МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Луцький національний технічний університет

АПАРАТНІ ТА ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання

Луцьк 2025

УДК 004.056(075.8)+681.518(075.8)
А76

Рекомендовано до видання вченою радою факультету комп'ютерних та інформаційних технологій ЛНТУ, протокол № ___ від _____ 2025 року.

Голова Вченої ради факультету КІТ _____ І. С. Кондіус

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Н. П. Поліщук

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № 7 від 03 січня 2025 року.

Укладачі: _____ О. Л. Кайдик, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Т. В. Терлецький, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ С. В. Гринюк, кандидат технічних наук, доцент кафедри кафедри комп'ютерної інженерії та безпеки ЛНТУ

Відповідальний за випуск: _____ Т. В. Терлецький, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

А76 **Апаратні та програмні засоби захисту інформації**: методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 60 с.

У пропонованому виданні містяться матеріали до практичних занять з курсу «Апаратні та програмні засоби захисту інформації».

Методичні вказівки покликані сприяти більш якісній підготовці здобувачів освіти, оскільки містять необхідний теоретичний матеріал до виконання семи практичних робіт, що дозволяє більш повно засвоїти знання під час одержання ними практичних навиків у сфері захисту інформації та безпеки інформаційно-комунікаційних систем.

ВСТУП

Стрімкий розвиток інформаційних технологій дозволяє відкривати нові можливості у будь-яких сферах науки і техніки, але ставить, при цьому, численні виклики у сфері інформаційної безпеки. В умовах глобалізації та цифровізації, де дані стали одним із найцінніших активів, захист інформації набуває особливої актуальності.

Широке впровадження інформаційних технологій володіє певним потенціалом, який дозволяє покращити якість життя громадян та підвищити ефективність роботи держустанов та підприємств. В умовах постійного зростання кіберзагроз й складності інформаційних систем, захист інформації стає не лише технічною, але й стратегічною задачею.

Власник інформації має бути впевненим у тому, що його дані знаходяться під надійним захистом, а, отже, готовий інвестувати у сучасні рішення для забезпечення безпеки.

Важливість комплексного підходу до захисту інформації – це питання не лише бізнесу, але й національної безпеки. Для успішної реалізації цих ініціатив необхідно забезпечити надійний захист інформації, що включає у себе як технічні рішення, так і правові норми.

Практичні роботи з курсу «Апаратні та програмні засоби захисту інформації» є важливою складовою навчального процесу, оскільки дозволяють здобувачам освіти закріпити теоретичні знання та отримати практичний досвід у сфері інформаційної безпеки та технічного захисту інформації.

ЗМІСТ

Сторінка

ПРАКТИЧНА РОБОТА №1

Тема: вивчення міжнародного стандарту ISO/IEC 15408 з оцінювання безпеки інформаційних технологій.

Мета: ознайомитись з європейськими підходами до оцінювання безпеки інформаційних технологій.

Завдання: опрацювати теоретичний матеріал, описати методику оцінювання безпеки інформаційних технологій та дати відповіді на запитання.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Завдання стандарту ISO/IEC 15408. Основними завданнями із розроблення цього стандарту були:

– уніфікація національних стандартів у сфері оцінювання безпеки ІТ;

– підвищення рівня довіри до оцінювання безпеки ІТ;

– скорочення витрат на оцінювання рівня безпеки ІТ на основі взаємного визнання сертифікатів.

Зміст «Загальних критеріїв» та область їх застосування, структура стандарту ISO/IEC 15408. Документ ISO/IEC 15408 формується із наступних розділів: вступ і загальна модель, функціональні вимоги безпеки та вимоги до забезпечення безпеки. У цьому документі зроблено акцент на основних аспектах безпеки – забезпечення конфіденційності, цілісності та доступності інформації або, інакше кажучи, захист від несанкціонованого доступу, модифікації чи втрати доступу до інформації під час реалізації загроз.

Під керівництвом ISO було розроблено й нормативно-методичну документацію, як додаток до стандарту, що містить: вказівки щодо розроблення профілів захисту та визначення завдань захисту; процедури реєстрації профілів захисту; загальну методологію оцінювання безпеки ІТ.

ISO/IEC 15408, призначений для оцінювання безпеки продуктів ІТ. «Загальні критерії» можуть стати у пригоді: розробникам об’єктів оцінювання; експертам з оцінювання об’єктів; користувачам об’єкта оцінювання.

Об’єктом оцінювання прийнято називати продукт або систему ІТ, яка має ресурси, що можна використовувати для оброблення та зберігання інформації. Об’єктами оцінювання можуть бути операційні системи, інформаційні системи, обчислювальні мережі, прикладні програми тощо.

Недоліки стандарту ISO/IEC 15408. У «Загальних критеріях» не приділено достатньо уваги адміністративним заходам і технічним засобам безпеки, стандарт не містить критеріїв оцінювання криптографічних методів захисту інформації та рекомендацій щодо самих методик оцінювання. Певною

мірою це було враховано лише в нормативно-методичній документації, виданій на підтримку стандарту.

Базові поняття. Згідно з концепцією «Загальних критеріїв» вимоги до безпеки об'єкта оцінювання поділяють на дві категорії:

– функціональні вимоги, тобто вимоги до тих функцій об'єкта оцінювання, що відповідають за безпеку ІТ-продукту;

– вимоги адекватності (або гарантованості) описують такі властивості об'єкта оцінювання, які гарантують ефективність і коректність реалізації необхідних засобів його безпеки.

У стандарті використано єдину термінологію для визначення функціональних вимог і вимог гарантованості:

– клас: найбільш загальна група вимог безпеки;

– сімейство: член класу, який визначає групу вимог, що забезпечують виконання певної частини цілей безпеки;

– компонент: член сімейства, який визначає мінімальний набір вимог безпеки для включення до структур, визначених у «Загальних критеріях»;

– елемент: неподільна складова компонента.

Така ієрархія дає змогу під час ідентифікації загроз безпеці виділити з їх загальних характеристик окремі компоненти і елементи.

У «Загальних критеріях» визначено також сукупність структур, які поєднують компоненти вимог безпеки. До таких структур належать:

– пакет (Package): проміжна комбінація компонентів, яка містить набір вимог, що відповідають визначеному піднабору цілей безпеки (пакет призначений для багаторазового використання);

– рівень гарантованості оцінювання (Evaluation Assurance Level): визначений пакет вимог гарантованості;

– профіль захисту (Protection Profile): набір вимог, що складається з компонентів або пакетів функціональних вимог і одного з рівнів гарантованості (профіль захисту специфікує сукупність вимог, необхідних і достатніх для досягнення заданих цілей безпеки);

– завдання з безпеки (Security Target): набір вимог, визначених одним із профілів захисту або сформульованих явно.

Розроблення ІТ-продукту та його кваліфікаційний аналіз. Стандарт ISO/IES 15408 використовують на різних етапах життєвого циклу ІТ-продукту, насамперед під час його розроблення та кваліфікаційного аналізу. На рисунку 1.1 подано застосування «Загальних критеріїв» на різних етапах життєвого циклу ІТ-продукту.

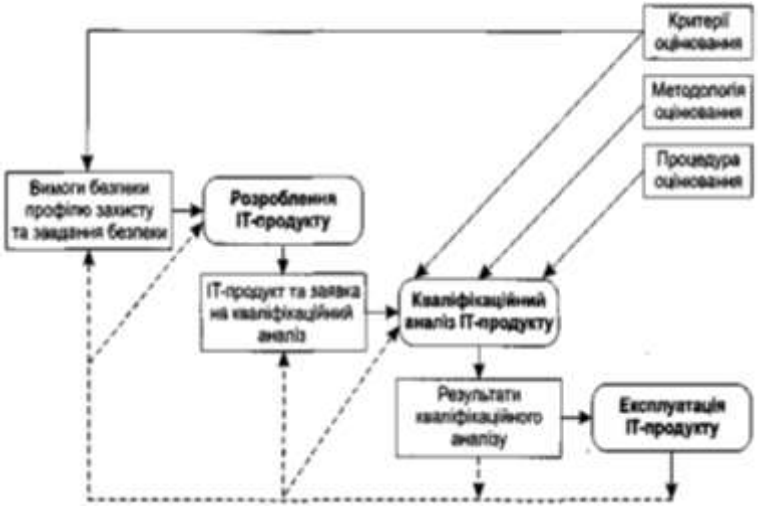

Рисунок 1.1 – Використання «Загальних критеріїв» на етапах існування ІТ-продукту

Піддаючи ІТ-продукт кваліфікаційному аналізу, окрім «Загальних критеріїв» слід використовувати документ «Загальна методологія», де подано перелік дій, які необхідно виконати під час оцінювання.

Основні принципи, на яких ґрунтується «Загальна методологія»: результати оцінювання є об'єктивними і не залежними від суб'єктивного бачення експерта, дії експерта, який використовує одну й ту саму методику оцінювання, приводять до несуперечливих результатів, дії експерта забезпечують точне технічне оцінювання.

Процес оцінювання об'єкта здійснюється у три етапи: отримання вихідних даних для оцінювання, проведення оцінювання, оформлення результатів оцінювання.

Це етапи узагальненої моделі процесу оцінювання, де передбачено взаємодію таких учасників:

– заявник: ініціатор та замовник оцінювання (він є відповідальним за надання експерту-оцінювачу необхідних відомостей);

– розробник: демонструє об'єкт оцінювання і відповідає за надання відомостей;

– експерт-оцінювач: приймає відомості від розробника або безпосередньо від заявника, здійснює оцінювання об'єкта та надає його результати відповідному органу;

– орган оцінювання: організовує, підтримує і контролює процес оцінювання (на основі отриманих від експертів-оцінювачів результатів оцінювання надає сертифікати і випускає звіти про сертифікацію).

Оцінювання може бути здійсненим із використанням різних методів і прийомів; це залежить від заявлених вимог довіри та предмета оцінювання.

Формування критеріїв оцінювання об'єкта виконується шляхом висування якісних вимог до функціональних механізмів гарантування безпеки та визначення кількісних показників для проведення оцінювання.

Серед матеріалів, які використовують для проведення кваліфікаційного аналізу, можна виділити:

– завдання з безпеки, де описано функції захисту ІТ-продукту та вимоги безпеки, що відповідають вимогам профілю захисту, на реалізацію якого претендує продукт;

– відомості про можливості ІТ-продукту, подані його розробником;

– додаткові відомості, отримані після проведення різних експертиз.

Етапи здійснення кваліфікаційного аналізу. Кваліфікаційний аналіз ІТ-продукту здійснюють у кілька етапів:

– аналіз профілю захисту на його повноту, несуперечність, можливість реалізації та використання як набору вимог до продукту, що аналізують;

– аналіз завдання з безпеки на його відповідність вимогам профілю захисту, а також на повноту, несуперечність, можливість реалізації та використання як опису ІТ-продукту;

– аналіз ІТ-продукту на його відповідність завданню з безпеки.

Профіль захисту. Профіль захисту у стандарті ISO/IEC 15408 є одним із найважливіших інструментів, який приймає участь в управлінні ризиками безпеки й забезпечення відповідності ІТ-продуктів та систем сучасним стандартам цієї сфери діяльності. Основними його розділами є: вступ; опис об'єкта оцінювання; середовище експлуатації; задачі захисту; вимоги безпеки; додаткові відомості; обґрунтування.

1. Вступ – у вступі подано інформацію, яка є необхідною для пошуку профілю в бібліотеці профілів (ідентифікатор) і огляд змісту.

2. Опис об'єкта оцінювання – тут, зазвичай, зазначають стислу характеристику об'єкта оцінювання, його функціональне призначення, принцип роботи, методи використання тощо (дана інформація не підлягає аналізу і сертифікації).

3. Середовище експлуатації – у цьому розділі подають опис усіх аспектів функціонування об'єкта оцінювання, які пов'язані із безпекою:

– загрози безпеці – опис загроз безпеці, яким має протистояти захист (для кожної загрози вказуються джерело, метод впливу, об’єкт;

– політика безпеки – тут подають визначення та пояснення правил політики безпеки;

– умови експлуатації – тут надають вичерпну характеристику середовища експлуатації в контексті безпеки.

4. Задачі захисту – у даному розділі йдеться про потреби користувачів протидіяти зазначеним загрозам безпеці та (або) реалізовувати політику безпеки. До задач захисту зазвичай відносять: задачі захисту, які вирішує сам ІТ-продукт або інші задачі захисту.

5. Вимоги безпеки – у цьому розділі йдеться про вимоги безпеки, які має задовольняти ІТ-продукт для вирішення задач захисту. До них належать:

– функціональні вимоги – лише типові вимоги, які передбачено у відповідних розділах «Загальних критеріїв», які можуть зобов’язувати або забороняти використовувати конкретні методи та засоби;

– вимоги адекватності (лише типові вимоги);

– вимоги, які висуваються до середовища експлуатації.

6. Додаткові відомості – цей розділ не є обов’язковим, оскільки у ньому, зазвичай, викладають вказівки щодо застосування профілю захисту.

7. Обґрунтування – у цьому розділі наведено доводи того, що профіль захисту містить повну і зв’язну множину вимог, а ІТ-продукт, який їх задовольняє, здатний ефективно протистояти загрозам безпеці середовища експлуатації.

Завдання з безпеки. Завдання з безпеки – це ключовий елемент у визначенні специфічних вимог, які висуваються до безпеки інформаційних систем і продуктів. Ці завдання формують основу для оцінки безпеки та сертифікації ІТ-продуктів. Нижче наведено інформацію про структуру завдання з безпеки та зміст основних її розділів.

1. Вступ – цей розділ спрямовано на призначення завдання з безпеки, а також подання інформації, яка є необхідною для ідентифікації завдання:

– ідентифікатор – унікальне ім’я, яке використовують для пошуку й ідентифікації завдання з безпеки і відповідного йому ІТ-продукту;

– огляд змісту – докладна анотація завдання з безпеки, ознайомившись із якою користувач зможе дізнатися, чи здатний ІТ-продукт вирішити його задачі;

– заявка на відповідність «Загальним критеріям» – це опис усіх властивостей ІТ-продукту, що підлягають кваліфікаційному аналізу на основі «Загальних критеріїв».

2. Опис ІТ-продукту – стислий опис продукту.

3. Середовище експлуатації – являє собою вміст усіх підрозділів цього розділу відповідає вмісту аналогічних підрозділів зі структури профілю захисту: загрози безпеці; політика безпеки; умови експлуатації.

4. Задачі захисту – цей розділ збігається із однойменним розділом профілю захисту: задачі захисту, що вирішує ІТ-продукт; інші задачі захисту.

5. Вимоги безпеки – наведено вимоги безпеки, якими керується розробник ІТ-продукту, що дає йому змогу заявляти про успішне вирішення задач захисту.

6. Загальні специфікації ІТ-продукту – тут відображається реалізації ІТ-продуктом вимог безпеки за допомогою визначення високорівневих специфікацій функцій захисту. Серед цих специфікацій виокремлюють наступні:

– специфікації функцій захисту: опис функціональних можливостей засобів захисту ІТ-продукту, заявлених розробником як такі, що реалізують вимоги безпеки (форма подання специфікацій сприяє визначенню відповідності між функціями захисту і вимогами безпеки);

– специфікації рівня адекватності: визначається заявлений рівень адекватності захисту ІТ-продукту та його відповідність вимогам адекватності через подання параметрів технології проектування і створення ІТ-продукту.

7. Заявка на відповідність профілю захисту – цей розділ є необов'язковим (завдання з безпеки претендує на задоволення вимог одного чи кількох профілів захисту, для кожного з яких розділ буде містити таку інформацію).

