ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

Кафедра спеціалізованих комп'ютерних систем

МЕТОДИЧНІ ВКАЗІВКИ

до практичних занять і самостійної роботи з дисципліни

«ТЕОРІЯ КОДУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

Харків – 2019

Методичні вказівки розглянуто і рекомендовано до друку

на засіданні кафедри спеціалізованих комп'ютерних систем 25 лютого 2019 р., протокол № 9.

У методичних вказівках наведено алгоритми та моделі загроз безпеки інформації, розглянуто традиційні алгоритми шифрування для вирішення індивідуальних завдань практичних занять. Тематика занять пов'язана з майбутньою професійною діяльністю студентів і носить прикладний характер.

Призначено для студентів факультету ІКСТ зі спеціальності 123 «Комп'ютерна інженерія» першого освітнього рівня (бакалавр) усіх форм навчання.

Укладач

доц. Є. П. Павленко

Рецензент

проф. С. І. Доценко

МЕТОДИЧНІ ВКАЗІВКИ

до практичних занять і самостійної роботи
з дисципліни

«ТЕОРІЯ КОДУВАННЯ ТА ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

Відповідальний за випуск Павленко Є. П.

Редактор Третьякова К. А.

Підписано до друку 01.04.19 р.

Формат паперу 60х84 1/16. Папір писальний.

Умовн.-друк.арк. 1,25. Тираж 30. Замовлення №

Видавець та виготовлювач Український державний університет залізничного транспорту,
61050, Харків-50, майдан Фейєрбаха, 7.
Свідоцтво суб'єкта видавничої справи ДК № 6100 від 21.03.2018 р.

ЗМІСТ

ВСТУП

Методичні вказівки мають допомогти студенту навчитися використовувати математичний апарат під час розв'язання задач криптографічного захисту даних при їхній передачі в інформаційних і телекомунікаційних системах [1].

Захист інформації – це сукупність заходів і дій, спрямованих на забезпечення її безпеки – конфіденційності і цілісності – в процесі збору, передачі, обробки та зберігання.

Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації негативних джерел, причин і умов впливу на інформацію. Ці джерела становлять загрозу безпеці інформації. Цілі і методи захисту інформації відображують її сутність.

У цьому сенсі захист інформації ототожнюється з процесом забезпечення інформаційної безпеки, як глобальної проблеми безпечного розвитку світової цивілізації, держав, спільноти людей, окремої людини, існування природи.

Криптографія – наука про методи забезпечення конфіденційності (блокування доступу до інформації стороннім) та аутентичності (цілісності і справжності авторства, а також неможливості відмови від авторства) інформації.

Криптоаналіз – наука, що займається питаннями оцінювання сильних і слабких сторін методів шифрування, а також розробленням методів, які дозволяють долати криптографічний захист.

ПРАКТИЧНЕ ЗАНЯТТЯ 1
Аналіз загроз безпеці інформації

Мета заняття – ознайомитися з класифікацією загроз, які можуть привести до порушення політики безпеки інформації, та методами їхнього визначення.

Завдання і порядок виконання

1 Вивчити теоретичний матеріал.

2 Підготувати відповіді на контрольні запитання.

3 Обрати кілька уривків з літературного твору, проаналізувати на предмет загроз та їхніх способів реалізації. Загрози описати у звіті.

Контрольні запитання

1 Які різновиди загроз можна віднести до перехоплення та несанкціонованого доступу?

2 Якими заходами досягається інформаційна безпека?

3 Як забезпечити попередження основних загроз?

Зміст звіту

1 Назва заняття, визначення цілі.

2 Стислий зміст теоретичного матеріалу та відповіді на контрольні запитання.

3 Результати виконання завдання: уривки з літературного твору.

4 Висновки до роботи.

Навчальний матеріал

Поняття «інформаційна безпека» характеризує стан (властивість) інформаційної захищеності людини, суспільства, природи в умовах можливого впливу загроз і досягається системою заходів, спрямованих:

- на попередження загроз. Попередження загроз – це превентивні заходи щодо забезпечення інформаційної безпеки в інтересах попередження можливості їхнього виникнення;
- на виявлення загроз. Виявлення загроз полягає у систематичному аналізі та контролі можливості появи реальних або потенційних загроз і своєчасних заходів щодо їхнього попередження;
- на локалізацію злочинних дій і вжиття заходів щодо ліквідації загрози.

Наведемо декілька прикладів загроз інформаційній безпеці.

