Вступ

Метою проведення циклу лабораторних робіт є набуття студентами необхідних практичних навичок розробки та дослідження макетних зразків підсистем захисту інформації, які являють собою втілення ефективних підходів та алгоритмів створення комплексної системи захисту інформації від несанкціонованого доступу, дослідження характеристик необхідних структур даних, розробки та налагодження окремих компонентів інтерфейсу консолі адміністратора безпеки під ОС Linux, Windows, FreeBSD з застосуванням будь якої мови програмування для дослідження механізмів захисту в автоматизованих системах різного призначення.

Лабораторна робота включає:

- постановку вхідної задачі,
- теоретичні відомості з методів та засобів рішення задачі,
- аналіз математичного та алгоритмічного забезпечення,
- обґрунтування вибору програмних засобів дослідження,
- розробку структурної схеми взаємодії підсистем захисту,
- результати виконання покрокової верифікації алгоритмів,
- результати виконання модельних експериментів,
- інтерпретація результатів та висновки,
- лістинг програми.

Лабораторні роботи виконуються на персональних комп’ютерах із застосуванням сучасних компіляторів та відповідних оболонок.

В посібнику до кожної лабораторної роботи подано ґрунтовні, теоретичні відомості, зміст та обсяг яких достатній для підготовки, виконання та захисту виконаної роботи. Крім того, посібник містить завдання на лабораторні роботи, зміст звіту та контрольні запитання. Для поглибленого вивчення матеріалу необхідно звернутися до рекомендованої літератури.

Заключний етап лабораторної роботи – оформлення звіту, який подається на аркушах паперу формату А4 з урахуванням вимог стандартів.

ПЕРЕЛІК ЛАБОРАТОРНИХ РОБІТ

за курсом: «Системи безпеки програм і даних»

Лаб. Робота 1. Розробка програми керування доступом до захищеного носія інформації (в макетному варіанті - диску). Програма після завантаження в оперативну пам'ять здійснює контроль за спробами доступу до диску шляхом перехоплення відповідних переривань (21H та ін). У результаті управління передається програмам парольного захисту, і в залежності від статусу “admin” чи “user”, після реєстрації вони отримують відповідні дискретні права доступу до логічних дисків A, B, C та / або права читання, запису і / або виконання (за варіантами) до файлів на дисках.

Лаб. Робота 2.1. Розробка програми реєстрації користувачів. На диску створюється розділ, доступний тільки адміністратору, в якому формується системний журнал реєстрації (ЖР) користувачів, а в подальшому також інші засоби (операційний журнал, генератори ключів шифрування і т.д.). Адміністратор фіксує логін та пароль, а також перевіряє пароль на відповідність вимогам (по довжині, словнику і часу використання). Крім пароля в ЖР фіксуються дані, необхідні для подальшої аутентифікації користувачів.

Лаб. Робота 2.2. Розробка програми аутентифікації (підтвердження автентичності) користувачів у процесі їх роботи за комп'ютером. З інтервалом дельта-Т (за варіантами) програма задає питання або випадкові числа (3-4 знака) на які користувач попередньо сформував відповіді та / або визначив секретну функцію для аутентифікації. Всі помилки при аутентифікації викликають відмову в доступі і необхідність повторного входу. Деяка кількість (за варіантами) помилок викликає необхідність повторної реєстрації через адміністратора.

Лаб. Робота 3. Розробка програми моніторингу безпеки для виявлення небезпечних або аномальних дій користувачів. Програма забезпечує ведення операційного журналу (ОЖ) реєстрації всіх дій користувачів при зверненні до логічних дисків, файлів, службових програм. У ОЖ фіксується час і виділяються особливі події - звернення до системних таблиць, зашифрованих файлів, а головне фіксуються всі відмови в доступі: куди звертався і коли отримав відмову. За даними ОЖ формується список небезпечних або аномальних дій кожного користувача і шаблони їхньої нормальної роботи.