8. Обґрунтування – у цьому розділі доводиться, що завдання з безпеки містить повну і зв'язну множину вимог, що ІТ-продукт, який їх реалізує, здатний ефективно протистояти загрозам безпеці середовища експлуатації і що загальні специфікації функцій захисту відповідають вимогам безпеки.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Виконати аналіз змісту стандарту ISO/IEC 15408 і описати методику оцінювання безпеки інформаційних технологій.

2. Ознайомитись з новою редакцією стандарту ISO/IEC 15408:2008 (ДСТУ ISO/IEC 15408-3:2017) на основі третьої версії «Загальних критеріїв» або з діючою версією – ISO/IEC 18045:2005 (ISO/IEC 18045:2005 Information technology – Security technigues – Methodology for security evalution) та охарактеризувати основні зміни у ньому.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Назвіть основні розділи стандарту ISO/IEC 15408 та для чого він призначений?

2. Основні завдання стандарту ISO/IEC 15408.

3. Охарактеризуйте базову термінологію стандарту ISO/IEC 15408.

4. Назвіть які загальні критеріїв стандарту ISO/IEC 15408 притаманні кожному етапу життєвого циклу IT-продукту.

5. Що включає у себе процес оцінювання об'єкта за «Загальною методологією»?

6. Назвіть категорії вимог, які висуваються до безпеки об'єкта оцінювання за стандартом ISO/IEC 15408.

7. Що являє собою профіль захисту та яка його структура?

8. Чим структура завдання з безпеки відрізняється від структури профілю захисту?

Рекомендована література: [1-12].

ПРАКТИЧНА РОБОТА №2

Тема: управління безпекою інформаційно-комунікаційних систем.

Мета: ознайомитись із основними підходами до управління безпекою роботи інформаційно-комунікаційних систем.

Завдання: опрацювати теоретичний матеріал, описати методику оцінювання безпеки інформаційних технологій та дати відповіді на запитання.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Стандарт ISO/IEC 27002 «Інформаційні технології – Методики безпеки – Практичні правила менеджменту інформаційної безпеки». Для врегулювання комплексу питань із захисту інформації в організаціях окрім цієї групи документів використовують й інші, зокрема міжнародні стандарти. Найбільш поширеними міжнародними стандартами, з цього питання є стандарт BSI «Настанова із захисту інформаційних технологій для базового рівня захищеності» та новітні стандарти серії ISO/IEC 27000 зі створення, розвитку та підтримки системи менеджменту інформаційної безпеки (СМІБ).

Розглянемо докладніше міжнародний стандарт ISO/IEC 27002. Цей стандарт вирізняється з-поміж інших високим рівнем абстрактності та лаконізмом, тому його можуть успішно застосовувати висококваліфіковані та досвідчені фахівці з інформаційної безпеки.

Структура й основний зміст стандарту. Нормативний документ ISO/IEC 27002 складається із передмови, вступу та 15 розділів (розділи нумерують від 1 до 15, а вступ позначають у вигляді 0-го розділу).

Далі наведено перелік усіх розділів і подано їх стислий зміст.

0. Вступ.
1. Сфера застосування.
2. Терміни та визначення.
3. Структура стандарту.
4. Оцінювання й оброблення ризиків.
5. Політика безпеки.
6. Організація забезпечення безпеки інформації.
7. Управляння ресурсами.
8. Безпека персоналу.
9. Фізична безпека і безпека середовища.
10. Управління комунікаціями й операціями.
11. Управління доступом.
12. Придбання, розроблення та супроводження інформаційних систем.
13. Управління інцидентами безпеки.
14. Управління безперебійністю бізнесу.
15. Дотримання вимог.

Вступ. У вступі розглянуто наступні питання: що таке безпека інформації; навіщо необхідна безпека інформації; як затвердити вимоги до безпеки; визначення ризиків безпеки; вибір засобів управління; відправна точка безпеки інформації; критичні фактори успіху; розроблення власних рекомендацій із захисту інформації організації.

Розглянемо окремі положення вступу більш детально. У перших двох підрозділах вступу наведено визначення поняття безпеки інформації, її мету, завдання, мотивацію необхідності захисту. Підпункт «Як затвердити вимоги до безпеки» визначає три головних джерела вимог до системи безпеки організації:

– специфічні ризики порушення безпеки, які загрожують ресурсам організації і для яких оцінюють уразливість та ймовірність її виникнення, а також потенційний вплив;

– набір правових і договірних вимог, які мають виконувати організація, її торговельні партнери, підрядники та постачальники послуг;

– набір специфічних принципів, цілей та вимог до оброблення інформації, розроблений організацією.

У підпункті «Визначення ризиків безпеки» відзначають важливість відповідності між цінністю інформаційних ресурсів організації та витратами на систему їх захисту. При цьому слід ураховувати рівень ризику та збитки, яких може бути завдано організації внаслідок порушення безпеки інформації. Ризики визначають періодично, враховуючи будь-які зміни, які впливають на безпеку.

Після визначення вимог до безпеки та ризиків необхідно обрати й упровадити прийнятні засоби управління для зниження ризиків. Питання добирання таких засобів обговорено у підрозділі «Вибір засобів управління».

У підпункті «Відправна точка безпеки інформації» зазначено, що використання багатьох із засобів управління можна вважати відправною точкою для впровадження системи безпеки інформації. Засоби управління, які є суттєвими для організації з позиції законодавства, можуть здійснювати захист: конфіденційності даних та особистої інформації, документів організації і прав інтелектуальної власності. До заходів й засобів, які вважають необхідними для створення системи безпеки інформації, належать:

– створення документа про політику безпеки інформації;
– розподіл обов'язків із забезпечення безпеки інформації;
– навчання й підготовка персоналу з питань дотримання режиму безпеки інформації;
– технічне управління вразливостями;
– підтримка безперебійної роботи;
– управління інцидентами безпеки інформації.

У підпункті «Критичні фактори успіху» визначено фактори, критичні для успішного впровадження безпеки інформації в організації:

– політика, цілі й діяльність із захисту інформації, що відображають цілі бізнесу;
– підхід і структурна основа для впровадження, супроводження і вдосконалення захисту інформації;
– суттєва підтримка і зобов'язання всіх рівнів керівництва;
– розуміння вимог безпеки інформації, визначення ризиків і управління ними;
– надання рекомендацій з політики й стандартів безпеки інформації всім керівникам, співробітникам та іншим сторонам;
– фінансування заходів з управління безпекою інформації;
– забезпечення належних знань, навчання й освіти персоналу;
– управління інцидентами інформаційної безпеки;
– упровадження системи показників, призначеної для оцінювання ефективності управління безпекою інформації.

У підпункті «Розроблення власних рекомендацій із захисту інформації організації» визначено, що кожна організація може мати власний набір вимог, проблем, пріоритетів і керівних принципів безпеки інформації. Якщо організація має документи із власними рекомендаціями щодо захисту інформації, то вони

мають містити посилання на цей стандарт задля встановлення взаємозв'язків між відповідними розділами.

Сфера застосування. Уданому розділі подано інформацію щодо призначення стандарту. Стандарт містить рекомендації та загальні принципи з ініціювання, впровадження, супроводження й удосконалення управління безпекою інформації в організації. Стандарт можна використовувати як практичну рекомендацію з розроблення власних стандартів організацій та ефективної практики управління безпекою інформації, а також для сприяння встановленню довірчих відносин під час взаємодії між організаціями.

Терміни та визначення. Розділ містить інформацію про основні терміни та визначення безпеки інформації. Зокрема, термін «безпека інформації» тут визначено як збереження властивостей інформації, на кшталт конфіденційності, цілісності та доступності.

Структура стандарту. У розділі описано структуру стандарту, а вимоги викладено в його розділах. У них сформульовано 39 цілей управління, досягнення яких забезпечує захист інформаційних ресурсів від загроз їх конфіденційності, цілісності та доступності. Опис цілей керування фактично містить специфікації функціональних вимог до архітектури управління безпекою інформації організації. Для кожної із цілей керування названо засоби керування, що можуть бути застосовані для досягнення загальної мети керування.

Оцінювання й оброблення ризиків. У розділі показано відповідність між цінністю інформаційних ресурсів організації та витратами на систему захисту інформації. Для визначення витрат на систему захисту мають бути враховані рівень ризику та збитки, яких може бути завдано організації. Ризики мають зумовлювати належні пріоритети і дії керівництва щодо управління безпекою інформації та впровадження засобів, обраних для захисту від цих ризиків. Під час визначення ризиків слід застосовувати системний підхід до обчислення величини ризиків і порівняння обчислених ризиків із критеріями їх значущості. Для кожного з ризиків слід прийняти рішення щодо його оброблення (усунення чи зниження). Можливі варіанти оброблення ризиків:

– застосування прийнятних засобів управління для зниження ризиків;

– свідоме прийняття ризиків за умови забезпечення їх відповідності політиці організації й критеріям прийняття ризиків;

– усунення ризиків шляхом заборони дій, що можуть викликати ці ризики;

– перекладання ризиків на інші сторони, наприклад на страховиків або постачальників.

Для оброблення ризиків необхідно обрати й впровадити засоби управління

з урахуванням: вимог та обмежень національного й міжнародного законодавства, цілей організації, робочих вимог і обмежень, вартості впровадження засобів управління ризиками.

Політика безпеки. Роз'яснення цілей і здійснення всебічної підтримки захисту інформації шляхом чіткого формулювання політики безпеки – обов'язок вищого керівництва. Наявність документа про політику безпеки інформації є однією з цілей керівництва. У розділі рекомендовано наступний зміст цього документа:

– визначення захисту інформації, його головні цілі та сфера застосування, значення захисту інформації як механізму, що дає змогу використовувати її колективно;

– викладення позиції керівництва з питань реалізації цілей і принципів захисту інформації;

– тлумачення конкретних варіантів політики безпеки, принципів, стандартів і вимог до її дотримання, зокрема: виконання правових і договірних вимог, вимоги щодо навчання персоналу правил безпеки, політика попередження і виявлення вірусів;

– політика забезпечення безперебійної роботи організації;

– визначення загальних і конкретних обов'язків із забезпечення режиму безпеки інформації;

– роз'яснення процедури сповіщення про події, які можуть впливати на безпеку інформації.

Окремий підпункт присвячено порядку ревізії політики безпеки. Ревізію необхідно проводити періодично із запланованим інтервалом, а також у випадку суттєвих змінень, що можуть впливати на політику безпеки.

Організація забезпечення безпеки інформації. У цьому розділі визначено дві цілі управління в таких підрозділах.

1. Інфраструктура безпеки інформації організації – для забезпечення захисту інформації слід створити відповідну структуру управління в організації. Необхідно проводити регулярні наради керівництва, присвячені коригуванню політики безпеки інформації, розподілу обов'язків із забезпечення захисту та координації дій, спрямованих на підтримку режиму безпеки. За потреби для консультацій слід залучити фахівців відповідного рівня. З метою обміну досвідом необхідно встановлювати контакти з фахівцями інших організацій. Слід всебічно впроваджувати комплексний підхід до розв'язання проблем безпеки інформації.

2. Питання безпеки доступу сторонніх організацій – під час взаємодії із

сторонніми організаціями, зокрема, у разі застосування їхніх продуктів або послуг, необхідно унеможливити компрометацію безпеки інформації. Для цього слід уживати узгоджених з іншими організаціями заходів із підтримки режиму безпеки. Потрібно провести аналіз ризиків і визначити вимоги до засобів управління, що знижують ці ризики. Відповідні засоби та заходи управління мають бути зафіксовані в угоді зі сторонньою організацією.

Управління ресурсами. Організація має чітко усвідомлювати, якими інформаційними ресурсами вона володіє, і керувати їхньою безпекою належним чином. У підпунктах цього розділу визначають такі цілі такого управління:

– відповідальність за ресурси: усі ресурси повинні бути враховані та мати своїх відповідальних (обладнання та інший інвентар, що можуть впливати на інформаційні ресурси (апаратне та програмне забезпечення, дані, документація, носії інформації, допоміжні пристрої і системи на кшталт кондиціонерів повітря та джерел безперебійного живлення) також необхідно належним чином супроводжувати);

– класифікація інформації: з метою визначення пріоритетів щодо захисту інформації необхідно провести її класифікацію за категоріями значущості (таку систему класифікації слід використовувати задля визначення рівнів захисту інформації та сповіщення користувачів щодо необхідності спеціального поводження з нею).

Безпека персоналу. Розділ присвячено питанням відображення завдань безпеки в посадових інструкціях, а також під час надання інформаційних ресурсів, навчання користувачів, реагування на події, що містять загрозу безпеці тощо. Головна мета заходів безпеки, відображених у посадових інструкціях, полягає у зменшенні ризиків на кшталт помилок персоналу, крадіжок, шахрайства чи незаконного використання ресурсів. Основним механізмом управління є надання персоналу певних прав доступу до ресурсів. Цей розділ складається з наступних трьох підпунктів.

1. Наймання персоналу – усі пов’язані з безпекою питання слід враховувати ще під час наймання персоналу на роботу. Вимоги щодо безпеки потрібно висвітлювати в описі вакансій, обговорювати в ході інтерв'ю, долучати до посадових інструкцій і угод, а також контролювати їх протягом усього перебування співробітника в організації. Керівництво організації має переконатися, що в посадових інструкціях враховано всі вимоги безпеки, які виконуватиме працівник, перебуваючи на своїй посаді. Осіб, яких наймають на роботу, передусім тих, хто працюватиме з конфіденційною інформацією, потрібно належним чином перевіряти. Увесь персонал організації та користувачі

інформаційних ресурсів зі сторонніх організацій мають підписати зобов'язання про нерозголошення конфіденційної інформації.

2. Виконання посадових обов'язків (навчання персоналу) – одне з важливих питань управління безпекою інформації в організації. Метою навчання є надання користувачам інформаційних ресурсів відомостей про загрози порушення режиму безпеки інформації, а також необхідних навичок із забезпечення режиму нормального функціонування системи безпеки цієї організації. Усі співробітники та підрядники мають бути ознайомлені з процедурою оповіщення про інциденти різного типу (порушення безпеки, загрози тощо), які можуть вплинути на безпеку ресурсів організації. В організації має бути впроваджена процедура поширення дисциплінарних стягнень на співробітників, які порушують режим безпеки.

3. Звільнення з посади чи її змінення – особливу увагу слід приділяти питанням безпеки під час звільнення співробітників або їх переведення на інші посади. Слід контролювати повернення співробітником ресурсів, які йому було надано, а також скасування прав доступу.

Фізична безпека і безпека середовища. У розділі розглянуто заходи зі створення та адміністрування зон безпеки і контрольованих периметрів, а також заходи щодо здійснення контролю за доступом до приміщень. Велику увагу приділено заходам із захисту обладнання організації. Тут ідеться про те, що вимоги до фізичного захисту можна змінювати залежно від масштабів і структури інформаційних сервісів, а також з урахуванням уразливості та критичності виробничих процесів, які підтримуються. Визначено також цілі управління, які наведено нижче.

1. Зони безпеки. Мета заходів зі створення та адміністрування зон безпеки – запобігти несанкціонованому доступу до інформаційних ресурсів, їх пошкодженню і створенню перешкод у їх роботі. Для цього організують концентричні зони із засобами фізичного контролю доступу між ними. Інформаційні системи, які підтримують критично важливі чи вразливі сервіси, мають бути розташовані в зонах із належним контролем доступу. Для зменшення ризику несанкціонованого доступу чи ушкодження паперової , документації та носіїв інформації пропонується встановлювати чіткі правила використання робочого місця.

