МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ

Ректор _____ С.В. Іванов
(підпис)
«____»_____2014 р.

О.А. ХЛОБИСТОВА
Ю.Г. САВЧЕНКО
М.В. ГЛАДКА

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Всі цитати, цифровий та фактичний матеріал, бібліографічні відомості перевірені. Написання одиниць відповідає стандартам
Підписи авторів_____
«12» лютого 2014 р.

Реєстраційний номер електронного навчального посібника у НМВ
_____

Київ НУХТ 2014

УДК 004.451.36:681.5:002
Рецензент: В.А.Литвинов, доктор технічних наук, професор

Хлобистова О.А. Технології захисту інформації [Електронний ресурс]: навчальний посібник / О.А. Хлобистова, Ю.Г. Савченко, М.В. Гладка – К.: НУХТ, 2014. – 84 с.

Метою навчального посібника є забезпечення цілісності сприйняття методології і методів захисту інформації, аспекти котрих знаходять широке застосування при використанні сучасних інформаційних систем. Послідовно і комплексно викладено на інженерному рівні всі етапи організації захисту інформації, організації конфіденційності, безпеки і надійності. Матеріали супроводжуються малюнками, задачами і питаннями для самоперевірки, анотованим списком літератури.

Навчальний посібник призначено для студентів вищих навчальних закладів які навчаються за напрямом підготовки «Комп'ютерні науки».

О.А. ХЛОБИСТОВА, кандидат технічних наук, доцент
Ю.Г. САВЧЕНКО, доктор технічних наук, професор
М.В. ГЛАДКА, асистент

Рекомендовано Вченою радою
Національного університету харчових технологій
протокол № 5 від «27» лютого 2014 р.

Подано в авторській редакції

ЗМІСТ

ВСТУП

З розвитком і розширенням сфери застосування обчислювальної техніки, розвитком локальних мереж і підключенням до глобальної мережі постала проблема захисту інформації, яка використовується в цих системах. Інформація, що проникає у всі сфери діяльності суспільства, набуває конкретного політичного, матеріального і вартісного вираження.

Інформація, як сукупність знань про фактичні дані і залежності між ними, стала стратегічним ресурсом; вона – основа для прийняття будь-якого рішення. В інформаційних системах, які створюються в органах державної влади і у комерційних структурах, циркулює інформація, що містить секретні відомості про досягнутий потенціал в області економіки, оборони, науки і техніки, конфіденційні відомості про управлінську, господарську, комерційну, фінансову й іншу діяльність. Тому захист інформації як складна, наукомістка і багатогранна проблема в умовах упровадження сучасних інформаційних технологій, створення розподілених обчислювальних систем і мереж зв'язку набуває особливої гостроти.

Відомі різні варіанти захисту – від охоронця на вході до математично вивірених засобів захисту даних. Але слід зазначити, що абсолютно захищених систем немає. Можна говорити лише про деяку імовірність захищеності системи щодо певної категорії зловмисників. В інформаційних системах, що використовують в роботі конфіденційну або секретну інформацію, засоби захисту абсолютно необхідні для нормального функціонування системи, хоча в процесі роботи вони завдають певні незручності користувачам. До них в першу чергу відноситься:

- додаткове навантаження на системні ресурси, що потребує збільшення робочого часу для виконання такого ж самого завдання внаслідок уповільнення доступу до даних та виконання операцій в цілому;
- потреба залучення допоміжного персоналу, який відповідає за підтримку працездатності системи захисту;
- збільшення вартості захищеної системи.

Останнім часом повідомлення про атаки на інформацію, про хакерів і комп’ютерні атаки наповнили всі засоби масової інформації. Що ж таке «атака на інформацію»? Дати визначення цій дії насправді дуже складно, оскільки інформація, особливо в електронному вигляді, представлена сотнями різних видів. Інформацією можна вважати окремий файл, базу даних, один запис в ній, і цілком програмний комплекс. І всі ці об’єкти можуть піддатися і піддаються атакам з боку деякої соціальної групи.

При зберіганні, підтримці і наданні доступу до будь-якого інформаційного об’єкту його власник або уповноважена ним особа, накладає набір правил по роботі з ним. Умисне їх порушення класифікується як атака на інформацію.

Атаки на інформацію можуть причинити наступні економічні втрати:

Розкриття комерційної інформації може привести до серйозних збитків на ринку.

Звістка про крадіжку великого об'єму інформації зазвичай серйозно впливає на репутацію фірми, приводячи побічно до втрат в об'ємах торгових операцій.

Фірми-конкуренти можуть скористатися крадіжкою інформації, якщо та залишилася непоміченою, для того, щоб повністю розорити фірму, нав'язуючи їй фіктивні або свідомо збиткові операції.

Підміна інформації як на етапі передачі так і на етапі зберігання може привести до величезних збитків.

Багатократні успішні атаки на фірму, що надає буль-який вид інформаційних послуг, знижують довіру до фірми у клієнтів, що позначається на об'ємі доходів.