Лаб. Робота 4.1. Розробка програми швидкого дискретного потенціювання (ШДП) для виконання обчислювальних операцій в алгоритмах шифрування RSA і El-Gamal та в інших схемах і алгоритмах. Програма повинна реалізувати арифметику (додавання, множення, зведення в квадрат, визначення залишків по модулю) з довжиною вихідних чисел до декількох десятків (за варіантами) десяткових розрядів.

Лаб. Робота 4.2. Розробка програми генератора великих простих чисел (ВПЧ). Для шифрування і розрахунку ключів за схемою RSA необхідно використовувати два великих простих десяткових числа з кількома десятками десяткових розрядів (за варіантами). Для генерації таких простих чисел можна використовувати формули у відповідності з тестом Рабіна або іншими алгоритмами, але для перевірки властивостей сформованих кандидатів у прості числа необхідно використовувати малу теорему Ферма і алгоритм ШДП.

Лаб. Робота 5. Розробка програми керування ключами шифрування за схемою RSA або El-Gamal (за варіантами). Програма реалізує ту чи іншу схему розрахунку ключів шифрування, обов'язково використовуючи для цього розширений або класичний алгоритми Евкліда, і формуючи відкриті і

закриті (секретні) ключі шифрування, які відразу ж використовуються для шифрування повідомлень. Програма реалізує два режими шифрування і дешифрування повідомлень з перевіркою достовірності результатів на основі аналізу цифрового паспорта-сертифіката відкритих ключів.

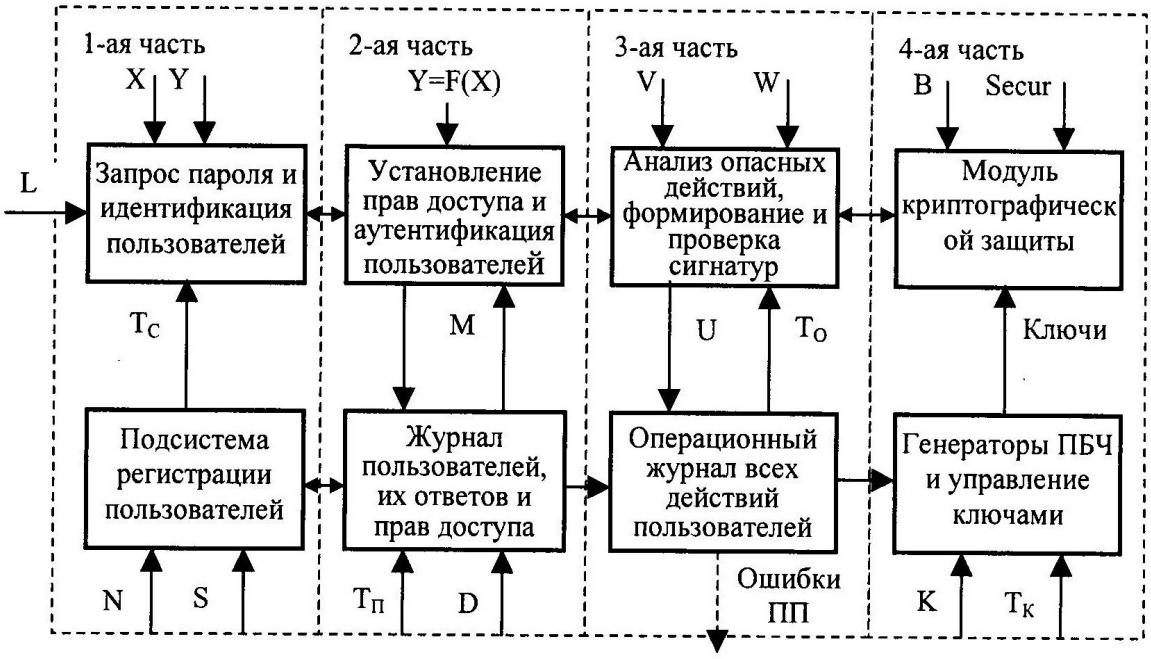
Лаб. Робота 6. Розробка програми формування сигнатури повідомлення (цифровий підпис) на основі симетричного алгоритму шифрування. Програма реалізує два режими роботи: просте поблокове шифрування і дешифрування повідомлень (режим електронної кодової книги), а також зчеплення блоків шифру при формуванні цифрового підпису. Схема управління ключами шифрування генерує ключі як випадкові двійкові числа довжиною декількох десятків біт (за варіантами), які зберігаються і можуть бути повторно використані.