2. Безпека обладнання. Мета заходів з організації захисту обладнання – запобігати втраті, ушкодженню, компрометації ресурсів і збоям у роботі організації. Слід забезпечити захист критичного обладнання інформаційних систем від навмисного чи випадкового фізичного пошкодження, пожежі,

затоплення, крадіжки, перегрівання, раптових вимкнень електричного живлення тощо. Розглянуто питання захисту допоміжного обладнання (системи електричного живлення чи структурованої кабельної системи) та необхідності безпечної утилізації обладнання і носіїв інформації.

Управління комунікаціями й операціями. Розділ присвячено організаційним заходам адміністрування комп'ютерних систем і мереж задля забезпечення їх коректної та надійної роботи. Вимоги до безпечного адміністрування комп'ютерних систем і мереж можна змінювати залежно від масштабу та структури інформаційних сервісів, а також від ступеня вразливості та критичності виробничих процесів, які ця система підтримує. У підпунктах цього розділу визначено десять цілей управління.

1. Робочі процедури та відповідальність. Для безпечного адміністрування комп'ютерних систем і мереж необхідно визначити обов'язки персоналу та відповідні процедури. Ці заходи слід підтвердити відповідними робочими інструкціями та операційними процедурами реагування на події для зменшення ризику недбалого чи несанкціонованого використання систем. За потреби слід застосовувати принцип розмежування обов'язків, наприклад відокремити доступ до засобів розроблення та робочих програм.

2. Управління послугами сторонніх підрядників. Залучення стороннього підрядника може призвести до порушення режиму безпеки. Необхідно заздалегідь виявити такий ризик і долучити до контракту належні захисні заходи, узгоджені з підрядником.

3. Планування й приймання систем. Планування систем і їх приймання дають змогу звести ризики відмов систем до мінімуму. Для забезпечення досяжності ресурсів систем та їх належного навантаження ці ресурси необхідно попередньо спланувати і підготувати. З цією метою слід спрогнозувати потенційні вимоги до параметрів обладнання, задати критерії приймання нових систем і провести відповідні випробування. Слід також спланувати заходи щодо ймовірного переходу на аварійний режим роботи та постійно контролювати процес внесення змін у робочі системи.

4. Захист від шкідливого та мобільного коду. Дієвим заходом із забезпечення цілісності даних і програм є захист від шкідливого програмного забезпечення. Для попередження і виявлення випадків проникнення шкідливого програмного забезпечення потрібно впроваджувати належні застережливі заходи. Окремо розглянуто заходи захисту для мобільного коду, що підтримується зв'язувальним програмовим забезпеченням.

5. Резервне копіювання. Заходи із обслуговування систем дають змогу

підтримувати цілісність і доступність сервісів. Необхідно визначити щоденні процедури резервного копіювання даних, реєстрації подій і збоїв, а також процедури спостереження за середовищем функціонування обладнання.

6. Управління безпекою мережі. Заходи з адміністрування мережі забезпечують захист інформації, яка циркулює в мережі, а також в інфраструктурі її підтримки. Управління безпекою комп'ютерних мереж, окремі сегменти яких розміщено поза межами організації, потребує особливої уваги. Необхідно вжити спеціальних заходів захисту до конфіденційних даних, які передаються через мережі загального доступу. Тут розглянуто такі сервіси безпеки, як приватні мережі та міжмережне екранування.

7. Захист носіїв даних. Слід визначити порядок безпечної роботи з комп'ютерними носіями даних, паперовими документами, системною документацію для забезпечення фізичного захисту під час їх використання, перевезення, зберігання. Потрібно ретельно контролювати процедури знищення носіїв даних.

8. Інформаційний обмін. З метою запобігання втратам, модифікаціям і несанкціонованому використанню інформації обмін даними і програмами між організаціями необхідно контролювати, наприклад, впровадженням політик і процедур, а також укладанням відповідних угод. Особливу увагу слід приділити захисту електронного обміну повідомленнями, електронної пошти, документообігу.

9. Сервіси електронної комерції. Застосування систем електронної комерції потребує ретельної уваги до питань безпеки. Слід також захищати цілісність і доступність інформації, яку публікують у комп'ютерній мережі.

10. Моніторинг. Слід впроваджувати реєстрацію пов'язаних із безпекою подій і здійснювати їх аудит, вести протокол збоїв, забезпечити сповіщення вповноважених адміністраторів про події задля виявлення неавторизованого доступу. Необхідними допоміжними заходами є убезпечення журналів реєстрації та синхронізація системних годинників.

Управління доступом. Даний розділ присвячено розгляду питань із здійснення контролю за логічним доступом до комп'ютерних систем і даних, що дає змогу запобігати несанкціонованому доступу. У розділі сформульовано сім цілей управління.

1. Вимоги бізнесу щодо контролю доступу. Вимоги організації щодо управління доступом користувачів до інформаційних ресурсів повинні бути прозоро задокументовані у політиці управління доступом, що має враховувати правила поширення інформації та розмежування доступу. Можна застосовувати

профілі доступу, що відповідають посадам співробітників.

2. Управління доступом користувачів. Надання прав доступу користувачам слід здійснювати з дотриманням певних формальних процедур реєстрації й адміністрування користувачів – від початкової реєстрації нових користувачів до видалення облікових записів користувачів, з обов'язковою періодичною ревізією прав і повноважень користувачів. Особливу увагу слід приділяти процедурі надання привілейованих прав доступу користувачам, які надають їм можливість обійти засоби системного контролю.

3. Відповідальність користувачів. Користувачі мають добре знати свої обов'язки із забезпечення ефективного контролю доступу, насамперед щодо використання паролів та захисту обладнання від доступу сторонніх осіб.

4. Управління доступом до мережі. Управління доступом до мережі забезпечує захист систем, об'єднаних у таку мережу. Контроль слід забезпечувати як усередині корпоративної мережі, так і під час обміну між організаціями. До числа засобів контролю необхідно долучити механізми автентифікації віддалених користувачів та обладнання. Інформаційні мережні сервіси, користувачі та системи мають бути розподілені на логічні мережні домени з урахуванням встановленої в організації політики доступу.

5. Управління доступом до операційних систем. Одним з важливих заходів управління безпекою інформації є управління доступом до комп'ютерів, здійснюваним на рівні операційних систем. Доступ слід надавати лише зареєстрованим користувачам. У випадку багатокористувацьких систем слід ідентифікувати та перевіряти справжність (автентичність) користувачів наданням їм унікальних ідентифікаторів і паролів доступу. Необхідно фіксувати випадки успішного та невдалого доступу до систем і використання привілеїв, підтримувати систему управління паролями, яка забезпечує добирання надійних паролів, за потреби обмежувати час підключення користувачів.

6. Управління доступом до прикладних програм та інформації. Управління доступом до прикладних програм дає змогу запобігати несанкціонованому доступу до прикладних систем і даних. Доступ до них слід надавати лише зареєстрованим користувачам згідно з визначеною політикою управління доступом. Особливо чутливі прикладні сервіси потребують виділених (ізольованих) платформ та додаткових засобів контролю.

7. Використання мобільних обчислень і віддалених робітників. Мають існувати формальні політики, які б врегульовували безпечне використання портативних ПК, комунікаторів, мобільних телефонів, а також безпечний режим взаємодії з віддаленими робітниками.

Придбання, розроблення та супроводження інформаційних систем. Цей розділ присвячено питанням урахування вимог безпеки в рамках загального плану робіт із створення інформаційної системи. Для цього вимоги до безпеки систем необхідно визначати та узгоджувати під час розроблення специфікацій, розроблення, придбання, тестування, введення в дію й супроводження інформаційно-комунікаційних систем. Цей розділ містить шість підрозділів.

1. Вимоги безпеки інформаційних систем. На стадії розроблення вимог до системи слід проаналізувати і повністю ідентифікувати вимоги безпеки. Придбане програмне забезпечення має пройти тестування безпеки.

2. Коректність прикладних систем. Під час проектування прикладних систем слід вбудувати в них засоби управління безпекою, зокрема засоби реєстрації подій в контрольному журналі. Необхідно контролювати захищеність файлів прикладних систем. Користувачі прикладної системи та їх розробники зобов'язані підтримувати цілісність цих програм.

3. Криптографічний захист. Слід визначити політику застосування засобів криптографічного захисту, яка може містити ролі та відповідальність, цифровий підпис, неможливість відмови, управління ключами та цифровими сертифікатами тощо.

4. Безпека системних файлів. Слід контролювати доступ до системних файлів: виконуваних програм, вихідного коду, тестових даних.

5. Безпека процесів розроблення і супроводження. Середовище розробки і робоче середовище слід жорстко контролювати. Необхідно здійснювати аналіз усіх змін, які планується внести у системи, задля гарантування того, що ними не буде порушено безпеку середовища розробки та робочого середовища. За потреби слід проводити перевірку ймовірних витоків інформації через приховані канали чи внаслідок дії «троянського коня». Додаткові заходи управління і моніторингу пропонують задіяти у разі залученні до розроблення зовнішніх виконавців.

6. Управління вразливостями. Управління вразливостями систем і прикладних програм здійснюється шляхом моніторингу оприлюдненої інформації про виявлені вразливості, оцінювання пов'язаних із ними ризиків і усунення вразливостей шляхом оновлень і виправлень програм.

Управління інцидентами безпеки інформації. Даний розділ присвячено питанням виявлення подій, що впливають на безпеку інформації, та слабких місць у системі безпеки задля гарантування можливості вживати своєчасних заходів протидії. Цей розділ містить два підпункти.

1. Повідомлення про інциденти безпеки інформації та слабкі місця.

Впровадження формального порядку сповіщень про різні типи подій і виявлених слабких місць, що можуть впливати на безпеку ресурсів організації. Усі співробітники та контрагенти мають бути поінформовані про такий порядок і зобов'язані невідкладно повідомляти про будь-які події та слабкі місця.

2. Управління інцидентами безпеки інформації та удосконаленнями. Впровадження порядку ефективного невідкладного оброблення подій і слабких місць. Забезпечення відповідності юридичним вимогам потребує наявності певної доказової бази.

Управління безперебійністю бізнесу. Розділ присвячено питанням планування безперебійної роботи організації. З метою вбереження критично важливих виробничих процесів від наслідків великих аварій і катастроф необхідно розробляти плани забезпечення можливості безперебійної роботи організації на ці випадки. Процес планування безперебійної роботи організації має містити заходи з ідентифікації та зменшення ризиків, ліквідації наслідків від реалізації загроз і швидкого поновлення виробничих процесів і сервісів.

Дотримання вимог. У розділі наведено рекомендації щодо дотримання юридичних вимог, а також вимог політик і стандартів безпеки. Він складається із трьох підрозділів.

1. Дотримання юридичних вимог. Необхідно забезпечити дотримання юридичних вимог з метою виключення порушень будь-яких законів, статутних, нормативних або договірних зобов'язань і будь-яких вимог безпеки, зокрема вимог із захисту фінансової інформації, обмежень у використанні криптографічного захисту, правил збирання доказів під час розслідування інцидентів тощо.

2. Дотримання вимог політик і стандартів безпеки. Стан безпеки інформаційних систем необхідно регулярно перевіряти. Ці перевірки слід проводити виходячи з відповідної політики безпеки, а технічні платформи й інформаційні системи необхідно перевіряти на відповідність прийнятим стандартам забезпечення безпеки. Необхідно мінімізувати втручання в процес тестування систем на рівень інформаційної безпеки. Для цього необхідно мати засоби контролю та захисту засобів тестування і робочих систем під час їх роботи.

3. Застосування аудита інформаційних систем. Слід упровадити засоби управління із захисту діючих систем та інструментів аудита під час проведення аудита інформаційних систем. Також необхідно здійснювати захист цілісності з метою запобігання неправомірному використанню інструментів аудита.

Інші стандарти серії ISO 27000 містять правила, рекомендації та

специфікації у сфері безпеки інформації для створення, розвитку й підтримки системи менеджменту інформаційної безпеки (СМІБ), яку ще називають системою управління інформаційною безпекою (СУІБ) (Information Security Management System, ISMS).

СМІБ є складовою загальної системи менеджменту, що базується на підході бізнес-ризиків під час створення, впровадження, функціонування, моніторингу, аналізу, підтримки й удосконалення інформаційної безпеки.

Окрім розглянутого вище ISO/IEC 27002 у цій серії оприлюднено ще такі стандарти:

– ISO/IEC 27001:2005 «Інформаційні технології – Методики безпеки – Системи менеджменту інформаційної безпеки – Вимоги»: стандарт, за яким може бути сертифікована організація;

– ISO/IEC 27005:2008 «Інформаційні технології – Методики безпеки – Управління ризиками інформаційної безпеки»: стандарт, що надає рекомендації з управління безпекою інформації на основі підходу управління ризиками;

– ISO/IEC 27006:2007 «Інформаційні технології – Методики безпеки – Вимоги до організацій, що проводять аудит і сертифікацію систем менеджменту інформаційної безпеки»: настанова з акредитації сертифікаційних організацій.

На даний час активно розробляють також такі стандарти:

– ISO/IEC 27000 – глосарій для стандартів СМІБ;

– ISO/IEC 27003 – новий довідник із створення СМІБ;

– ISO/IEC 27004 – новий стандарт для вимірювань у галузі інформаційної безпеки;

– ISO/IEC 27007 – стандарт з аудита СМІБ;

– ISO/IEC 27011 – настанова з телекомунікацій у СМІБ;

– ISO/IEC 27033 – стандарт із безпеки комп’ютерних мереж.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Виконати аналіз змісту нормативного документу ISO/IEC 27002 та описати методику оцінювання безпеки інформаційних технологій.

2. Ознайомитись з новою версією стандарту ДСТУ ISO/IEC 27002:2023 на основі правок (Cor 1:2014; Cor 2:2015) версії ДСТУ ISO/IEC 27002:2015 [ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls] та охарактеризувати основні зміни у ньому.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. В чому полягають необхідні заходи і засоби для створення системи безпеки інформації за стандартом ISO/IEC 270002?

2. Сфера застосування стандарту ISO/IEC 270002.
3. Охарактеризуйте політику безпеки за стандартом ISO/IEC 270002.
4. Що пропонує стандарт ISO/IEC 27002 у сфері організаційного забезпечення безпеки інформації?
5. Фізична безпека та безпека обладнання.
6. Управління комунікаціями і операціями.
7. Управління доступом.
8. Придбання, розроблення і супровід інформаційних систем.
9. Управління інцидентами безпеки інформації.

Рекомендована література: [1-12].

ПРАКТИЧНА РОБОТА №3

Тема: розробка політики інформаційної безпеки за стандартом ISO/IEC 17799.

Мета: ознайомитись із основними підходами формування політики безпеки організації.

Завдання: опрацювати теоретичний матеріал, розробити політику безпеки організації та дати відповіді на запитання.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Стандарт ISO 17799. Стандарт ISO 17799 визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, відповідальність співробітників, використання оцінки ризиків тощо. В контексті інформаційної безпеки. В процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої – скорочення матеріальних втрат, пов'язаних з порушенням інформаційної безпеки. Стандарт покликаний заощадити підприємству засоби, а в деяких випадках навіть врятувати від банкрутства, і не є якоюсь зовнішньою обов'язковою вимогою, що приводить до появи додаткової статті витрат.

