В статті проаналізовані питання забезпечення інформаційної безпеки та запропоновані вирази для оцінки залишкового ризику при захисті доступності інформаційних ресурсів локальної мережі

Ключові слова: інформаційна безпека, захист інформації

В статье проанализировано обеспечение информационной безопасности и предложены выражения для оценки остаточного риска при защите доступности информационных ресурсов локальной сети

Ключевые слова: информационная безопасность, защита информации

In this article the guaranteeing of information security is analyzed and expressions for estimating the residual risk are offers at protection of availability of LAN information resources

Keywords: information security, data protection

УДК 004.78

АНАЛІЗ ТА ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

Я.І. Заячук
Кандидат технічних наук, доцент*
Контактний тел.: 098-977-49-53
E-mail: yarikotm@gmail.com
П.С. Осташа*
*Кафедра комп'ютерних систем та мереж
Івано-Франківський національний технічний університет нафти і газу
вул. Карпатська, 15, м. Івано-Франківськ, Україна, 76019

1. Вступ

Забезпечення інформаційної безпеки є важливим завданням для будь-якої локальної мережі, оскільки від збереження конфіденційності, цілісності та доступності інформаційних ресурсів багато в чому залежать якість і оперативність прийняття технічних рішень, ефективність їх реалізації.

В умовах різних форм власності завдання забезпечення інформаційної безпеки повністю лягає на плечі підприємців, керівників організацій, різних комерційних структур. За підрахунками американських фахівців, втрата 20% інформації веде до розорення організації протягом місяця в 60 випадках зі 100. Інформація є основою для прийняття рішень людиною і від її достовірності, повноти, системної організованості залежить ризик прийняття неефективних і небезпечних рішень.

2. Актуальність

Рішення задач забезпечення інформаційної безпеки локальної обчислювальної мережі може бути отримано на базі використання систем підтримки прийняття рішень, застосування яких ефективно, тому що: по-перше, з'являється можливість вирішення погано формалізованих задач з залученням нового, спеціально розробленого для цих цілей математичного апарату (семантичних мереж, фреймів, нечіткої логіки); по-друге, такі системи орієнтовані на експлуатацію широким колом фахівців, спілкування з якими відбувається з використанням зрозумілої їм техніки міркувань і термінології; по-третє, застосування таких систем дозволяє значно підвищити ефективність і оперативність рішень за рахунок акумуляції знань експертів вищої кваліфікації.

3. Відомі рішеннями проблеми

У зв'язку із значною вагомістю забезпечення інформаційної безпеки, ринок програмного продуктів пропонує широкий спектр засобів підтримки прийняття рішень щодо даної галузі (CRAMM, COBRA, RiskWatch). Однак, більшість даних прикладних програм, якщо застосовувати їх для локальних мереж, характеризуються великою надмірністю реалізації алгоритмів та генерації рекомендацій та невеликою практичною корисністю результатів. Крім того, дані програмні продукти є дуже складними для кінцевого користувача і потребують спеціальної підготовки перед початком роботи з ними, та їх вартість, часто, є недосяжна для потенційного покупця.

4. Аналіз та оцінка ризиків інформаційної безпеки

У спектрі інтересів суб'єктів, пов'язаних з використанням локальних обчислювальних мереж, можна виділити необхідність забезпечення функціональних властивостей захищеності інформаційних об'єктів і які забезпечуються відповідними рівнями послуг інформаційної безпеки (ІБ):

1) конфіденційність;
2) цілісність;
3) доступність.

На сьогоднішній день вимоги щодо конфіденційності, цілісності та доступності викладені в досить розвиненій нормативно – правовій базі.

Забезпечення цих функціональних властивостей захищеності інформації локальних обчислювальних мережах є дуже важливою і актуальною проблемою. Для вирішення цієї проблеми потрібно використовувати такі системи захисту, які б надійно захищали той

чи інший ресурс такої мережі. Вибір чи побудова цих систем із відповідними характеристиками можу бути побудована і на методології аналізу та оцінки так званих залишкових ризиків.

Для оцінки ризику при забезпеченні конфіденційності, подію, пов'язану з порушенням конфіденційності, слід розглядати як складну, що складається з подій:

- несанкціонованого отримання користувачем інформації з метою ознайомлення з нею чи будь-якого подальшого використання;

- розкриття змісту інформації з обмеженим доступом (ІзОД) після її отримання. Останнє слід трактувати як можливість подолання порушником відповідних засобів криптозахисту.

Несанкціоноване отримання користувачем інформації є можливим при умові подолання неавторизованим користувачем засобів захисту у складі:

1) організаційного обмеження доступу;

2) охоронної сигналізації;

3) управління доступу, включаючи засоби управління фізичним доступом та адміністрування;

4) засобів канального захисту в телекомунікаційних мережах (ТКМ);

5) засобів захисту від вірусних атак.