РОЗРОБКА ПРОГРАМНИХ КОМПОНЕНТ БЕЗПЕКИ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ ОРГАНІЗАЦІЯ ПІДСИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ АУТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ ДОСТУПУ (ЗАВДАННЯ НА РОЗРОБЛЕННЯ)

Тема: Дослідження способів і засобів забезпечення безпеки інформаційно-аналітичних систем, що містять інтелектуальні компоненти для адаптації до змінюваних правил та умов зовнішнього середовища. Комплекси розміщуються на магнітних носіях, в навчальному макеті на диску, з вбудованими засобами дискретного управління доступом, криптографічного захисту та управління ключами шифрування, ідентифікації і аутентифікації користувачів з оперативним аналізом їх підозрілих (аномальних) дій.

Мета: створення програмного макета підсистеми забезпечення безпеки носія інформації з обмеженим доступом по заданій загальній структурі засобів захисту та індивідуальними параметрами відповідних алгоритмів (див. таблиці 1, 2, 3, 4).

ЗАГАЛЬНА СТРУКТУРА ПІДСИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ З ВБУДОВАНИМИ ЗАСОБАМИ ДИСКРЕТНИХ УПРАВЛІННЯ ДОСТУП ДО ІНФОРМАЦІЇ.



Зміст роботи.

У даній навчально-практичній роботі пропонується розробити підсистему захисту інформації на диску у відповідності з характеристиками, вибираними за варіантами з таблиць 1, 2, 3, 4, що дозволяє робити:

- реєстрацію користувача системи і його ідентифікацію за паролем з контролем безпечного часу використання пароля та наданих йому дискретних прав доступу на основі засобів ведення реєстраційного журналу;
- періодичну аутентифікацію користувача на основі одноразового або дворазового «рукостискання» з використанням запитань-відповідей і секретних математичних функцій: запит комп'ютера - X, відповідь користувача - Y, Y = F (X + a (дві останні цифри номера залікової книжки)) і навпаки;

- стеження за діями користувачів і ведення операційного журналу з реєстрацією та аналізом небезпечних дій;
- генерацію сеансових і особистих ключів та криптографічний захист користувацької і системної інформації (журналів і таблиць) на основі заданих алгоритмів шифрування.

ТАБЛИЦЯ 1-2.

Вариант по 1-ой букве Фамилии	**Таблица 1.** Параметры подсистемы авторизации доступа			
	Длина пароля	Число пользователей	Право доступа к дискам	Время смены паролей
	L (симв)	N	S (1 / 0)	T_C (суток)
А	6	10	C, E	6
Б	4	8	A, B	1
В	8	6	D, E	4
Г	3	5	A, E	3
Д	7	12	C, D, E	8
Е	5	8	B, C	10
Ж	6	10	B, E	7
З	8	5	D, C	6
И	3	4	A, C, E	2
К	4	8	C, D	4
Л	7	3	B, D	1
М	5	4	A, C	8
Н	6	7	D, A	4
О	5	10	A, B, C	9
П	8	5	B, A	3
Р	3	2	C, B	1
С	6	8	D, B	4
Т	8	5	C, E	5
У	4	9	A, B	7
Ф	7	4	D, E	8
Х	5	10	A, E	4
Ц	3	2	C, D, E	1
Ч	4	5	B, C	10
Щ	6	8	B, E	6
Ш	4	9	D, C	7
Э	8	3	A, C, E	3
Ю	5	6	C, D	5
Я	7	4	B, D	8