ISO 17799 – це модель системи менеджменту, і в цьому сенсі не є технічним стандартом. Цей підхід до інформаційної безпеки на основі цілей менеджменту, а не фіксованих технічних специфікацій є принциповим для ISO 17799 як стандарту системи управління.

У стандарті ISO 17799 приводяться рекомендації по управлінню інформаційною безпекою. Він складає загальну основу для різних організацій при розробці, реалізації і оцінці ефективності процедур управління безпекою, а також дає можливість встановити довірчі відносини між організаціями.

Даний документ можна використовувати як загальноприйнятий стандарт при встановленні ділових відносин між організаціями і при висновку контрактів з субпідрядниками або придбанні інформаційних систем або продуктів.

Зміст інформаційної безпеки. Мета інформаційної безпеки – забезпечити безперебійну роботу організації і звести до мінімуму збиток від подій, що таять загрозу безпеці, за допомогою їх запобігання і зведення наслідків до мінімуму.

Управління інформаційною безпекою дає можливість колективно використовувати інформацію, забезпечуючи при цьому її захист і захист обчислювальних ресурсів.

Інформаційна безпека складається з трьох основних компонентів.

1. Конфіденційність – захист конфіденційної інформації від несанкціонованого розкриття або перехоплення.
2. Цілісність – забезпечення точності і повноти інформації і комп'ютерних програм.
3. Доступність – забезпечення доступності інформації і життєвоважливих сервісів для користувачів, коли це потрібно.

Інформація існує в різних формах, її можна зберігати на комп'ютерах, передавати по обчислювальних мережах, роздруковувати або записувати на папері, а також озвучувати в розмовах. З погляду безпеки всі види інформації, включаючи паперову документацію, бази даних, плівки, мікрофільми, моделі, магнітні стрічки, дискети, розмови і інші способи, використовувані для передачі знань і ідей, вимагають належного захисту.

Необхідність захисту. Інформація та інформаційні системи і мережі, які її підтримують, є цінними виробничими ресурсами організації. Їх доступність, цілісність і конфіденційність можуть мати особливе значення для забезпечення конкурентоспроможності, руху грошової готівки, рентабельності, відповідності правовим нормам і іміджу організації. Сучасні організації можуть зіткнутися із зростаючою загрозою порушення режиму безпеки, що йде від цілого ряду джерел. Інформаційним системам і мережам можуть загрожувати такі небезпеки, як комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, а також інші джерела відмов і аварій. З'являються все нові загрози, здатні завдати збитку організації, такі, як, широко відомі комп'ютерні віруси або хакери. Передбачається, що такі загрози інформаційній безпеці з часом стануть поширенішими, небезпечнішими і витонченішими. В той же час із-за зростаючої залежності організацій від інформаційних систем і сервісів, вони можуть стати уразливішими по відношенню до загроз порушення захисту. Розповсюдження обчислювальних мереж надає нові можливості для несанкціонованого доступу

до комп'ютерних систем, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості централізованого контролю інформаційних систем фахівцями.

Захисні заходи виявляються значно дешевшими і ефективнішими, якщо вони вбудовані в інформаційні системи і сервіси на стадіях завдання вимог і проектування. Чим швидше організація прикмет міри по захисту своїх інформаційних систем, тим більше дешевими і ефективними вони будуть для неї згодом.

Структура стандарту ISO/IEC 17799. Пропоновані практичні правила розбиті на десять розділів.

1. Політика безпеки.
2. Організація захисту.
3. Класифікація ресурсів і їх контроль.
4. Безпека персоналу.
5. Фізична безпека і безпека навколишнього середовища.
6. Адміністрування комп'ютерних систем і обчислювальних мереж.
7. Управління доступом до систем.
8. Розробка і супровід інформаційних систем.
9. Планування безперебійної роботи організації.
10. Виконання вимог.

У цих розділах представлений увесь можливий набір засобів управління безпекою, заснованих на реальних заходах по захисту інформації, таких, що реалізовуються зараз в британських і міжнародних організаціях.

Застосовність засобів управління безпекою. Не всі засоби контролю застосовні до кожного інформаційного середовища; їх треба використовувати вибірково з урахуванням місцевих умов. Це ставати ясно з опису. Проте більшість засобів контролю, описаних в даному документі, широко застосовуються крупними організаціями з великим досвідом роботи, і їх використання рекомендується для всіх ситуацій, зрозуміло, з урахуванням обмежень, що накладаються технологією і навколишнім середовищем. Ці загальноприйняті засоби контролю називають базовими засобами управління безпекою, оскільки всі вони в сукупності визначають базовий промисловий стандарт на підтримку режиму безпеки.

Десять ключових засобів контролю, пропоновані цим стандартом, є особливо важливими. Ці ключові засоби є хорошою відправною точкою для управління інформаційною безпекою.

При використанні деяких із засобів контролю, наприклад, шифрування даних, можуть знадобитись поради фахівців з безпеки і оцінки ризиків, щоб визначити, чи потрібні вони і яким чином їх реалізувати. Для забезпечення вищого рівня захисту особливо цінних ресурсів або надання протидії виключно високим рівням загроз порушення режиму безпеки, в ряду випадках можуть потрібно сильніші засоби контролю, які виходять за рамки цих правил.

Ключові засоби контролю. Десять ключових засобів контролю є або обов'язкові вимоги, наприклад, вимоги чинного законодавства, або вважаються основними структурними елементами інформаційної безпеки, наприклад, навчання правилам безпеки. Ці засоби контролю застосовні до всіх організаціях і середовищам і відмічені символом ключа. Вони служать як основа для організацій, що приступають до реалізації засобів управління інформаційною безпекою.

Ключовими є наступні засоби контролю:

– документ про політику інформаційної безпеки;

– розподіл обов'язків по забезпеченню інформаційної безпеки;

– навчання і підготовка персоналу до підтримки режиму інформаційної безпеки;

– повідомлення про випадки порушення захисту;

– засоби захисту від вірусів;

– процес планування безперебійної роботи організації;

– контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;

– захист даних та документації організації;

– відповідність політиці безпеки.

Задання вимог до інформаційної безпеки організації. Існують три основні групи вимог, які висуваються до системи безпеки в будь-якій організації.

1. Унікальний набір ризиків порушення безпеки, що складається із загроз, яким піддаються інформаційні ресурси, та їх вразливостей і можлива дія цих ризиків на роботу організації. Більшість з цих ризиків описані в справжніх правилах і їм можна успішно протистояти, якщо скористатися наведеними тут рекомендаціями. Проте існують ризики, що вимагають спеціального звернення, і їх необхідно розглядати з урахуванням їх оцінки в кожній конкретній організації або для кожного конкретного компоненту системи.

2. Набір правових і договірних вимог, яким повинні задовольняти організація, її торгові партнери, підрядчики і постачальники послуг; при цьому зростає необхідність стандартизації у міру розповсюдження електронного

обміну інформацією по мережах між організаціями. Дані практичні правила можуть служити надійною основою для завдання загальних вимог цього типу.

3. Унікальний набір принципів, цілей і вимог до обробки інформації, який розроблений організацією для виробничих цілей. Важливо (наприклад, для забезпечення конкурентоспроможності), щоб в політиці безпеки були відображені ці вимоги, і життєвоважливо, щоб реалізація або відсутність засобів управління безпекою в інформаційній інфраструктурі не заважали виробничої діяльності організації.

Залучення належних засобів контролю і необхідна гнучкість з самого початку процесу планування інформаційних систем є необхідними умовами для успішного завершення роботи.

Оцінка ризиків порушення безпеки. Витрати на систему захисту інформації необхідно зіставити і привести у відповідність з цінністю інформації, що захищається, і інших інформаційних ресурсів, піддаються ризику, а також із збитком, який може бути нанесений організації із-за збоїв в системі захисту.

Зазвичай методики аналізу ризиків застосовуються до повних інформаційних систем і сервісів, але цими ж методиками можна скористатися і для окремих компонентів системи або сервісів, якщо це доцільно і практично. Для оцінки ризиків необхідно систематично розглядати наступні аспекти:

– збиток, який може нанести діяльності організації серйозне порушення інформаційної безпеки, з урахуванням можливих наслідків порушення конфіденційності, цілісності і доступності інформації;

– реальна вірогідність такого порушення захисту в світлі превалюючих загроз і засобів контролю.

Результати цієї оцінки необхідні для розробки основної лінії і визначення належних дій і пріоритетів для управління ризиками порушення інформаційної безпеки, а також для реалізації засобів контролю, що рекомендуються в справжніх практичних правилах.

Оцінка цих двох аспектів ризики залежить від наступних чинників:

– характеру виробничої інформації і систем;
– виробничій меті, для якої інформація використовується;
– середовища, в якому система використовується і управляється;
– захисту, що забезпечується існуючими засобами контролю.

Оцінка ризиків може виявити виключно високий ризик порушення інформаційної безпеки організації, що вимагає реалізації додаткових, сильніших засобів контролю, ніж ті, які рекомендуються в справжніх правилах.

Використання таких засобів контролю необхідно обґрунтувати виходячи з виводів, отриманих в результаті оцінки ризиків.

Умови успішної реалізації системи інформаційної безпеки. Перераховані нижче чинники є визначальний для успішної реалізації системи інформаційної безпеки в організації:

– цілі безпеки і її забезпечення повинні ґрунтуватися на виробничих цілях і вимогах; функції управління безпекою повинно узяти на себе керівництво організації;

– явна підтримка і прихильність до підтримки режиму безпеки вищого керівництва;

– хороше розуміння ризиків порушення безпеки (як загроз, так і вразливостей), яким піддаються ресурси організації, і рівня їх захищеності в організації, який повинен ґрунтуватися на цінності і важливості цих ресурсів;

– ознайомлення з системою безпеки всіх керівників і рядових співробітників організації;

– надання вичерпного посібника з політики і стандартів інформаційної безпеки всім співробітникам і підрядчикам.

Розробка власних рекомендацій. Не існує єдиної оптимальної структури захисту інформації. Кожна категорія користувачів або фахівців з інформаційних технологій, що працюють в конкретному середовищі, може мати свій власний, такий, що відрізняється від інших, набір вимог, проблем і пріоритетів, залежно від функцій конкретної організації і виробничого або обчислювального середовища.

Багато організацій вирішують цю проблему, розробляючи набір окремих керівних принципів для відповідних груп співробітників, щоб забезпечити ефективніше розповсюдження знань в області захисту інформації. Організаціям, що вирішили прийняти іншу структуру (або навіть розробити свої рекомендації), бажано ввести перехресні посилання на текст діючих правил, щоб їх майбутні ділові партнери або аудитори могли встановити прямі зв'язки між цим стандартом і прийнятими в даній організації принципами системи захисту інформації.

Політика інформаційної безпеки. Метою політики інформаційної безпеки сформулювати мету і забезпечити підтримку інформаційної безпеки керівництвом організації. Вище керівництво повинне поставити чітку мету і всесторонньо подавати свою підтримку інформаційної безпеки за допомогою розповсюдження політики безпеки серед співробітників організації.

Документ про політику інформаційної безпеки. Письмовий документ про політику безпеки повинен бути доступний всім співробітникам, що відповідають за забезпечення режиму інформаційної безпеки. Вище керівництво повинне надати задокументовану політику інформаційної безпеки всім підрозділам організації. Цей документ повинен містити принаймні наступне:

– визначення інформаційної безпеки, її основні цілі і область її застосування, а також її значення як механізму, що дає можливість колективно використовувати інформацію;

– виклад позиції керівництва по питаннях реалізації цілей і принципів інформаційної безпеки;

– роз'яснення конкретних варіантів політики безпеки, принципів, стандартів і вимог до її дотримання, включаючи: виконання правових і договірних вимог; вимоги до навчання персоналу правилам безпеки; політика попередження і виявлення вірусів; політика забезпечення безперебійної роботи організації;

– визначення загальних і конкретних обов'язків по забезпеченню режиму інформаційної безпеки;

– роз'яснення процесу повідомлення про події, що таять загрозу безпеці.

Необхідно розробити процес перевірки, визначити обов'язку і задати дати перевірок для дотримання вимог документа про політику безпеки.

Приклад політики безпеки. Нижче представлений витяг з еталонної політики безпеки «Підприємства», яка включає наступні розділи:

1. Загальні положення.
2. Політика управління паролями.
3. Ідентифікація користувачів.
4. Повноваження користувачів.
5. Захист інформаційних ресурсів ІС від комп'ютерних вірусів.
6. Правила установки і контролю мережних з'єднань.
7. Правила політики безпеки по роботі з системою електронної пошти.
8. Правила забезпечення безпеки інформаційних ресурсів.

Для прикладу представлено перші два розділи «Політики безпеки».

Загальні положення. Забезпечення інформаційної безпеки є необхідною умовою для здійснення діяльності «Підприємства». Порушення інформаційної безпеки може привести до серйозних наслідків, включаючи втрату довіри з боку клієнтів і зниження конкурентоспроможності.

Основою заходів по забезпеченню режиму інформаційної безпеки адміністративного рівня, тобто заходів, що робляться керівництвом організації, є

політика безпеки. Під політикою безпеки розуміється сукупність документованих управлінських рішень, направлених на захист інформації і асоційованих з нею ресурсів. Політика безпеки «Підприємства» визначає основні напрями і вимоги по забезпеченню інформаційної безпеки «Підприємства».

Забезпечення безпеки інформації включає будь-яку діяльність, направлену на захист інформації і/або підтримуючої інфраструктури. Справжня політика інформаційної безпеки охоплює всі автоматизовані і телекомунікаційні системи, власником і користувачем яких є «Підприємство». Положення цього документа відносяться до всього штатного персоналу, тимчасових службовців і інших співробітників «Підприємства», а також клієнтів «Підприємства» і третіх осіб, що мають доступ до автоматизованих і телекомунікаційних систем «Підприємства».

Політика управління паролями. Користувачі повинні вибирати нестандартні паролі. Це означає, що паролі не повинні бути пов'язані із заняттями або особистим життям користувачів. Наприклад, не можна використовувати як пароль номер власного автомобіля, ім'я дружини або частину адреси. Це також означає, що пароль не повинен бути просто словом із словника. Так, не повинні використовуватися як паролі імена власні, географічні назви, технічні терміни і сленг. Якщо є відповідні системні програмні засоби для здійснення контролю надійності що призначаються користувачам паролів, то необхідно використовувати ці засоби для того, щоб заборонити користувачам вибір легко вгадуваних паролів.

Користувачі можуть вибрати паролі, що легко запам'ятовуються, які в теж час є важко вгадуваними для третіх осіб, якщо буде виконано хоч би одна з наступних умов:

– декілька слів написано разом (такі паролі відомі під назвою «passphrases»);

– при наборі слова на клавіатурі використані клавіші, зміщені щодо потрібних, на один ряд вгору, вниз, управо або вліво;

– слово набране із зсувом на певну кількість букв вгору або вниз за абеткою;

– комбінація цифр і звичайного слова;

– навмисно неправильне написання слова (але не звичайна в даному слові орфографічна помилка).

Рекомендується, щоб в паролі були не тільки букви, але і інші символи, тобто цифри (0…9) і знаки пунктуації. Використання символів, що управляють, і

інших знаків, що не відображаються, не рекомендується, оскільки через це можуть виникнути проблеми при передачі даних по мережі, несподівано активізуватися певні системні утиліти або виникнути інші побічні ефекти.

Всі паролі повинні полягати не менше чим з шести символів. Довжина паролів винна завжди автоматично перевірятися в той момент, коли користувачі створюють або вибирають паролі.