Відеоперехоплення здійснюється шляхом використання різної відео- та оптичної техніки з метою отримання інформації з монітора або клавіатури.

Аудіоперехоплення може бути двох видів. При першому у приміщенні встановлюють підслухувальні пристрої. При другому

використовують акустичні та вібраційні датчики зняття інформації – дистанційно направлені мікрофони. Мета цього методу – підслуховування розмов працюючого персоналу та звукових сигналів технічних пристроїв.

«Прибирання сміття» – метод пошуку інформації, залишеної користувачем після роботи за комп'ютером: фізичний варіант – збір використаних роздруківок, викинутих службових паперів та ін.; електронний варіант – збір даних, залишених у пам'яті комп'ютера.

«Абордаж». Хакери проникають до чужої комп'ютерної системи, підбираючи номери, вгадуючи коди та ін. Коли злочинець отримує доступ до комп'ютера, він не може одразу отримати потрібні дані, тому що на корисну інформацію, зазвичай, встановлений пароль доступу. Для реалізації цього способу треба підібрати код. З цією метою використовують спеціальні програми, яким передаються деякі особисті дані (імена, прізвища, номери телефонів), добуті за допомогою інших засобів здійснення комп'ютерних злочинів. З таких даних складаються паролі, тому метод достатньо ефективний.

Крадіжка часу – незаконне використання комп'ютерної системи або мережі без сплати за послуги.

Відкачування даних. Збір інформації, яка потрібна для отримання основних матеріалів, наприклад, технології її проходження в системі. При цьому досліджується не сам зміст інформації, а схеми її руху.

«За хвіст»/робота «між рядків». Перехоплення сигналу, який позначає кінець роботи законного користувача або у проміжках між роботою законного користувача з подальшим здійсненням доступу до системи. Під час роботи користувача виникають «вікна» (наприклад, відгук системи випереджає дії користувача, якому необхідний час для обдумування подальших дій). Ці вікна можна використати для роботи із системою під маскою користувача.

«Неспішний вибір». Несанкціонований доступ до файлів законного користувача здійснюється шляхом знаходження слабих місць у захисті системи. Одного разу виявивши їх, порушник може не поспішаючи досліджувати зміст системи, копіювати його, повертатися до нього багато разів.

«Пролом». На відміну від «неспішного вибору», де шукаються слабкості у захисті системи, при даному способі проводиться пошук проломів, обумовлених помилками або невдалою логікою побудови програми.

«Системні роззяви». Розрахунок на неадекватну перевірку повноважень користувача (імена, коди, шифр-ключі та ін.). Несанкціонований доступ здійснюється знаходженням «пролому» у програмі входу до системи.

«Маскарад» може бути у фізичному або електронному варіантах.

У фізичному варіанті для отримання допоміжної інформації зловмисники видають себе за інших осіб.

В електронному варіанті виконується проникнення до комп'ютерної системи за кодами й іншими ідентифікаційними шифрами законних користувачів.

«Містифікація». Користувач віддаленого терміналу підключається до чиєїсь системи, будучи абсолютно впевненим, що працює з тією системою, з якою мав намір. Власник системи, до якої відбулося фактичне підключення, формуючи правдоподібні відгуки, може підтримувати це помилкове враження протягом певного часу й отримувати деяку інформацію, зокрема коди доступу або дані, які дозволять ідентифікувати користувача.

«Підкласти свиню» здійснюється шляхом під’єднання до каналів зв’язку та імітації роботи системи з метою отримання незаконних маніпуляцій. Наприклад, можна імітувати сеанс зв’язку та отримати дані під виглядом легального користувача.

Програмні закладки – програми, які зберігають інформацію, що вводиться з клавіатури (у тому числі паролі), у зарезервованій для зберігання області. Даний тип програмних зловживань містить:

– закладки, які асоціюються з програмно-апаратним середовищем (BIOS);

– закладки, які асоціюються з програмами первинного завантаження (з Master Boot Record або Root-секторів активних розділів);

– закладки, які асоціюються із завантаженням драйверів, командного інтерпретатора, мережних драйверів;

– виконувані модулі, які мають тільки код (впроваджені у пакетні файли типу .bat);

– модулі-імітатори, які співпадають за зовнішнім виглядом з програмами, що потребують введення конфіденційної інформації;

– закладки, замасковані під програмні засоби оптимізаційного призначення (архіватори, прискорювачі та ін.).