Вариант по 1-ой букве Имени	**Таблица 2.** Параметры подсистемы аутентификации пользователей			
	Секретная функция	Число ответов	Требование перерегистрации	Темп предъявления вопрос.
	F(X)	M ответ	D ошибок	$T_П$ (мин)
А	exp(a*x)	4	3	1
Б	a*x+1.5	3	5	3
В	lg(a*x)	2	4	2
Г	sqrt(x+a)	5	2	3
Д	a*sin(x)	3	4	5
Е	tg(a-x)	2	5	2
Ж	lg(a/x)	1	4	1
З	sqrt(x-a)	4	3	3
И	x/sin(a)	3	2	5
К	tg(a*x)	2	5	4
Л	lg(a+x)	5	3	2
М	sqrt(x/a)	1	5	3
Н	a*sin(1/x)	3	3	1
О	tg(a*x)	2	4	4
П	a*ln(2+x)	4	2	2
Р	exp(x-a)	3	4	3
С	lg(a/x)	2	5	5
Т	sqrt(x-a)	1	4	1
У	x/sin(a)	5	3	3
Ф	tg(a*x)	2	5	2
Х	a*ln(7^x)	4	2	1
Ц	a/x+1.9	3	3	4
Ч	0.4/(a+x)	2	4	3
Щ	6.1*(a-x)	4	3	5
Ш	exp(-a/x)	1	5	2
Э	a*x+3.1	5	2	1
Ю	lg(a+x)	2	4	3
Я	sqrt(x/a)	3	5	2

Програма реєстрації призначена для реєстрації або видалення користувачів. Право реєструвати або видаляти користувачів в Реєстраційному Журналі (РЖ) надається тільки одному користувачеві-Адміністратору системи, що має найбільш захищений пароль (2L символів)

для входу в систему реєстрації та видалення. При реєстрації кожен користувач вводить свій пароль, який має не менш ніж L символів (Таблиця 1).

Еходрук при введенні пароля замінюється службовими символами. У разі введення пароля меншої довжини підсистема реєстрації попереджає користувача. Необхідно стежити за часом використання пароля не більше Tc доби та попереджати користувача про необхідність зміни пароля. Кількість N користувачів в РЖ обмежена завданням, і більшу кількість не може бути зареєстровано.

При реєстрації кожного користувача в Журналі системи адміністратором задаються певні S (1 або 0) права доступу до одного або декількох заздалегідь створених дискретних логічних дисків: A, B, C, D, E і відповідним файлам на диску, до яких дискретні права доступу задаються вектором REWACO.

За даними (Таблиця 3) визначаються конкретні V-дискретні права доступу до файлів на доступних дисках. Максимальні права доступу: R-читання, E-виконання, W-запис, A-додаток (запис без стирання), C-управління (створення-знищення каталогів), O - володіння (виключення доступу іншим користувачам). Мінімальні права 2: R і E, або R і A, звичайні права 3: R, E, A чи R, E, W, повні права 4: R-читання, E-виконання, W-запис, C-керування. У випадку 1 для кожного користувача надаються повні права володіння одним з логічних дисків.

Імена користувачів, їхні паролі та права доступу, а також секретна функція F (X) і відповіді на M контрольних питань для аутентифікації (Таблиця 2) зберігаються спочатку в явному, а потім зашифрованому вигляді у файлі РЖ в певному форматі. Загальний список контрольних питань (КП) об'ємом не менше ніж N * M питань зберігається в окремому файлі КП. З нього при черговій зміні пароля задаються випадковим чином нові M питань, а відповіді на них реєструються в РЖ.

Програма ідентифікації, що викликається при вході в систему, призначена для встановлення автентичності зареєстрованого користувача і надання йому відповідних прав доступу в систему. Ідентифікація користувача здійснюється шляхом порівнювання введеного імені (login) та пароля (password) користувача із записаними ім'ям і паролем, які зберігаються у файлі РЖ.

Після встановлення ідентичності введеного імені і пароля резидентна частина програми securit.com відстежує звернення до каталогів в системі та у відповідності з правами доступу приховує від користувача ті каталоги, які йому недоступні.

2. Функції Модуля аутентифікації.