При цьому ймовірність подолання засобів управління доступом q_1 можна визначити з виразу

$$q_1 = q_{уд} [1-(1-q_{ood} \cdot (1-d_{oc})],$$

де $q_{уд}$ – ймовірність подолання засобів управління доступом;

q_{ood} – ймовірність подолання засобів організаційного обмеження доступу;

d_{oc} – ймовірність подолання засобів охоронної сигналізації.

Тут і надалі при відсутності того чи іншого виду захисту ймовірність його подолання вважається такою, що дорівнює одиниці.

В свою чергу, ймовірність $q_{уд}$ подолання засобів управління доступом є також ймовірністю складної події, яка полягає в подоланні порушником як засобів управління фізичним доступом, так і засобів адміністрування доступом з використанням механізмів базового та прикладного програмного забезпечення. Якщо позначити ці ймовірності через $q_{уфд}$ і $q_{ад}$ відповідно, тоді

$$Q_{уд} = q_{уфд} \cdot q_{ад}.$$

Тоді, зрозуміло, що

$$q_1 = q_{уфд} \cdot q_{ад} [1 – (1 – q_{ood}) (1-q_{oc})].$$

Для зменшення імовірності подолання засобів управління доступом необхідно забезпечити чітке дотримання політики безпеки в частині правил розмежування доступу та надання тих чи інших привілеїв користувачам.

Окрім того, несанкціоноване отримання користувачем інформації є можливим і через засоби віддаленого доступу до інформаційних об'єктів, використовуючи витоки інформації технічними каналами, засоби телекомунікаційної мережі та вірусні атаки при умові подолання неавторизованим користувачем відповідних засобів захисту.

Нехай ймовірність подолання засобів захисту від витоків інформації технічними каналами дорівнює $q_{зв}$, ймовірність подолання засобів антивірусного захисту - $q_{ав}$, а ймовірність подолання засобів захисту конфіденційності інформацій в телекомунікаційних мережах - $q_{кткм}$.

Після отримання ІзОД порушнику необхідно здійснити розкриття її змісту. Подія, яка полягає в тому, що порушник може розкрити зміст ІзОД є також складною і складається з трьох подій:

1) порушник знає мову, якою представляється інформація;

2) порушник знає і може застосувати дешифрування інформації;

3) має необхідні ключі для такого перетворення.

Ймовірності цих подій $P_{зм}$, $P_{зкп}$, $P_{кн}$ відповідно. При цьому $P_{кзі}$ – ймовірність подолання неавторизованим користувачем засобів криптозахисту (можливість розкрити зміст ІзОД) інформації можна визначити з виразу

$$Q_{кзі} = P_{зм} \cdot P_{зкп} \cdot P_{кн}.$$

Тоді вираз для розрахунку ймовірності qпк порушення конфіденційності інформації з подоланням розглянутих засобів захисту можна записати у вигляді

$$q_{пк} = q_{кзі} [1-(1 - q_1) \cdot (1 – q_{зв}) \cdot (1 –q_{ав}) \cdot (1 - q_{кткм})].$$

Розглянуте дозволяє зробити, висновок про те, що для забезпечення конфіденційності за рахунок унеможливлення доступу неавторизованих користувачів до інформації та розкриття її змісту необхідно застосовувати засоби (апаратурні чи програмні) для адміністрування доступу, для криптографічного перетворення (для шифрування та дешифрування закритої інформації, а також засоби генерації та розповсюдження ключів), засоби управління фізичним доступом, засоби охоронної сигналізації та організаційного обмеження доступом.

Для оцінки залишкового ризику при забезпеченні цілісності подію, пов'язану з її порушенням, слід розглядати як складну, що складається з подій:

- виведення з ладу, зміни режимів функціонування або несанкціонованого використання засобів зберігання носіїв інформації і порушення її цілісності;

- несанкціонованої модифікації ІзОД в середовищах її оброблення, зберігання чи передавання з метою унеможливлення подальшого її використання чи нанесення іншої шкоди власнику даного ресурсу.

Подолання неавторизованим користувачем системи захисту з імовірністю $q_{пц}$ можливе, якщо:

- подолано засоби охоронної сигналізації або засоби організаційного обмеження доступу та (і) засоби управління доступом, включаючи засоби управління фізичним доступом та адміністрування доступу. Ймовірність такої події q_1 уже визначена раніше.

- з імовірністю $q_{цткм}$ подолано засоби захисту цілісності від загроз в ТКМ;

- з імовірністю $q_{св}$ подолано засоби захисту від спеціальних впливів на інформацію технічними каналами;

- з імовірністю $q_{ав}$ подолано засоби антивірусного захисту;

- з імовірністю $q_{кц}$ подолано засоби контролю та поновлення цілісності інформації.