Комп'ютерні атаки можуть принести і величезний моральний збиток. Поняття конфіденційного спілкування давно вже стало відомим широкому загалу. Само собою зрозуміло, що жодному користувачеві комп'ютерної мережі не хочеться, щоб його листи окрім адресата отримували ще 5÷10 чоловік або, наприклад, весь текст, що набирається на клавіатурі, копіювався в буфер, а потім при підключенні до Інтернету відправлявся на певний сервер. А саме так і відбувається в тисячах і десятках тисяч випадків.

Навчальний посібник допоможе майбутнім фахівцям з розроблення інформаційних систем визначати уразливі з точки зору безпеки місця в системах, які проектуються, оцінювати ризик порушення безпеки і можливі збитки від проникнення в систему, а також вживати відповідні заходи із попередження таких небажаних наслідків.

Основні терміни та визначення.

Безпека ІС – здатність протидіяти спробам завдати шкоди її власникам та користувачам при здійсненні навмисних і ненавмисних дій проти неї. Безпека АС досягається забезпеченням конфіденційності інформації, що нею обробляється, а також цілісності та доступності компонентів і ресурсів системи.

Конфіденційність – це властивість інформації бути відомою тільки допущеним та тим суб'єктам системи, що пройшли перевірку (авторизацію) – користувачам, програмам, процесам тощо. Для інших суб'єктів системи ця інформація є закритою.

Цілісність компонента (ресурсу) системи – властивість його бути незмінним (у семантичному розумінні) при функціонуванні системи.

Доступність компонента (ресурсу) системи – властивість його бути доступним для використання авторизованими суб'єктами системи в будь-який час.

Доступ – це взаємодія між суб'єктом і об'єктом, яка призводить до виникнення інформаційного потоку між ними.

Прихованим каналом називається шлях передачі інформації, який дає змогу двом взаємодіючим процесам обмінюватися інформацією в такий спосіб, що порушує системну політику безпеки.

Атакою називають реакцію загрози.

Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких здійснюється управління критичною інформацією в системі, її захист та розподіл. Політика безпеки має бути індивідуальною, залежати від конкретної технології обробки інформації, використання програмних та технічних засобів.

У сучасному комп'ютерному світі атаки на інформацію стали буденною практикою. Зловмисники використовують як помилки в написанні і адмініструванні програм, так і методи соціальної психології для отримання бажаної інформації.

Атака на інформацію – це умисне порушення правил роботи з інформацією. Атаки на інформацію можуть принести підприємству величезні збитки. На сьогоднішній день приблизно 90% всіх атак на інформацію проводять нині працюючі або звільнені з підприємства співробітники.

Важлива інформація – незамінна та необхідна для діяльності інформація, процес відновлення якої після знищення неможливий або ж дуже трудомісткий і пов'язаний з великими затратами, а її помилкове застосування чи підробка призводить до великих втрат.

Корисна інформація – необхідна для діяльності інформація, яка може бути відновлена без великих втрат, при чому її модифікація чи знищення призводить до відносно невеликих втрат.

Конфіденційна інформація – інформація, доступ до якої для частини персоналу або сторонніх осіб небажаний, оскільки може спричинити матеріальні та моральні втрати.

Відкрита інформація – це інформація, доступ до якої відкритий для всіх.

Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких здійснюється управління критичною інформацією в системі, її захист та розподіл. Політика безпеки має бути індивідуальною. Вона залежить від конкретної технології обробки інформації, використання програмних та технічних засобів.

1 ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Як визначається політика безпеки?

Інформаційна система (ІС) [1] – організаційно-технічна система, що реалізує інформаційні технології і включає апаратне, програмне та інші види забезпечення, а також відповідний персонал.

За результатами роботи інформаційних систем приймається значна кількість управлінських рішень щодо діяльності промислових і комерційних підприємств, органів державного управління, тощо. Тому користувачі ІС зацікавлені одержувати своєчасно і неспотворену інформацію. До того ж частина цієї інформації може бути надана обмеженому колу користувачів, тобто є секретною або конфіденційною.

На практиці найчастіше використовуються наступні категорії інформації:

- важлива інформація;
- корисна інформація;
- конфіденційна інформація;
- відкрита інформація.

Керівництво повинно приймати рішення про те, хто і яким чином буде визначати степінь конфіденційності і важливості інформації. На жаль, в нашій країні ще не повністю сформоване законодавство, щоб розглядати інформацію, як товар та регламентувати права інтелектуальної власності на ринку інтелектуального продукту, як це робиться в світовій практиці.

Політика безпеки формується на основі аналізу поточного стану і перспективи розвитку інформаційної системи, можливих загроз і визначає:

- мету, задачі і пріоритети системи безпеки;
- галузь дії окремих підсистем;
- гарантований мінімальний рівень захисту;
- обов’язки персоналу по забезпеченню захисту;
- санкції за порушення захисту.