Аутентифікація полягає в періодичній (стохастичній) перевірці справжності легального користувача, щоб уникнути його заміни зловмисником безпосередньо на робочому місці. Перший етап аутентифікації виконується відразу ж після ідентифікації та входу в систему (Таблиця 2). Програма securit.com періодично з кроком перевірки Тп задає випадковим чином питання з файлу ask.txt або випадкові двох-, трьох розрядні десяткові числа користувачеві для перевірки на додаткові знання користувачем секретної функції F (X) або раніше даних «алогічних» відповідей, порівнює отримані відповіді з заздалегідь зареєстрованими або обчисленими відповідями та оперативно підтверджує або забороняє роботу користувача. У випадку правильної відповіді за користувачем залишаються його права, але в список ask.txt додається новий № питання і відповідь, а в випадку неправильної відповіді - користувач втрачає право доступу і повинен знову ввійти в систему. При паузі у відповіді користувача більш ніж Тп реєструється помилка і користувач повинен знову ввійти в систему. При реєстрації більш D помилок аутентифікації користувач втрачає свої права доступу і повинен перереєструватися в системі.

ТАБЛИЦЯ 3-4

Вариант по 1-ой букве Отчества	**Таблица 3.** Параметры подсистемы слежения за системными событиями (ошиб.)			
	Дискретные права доступа	Уровени опасности событий	Способ вызова программ слежения	Темп выдачи отчетов
	V (REAW)	U	W	T_O (суток)
А	2	2	при входе	1
Б	4	1	при обращ	2
В	3	3	при иници	3
Г	1	4	при входе	1
Д	2	2	при входе	3
Е	3	1	при обращ	2
Ж	1	4	при иници	1
З	4	2	при входе	2
И	3	1	при обращ	3
К	2	3	при входе	1
Л	4	2	при иници	4
М	3	2	при обращ	2
Н	1	3	при входе	1
О	2	4	при иници	3
П	4	3	при обращ	2
Р	3	2	при иници	1
С	4	1	при входе	4
Т	1	3	при обращ	2
У	2	3	при иници	1
Ф	4	2	при иници	1
Х	2	4	при обращ	3
Ц	3	1	при входе	2
Ч	2	2	при обращ	1
Щ	1	3	при иници	4
Ш	4	2	при обращ	2
Э	3	2	при иници	3
Ю	2	3	при входе	1
Я	1	4	при обращ	2

Вариант по 2 последним цифрам	**Таблица 4.** Параметры подсистемы криптографической защиты			
	Алгоритм шифрования	Длина ключа	Размер блока сообщения	Время смены ключей
	Secur.	K (бит)	B (байт)	T_K (суток)
01	RSA	64	4	4
02	ElGamal	110	3	3
03	DES	56	8	10
04	SHA	56	8	5
05	FEAL	64	16	6
06	DSA	48	12	4
07	RSA	120	4	3
08	ГОСТ	128	16	8
09	ElGamal	80	5	2
10	DES	64	8	3
11	IDEA	64	8	2
12	DES	112	8	4
13	FEAL	64	16	10
14	DSA	128	8	5
15	DES	56	8	3
16	ElGamal	96	6	6
17	DSA	104	10	4
18	IDEA	64	8	7
19	DES	56	8	8
20	RSA	80	4	3
21	ГОСТ	128	16	4
22	ElGamal	128	3	8
23	FEAL	64	8	5
24	SHA	80	6	3
25	IDEA	128	16	7
26	DES	56	8	10
27	ElGamal	192	8	2
28	RSA	72	5	6

3. Функції Модуля спостереження (моніторингу).

Програма securit.com виробляє виклик програми стеження за діями користувача з метою реєстрації часу і всіх особливих подій в Операційному Журналі (ОЖ) системи, які можуть бути пов'язані з можливими небезпечними діями користувача і його програм (Таблиця 3). Програма стеження і ведення ОЖ може викликатися відразу при ініціалізації системи захисту, при вході користувача в систему або при першому зверненні до ресурсів, що захищаються, наприклад, до зашифрованих файлів або

системних ресурсів. Залежно від способу W в конкретній системі реалізується той чи інший механізм виклику програм спостереження.