Користувачі не повинні створювати паролі, які ідентичні або в значній мірі повторюють раніше використовувані ними паролі. Якщо є відповідні системні програмні засоби, необхідно заборонити користувачам, повторно використовувати свої попередні паролі.

Паролі не повинні зберігатися в доступній для читання формі в командних файлах, сценаріях автоматичної реєстрації, програмних макросах, функціональних клавішах терміналу, на комп'ютерах з неконтрольованим доступом, а також в інших місцях, де не уповноважені особи можуть дістати до них доступ. Наприклад, ні в яких застосуваннях користувачі не повинні вибирати таку опцію конфігурації, як автоматичне збереження пароля.

Не можна записувати паролі і залишати ці записи в місцях, де до них можуть дістати доступ не уповноважені особи. Пароль повинен бути негайно змінений, якщо є підстави вважати, що цей пароль став відомий кому-небудь ще, окрім самого користувача.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Розробити політику безпеки організації у відповідності з рекомендаціями стандарту ISO/IEC 17799.
2. Обґрунтувати запропоновану політику безпеки.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Охарактеризуйте спрямованість стандарту ISO/IEC 17799.
2. У чому полягає зміст інформаційної безпеки?
3. Структура стандарту ISO/IEC 17799.
4. Назвіть які засоби контролю використовуються під час управління безпекою та яких умов дотримуються під час реалізації системи ІБ?
5. Які групи вимог, що висуваються до системи безпеки організації встановлено у стандарті ISO/IEC 17799.
6. На які аспекти слід звертати увагу під час оцінювання ризиків безпеки?
7. Структура документу про політику інформаційної безпеки організації.

Рекомендована література: [1-12].

ПРАКТИЧНА РОБОТА №4

Тема: дослідження алгоритмів криптографічного захисту на основі підстановок та перестановок.

Мета: ознайомитись із принципом роботи та алгоритмами блочних шифрів.

Завдання: опрацювати теоретичний матеріал, описати алгоритм роботи шифру та дати відповіді на запитання.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Класифікація шифрів. Шифр системи прийнято класифікувати за різними ознаками:

– за видами інформації (текст, мова, відеоінформація), яка захищається;

– за криптографічною стійкістю;

– за принципами забезпечення захисту інформації (симетричні, асиметричні, гібридні);

– за конструктивними принципами (блокові і потокові).

При побудові шифру використовуються, з математичної точки зору, два види відображень:

– перестановки елементів відкритого тексту;

– заміни елементів відкритого тексту на елементи деякої множини.

У зв'язку з цим безліч шифрів ділиться на три види:

– шифри перестановки;

– шифри заміни;

– композиційні шифри, які використовують поєднання перестановок і замін.

Блочні шифри – це алгоритми шифрування, які здатні обробляти дані блоками фіксованого розміру. Вони використовуються для забезпечення конфіденційності інформації, перетворюючи відкритий текст у шифрований текст за допомогою ключа. Основна ідея полягає в тому, що дані діляться на блоки, і кожен блок шифрується окремо.

Алгоритм Lucifer. В кінці шестидесятих років корпорація IBM запустила дослідницьку програму по комп'ютерній криптографії, названу Lucifer (Люцифер) і керовану спочатку Хорстом Файстелем (Horst Feistel), а потім Уолтом Тачменом (Walt Tuchman). Таке ж ім'я – Lucifer – одержав блоковий алгоритм, який з'явився в результаті цієї програми на початку сімдесятих років. Насправді існує, щонайменше, два різні алгоритми з таким ім'ям. Один з них містить ряд пропусків в специфікації алгоритму. Все це привело до помітної плутанини.

Алгоритм Lucifer є мережею перестановок і підстановок, його основні блоки нагадують блоки алгоритму DES. У DES результат функції f складається операцією XOR з входом попереднього раунду, утворюючи вхід наступного раунду. У S-блоків алгоритму Lucifer 4-бітові входи і виходи, вхід S-блоків є перетасованим виходом S-блоків попереднього раунду, входом S-блоків першого раунду служить відкритий текст. Для вибору використовуваного Sблоку з двох можливих використовується біт ключа. (Lucifer реалізує все це в єдиному T-блоці з 9 бітами на вході і 8 бітами на виході). На відміну від алгоритму DES, половини блоку між раундами не переставляються, та і саме поняття половини блоку в алгоритмі Lucifer не використовується. У цього алгоритму 16 раундів, 128-бітові блоки і простіша, ніж в DES, схемі розгортки ключа.

Деякі вважають, що Lucifer надійніше за DES через більшу довжину ключа і нечисленності опублікованих відомостей. Але очевидно, що це не так.

Алгоритм Madryga. Цей блоковий алгоритм було запропоновано в 1984 році та названо на честь автора У. Е. Мадріга. Його можна ефективно реалізувати програмним шляхом: у алгоритмі немає дратівливих перестановок, і всі операції виконуються над байтами.

Варто перерахувати завдання, які вирішує користувач при проектуванні алгоритму:

– без допомоги ключа відкритий текст неможливо одержати з шифр-тексту;

– число операцій, необхідних для відновлення ключа за зразком шифр-тексту і відкритого тексту, повинно бути статистично рівно твору числа операцій при шифруванні на число можливих ключів;

– публікація алгоритму не впливає на стійкість шифру;

– зміна одного біта ключа повинна радикально змінювати шифр-текст одного і того ж відкритого тексту, а зміна одного біта відкритого тексту повинна радикально змінювати шифртекст для того ж ключа;

– алгоритм повинен містити некомутативну комбінацію підстановок і перестановок;

– підстановки і перестановки, використовувані в алгоритмі, повинні визначатися як вхідними даними, так і ключем;

– надмірні групи бітів відкритого тексту повинні бути повністю замасковані в шифр-тексті;

– довжина шифр-тексту повинна співпадати з довжиною відкритого тексту;

– між будь-якими можливими ключами і особливостями шифр-тексту недопустимі прості взаємозв'язки;

– усі можливі ключі повинні забезпечувати стійкість шифру;

– довжина ключа і текст повинні мати можливість варіювання для реалізації різних вимог до безпеки;

– алгоритм повинен допускати ефективну програмну реалізацію на мейнфреймах, міні- і микрокомпьютерах і за допомогою дискретної логіки.

Опис алгоритму: алгоритм Madryga складається із двох вкладених циклів. Зовнішній цикл повторюється вісім разів (для гарантії надійності число циклів доцільно збільшити) та полягає в застосуванні внутрішнього циклу до відкритого тексту. Внутрішній цикл перетворює відкритий текст в шифртекст і виконується одноразово над кожним 8-бітовим блоком (байтом) відкритого тексту. Таким чином, весь відкритий текст послідовно вісім разів обробляється алгоритмом.

Алгоритми REDOC. Алгоритм REDOC II є ще одним блоковим алгоритмом, розробленим Майклом Вудом (M. Wood) для корпорації Cryptech. У ньому використовуються 20 байтовий (160-бітовий) ключ і 80-бітовий блок.

Алгоритм REDOC II виконує всі маніпуляції – перестановки, підстановки і операції XOR з ключем – з байтами. Цей алгоритм зручний для програмної реалізації. У REDOC II використані змінні таблиці функцій. На відміну від алгоритму DES, що має фіксований (хоч і оптимізований з погляду стійкості) набір таблиць підстановок і перестановок, в REDOC II використовуються залежні від ключа і відкритого тексту набори таблиць (по суті, S-блоки). У REDOC II 10 раундів, кожен раунд складається з складної послідовності маніпуляцій з блоком.

Інша унікальна особливість REDOC II – використання масок. Це числа – похідні таблиці ключів, які використовуються для вибору таблиць даної функції для даного раунду. Для вибору таблиць функцій використовуються як значення даних, так і маски.

За умови, що найефективніший засіб злому цього алгоритму – лобовий розтин, REDOC II дуже надійний: для відновлення ключа необхыдно провести 2160 операцій. Томас Кузік (T. Cusick) виконав криптоаналіз одного раунду REDOC II, але розширити розтин на декілька раундів йому не вдалося. Використовуючи диференціальний криптоаналіз, Біхам і Шамір успішно виконали криптоаналіз одного раунду REDOC II за допомогою 2300 підібраних відкритих текстів. Вони не зуміли розширити цю атаку на декілька раундів, але їм вдалося набути трьох значення маски після чотирьох раундів.

Алгоритм REDOC III –це спрощена версія REDOC II, теж розроблена М. Вудом. Він оперує з 80-бітовим блоком. Довжина ключа може змінюватися і досягати 2560 байт (204800 біт). Алгоритм складається тільки з операцій XOR над байтами ключа і відкритого тексту, перестановки і підстановки не використовуються.

1. Створюють таблицю ключів з 256 10-байтових ключів, використовуючи секретний ключ.

2. Створюють два 10-байтові блоки масок M_1 і M_2. M_1 є результатом операції XOR перших 128 10-байтових ключів, а M_2 – результат операції XOR других 128 10-байтових ключів.

3. Для шифрування 10-байтового блоку виконують операцію XOR з першим байтом блоку даних і першим байтом M_1. Вибирають ключ в таблиці ключів, розрахованій в раунді 1. Використовують обчислене значення XOR як індекс таблиці. Виконують операцію XOR з кожним, окрім першого, байтом блоку даних і відповідним байтом вибраного ключа.

Виконують операцію XOR з другим байтом блоку даних і другим байтом M_1. Вибирають ключ в таблиці ключів, розрахованій в раунді 1. Використовують обчислене значення XOR як індекс таблиці. здійснюють операцію XOR з кожним, окрім другого, байтом блоку даних і відповідним байтом вибраного ключа.

Продовжують ці дії зі всім блоком даних (з 3…10 байтами), поки не буде використаний кожен байт для вибору ключа з таблиці після виконання операції XOR з ним і відповідним значенням M_1. Потім виконують операцію XOR з кожним, окрім використаного для вибору ключа, байтом, і ключем.

Повторюють етапи 1…3 для M_2.

Це нескладний і швидкісний алгоритм. На процесорі 80386 з тактовою частотою 33МГц він шифрує дані із швидкістю 2,75 Мбіт/с. За оцінкою Вуда, конвейерний процесор з трактом даних 64 біт і тактовою частотою 20 МГц дозволяє шифрувати дані зі швидкістю понад 1,28 Гбіт/с.

Зауважимо, що алгоритм REDOC III нестійкий. Він вразливий до диференціального криптоаналізу. Для відновлення обох масок достатнім є приблизно 223 підібраних відкритих текстів.

Алгоритм LOKI. Даний алгоритм розроблено в Австралії і вперше був представлений у 1990 році, у якості можливої заміни DES. У ньому використовують 64-бітовий блок і 64бітовий ключ.

Використовуючи диференціальний криптоаналіз, Біхам і Шамір зламували алгоритм LOKI з 11 і менш раундами швидше, ніж за лобовим розтином. Більш

того, алгоритм характеризується 8-бітовою комплементарністю, яка спрощує лобовий розтин в 256 разів.

Як показав Ларс Кнудсен (L. Knudsen), алгоритм LOKI з 14 і менш раундами уразливий диференціальному криптоаналізу. Крім того, якщо в LOKI використовуються альтернативні S-блоки, то одержаний шифр, ймовірно, теж уразливий диференціальному криптоаналізу.

Алгоритм LOKI91. У відповідь на описані вище розтини розробники LOKI повернулися до перегляду свого алгоритму. В результаті з'явився алгоритм LOKI91. (Попередня версія LOKI була перейменована LOKI89).

Щоб підвищити стійкість алгоритму до диференціального криптоаналізу і позбавитися комплементарності, в початковий проект було внесено наступні зміни:

– алгоритм генерації підключів модифікований з тим, щоб половини переставлялися не після кожного, а після кожного другого раунду;

– алгоритм генерації підключів модифікований так, що число позицій циклічного зрушення лівого підключа складало або 12, або 13 бітів;

– виключено початкову і завершальну операції XOR з блоком і ключем;

– змінено функцію S-блоку з метою згладити профілі XOR S-блоків (щоб підвищити їх стійкість до диференціального криптоаналізу), і виключити всі значення x, для яких f(x)=0 (де f – комбінація E-, S- і P-блоків).

Алгоритм LOKI не запатентований – реалізувати і використати LOKI може хто завгодно.

Алгоритми Khufu і Khafre. У 1990 році Ральф Меркл (R. Merkle) запропонував два алгоритми. У основу конструкції закладено наступний принцип: 56-бітовий розмір ключа DES дуже малий. Оскільки вартість збільшення розміру ключа нехтує мала (комп'ютерна пам'ять недорога і доступна), довжину ключа слід збільшити.

Широке використання в DES перестановок, хоч і зручно для апаратних реалізацій, надзвичайно утрудняє програмні реалізації. Найшвидкісніші реалізації DES виконують перестановки за допомогою таблиць підстановок. Таблиці підстановок можуть забезпечити ті ж характеристики «розсіювання», що і власне перестановки, і набагато підвищити гнучкість реалізації.

S-блоки DES, що містять всього 64 4-бітових елемента, дуже малі. Тепер, із збільшенням об'єму пам'яті, повинні зрости і S-блоки. Більш того, всі вісім S-блоків в DES використовуються одночасно. Хоча це і зручніше для апаратури, для програмної реалізації це представляється непотрібним обмеженням. Повинні бути реалізовані більший розмір S-блоків і послідовне їх використання.

Загальновизнано, що початкова і завершальна перестановки криптографічних ключів лишня, а тому їх виключають.

Всі швидкісні реалізації DES наперед обчислюють ключі для кожного раунду. Звідси, немає причин не зробити ці обчислення складнішими.

На відміну від DES, критерії проектування S-блоків повинні бути загальнодоступні.

На сьогодні до цього переліку Р. Меркл, можливо, додав би «стійкість до диференціального і лінійного криптоаналізу, адже у той час ці методи розтину не були відомі.

Алгоритми Khufu і Khafre запатентовані, а їх початковий код наведено у патенті.

Алгоритм MMB. Незадоволеність використанням в одному із криптоалгоритмов 64-бітового блоку шифрування привела до створення Джоаною Деймен алгоритму під назвою MMB (Modular Multiplication-based Block cipher – модулярный мультиплікативний блоковий шифр). У основі MMB лежить змішування операцій різних груп алгебри. MMB – ітеративний алгоритм, що головним чином складається з лінійних дій (XOR і використання ключа) і паралельного застосування чотирьох крупних оборотних нелінійних підстановок. Ці підстановки визначаються за допомогою множення по модулю 232-1 з постійними множниками. У результаті з'являється алгоритм, що використовує 128-бітовий ключ і 128-бітовий блок.

Алгоритм Blowfish. Blowfish – це алгоритм, розроблений Брюсом Шнайером спеціально для реалізації на великих мікропроцесорах. Алгоритм Blowfish не запатентований. При проектуванні алгоритму Blowfish Шнайер намагався задовольнити наступним критеріям:

– швидкість: програма, що реалізовує алгоритм Blowfish на 32-бітових мікропроцесорах, шифрує дані із швидкістю 26 тактів на байт;

– компактність: для виконання програмної реалізації алгоритму Blowfish достатньо 5 Кбайт пам'яті;

– простота: у алгоритмі Blowfish використовуються тільки прості операції (додавання, XOR і підстановка з таблиці по 32-бітовому операнду). Аналіз його схеми нескладний, що знижує ризик помилок реалізації алгоритму;

– стійкість, яка налаштовується: довжина ключа Blowfish змінна і може досягати 448 біт.