Політика безпеки інформації і механізми підтримки її реалізації утворюють єдине захищене середовище опрацювання інформації. Це середовище має ієрархічну структуру, де верхні рівні подані вимогами політики безпеки, далі – інтерфейс користувача, потім йдуть декілька програмних рівнів захисту (включаючи рівні ОС) і, нарешті, нижній рівень цієї структури поданий апаратними засобами захисту. На всіх рівнях, крім верхнього, повинні бути реалізовані вимоги політики безпеки, за що, власне, і відповідають механізми захисту.

Оскільки, як було зазначено вище, засоби захисту, абсолютно необхідні для нормального функціонування системи, в процесі роботи завдають певні незручності користувачам системи, слід виявити реальні загрози для конкретної ІС, оцінити можливі збитки від їх реалізації і тоді конкретизувати вибір цих засобів.

Визначення політики безпеки неможливе без аналізу ризику. Аналіз ризику підвищує рівень поінформованості про слабкі та сильні процеси захисту, створює базу для підготовки і прийняття рішень, оптимізує розмір затрат на захист, оскільки більша частина ресурсів спрямовується на блокування загроз, що можуть принести найбільшу шкоду. Аналіз ризику складається з наступних основних етапів:

1. Опис складу системи: апаратних засобів, процес забезпечення, даних, документації, персоналу.
2. Визначення слабких місць – з'ясовуються слабкі місця по кожному елементу процесу оцінкою можливих джерел загроз.
3. Оцінка імовірності реалізації загроз.
4. Оцінка очікуваних розмірів втрат – цей етап складний, оскільки не завжди можлива кількісна оцінка процесу показниками.
5. Аналіз можливих методів і засобів захисту.
6. Оцінка виграшу від прийнятих заходів. Якщо очікувані втрати більші допустимого рівня, необхідно посилити заходи безпеки.

Аналіз ризику завершається прийняттям політики безпеки і складанням плану захисту з наступними розділами:

1. *Поточний стан.* Опис статусу системи безпеки в момент підготовки плану.
2. *Рекомендації.* Вибір основних засобів захисту, що реалізують політику безпеки.
3. *Відповідальність.* Список відповідальних працівників і зон відповідальності.
4. *Розклад.* Визначення порядку роботи механізмів захисту, в тому числі і засобів контролю.

Перегляд положень плану, які повинні періодично переглядатися

Якщо виконання політики безпеки проводиться не в повній мірі або непослідовно, тоді імовірність порушення захисту інформації різко зростає.

1.2. Класифікація загроз

Загрозу безпеці ІС можна класифікувати за такими ознаками:

1. За метою реалізації загрози:

- порушення конфіденційності інформації;
- порушення цілісності інформації (втрати від таких дій можуть бути набагато більшими, ніж при порушенні конфіденційності);
- порушення (повне або часткове) працездатності ІС (порушення доступності).

2. За принципом впливу на ІС:

- з використанням доступу суб'єкта системи (користувача, процесу) до об`єкта (файлу даних, каналу зв`язку тощо);
- з використанням прихованих каналів.

Вплив, заснований на першому принципі, простіший, але від нього легше знайти протизахист. Другий принцип важче реалізувати, але й важче виявити та усунути.

3. За характером впливу на ІС:

- активна загроза;
- пасивна загроза.

Активна загроза веде до зміни стану об`єкта і може здійснюватися або з використанням доступу (наприклад, до набору даних), або з використанням як доступу, так і прихованих каналів.

Пасивна загроза здійснюється шляхом спостереження зацікавленою особою за деякими побічними ефектами (наприклад, за роботою програм, прослуховування лінії зв’язку між двома вузлами мережі). Пасивний вплив не веде до зміни стану об`єкту, але порушує конфіденційність інформації в ІС.

4. За способом використання помилки захисту:

- використання помилок в алгоритмах, у зв`язках між ними, у програмах тощо, що дає можливість використовувати їх зовсім не так, як описано в документації;
- використання помилок адміністративного управління.

5. За способом активного впливу на об’єкт атаки:

- безпосередній вплив на об`єкт атаки (порушення доступу);
- порушення системи доступу;
- опосередкований вплив (через інших користувачів);
- «маскування»;
- «користувач наосліп» (коли один користувач примушує іншого виконувати певні дії, причому останній про це навіть не здогадується, наприклад вірус.

6. За режимом впливу на ІС:

- в інтерактивному режимі;
- в пакетному режимі.

7. За об`єктом атаки:

- ІС в цілому («маскування», злом або підробка паролю, несанкціонований доступ через мережу;
- окремі об`єкти ІС – дані або програми, окремі пристрої системи, канали передачі даних;
- суб`єкти ІС – процеси і підпроцеси користувачів, наприклад, введення вірусу;
- канали передачі даних.

8. За станом об’єкта атаки. Об`єкт може знаходитися в одному з трьох станів:

- збереження (вплив на об`єкт, як правило, здійснюється використанням доступу);
- передачі (здійснюється або доступ до фрагментів, що передаються, або прослуховування з використанням прихованих каналів);