Тоді, з використанням застосованих вище підходів, ймовірність порушення цілісності $q_{пц}$ можна знайти з виразу

$$q_{пц} = q_{кц} [1 – (1 – q_1) \cdot (1 – q_{св}) \cdot (1 – q_{ав}) \cdot (1 – q_{цткм})].$$

Розглянуте дозволяє зробити, по-перше, висновок про те, що для забезпечення цілісності за рахунок унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об'єкту необхідно застосовувати засоби (апаратурні чи програмні) для адміністрування доступу, для контролю цілісності, для управління фізичним доступом, засоби охоронної сигналізації та організаційного обмеження доступу.

По-друге, з останнього виразу витікає необхідність, на відміну від моделі взаємодії засобів реалізації загроз та засобів забезпечення конфіденційності, застосування для забезпечення цілісності інформаційних об'єктів засобів з відповідними механізмами контролю цілісності та замість засобів захисту від витоків – засобів захисту від спеціального впливу.

Виходячи із наведеного вище для оцінки ризику при забезпеченні доступності, подію, пов'язану з її порушенням, слід розглядати як наслідок впливу на інформаційний об'єкт загроз, найбільш суттєвими з яких є:

1) несанкціонована модифікація інформаційного ресурсу, включаючи зміни режимів його функціонування, місця зберігання, що потребує поновлення цілісності ресурсу шляхом, наприклад, використання його резервної копії;

2) перевід ресурсу в режим штучної відмови шляхом:

- несанкціонованого використання інформаційного ресурсу в той час, коли ресурс є необхідним користувачеві, і створенню, таким чином, перешкод іншим користувачам у використанні цих ресурсів;

- постійного використання ресурсу, наприклад, шляхом генерації потоку запитів, коли захищений ресурс обслуговує лише ці запити;

- постійного порушення цілісності з періодичністю меншою ніж час відновлення інформаційного ресурсу.

Ймовірність першої з цих подій визначено вище і вона дорівнює $q_{пц}$.

Для оцінки ймовірності порушення доступності шляхом переводу ресурсу в режим штучної відмови необхідно визначити інтенсивність потоку впливів на доступність ресурсу. Для цього скористаємося відомими підходами для розрахунку результуючої інтенсивності як природних, так і штучних впливів на інформаційні ресурси технічними каналами [1-5]. Під природними впливами будемо розуміти потоки будь-яких подій, які здатні вивести інформаційно – телекомунікаційну систему (ІТС) з ладу тимчасово, чи на тривалий термін, тобто потоки відмов. Такі події впливають як безпосередньо на інформаційні ресурси ЛОМ, так і на засоби технічного захисту цієї системи.

Під штучними впливами розуміються події, які є наслідком діяльності користувачів по відношенню до ресурсів ІТС, що є забороненими для них. Такі спроби несанкціонованого доступу (НСД) можуть бути випадковими або зловмисними.

Будемо вважати потік загроз найпростішим з інтенсивністю $\lambda_з$. Потік складається із штучних загроз з інтенсивністю $\lambda_ш$ та природних з інтенсивністю λ, так що $\lambda_з = \lambda_ш + \lambda$. В свою чергу, штучні загрози можуть бути внутрішніми з інтенсивністю $\lambda_{шв}$ та зовнішніми з інтенсивністю $\lambda_{шз}$ Виявлення і подальша протидія загрозі залежить від того, чи запобігла система ТЗІ впливу загрози, чи установила факт її впливу і ліквідувала відповідні наслідки.

Ця задача вирішується, по-перше, шляхом управління доступом до інформаційних ресурсів ЛОМ (ідентифікація, автентифікація, надання повноважень чи привілеїв, з їх перевіркою під час кожної із спроб доступу до ресурсів). Для цього в системі ТЗІ повинен виділятись адміністратор (адміністратор безпеки), який вирішує ці питання з використанням засобів системи захисту, можливо через автоматизоване робоче місце (АРМ) адміністратора безпеки.

Слід вважати, що стійкість (в розумінні імовірності не подолання) системи управління доступом $p_д = 1 – q_1$ визначається стійкістю процесів ідентифікації та автентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями. В наслідок відсіву (фільтрації) внутрішніх впливів системою на її виході інтенсивність завад буде дорівнювати $\lambda_{шз} \cdot q_1$.