Алгоритм Blowfish оптимізований для застосування в системах, що не практикують частої зміни ключів, наприклад, в лініях зв'язку і програмах автоматичного шифрування файлів. При реалізації на 32-бітових

мікропроцесорах з великим розміром кеша даних, наприклад, процесорах Pentium і PowerPC, алгоритм Blowfish помітно швидший за DES. Алгоритм Blowfish не підходить для застосування у випадках, де необхідною є часта зміна ключів, наприклад, в комутаторах пакетів, або як однонаправлена хеш-функція.

Великі вимоги до пам'яті не дозволяють використовувати цей алгоритм в смарткартах.

Алгоритм RC5. RC5 є блоковим шифром з безліччю параметрів: розміром блоку, розміром ключа і числом раундів. Він винайдений Роном Рівестом і проаналізований в RSA Laboratories.

У алгоритмі RC5 передбачено три операції: XOR, додавання і циклічні зрушення. На більшості процесорів операції циклічного зрушення виконуються за сталий час, змінні циклічні зрушення є нелінійною функцією. Ці циклічні зрушення, залежні як від ключа, так і від даних.

Об'єднання блокових шифрів. Відомо про безліч шляхів об'єднання блокових алгоритмів для отримання нових алгоритмів. Створення подібних схем стимулюється бажанням підвищити безпеку, уникнувши трудності проектування нового алгоритму. Так, алгоритм DES відноситься до надійних алгоритмів, він піддавався криптоаналізу понад 20 років, проте, якнайкращим способом злому залишається лобовий розтин. Проте ключ DES дуже короткий. Хіба не погано було б використовувати DES як компоненту іншого алгоритму з довшим ключем? Це дозволило б скористатися перевагами обох систем: стійкістю, гарантованою двома десятиліттям криптоаналізу, і довгим ключем.

Один з методів об'єднання є багатократне шифрування. В цьому випадку для шифрування одного і того ж блоку відкритого тексту алгоритм шифрування використовується кілька разів із декількома ключами. Каскадне шифрування є подібним до багатократного шифрування, але використовує різні алгоритми.

Повторне шифрування блоку відкритого тексту одним і тим же ключем за допомогою того ж або іншого алгоритму є неефективним. Повторне використання того ж алгоритму не підвищує складність лобового розтину. При використанні різних алгоритмів складність лобового розтину може, як зростати, так і залишатися незмінною. При цьому потрібно переконатися в тому, що ключі для послідовних шифрувань різні і незалежні.

Алгоритм DES. Стандарт шифрування даних DES (Data Encryption Standard) опубліковано в 1977 р. Національним бюро стандартів США.

Стандарт DES призначений для захисту від несанкціонованого доступу до важливої, але несекретної інформації в державних і комерційних організаціях США. Алгоритм закладений в основу стандарту, розповсюджувався досить

швидко, і вже в 1980 р. був схвалений Національним інститутом стандартів і технологій США (НІСТ). До теперішнього часу DES є найбільш поширеним алгоритмом, що використовується в системах захисту комерційної інформації.

Основні переваги алгоритму DES:

– використовується тільки один ключ довжиною 56 біт;

– зашифрувавши повідомлення за допомогою одного тексту програм, для дешифрування можна використати будь-який інший пакет програм, що відповідає стандарту DES;

– відносна простота алгоритму забезпечує високу швидкість обробки;

– достатньо висока стійкість алгоритму.

Алгоритм DES використовує комбінацію підстановок і перестановок. DES здійснює шифрування 64-бітових блоків даних за допомогою 64-бітового ключа, в якому значущими є 56 біт (інші 8 біт – перевірочні біти для контролю на парність). Дешифрування в DES є операцією, оберненою шифруванню, і виконується шляхом повторення операцій шифрування в оберненій послідовності. Узагальнена схема процесу шифрування в алгоритмі DES показана на рисунку 4.1.

Рисунок 4.1 – Узагальнена схема шифрування в алгоритмі DES

Процес шифрування полягає в початковій перестановці бітів 64-бітового блоку, шістнадцяти циклах шифрування і, нарешті, в кінцевій перестановці бітів.

Всі перестановки і коди в таблицях підібрані розробниками таким чином, щоб максимально ускладнити процес дешифрування шляхом підбору ключа. При описі алгоритму DES (рис. 4.2) застосовані наступні позначення: L і R – послідовності бітів (ліва (left) і права (right)); LR – конкатенація послідовностей L і R, тобто така послідовність бітів, довжина якої рівна сумі довжин L і R, в

послідовності LR біти послідовності R слідують за бітами послідовності L; «+» – операція побітового додавання по модулю 2.

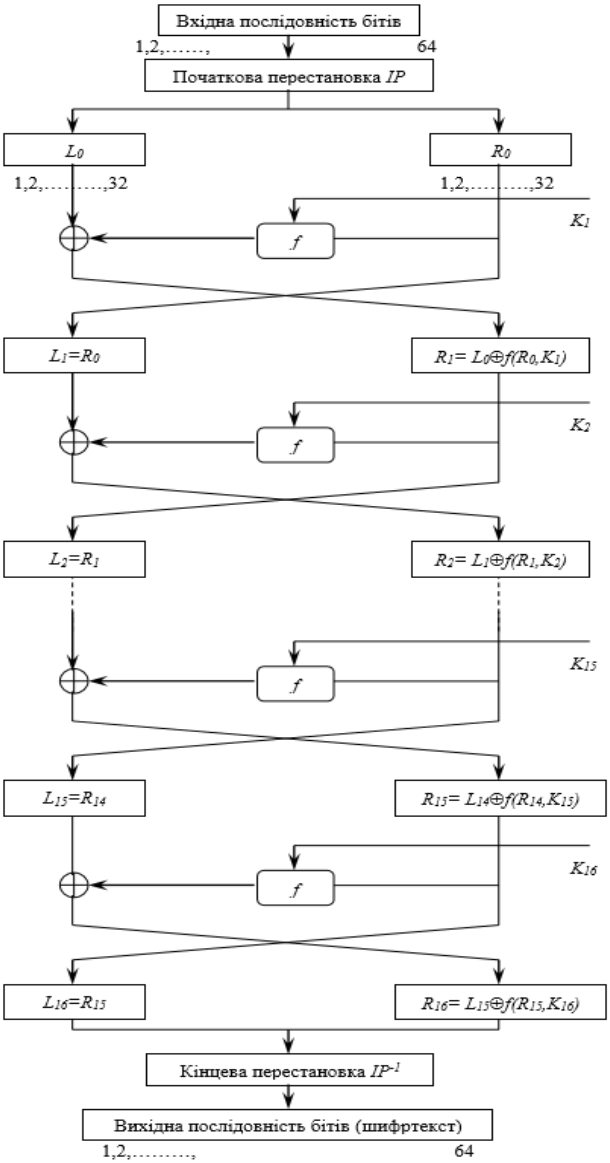

Рисунок 4.2 – Структура алгоритму DES

Розглянемо роботу алгоритму DES. Нехай з файлу вихідного тексту прочитаний черговий 64-бітовий (8-байтовий) блок T. Цей блок T перетворюється за допомогою матриці початкової перестановки IP. Біти вхідного блоку T (64 біта) переставляються відповідно до матриці IP. Біт 58 вхідного блоку T стає бітом 1, біт 50 – бітом 2 тощо. Цю перестановку можна описати виразом T0=IP(T). Отримана послідовність бітів T0 розділяється на дві послідовності: L0 – ліві або старші біти; R0 – праві або молодші біти, кожна з яких містить 32 біти.

Потім виконується ітеративний процес шифрування, що складається з 16 кроків (циклів). Нехай Ti - результат i-ої ітерації , тоді:

$$Ti=LiRi,$$

де Li=t1, t2, …, t32 – перші 32 біти;

Ri=t33, t34, …, t64 – (останні 32 біти).

Тоді результат i-ої ітерації будуть описуватись наступними формулами:

$$L_i = R_{i-1}, i = 1, 2, ..., 16;$$

$$R_i = L_{i-1} \oplus f(R_{i-1}; K_i), i = 1, 2, ..., 16.$$

Функція f називається функцією шифрування, а її аргументами є послідовність Ri-1, що отримується на попередньому кроці ітерації, і 48-бітовий ключ Ki, який є результатом перетворення 64-бітового ключа шифру K.

На останньому кроці ітерації отримують послідовності R16 і L16 (без перестановки місцями), які конкатенуються в, 64-бітову послідовність R16L16.

Після закінчення шифрування здійснюється відновлення позицій бітів за допомогою матриці зворотної перестановки IP-1. Процес дешифрування даних є обернений по відношенню до процесу шифрування. Всі дії повинні бути виконані в оберненому порядку. Це означає, що дані, які дешифруються спочатку переставляються відповідно до матриці IP/1, а потім над послідовністю бітів R16L16 виконуються ті ж дії, що і в процесі шифрування, але в оберненому порядку.

Ітеративний процес дешифрування можна описати наступними формулами:

$$R_i = L_{i-1}, i = 1, 2, ..., 16;$$

$$L_i = R_{i-1} \oplus f(L_i; K_i), i = 1, 2, ..., 16.$$

Таким чином, для процесу дешифрування з переставленим вхідним блоком R16L16 на першій ітерації використовується ключ K16, на другій ітерації – K15 тощо. На 16-й ітерації використовується ключ K. На останньому кроці ітерації

будуть отримані послідовності L0 і R0, які конкатенуються в 64-бітову послідовність L0R0. Потім в цій послідовності 64 біти переставляються відповідно до матриці IP. Результат такого перетворення – початкова послідовність бітів (дешифроване 64-бітове значення).

Розглянемо реалізацію функції для перетворення f, схему обчислення функції шифрування подано на рисунку 4.3.

Для обчислення значення функції f використовуються:

– функція f (розширення 32 біт до 48);
– функція S (перетворення 6-бітовогочисла в 4-бітове);
– функція P (перестановка бітів в 32-бітовій послідовності).

Отриманий результат додається за модулем 2 (операція XOR) з поточним значенням ключа Ki, після чого розбивається на вісім 6-бітових блоків.

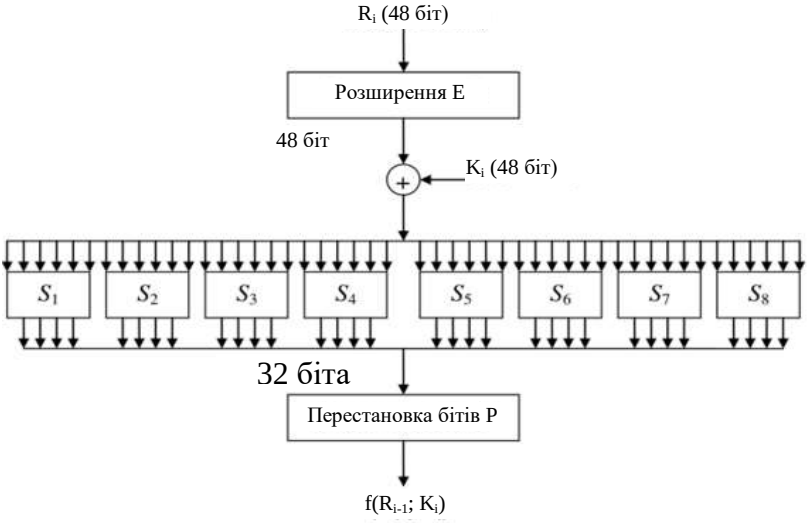

Рисунок 4.3 – Схема обчислень функції шифрування

Далі кожний з цих блоків використовується як номер елемента в функціях-матрицях S, які містять 4-бітові значення. В результаті отримуємо 32-бітовий блок, який перетворюється за допомогою функції перестановки бітів P.

На кожній ітерації використовується нове значення ключа K, (довжиною 48 біт). Нове значення ключа K прийнято встановлювати з початкового ключа K (рис. 4.4).

Ключ K являє собою 64-бітовий блок з 8-бітами контролю по парності, розташованими в позиціях 8, 16, 24, 32, 40, 48, 56, 64. Для видалення

контрольних бітів і підготовки ключа до роботи використовується функція G первинної підготовки ключа.

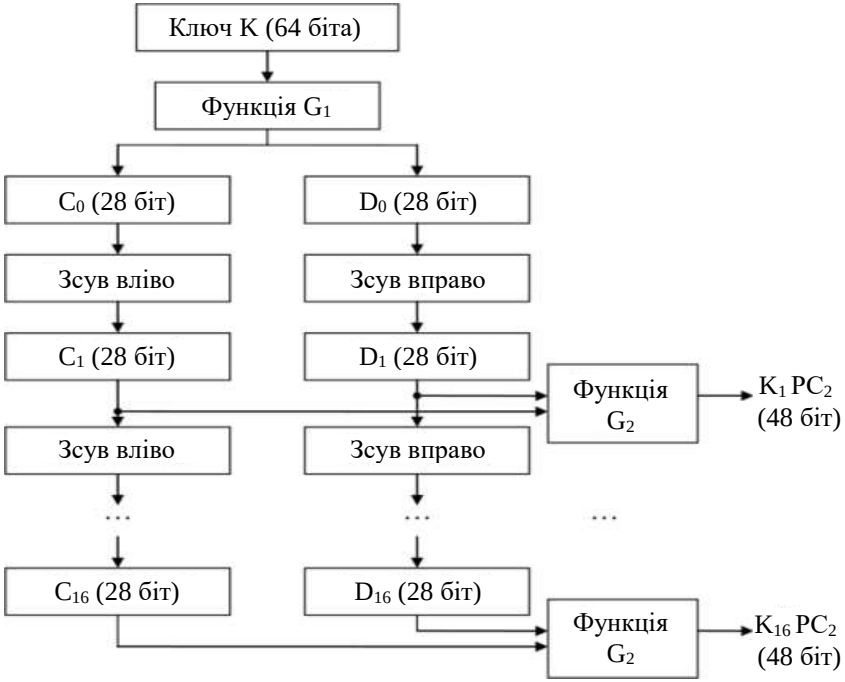

Рисунок 4.4 – Схема алгоритму обчислення ключів

Результат перетворення G(K) розбивається на дві половини C0 і D0 по 28-біт кожна. Перші чотири рядки матриці G визначають, як вибираються біти послідовності C0 (першим бітом C0 буде біт 57 ключа шифру, потім біт 49 тощо, а останніми бітами – біти 44 і 36 ключа). Наступні чотири рядки матриці G визначають, як вибираються біти послідовності D0 (тобто послідовність D0 буде складатися з бітів 63, 55, 47, ..., 12, 4 ключа шифру). Як видно, для генерації послідовностей C0 і D0 не використовуються біти 8, 16, 24, 32, 40, 48, 56 і 64 ключа шифру. Ці біти не впливають на шифрування і можуть бути призначеним для іншої мети (наприклад, для контролю по парності). Таким чином, насправді ключ шифру є 56-бітовим.

Після визначення C0 і D0 рекурсивно визначаються C і D i=1, 2, ..., 16. Для цього застосовуються операції циклічного зсуву вліво на один або два біти в залежності від номера кроку ітерації.

Операції зсуву виконуються для послідовностей C і D, незалежно. Наприклад, послідовність C3 виходить за допомогою циклічного зсуву вліво на дві позиції послідовності C2, а послідовність D3 за допомогою зсуву вліво на дві позиції послідовності D2. C16 і D16 виходять з C15 і D15 за допомогою зсуву вліво на одну позицію. Ключ K, який визначається на кожному кроці ітерації, є результатом вибору конкретних бітів з 56-бітової послідовності C і D та їхньої перестановки. Іншими словами, ключ K, є функцією G, яка визначається матрицею завершальної обробки ключа. Першим бітом ключа K буде 14-й біт послідовності CiDi, другим – 17-й біт, 47-м бітом ключа K, буде 29-й біт C, D, а 48-м бітом – 32-й біт C, D.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Описати особливості шифру у відповідності до виданого варіанту та навести алгоритм роботи шифру.