Несанкціонований доступ – найбільш поширений вид комп'ютерних порушень. Він полягає в отриманні користувачем (працівником організації) доступу до об'єкта, на який у нього немає дозволу відповідно до прийнятої в організації політики безпеки. Зазвичай найголовніша проблема – визначити, хто і до яких наборів даних повинен мати доступ.

Незаконне використання привілеїв. Зловмисники, які застосовують даний спосіб атаки, зазвичай використовують штатне програмне забезпечення, що функціонує у позаштатному режимі. Незаконне захоплення привілеїв можливе або за наявності помилок у самій системі захисту, або у випадку недбалості при керуванні системою і привілеями.

Подолання програмних засобів захисту. Це допоміжний спосіб вчинення злочину. Він є умисним подоланням системи захисту. Існує кілька різновидів даного способу.

Створення копії ключового носія. Для запуску деяких систем потрібен ключовий носій, на якому записані необхідні системні файли. Злочинець може незаконно створити копію такого носія. Пізніше це допоможе йому потрапити до потрібної системи або встановити таку систему на власному ПК.

Модифікація коду системи захисту. Модифікуючи цей код, злочинець обходить функції системи захисту. Даний спосіб може бути реалізований тільки висококласним фахівцем, що має досвід у цій справі. Час обходу системи захисту може обчислюватися тижнями.

Програма – «шукач» – приховане перехоплення паролів користувачів під час їхньої реєстрації. Оскільки користувачі часто оперують одним і тим самим паролем у більш, ніж одній комп'ютерній системі, оволодіння паролем користувача часто дає злочинцеві можливість легкого доступу до іншої комп'ютерної системи, в якій цей користувач має рахунки.

Анонімайзер – засіб для приховування інформації про комп'ютер або користувача у мережі від віддаленого сервера. Сфера використання анонімайзерів сьогодні змістилася від забезпечення конфіденційності інформації про користувача у бік надання доступу до заборонених у мережі веб-сайтів.

«Троянський кінь». Таємне введення до чужого програмного забезпечення навмисне створених програм або блоку команд, які дозволяють здійснити нові, не заплановані власником програмні функції, але одночасно зберігати і колишню працездатність.

«Логічна бомба». Таємне вбудовування до програми користувача іншої програми або блоку команд, які повинні спрацювати за певних логічних умов. При цьому «бомба» автоматично ліквідується після виконання заданого зловмисником алгоритму.

«Часова бомба» – різновид «логічної бомби», яка спрацьовує при досягненні певного моменту часу.

Комп'ютерні віруси – це невеликі виконувані або інтерпретовані програми, що мають властивість несанкціонованого користувачем поширення і самовідтворення в комп'ютерах або комп'ютерних мережах.

В отриманих копіях також є ця можливість.

Вірус може бути запрограмований на зміну чи знищення програмного забезпечення або даних, що зберігаються на об'єктах і пристроях комп'ютерної мережі.

У процесі поширення віруси можуть себе модифікувати.

«Черви» – різновид програми-віруса, що поширюється по глобальній мережі. «Черв'як» розмножується (відтворює себе), заражаючи інші файли. Він впроваджується один раз на конкретний комп'ютер і шукає способи поширитися далі на інші комп'ютери. Різновиди: Net-Worm (мережний черв'як), Email-Worm (поштовий черв’як).

Backdoor (бекдор) – шкідлива програма, призначена для прихованого керування зловмисником ураженого комп'ютера.

За своєю функціональністю бекдори багато в чому нагадують різні системи адміністрування, що розробляються фірмами-виробниками програмних продуктів.

Наведемо уривки з творів Агати Крісті, які містять опис загроз.

«Твої листи останнім часом так змінилися. Я стала боятися – що, якщо ти розлюбив мене? Але це неможливо. Яка я дурепа – завжди щось вигадую. А якщо ти дійсно розлюбив мене, я не знаю, що зроблю, може, вб'ю себе! Я не зможу жити без тебе. Іноді мені здається, що між нами стала інша жінка. Нехай вона побережеться! І ти теж!» (абордаж або злам).

«- Справа ось якого роду, міс Екройд. Паркер говорить, що бачив, як ви вийшли з кабінету вашого дядька приблизно за чверть десята. Це так?

- Так. Я заходила побажати йому спокійної ночі.
- Ваш дядько був один?
- Так. Доктор Шепард вже вийшов.
- Ви не помітили, чи було відкрито вікно?
- Не знаю. Фіранки були спущені.
- Так. А ваш дядько поводився як зазвичай?
- Ніби.» (відкачування даних).

