинні створювати пару з різними «вразливостями» U з множини U(O) та U(C), тобто «зовнішня дія» (загроза з боку порушника) повинна відповідати «можливості такої дії» (уразливості) для створення пари (t, u) (якщо така зовнішня дія не конкретизована, крім того для певного об'єкта, як t=t(i) або t=t(i,j)). В результаті такої зовнішньої «посилки» загроза може «розвиватись», як по відповідних технологічних (санкціонованих) зв'язках моделі, так і по нетехнологічних, які в загальному випадку являються парами виду: (v,u). Відповідно, до складу моделі, яка описує порушника, окрім безпосередніх загроз входять множини вразливостей U та внутрішніх дій V, по-перше, як фактори, які сприяють нападу та, по-друге, як єдине джерело дій за відсутності зовнішнього порушника. Модель пасивного витоку інформації припускає, що порушник не проявляє активних дій. Відповідно, для опису порушника достатній набір T={t}, який описує подібні загрози. В термінах загальної моделі такий набір загроз можливо позначити як T1.

Для опису об'єкта необхідно врахувати: O – окремий елемент об'єкта;

C – інформаційні зв'язки (позначені C1 в термінах загальної множини);

U – неконтрольовані елементи, тобто ті, які можуть слугувати джерелами інформації для загроз T1 (в загальній моделі можна ввести позначення U1).

В описанні об'єкта передбачається, що всі елементи надійні та, відповідно, всі інші множини для загальної моделі залишаються пустими. Засоби захисту Z={z} для спрощення передбачається зв'язаними тільки з елементами моделі об'єкта, тобто z=z(o). В цьому випадку для описання моделі пасивного каналу витоку інформації використовуються найпростіші предикати:

Об'єкт: Елемент (o) – якщо «o» належить множині O; інформаційний зв'язок (o,e) – якщо «o» та «e» належать множині O; неконтрольований (o) – якщо з елемента «o» можливе перехоплення інформації, що відповідає множині U1 загальної моделі.

Захист: захист (o) – якщо є засоби захисту пов'язані з «o».

Порушник: читання(o) – якщо порушник намагається отримати інформацію з «o» (конкретного елемента, сукупності елементів, з яких здійснюється спроба отримання інформації).

Література:

1. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

НАУКОВЕ ВИДАННЯ

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Збірник тез доповідей семінару кафедри Систем інформаційного та кібернетичного захисту від 07 травня 2019 року

Адреса оргкомітету:
Україна, 03680, Київ, вул. Солом'янська, 7, тел. (044) 249-25-91
Державний університет телекомунікацій, Київ
e-mail: amina.zidan13@gmail.com