1. LUCIFER;	6. LOKI;	11. CA-1.1;	16. SAFER;
2. MADRYGA;	7. KHAFRE;	12. SKIPJACK;	17. 3-WAY;
3. NewDES;	8. RC2;	13. CAST;	18. CRAB;
4. FEAL;	9. IDEA;	14. KHUFU;	19. SXAL8/MBAL;
5. REDOC;	10. MMB;	15. BLOWFISH;	20. RC5.

2. Зашифрувати журнал в якому зберігаються ідентифікатори користувачів.
3. Передбачити систему дешифрування.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які шифри називають симетричними? Приклади симетричних шифрів.
2. Переваги та недоліки симетричних шифрів.
3. Що являють собою блочні шифри?
4. Охарактеризуйте операції підстановки та перестановки.
5. Чим, на практиці, забезпечують криптостійкість алгоритму?
6. У яких основних областях застосовують алгоритми блочних шифрів?

Рекомендована література: [1-12].

ПРАКТИЧНА РОБОТА №5

Тема: дослідження процедури шифрування та дешифрування в криптосистемі RSA.

Мета: оволодіти методикою побудови засобів захисту інформації на основі криптосистеми RSA.

Завдання: опрацювати теоретичний матеріал, провести шифрування й дешифрування за алгоритмом RSA та дати відповіді на запитання.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Алгоритм RSA. Цей алгоритм було запропонувано у 1978 р. троє авторів: Рон Райвест (R. Rivest), Аді Шамір (A. Shamir) та Лено Адлеман (L. Adleman). Алгоритм одержав свою назву за першими літерами прізвищ його авторів. Алгоритм RSA став першим повноцінним алгоритмом: відкритим ключем, який може працювати як у режимі шифрування даних, так і в режимі електронного цифрового підпису.

Надійність алгоритму ґрунтується на складності задач факторизації великих чисел та обчислення дискретних логарифмів.

У криптосистемі RSA відкритий ключ K_B, секретний ключ k_B, повідомлення M і криптограма C належать множині цілих чисел:

$$Z_N=\{1, 2, \ldots Z-1\},$$

де P і Q – випадкові великі прості числа.

Для забезпечення максимальної безпеки вибирають P і Q рівної довжини і зберігають у секреті.

Множина Z_N з операціями додавання і множення за модулем N утворює розв'язок за модулем N.

Відкритий ключ K_B вибирають випадковим чином так, щоб виконувалися наступні умови:

$$1<K_B\leq\varphi(N);\ НСД(K_B, \varphi(N))=1;\ \varphi(N))=(P-1)(Q-1),$$

де φ(N) – функція Ейлера;

НСД – найбільший спільний дільник.

Функція Ейлера вказує на кількість додатних цілих чисел в інтервалі від 1 до N, які є взаємно простими по відношенню до N. Друга із зазначених вище умов означає, що відкритий ключ K_B і функція Ейлера φ(N) повинні бути взаємно простими.

Використовуючи розширений алгоритм Евкліда, обчислюють секретний ключ k_B:

$$k_B\times K_B\equiv 1(\text{mod } \varphi(N)),$$

або:

$$k_B=K_B^{-1}(\text{mod } (P-1)(Q-1)).$$

Це нескладно здійснити, оскільки відома пара простих чисел (P, Q) і можна легко знайти φ(N). Слід зауважити, що k_B і N повинні бути взаємно простими.

Відкритий ключ K_B використовують для шифрування даних, а секретний ключ k_B – для дешифрування.

Процедура шифрування визначає криптограму C через пару (відкритий ключ K_B, повідомлення M) у відповідності з наступного виразу:

$$C=E_{K_B}(M)=E_B(M)=M^{K_B}(\text{mod } N).$$

Як алгоритм швидкого обчислення значення C використовують ряд послідовних піднесень до квадрату цілого M множень на M з приведенням за модулем N.

Зворотна операція, тобто визначення значення M за відомим значенням C, K_B і N, практично не здійсненна при N≈2512.

Однак обернену задачу, тобто задачу дешифрування криптограми C, можна вирішити, використовуючи пари (секретний ключ k_B, криптограма C) за наступним виразом:

$$M=D_{k_B}(C)=D_B(C)=C^{k_B}(\text{mod } N).$$

Таким чином, якщо криптограму $C=M^{K_B}(\text{mod } N)$ піднести до степеня k_B, то в результаті відновлюється вихідний відкритий текст M, тому що:

$$(M^{K_B})^{k_B}=M^{K_Bk_B}=M^{n-\varphi(N)+1}\equiv M(\text{mod } N).$$

Таким чином, одержувач B, який створює криптосистему, захищає два параметри: секретний ключ k_B та пару чисел (P, Q), добуток яких формує значення модуля N.

З іншого боку, одержувач B відкриває значення модуля N і відкритий ключ K_B.

Зловмиснику відомі лише значення K_B і N. Якби він зміг розкласти число N на множники P і Q (задача факторизації), то він довідався б «таємний хід» – трійку чисел $\{P, Q, K_B\}$, обчислив значення функції Ейлера $\varphi(N)=(P-1)(Q-1)$ і визначив значення секретного ключа k_B.

Однак, як уже було відзначено, розкладання дуже великого N на множники не здійснено за реальний час (за умови, що довжини обраних P і Q складають не менш 100 десяткових знаків).

Процедура шифрування і дешифрування в криптосистемі RSA. Припустимо, що користувач A хоче передати користувачу B повідомлення в зашифрованому виді, використовуючи криптосистему RSA.

У такому випадку користувач A виступає в ролі відправника повідомлення, а користувач B – у ролі одержувача. Як уже зазначалось вище, криптосистему RSA повинен сформувати одержувач повідомлення, тобто користувач B.

Розглянемо послідовність дій користувача В і користувача А.

1. Користувач В вибирає два довільних великих простих числа P і Q.

2. Користувач В обчислює значення модуля $N=P\times Q$.

3. Користувач В обчислює функцію Ейлера $\varphi(N)=(P-1)(Q-1)$ і вибирає випадковим чином значення відкритого ключа K_B із врахуванням виконання наступної умови:

$$1<K_B\leq\varphi(N);\ НСД(K_B, \varphi(N))=1.$$

4. Користувач В обчислює значення секретного ключа k_B, використовуючи розширений алгоритм Евкліда:

$$k_B\equiv K_B^{-1}(\mathrm{mod}\ \varphi(N)).$$

5. Користувач В пересилає користувачу А пари чисел (N, K_B) по незахищеному каналі.

Якщо користувач А хоче передати користувачу В повідомлення М, він виконує наступні кроки.

6. Користувач А розбиває вихідний відкритий текст М на блоки, кожний з яких може бути представлений у вигляді числа:

$$M_i=1, 2, ..., N-1.$$

7. Користувач А шифрує текст, представлений у вигляді послідовності чисел М, за наступним виразом:

$$C_i=M_i^{K_B}(\mathrm{mod}\ N),$$

і відправляє криптограму «$C_1, C_2, C_3, \ldots, C_i$» користувачу В.

8. Користувач В розшифровує прийняту криптограму «$C_1, C_2, C_3, \ldots, C_i$» використовуючи секретний ключ k_B, за формулою:

$$M_i=C_i^{k_B}(\mathrm{mod}\ N).$$

У результаті буде отримана послідовність чисел M_i, що являють собою вихідне повідомлення М. Щоб алгоритм RSA мав практичну цінність, необхідно мати можливість без істотних витрат генерувати великі прості числа, вміти оперативно обчислювати значення ключів K_B і k_B.

Приклад. Шифрування повідомлення С А В.

Для простоти обчислень будуть використовуватися невеликі числа (на практиці прийнято застосовувати дуже великі числа).

Дії користувача В.

1. Вибирає P=3 і Q=11.

2. Обчислює модуль $N=P\times Q=3\times 11=33$.

3. Обчислює значення функції Ейлера для N=33:

$$\varphi(N)=\varphi(33)=(P-1)(Q-1)=2\times 10=20.$$

У якості відкритого ключа K_B вибирає довільне число із урахуванням

виконання умови:

$$1<K_B\leq 20;\ НСД(K_B, 20)=1.$$

Нехай K_B =7.

4. Обчислює значення секретного ключа kB, використовуючи розширений алгоритм Евкліда для розв'язку конгруенції:

kB≡7-1(mod 20)≈3.

5. Пересилає користувачу А пари чисел (N=33, КВ=7).

Дії користувача А.

6. Представляє шифроване повідомлення у вигляді послідовність цілих чисел у діапазоні 0 ...33.

Нехай літера А представляється у вигляді числа 1, літера В – як число 2, літера С – як число 3. Тоді повідомлення С А В можна представити як послідовність чисел 3, 1 та 2 (тобто M_1=3, M_2=1, M_3=2).

7. Шифрує, текст, представлений у виді послідовності чисел M_1, M_2 і M_3, використовуючи ключ K_B=7, за наступним виразом:

$$C_i=M_i^{K_B}(\text{mod } N)=M_i^7(\text{mod } 33),$$

та отримує:

$$C_1=3^7(\text{mod } 33)=2187(\text{mod } 33)=9,$$
$$C_2=1^7(\text{mod } 33)=1(\text{mod } 33)=1,$$
$$C_3=2^7(\text{mod } 33)=128(\text{mod } 33)=29,$$

Відправляє користувачу В криптограму: C_1=9; C_2=1; C_3=29.

Дії користувача В.

8. Розшифровує прийняту криптограму C_1, C_2, C_3 використовуючи секретний ключ k_B=3, за таким виразом:

$$M_i=C_ik^B(\text{mod } N)=C_i^3(\text{mod } 33),$$

та одержує:

$$M_1=9^3(\text{mod } 33)=729(\text{mod } 33)=3,$$
$$M_2=1^3(\text{mod } 33)=1(\text{mod } 33)=1,$$
$$M_3=29^3(\text{mod } 33)=24389(\text{mod } 33)=2.$$

Таким чином, відновлене вихідне повідомлення:

C	A	B
3	1	2

Безпека і швидкодія криптосистеми RSA. Як було зазначено вище безпека алгоритму RSA базується на складності задачі факторизації великих чисел, що являє собою добуток двох великих простих чисел. Насправді, криптостійкість алгоритму RSA визначається тим, що після формування секретного ключа k_B і відкритого ключа K_B «стираються» значення простих

чисел P і Q, а тоді уже надзвичайно важко визначити секретний ключ k_B за відкритим ключем K_B. Оскільки для цього необхідно знайти дільники P і Q модуля N.

Розкладання величини N на прості множники P і Q дозволяє обчислити функцію $\varphi(N)=(P-1)(Q-1)$, а відтак значення секретного ключа k_B, використовуючи рівняння $K_B \times k_B \equiv 1 (\mathrm{mod}\ \varphi(N))$.

Іншим можливим способом криптоаналізу алгоритму RSA є безпосереднє обчислення або підбір значення функції $\varphi(N)=(P-1)(Q-1)$. Якщо буде встановлено значення $\varphi(N)$, то співмножники P й Q відносно просто обчислюються.

Нехай:

$$x=P+Q=N+1-\varphi(N);$$

$$y=(P-Q)^2=(P+Q)^2-4N.$$

Знаючи $\varphi(N)$, можна визначити x, а потім y. Знаючи x і y встановлюють числа P і Q із наступних співвідношень:

$$P=\frac{1}{2}\left(x+\sqrt{y}\right) \text{ та } Q=\frac{1}{2}\left(x-\sqrt{y}\right).$$

Однак ця атака не буде простішою за задачу факторизації модуля N.

Задачу факторизації відносять до складу задач, які тяжко розв'язувати коли вона містить великих значення модуля N.

В таблиці 5.1 наведено оцінки довжин ключів для асиметричних криптосистем. Ці оцінки дані для трьох груп користувачів (індивідуальних користувачів, корпорацій і державних організацій), відповідно до вимог щодо їх інформаційної безпеки.

Таблиця 5.1 – Оцінки довжин ключів для асиметричних криптосистем (біт)

Рік	Окремі користувачі	Корпорації	Державні організації
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

Звичайно, подану оцінку варто розглядати у якості приблизної, якій властиві зміни внаслідок можливих тенденцій змін безпечних довжин ключів асиметричних криптосистем згодом.

Криптосистеми RSA реалізуються як апаратним, так і програмним шляхом.

Для апаратної реалізації операцій шифрування і дешифрування RSA розроблені спеціальні процесори. Ці процесори, реалізовані на надвеликих

інтегральних схемах (НВІС), дозволяють виконувати операції RSA, пов'язані із зведенням великих чисел у надвеликий степінь за модулем N, за відносно короткий час. І все-таки апаратна реалізація RSA приблизно в 1000 разів повільніше апаратної реалізації симетричного криптоалгоритма DES.

Одна з найшвидших апаратних реалізацій RSA з модулем 512 біт на надвеликій інтегральній схемі володіє швидкодію у 64 Кбіт/с. Кращими із серійного випуску НВІС є процесори фірми CYLINK, що виконують 1024-бітове шифрування RSA.

Програмна реалізація RSA приблизно в 100 разів повільніша за програмну реалізацію DES. З розвитком технології даним оцінкам властиво змінюватись, але асиметрична криптосистема RSA ніколи не досягне швидкодії симетричних криптосистем.

Слід зазначити, що мала швидкодія криптосистем RSA обмежує область їх застосування, але не анулює їх цінність.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Розробити структуру алгоритму RSA.
2. Реалізувати алгоритм RSA та провести шифрування.

Текст для шифрування	P (к-сть літер)	Q (к-сть літер)
Прізвище здобувача	Ім'я здобувача	По-батькові здобувача

3. Порівняти отримані результати з алгоритмом шифрування DES.
4. Дослідити залежність швидкості роботи програми від об'єму вхідного тексту та оцінити стійкість до криптоаналізу.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які шифри прийнято називати асиметричними? Приклади цих шифрів.
2. Переваги та недоліки асиметричних шифрів.
3. Чим, на практиці, забезпечують криптостійкість алгоритму RSA?
4. Основні області застосування алгоритму RSA.
5. Як визначити найбільший спільний дільник двох чисел?
6. Що таке функція Ейлера?

Рекомендована література: [1-12].

ПРАКТИЧНА РОБОТА №6

Тема: розроблення та дослідження засобів ідентифікації користувачів в комп'ютерних системах.

Мета: оволодіти методикою побудови засобів ідентифікації користувачів.

Завдання: опрацювати теоретичний матеріал, розробити й реалізувати структуру комп'ютерної системи та дати відповіді на запитання.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Ідентифікація об'єкта – це одна із функцій підсистеми захисту. Перед тим, як отримати доступ до комп'ютерної системи, користувач повинен ідентифікувати себе, після чого засоби захисту повинні підтвердити, чи даний користувач є насправді тим, за кого себе видає. Програма ідентифікації призначена для одноразового встановлення особи користувача та надання йому прав доступу в систему. Одним з найпростіших способів ідентифікації є парольна ідентифікація, яка здійснюється шляхом порівняння введеного імені та паролю, із тими які зберігаються у файлі паролів (рис. 6.1).