ПРАКТИЧНЕ ЗАНЯТТЯ 2
Моделі загроз інформаційній безпеці комп'ютерної системи

Мета заняття – аналіз загроз і каналів витоку інформації в комп'ютерній системі, аналіз можливостей, які може мати порушник.

Завдання і порядок виконання

1 Вивчити теоретичний матеріал.

2 Підготувати відповіді на контрольні запитання.

3 Для обраного програмного продукту скласти модель загроз інформаційній безпеці, зробити опис загроз безпеці, методів боротьби, провести оцінювання ризику.

Контрольні запитання

1 Визначити поняття «інформаційна безпека».

2 Хто є суб'єктами інформаційних відносин?

3 Дайте визначення конфіденційності інформації.

4 На що спрямовані загрози порушення конфіденційності інформації?

Зміст звіту

1 Назва заняття, визначення мети.

2 Стислий зміст теоретичного матеріалу та відповіді на контрольні запитання.

3 Опис загроз безпеці, методів боротьби, оцінювання ризику.

Навчальний матеріал

Найбільш загальними ознаками захисту будь-якого виду інформації, що охороняється, є такі:

- захист інформації організовує і проводить власник інформації або уповноважені ним на те особи (юридичні або фізичні);
- захистом інформації власник охороняє свої права на володіння і розпорядження інформацією, прагне захистити її від незаконного заволодіння та використання на шкоду його інтересам;
- захист інформації здійснюється шляхом проведення комплексу заходів з обмеження доступу до інформації, що захищається, і створення умов, що виключають або істотно ускладнюють несанкціонований доступ до інформації.

Інформаційна загроза – потенційна можливість неправомірного або випадкового впливу на об'єкт захисту, що призводить до втрати або розголошення інформації.

Поряд з аналізом потенційно можливих загроз бажано провести й аналіз ризиків від реалізації цих загроз, тому що даний аналіз дозволяє визначити найбільш значущі загрози з усіх можливих загроз і засоби захисту від них.

Процес аналізу ризиків включає до себе:

– оцінювання можливих втрат через успішно проведені атаки на безпеку інформації;

– оцінювання ймовірності виявлення вразливих місць комп’ютерної системи, яка впливає на оцінювання можливих втрат;

– вибір оптимальних за витратами заходів і засобів захисту, які скорочують ризик до прийнятного рівня.

З метою підвищення ефективності аналізу ризиків він проводиться за різними напрямками:

– для процесів, процедур і програм обробки інформації;

– для каналів зв'язку;

– для побічних електромагнітних випромінювань;

– для механізмів керування системою захисту.

Аналіз ризиків передбачає вивчення і систематизацію загроз захисту інформації, а також визначення вимог до засобів захисту. Вивчення і систематизація загроз передбачає такі етапи:

– вибір об'єктів та інформаційних ресурсів, для яких буде проведено аналіз;

– розроблення методології оцінювання ризику;

– аналіз загроз і визначення слабких місць у захисті;

– ідентифікацію загроз і формування списку загроз;

– формування детального списку загроз або інформаційних ресурсів.

Для побудови надійного захисту необхідно виявити можливі загрози безпеки інформації, оцінити їхні наслідки, визначити необхідні заходи і засоби захисту, оцінити їхню ефективність. Різноманітність потенційних загроз настільки велика, що не дозволить передбачити кожну з них, тому аналізовані види доречно обирати з позицій здорового глузду, одночасно виявляючи не тільки загрози, ймовірність їхнього здійснення, масштаб потенційної шкоди, а також їхні джерела.

Для класифікації загроз безпеки може бути використана класифікація, яка називається STRIDE, за першими літерами англійських назв категорій:

1 Підміна мережних об'єктів (Spoofing identity). Атаки подібного типу дозволяють зламникові видавати себе за іншого користувача або підміняти реальний сервер підробленими. Приклад підміни особистості користувача – використання чужих аутентифікаційних даних (імені користувача, пароля) для атаки на систему. Типовий приклад подібного зламу – застосування ненадійних методів аутентифікації.

2 Модифікація даних (Tampering with data). Атаки цього типу передбачають зловмисне псування даних. Приклади: несанкціоновані зміни постійних даних (наприклад, тих, які зберігаються у базі даних); інформації, яка пересилається між комп'ютерами через відкриту мережу (наприклад, Інтернет).