Реєстровані події помилок при вході в систему, помилок при аутентифікації суб'єктів і повідомлень, помилок у перевищенні своїх повноважень, тобто наприклад, спроб запису у файл, дозволений тільки для R і E, всі події звернення до зашифрованих файлів або системних таблиць є небезпечними подіями. Однак рівень небезпеки, наприклад, помилок при вході є мінімальним - 1 рівень, помилок у перевищенні своїх повноважень - 2 -ий рівень небезпеки, помилок аутентифікації - 3-й рівень, помилок дешифрування або звернення до системних ресурсів - 4-й рівень, у тому числі, наприклад, при зміні дати або системного часу.

В залежності від заданого U - кількості реєстрованих рівнів небезпеки подій, програма стеження фіксує події всіх 4-х рівнів небезпеки, 3-х, 2-х або події тільки 1-ого рівня помилок при ідентифікації користувачів: коли і хто увійшов або отримав відмову в доступі.

Через період часу Те дані з Операційного Журналу обробляються та систематизуються по кожному з користувачів з метою визначення рівня небезпеки їх дій, що дозволить з деякою мірою вірогідності оцінити: чи є зареєстровані помилки випадковими або навмисними?

4. Функції Модуля шифрування.

Для шифрування інформації і формування сигнатур повідомлень (цифрових підписів) (Таблиця 4) в системі захисту можуть використовуватися алгоритми DES (Data Encryption Standard), FEAL (Fast Encipherment Algorithm), Шеа (International Data Encryption Algorithm), ГОСТ (28147-89), RSA (Rivest, Shamir, Adleman), El-Gamal, SHA (Secure Hash Algorithm), DSA (Digital Signature Algorithm). Чотири перші алгоритму передбачають симетричну схему шифрування секретними ключами, а чотири останніх методу припускають використання відкритих та закритих ключів.

У відповідності з принципом «відкритості» для забезпечення цілісності інформації, в тому числі сигнатур, закритий ключ використовується в

основному для шифрування даних, а відкритим ключем усі бажаючі зможуть розшифрувати і прочитати інформацію, якій можна довіряти, оскільки вона могла бути зашифрована лише за допомогою секретного ключа. Оригінальний текст зберігається в файлі з ім'ям - input.txt, зашифрований у файлі - close.txt, а розшифрований у файлі - open.txt. Будь-які зміни шифрованого повідомлення або коду ключа призведуть до збою при дешифруванні. Відкритий ключ дозволяє також будь-якому охочому сформувати свою сигнатуру для прийнятого повідомлення, і переконається в його достовірності при збігу своєї сигнатури з тією, що була прийнята разом із повідомленням.

Довжина ключа K (біт) приймається невеликий, що відповідає, наприклад, K/4 цифр десяткових чисел, прийнятих за відкритий і закритий ключі шифрування. Вихідні дані повинні бути прийняті за основу генераторів великих простих чисел (ВПЧ) і розрахунку ключів, наприклад, на основі тесту Рабіна та малої теореми Ферма, розширеного алгоритму Евкліда і формування додаткових чисел по модулю Q.

Програма rsa.com виробляє генерацію ключів загальною довжиною До / 4 десяткових знаків, шифрує поблочно по B байт повідомлення з файлу input.txt і записує закодоване повідомлення в close.txt, а потім поблочно декодує закрите повідомлення і записує відкрите в файл open.txt

Через час Тк (діб) повинно формуватися попередження про необхідність зміни ключів шифрування і адміністратором кожному користувачеві через час Тк видаються нові секретні «майстер» ключі.