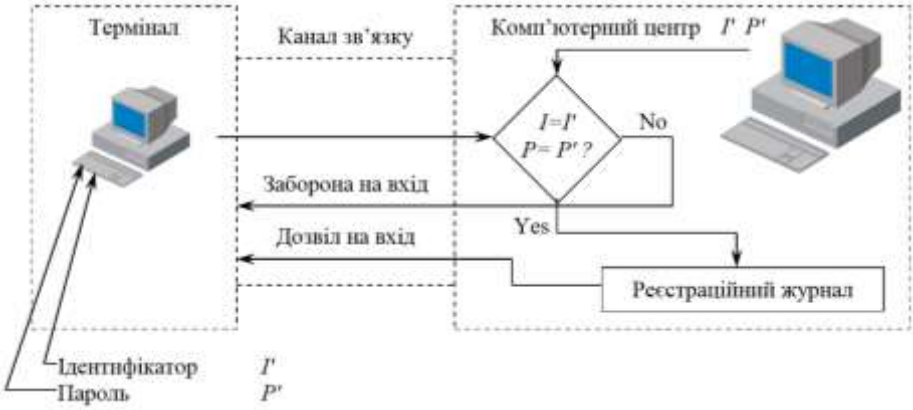

Рисунок 6.1 – Класичний спосіб парольної ідентифікації

Проте такий підхід не захищає комп'ютерну систему від програмних та апаратних засобів сканування клавіатури та ліній передачі, а отже може призвести до витоку конфіденційної інформації. Тому, як правило, в сучасних КС пароль не передається в явній формі по лініях передачі, а натомість в якості паролю використовують якесь його відображення використовуються важко оборотні однонапрямлені функції, застосування яких гарантує неможливість розкриття пароля за його відображенням за розумний час.

В такому випадку процедура ідентифікації описується таким алгоритмом (рис. 6.2).

1. Користувач вводить свій ідентифікатор.
2. Засоби ідентифікації переглядають список зареєстрованих ідентифіка

торів (якщо ідентифікатор не зареєстрований, то виводиться повідомлення, що такий користувач в системі не зареєстрований і далі перехід на крок 1, або ж завершення роботи програми входу в систему; якщо ідентифікатор зареєстрований, то перехід на крок 3).

3. Комп'ютерна система генерує випадкове число x, та обчислює значення важкооборотної однонапрямленої функції y, яка використовується в системі для відображення паролю користувача.

4. Число x передається користувачу.

5. Користувач обчислює значення важкооборотної функції y' та передає його в комп'ютерну систему.

6. Комп'ютерна система порівнює значення y і y' (якщо вони співпадають то така система дозволяє вхід користувача в систему; в іншому випадку видається повідомлення про помилку вводу паролю, перехід на крок 3, або ж завершення роботи програми входу в систему).

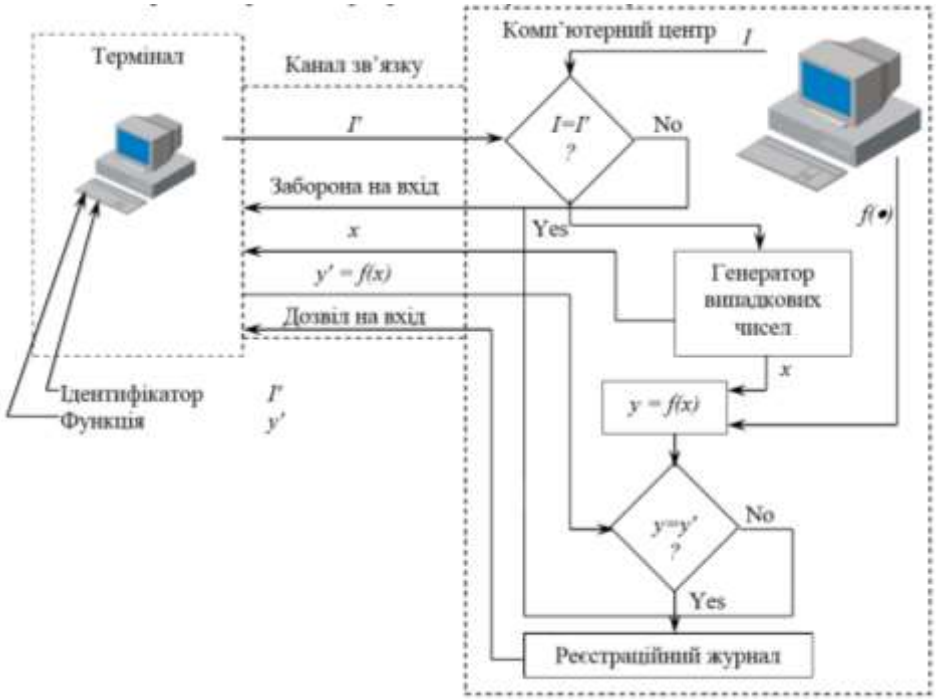

Рисунок 6.2 – Ідентифікація користувача за допомогою важкооборотної функції відображення паролю

Зрозуміло, що стійкість такої комп'ютерної системи до інтерполяції використовуваної функції визначається важкооборотністю функції у та частотою генерації і розподілу ключів в системі.

Іншою важливою складовою частиною комп'ютерної системи є програма реєстрації. Програма реєстрації призначена для реєстрації або видалення користувачів в Реєстраційному журналі системи із наданням їм певних правил доступу. Право реєстрації або видалення належить лише одному користувачу – адміністратору системи. Імена користувачів, їх паролі та права доступу зберігаються в явному вигляді в файлі. Розробник повинен оцінити розмір реєстраційного журналу, виходячи із заданих параметрів. Така інформація буде корисною для оцінки трудомісткості процедур сортування та фільтрування. Крім того, на основі отриманих даних розробник може дати рекомендації адміністратору комп'ютерної системи стосовно регулярності процедур генерування та розподілу ключів.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Розробити структуру заданої комп'ютерної системи та реалізувати її.
2. Провести розрахунки параметрів системи.

Варіант	Кількість користувачів	Кількість реалізованих функцій	Функція криптування пароля
1.	7	>10	ln(a×x)
2.	8	>10	exp(-a×x)
3.	9	>10	a×sin(x)
4.	10	>10	a×ln(x)
5.	8	>10	a/x
6.	7	>10	ln(a/x)
7.	10	>10	x/sin(a)
8.	9	>10	a×sin(1/x)
9.	8	>10	tg(a×x)
10.	7	>10	a×ln(2+x)

3. Розробити необхідне алгоритмічне забезпечення.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Що являє собою ідентифікація користувачів?
2. Види ідентифікації.
3. Парольна ідентифікація.
4. Недоліки класичного способу парольної ідентифікації.
5. Реєстраційний журнал та де його використовують?

Рекомендована література: [1-12].

ПРАКТИЧНА РОБОТА №7

Тема: розроблення та дослідження засобів автентифікації користувачів в комп'ютерних системах.

Мета: оволодіти методикою побудови засобів автентифікації користувачів.

Завдання: опрацювати теоретичний матеріал, розробити й реалізувати структуру комп'ютерної системи та дати відповіді на запитання.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Автентифікація полягає у періодичній (стохастичній) перевірці достовірності ідентифікації користувача. Така процедура проводиться для повторної перевірки користувача. Автентифікація може здійснюватися як апаратними, так і програмними методами за якимись особистими ознаками, чи персональними відомостями користувача.

При апаратній реалізації користувач може бути автентифікованим за певними фізичними ознаками: вага тіла, колір очей, відбитки пальців, геометрія долоні, код ДНК тощо. Окрім того, можуть використовуватись додаткові особисті пристрої: наручні браслети, ключі тощо. Даний вид автентифікації характеризується вищим рівнем надійності, проте є складнішим та дорожчим у використанні, тому він використовується на підприємствах, де необхідно забезпечити високий рівень захисту інформації.

Дешевший варіант автентифікації користувачів полягає у створенні програмних засобів. Резидентна програма періодично з певним кроком часу задає випадковим чином запитання із заздалегідь створеного файлу, або ж випадкові три- , чотири- розрядні десяткові числа. Комп'ютерна система порівнює відповіді з наперед зареєстрованими, або ж обчисленими відповідями, і на основі цього надає, або забороняє роботу користувача. У випадку правильної відповіді за користувачем залишаються його права, а у випадку неправильної відповіді – користувач втрачає права доступу і повинен заново ввійти в систему. Стійкість даного виду автентифікації забезпечується конфіденційністю інформації.

Загальна структура комп'ютерної системи автентифікації користувачів наведено на рисунку 7.1.

Наведемо основні способи автентифікації користувачів:

– наперед визначена інформація, якою може користуватися користувач: пароль, персональний ідентифікаційний номер, домовленість про використання спеціальних закодованих фраз;

– елементи апаратного забезпечення, якими може користуватися

користувач: ключі, магнітні картонки, мікросхеми тощо;

– характерні особисті ознаки користувача: відбитки пальців, рисунок сітківки ока, тембр голосу тощо;

– характерні навики та риси поведінки користувача в режимі реального часу: особливості динаміки та стиль роботи на клавіатурі, прийоми роботи з маніпулятором тощо;

– навики та знання користувачів, обумовлені освітою, культурою, навчанням, вихованням, звичками тощо.

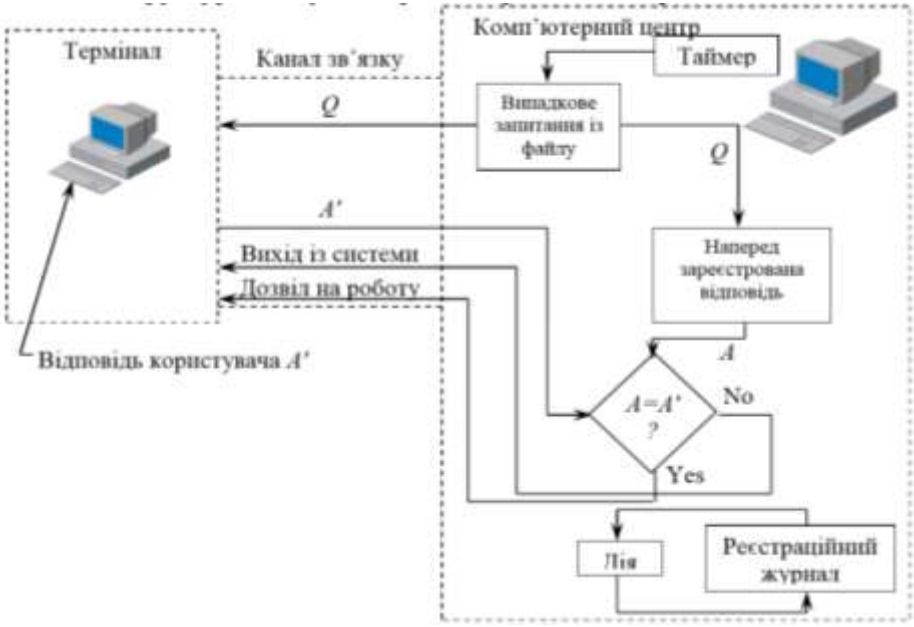

Рисунок 7.1 – Загальна структура комп'ютерної системи автентифікації

Процедура автентифікації користувачів може бути реалізована як з постійним, так і з адаптивним періодом повтору. Постійний період повтору використовується в тих комп'ютерних системах, в яких частота появи користувачів в системі та інтенсивність їх роботи є приблизно рівномірною. При виборі періоду процедури автентифікації слід керуватися такими міркуваннями: при досить великому періоду збільшується імовірність НСД, а при досить малому – зменшується ефективність роботи користувачів, оскільки вони постійно відволікаються від виконання основних своїх обов'язків. В системах, до яких ставляться вимоги підвищеної захищеності можуть застосовуватися

засоби автентифікації з адаптивним періодом повтору. Період повтору в таких комп'ютерних системах визначається як інтенсивністю роботи користувачів, так і спробами НСД.

Окрім того, після встановлення достовірності ідентифікації користувача виконується реєстрація в часі всіх дій користувача в Операційному журналі системи. В такому журналі окрім записів санкціонованого використання тих, чи інших ресурсів системи, можуть накопичуватися дані про спроби несанкціонованого доступу користувачів з автоматичною сигналізацією адміністратору системи для прийняття організаційних заходів з метою виявлення порушників. При створенні операційного журналу необхідно враховувати, що різні типи користувачів мають доступ до різних типів ресурсів.

Для періодичної автентифікації зручно використовувати переривання системного таймера INT 1Ch. Слід пам'ятати, що програма автентифікації повинна заборонити усі інші види переривань.

INT 10h використовується для тимчасового очищення екрану шляхом використання функцій прокрутки, чи перемиканням на іншу відео-сторінку.

INT 1Ah використовується для отримання точних значень системної дати та часу.

ЗАВДАННЯ ДО ПРАКТИЧНОЇ РОБОТИ

1. Розробити структуру заданої комп'ютерної системи та реалізувати її.
2. Провести розрахунки параметрів системи.

Варіант	К-сть запитань	Період повтору процедури автентифікації, хв	К-сть запитань в одній ітерації процедури автентифікації
1.	15	2	3
2.	14	2,5	4
3.	3	7	2
4.	8	3,5	3
5.	9	4	4
6.	10	4,5	2
7.	4	1,5	3
8.	12	5	4
9.	6	1	2
10.	11	5,5	3

3. Розробити необхідне алгоритмічне забезпечення.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Що являє собою автентифікація користувачів?

2. Види автентифікація.
3. Основні способи автентифікації користувачів програмними засобами.
4. Основні способи автентифікації користувачів апаратними засобами.
5. Операційний журнал та з якою метою його використовують?

Рекомендована література: [1-12].

ЛІТЕРАТУРА

1. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
2. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
3. Інформаційна безпека : підруч. / за ред. В. Остроухова. К. : Вид-во Ліра-К, 2021. 412 с.
4. Інформаційна безпека в комп'ютерних мережах : навч. посіб. / за ред. О. А. Смірнов та ін. Кропивницький : Видавець Лисенко В. Ф., 2020. 295 с.
5. Вакалюк Т. А. Захист інформації в комп'ютерних системах. URL: http://eprints.zu.edu.ua/9650/1/1.pdf (дата звернення: 20.08.2024).
6. Гуз А. М. Організація захисту інформації з обмеженим доступом. URL: http://za.inf.ua/bo/oziod18.pdf (дата звернення: 20.08.2024).
7. Заплотинський Б. А. Основи інформаційної безпеки. URL: http://surl.li/pfkpnk (дата звернення: 20.08.2024).
8. Інформаційна безпека / за ред. Ю. Я. Бобала та І. В. Горбатого. URL: http://surl.li/iglfxk (дата звернення: 20.08.2024).
9. Кавун С. В. Носов В. В. Манжай О. В. Інформаційна безпека : навч. посіб. URL: http://surl.li/ikprgx (дата звернення: 20.08.2024).
10. Комплексні системи захисту інформації. URL: http://surl.li/yptezr (дата звернення: 20.08.2024).
11. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації. URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf (дата звернення: 20.08.2024).
12. Пількевич І. А., Лобанчикова Н. М., Молодецька К. В. Захист інформації в автоматизованих системах управління. URL: http://surl.li/znnide (дата звернення: 20.08.2024).

ДЛЯ НОТАТОК

Апаратні та програмні засоби захисту інформації: методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 60 с.

Комп'ютерний набір та верстка: О. Л. Кайдик.

Редактор: в авторській редакції.

Підп. до друку «__» _____ 2025 р.
Формат 60х84/16. Папір офс. Гарн. Таймс.
Ум. друк. арк. 3,8. Обл. – вид. арк. 3,51.
Тираж _50_ прим. Зам. _____.

Луцький національний технічний університет
43018 м. Луцьк, вул. Львівська, 75