3 Відмова від авторства (Repudiation). Контрагент відмовляється від вчиненої ним дії (або бездіяльності), користуючись тим, що в іншої сторони нема жодного способу

довести зворотне. Наприклад, у системі, де не ведеться аудит, користувач може виконати заборонену операцію і відмовитися від її «авторства», а адміністраторові не вдасться нічого довести. Неможливість заперечення авторства (nonrepudiation) – це здатність системи опиратися такій небезпеці.

4 Розголошення інформації (Information disclosure). Мається на увазі розкриття інформації особам, доступ яким заборонений, наприклад, прочитання користувачем файла, доступ до якого йому не надавався, а також здатність зловмисника зчитувати дані при передачі між комп'ютерами.

5 Відмова в обслуговуванні (Denial of service). В атаках такого типу зламник намагається позбавити доступу до сервісу правомочних користувачів, наприклад, зробивши Web-сервер тимчасово недоступним або непридатним для роботи. Необхідно захищатися від певних видів DoS-атак – це підвищить доступність і надійність системи.

6 Підвищення привілеїв (Elevation of privilege). У даному випадку непривілейований користувач отримує привілейований доступ, який дозволяє йому «зламати» або навіть знищити систему. До підвищення привілеїв відносяться і випадки, коли зловмисник вдало проникає через захисні засоби системи і стає частиною захищеної і довіреної підсистеми.

Для вибору одного із запропонованих методів бажано виконати кількісне оцінювання ризику небезпеки для конкретної обчислювальної системи. Зазвичай застосовують такі методи кількісного оцінювання ризику:

1 Етап оцінювання ризику (Risk) – помножити важливість (розмір потенційного збитку) уразливого місця на ймовірність того, що ним скористаються. Критичність і ймовірність оцінюють за шкалою від 1 до 10:

<Risk> = <Потенційний збиток> * <Імовірність виникнення>,

чим більше отримане число, тим більше загроза системі. Так, максимально можлива оцінка ризику дорівнює 100 – добуткові максимальної важливості (10) і ймовірності виникнення (10).

2 Етап оцінювання ризику DREAD, що називається так за першими літерами англійських назв описаних далі категорій:

– потенційний збиток (Damage potential) – міра реального збитку від успішної атаки. Найвищий ступінь (10) небезпеки означає практично безперешкодний злам засобів захисту і виконання практично будь-яких операцій. Підвищенню привілеїв зазвичай привласнюють оцінку 10. В інших ситуаціях оцінка залежить від цінності даних, які захищають;

– відтворюваність (Reproducibility) – міра можливості реалізації небезпеки. Деякі проломи доступні постійно (оцінка – 10), інші – тільки залежно від ситуації, та їхня доступність не є передбачуваною, тобто не можна напевно знати, наскільки успішною виявиться атака. Проломи у встановлених за замовчуванням функціях характеризуються високою відтворюваністю;

– схильність до зламу (Exploitability) – міра зусиль і кваліфікації, необхідної для атаки. Якщо її може реалізувати недосвідчений програміст на домашньому комп'ютері – 10. Якщо для її проведення треба витратити 100 000 000 доларів, оцінка небезпеки – 1. Атака, для якої можна написати алгоритм (тобто розповсюдити у вигляді сценарію серед любителів), оцінюється у 10 балів. Слід також враховувати необхідний для атаки рівень аутентифікації та авторизації у системі. Наприклад, якщо це доступно будь-якому віддаленому анонімному користувачеві, подібна небезпека оцінюється 10 балами;

– коло користувачів, які потрапляють під удар (Affected users) – частка користувачів, робота яких порушується через успішну атаку. Оцінювання виконується на основі відсоткової частки: 100 % всіх користувачів відповідає оцінка 10, а 10 % – 1 бал. Іноді небезпека стає реальною тільки у системі, яка сконфігурована особливим чином. Надзвичайно важливо проводити межу між сервером і клієнтським комп'ютером: від шкоди, завданої серверові, постраждає більше клієнтів і, можливо, інші мережі. У такому випадку бал значно вище, ніж оцінка атаки тільки на клієнтські комп’ютери. Також не слід забувати про розміри ринку й абсолютну, а не тільки відсоткову кількість користувачів;

– ймовірність виявлення (Discoverability) – найскладніша для визначення оцінка. Зазвичай будь-яка небезпека піддається реалізації, тому можна ставити завжди 10 балів. Сумарна DREAD-оцінка дорівнює арифметичному середньому всіх оцінок.