СПИСОК ЛІТЕРАТУРИ

1. Столлингс В. Криптография и защита сетей. М: С-Пб: Изд. Дом «Вильямс», 2001. – 672 с.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Учебник. М: Радио и связь., 1999. - 328 с.
3. Широчин В.П. Архитектоника мышления и нейроинтеллект. – К: Юниор, 2004. - 560 с.
4. Широчин В.П., Мухин В.Е., Кулик А.В. Вопросы проектирования средств защиты информации в компьютерных системах и сетях. К: ВЕК. 2000. - 112 с.
5. Вербіцький О.В. Вступ до криптології. – Львів, НТЛ, 1998. – 248 с.
6. Щербаков А.Ю. Компьютерная безопасность: теория и практика. – М: «Молгачева», 2001. – 352 с.
7. Норткарт С., Новак Д. Обнаружение нарушений безопасности в сетях. Третье издание. – М:-К: «Вильямс», 2003. – 447 с.
8. Норткарт С., Купер М., Фирноу М., Фредерик К. Анализ типовых нарушений безопасности в сетях. – М:-К: «Вильямс», 2001. – 460 с.
9. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – С-Пб: Питер, 2001. – 544 с.
10. Манн С., Митчелл Э., Крелл М. Безопасность Linux. Руководство администратора. М: ИД Вильямс, 2003. – 624 с.
11. Брагг Р. Система безопасности Windows 2000. М: ИД Вильямс. 2001. – 592 с.
12. Коул Э. Руководство по защите от хакеров. –М:-К: «Вильямс», - 2002. – 633 с.
13. Хоффман Л.Дж. Современные методы защиты информации. М: Сов. радио. 1980. 264 с.
14. Мафтик С. Механизмы защиты в сетях ЭВМ. М: Мир, 1993.216 с.

15. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. К: Корнейчук, 2000, 152 с.
16. Бондаренко М, Скрипник Л., Горбенко И., Потий А. Перспективы применения международного стандарта ISO/IEC 15408 в Украине. Сб. Правове, нормативне та метрологічне забезпечення систем захисту информації в Україні, вып.3, 2001. с. 7- 26.
17. Шорошев В. Базова модель експертної системи оцінки безпеки інформації в комп’ютерних системах. Сб. Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, вып.3, 2001. с. 86-90.
18. Луцький Г.М., Широчин В.П., Пустоваров В.І., Жабин В.І. та інші. "Концепція та концептуальні підходи, нормативно-правова база захисту інформації в комп'ютерних системах" (Звіт з НДР) Депонір. в УкрІНТЕІ, No держреєстрації 0194UO38973, 1994., 7.5 п.л.
19. Національний стандарт ТЗІ України НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в компютерних системах від несанкціонованного доступу. Чинний з 01.07.1999 р.
20. Національний стандарт ТЗІ України НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищенності оброблювальної інформації від несанкціоновіанного доступу. Чинний з 01.07.1999 р.
21. Weissman C. Security Controls in the ADEPT-50 Time Sharing System. // Proceedings AFIPS, FJCC. – 1969. – v. 35. – pp. 119-133.
22. Hartson R., Hsiao D. Full protection specification in the semantic model for database protection languages. // Proceedings Annual Conference ACM. – Houston, New York. – 1976. – pp. 90-95.
23. Harrison M. A.. Russo W. L. Protection in Operating Systems. // Communications of the ACM. – 1976. – v. 19, № 8. – pp. 461-471.

24. Spier M. J. A Model Implementation for protective domains. // International Journal on Computer Information Science. – 1973. – v. 2, № 3. – pp. 201-229.
25. Bell D. E., LaPadula L. J. Secure computer systems: mathematical foundations and model. // M74-244, The MITRE Corp., Bedford, Mass.- May 1973.
26. Bell D. E. Secure computer systems: a refinement of the mathematical model. // Springfield, The MITRE Corp. – 1974. – Report № 2574, pp. 75
27. Graham R. M., Denning P. J. Protection – Principles and Practice. // Proceedings AFIPS. – 1972. – v.40, pp. 417-429.
28. Denning D. E. A Lattice Model of Secure Information Flow. // Communications of the ACM. –1976. – v. 19, № 5. – pp. 236-243
29. Landwehr C., Heitmeyer C., McLean J. A security model for military message systems. // ACM Trans. on Computer Systems. – 1984. – V. 2, № 3. – pp. 198-222.