Ця задача може вирішуватися, по-друге, застосуванням в ІТС засобів фільтрації зовнішніх штучних впливів, які впливають на дану ЛОМ (засоби фільтрації типу міжмережних екранів (firewall, брандмауерів), сервісів-посередників (proxyservices)). Якщо стійкість таких засобів дорівнює $p_ф = 1 - q_ф$, то в наслідок фільтрації зовнішніх впливів на виході системи інтенсивність завад буде дорівнювати $\lambda_{шз} \cdot q_ф$, а інтенсивність $\lambda_р$ штучних впливів, які не відфільтровані системами управління доступом та фільтрації, складе:

$$\lambda_{рш} = \lambda_{шв} \cdot q_1 + \lambda_{шз} \cdot q_ф + \lambda.$$

З урахуванням інтенсивності справжніх запитів $\lambda_{сз}$ загальна інтенсивність $\lambda_з$ впливів дорівнює

$$\lambda_з = \lambda_{сз} + \lambda_{шв} \cdot q_1 + \lambda_{шз} \cdot q_ф + \lambda.$$

При середній тривалості обслуговування в ІТС одного запиту $t_{вр}$ і Пуассонівському законі розподілу, ймовірність того, що під час звернення до ресурсу він уже використовується дорівнює

$$q_{пз} = 1 – p_0 = 1 – \exp\{-t_{вр} \cdot \lambda_з\},$$

Де p_0 – ймовірність відсутності впливів;

а отже ймовірність порушення доступності ресурсу

$$q_{пд} = 1 – (1 – q_{пз}) \cdot (1 – q_{пц}).$$

Таким чином, величину загального залишкового ризику у вигляді ймовірності порушення (подолання, злому) комплексної системи захисту можна розраховувати за виразом:

$q = 1 - (1 - q_{пк}) \times (1 - q_{пц}) \cdot (1 - q_{пд})$.

Усі невизначені змінні в виразах, наведених для розрахунку запропонованих показників захищеності інформації (ймовірностей порушення тієї чи іншої властивості захищеності інформації), можуть бути розрахованими, якщо відомі чи їх складові, чи закони розподілу відповідних ймовірностей.

В багатьох випадках можна вважати розподіл ймовірностей таких подій рівномірним. В інших випадках для розрахунку ймовірностей можна використати параметри потоків відповідних випадкових величин.

5. Висновки

Розроблена концепція і методика можуть використовуватися керівниками, співробітниками служби інформаційної безпеки для створення системи забезпечення інформаційної безпеки локальної обчислювальної мережі.

Література

1. Василенко, В.С. Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах [Електроний ресурс] Василенко В.С., Бордюк О.С., Полонський С.М. - Режим доступу: URL: http://www.rusnauka.com /11_EISN_2010/Informatica/64-068.doc.htm - 1.05.2012 р.
2. Хади, Р.А. Разработка архитектуры программной системы конфиденциального доступа к информационным ресурсам электронно-вычислительных сетей[Текст]/ Р.А.Хади. – М.: Атомиздат, 2003. – 140 с.
3. Лобанов, С.Г. Информационная безопасность как диалектика закрытости и открытости [Текст]/ С.Г. Лобанов // Информ. ресурсы России. – 2002. – № 7. – С. 25-28.
4. Каторин, Ю.Ю. Большая энциклопедия промышленного шпионажа [Текст]/ Ю.Ю.Каторин. – М.: Почтальйон, 2002. – 512 с.
5. Куканова, Н. Описание классификации угроз [Електроний ресурс] / П. Куканова. - Режим доступу: www. URL: http://www.dsec.ru/products/grif/. – 13.11.2006 р.

У статті розглянута комп'ютерна система для зняття магнітних характеристик. Описана структурна схема і основні модулі програмного забезпечення

Ключові слова: комп'ютерна система, модель Джілса – Аттертона

В статье рассмотрена компьютерная система для снятия магнитных характеристик. Описана структурная схема и основные модули програмного обеспечения

Ключевые слова: компьютерная система, модель Джилса – Аттертона

The article describes a computer system for measuring of the magnetic characteristics. We describe a block diagram and basic modules of the software

Keywords: computer system, the magnetic characteristics, Jiles – Atherton model

УДК 004.94:004.896

КОМПЬЮТЕРНАЯ СИСТЕМА ДЛЯ СНЯТИЯ МАГНИТНЫХ ХАРАКТЕРИСТИК

Е.В. Шкурников
Программист
ООО «Генстар»
ул. Криничная, 2, г. Киев, Украина, 03138
Контактный тел.: 099-931-93-42
E-mail: nikshev@i.ua

1. Вступление

Практически все известные виды вторичных источников питания содержат в своём составе электромагнитные компоненты, такие как трансформаторы и индукторы.

Обычно эти компоненты изготавливаются с использованием различных магнитных материалов, позволяющих улучшить их электрические параметры, а так же уменьшить размеры и массу.

2. Постановка задачи

Каждая современная система автоматического проектирования радиоэлектронной аппаратуры со-