ПРАКТИЧНЕ ЗАНЯТТЯ 3
Основи інформаційної безпеки. Традиційні алгоритми шифрування

Мета заняття – ознайомлення з основними підходами до шифрування інформації як частини системи інформаційної безпеки організацій; вивчення найбільш ранніх відомих алгоритмів шифрування: Скітала, магічні квадрати, полібіанські квадрати для захисту інформації від несанкціонованого ознайомлення.

Завдання та порядок виконання

1 Вивчити теоретичний матеріал.

2 Підготувати відповіді на контрольні запитання.

3 Виконати шифрування заданого відкритого тексту із застосуванням шифру Скітала, проаналізувати можливість його розкриття.

4 Виконати шифрування заданого відкритого тексту із застосуванням магічного квадрата, проаналізувати можливість його розкриття.

5 Виконати шифрування заданого відкритого тексту із застосуванням полібіанського квадрата, проаналізувати можливість його розкриття.

6 Виконати шифрування заданого відкритого тексту із застосуванням шифру Playfair, проаналізувати можливість його розкриття.

Контрольні запитання

1 Чим обумовлена актуальність проблеми інформаційної безпеки у спеціалізованих комп’ютерних системах?

2 В чому відмінність таких понять, як доступність інформації та доступ до інформації?

3 В чому суть застосування адміністративно-організаційних, фізичних і програмно-технічних засобів у організації політики безпеки підприємства?

4 В чому суть застосування шифру Скітала. Які він має переваги та недоліки?

5 В чому суть застосування шифру на полібіанському квадраті. Які він має переваги та недоліки?

Зміст звіту

1 Назва заняття, визначення мети.

2 Стислий зміст теоретичного матеріалу та відповіді на контрольні запитання.

3 Вхідний текст і результати шифрування.

4 Висновки до заняття.

Навчальний матеріал

Забезпечення інформаційної безпеки

Одним із засобів керування інформаційною безпекою є розробка політики безпеки [1, 2], яка являє собою сукупність норм, правил і практичних рекомендацій, що регламентують роботу засобів захисту комп'ютерної системи від заданої множини загроз безпеки. Політика інформаційної безпеки залежить від засобу керування доступом, який визначає порядок доступу до об'єктів спеціалізованих комп'ютерних систем.

Для регламентації прав доступу до ресурсів чи компонентів систем розробляються правила розподілу доступу. Властивість ресурсів бути доступними для законних користувачів комп'ютерних систем називається доступністю.

Підхід до забезпечення інформаційної безпеки може бути фрагментарним чи комплексним. Фрагментарний підхід направлений на протидію певним загрозам в заданих умовах. Прикладом реалізації цього підходу можуть бути автономні засоби шифрування, спеціалізовані антивірусні програми, засоби керування доступом. Перевагою фрагментарного підходу є висока чутливість до конкретної загрози. Використання фрагментарного підходу виправдано для необхідності захисту конкретного об'єкта інформаційної системи від конкретної загрози.

Комплексний підхід направлений на створення захищеного середовища в межах всієї системи шляхом об'єднання в єдиний комплекс заходів протидії усім виявленим загрозам. Наявність захищеного середовища дозволяє гарантувати певний рівень безпеки системи, що є перевагою комплексного підходу. Недоліком цього підходу є обмеження на свободу дій

користувачів системи, чутливість до помилок налаштування та установлення засобів захисту. Комплексний підхід застосовується, коли порушення інформаційної безпеки може привести до суттєвої матеріальної шкоди організації чи її клієнтам. Тому комплексного підходу дотримується більшість державних і великих комерційних підприємств. Політика безпеки реалізується шляхом сумісного застосування адміністративно-організаційних і програмно-технічних заходів.

Для конкретної системи політика безпеки носить індивідуальний характер і залежить від технології обробки інформації, що використовується.

Залежно від порядку доступу до об'єктів системи існує два види політики безпеки: вибірковий і мандатний. Вибіркова політика базується на вибірковому керуванні доступом, яке задається адміністратором у вигляді множини дозволених відносин доступу. Для формального опису множини дозволених відносин використовується матриця доступу, в якій стовпці відповідають об'єктам системи (ресурсам), рядки – суб'єктам (користувачам), а на їхньому перетині вказується тип дозволеного доступу суб'єкта до об'єкта (читання, запис, виконання). Вибіркова політика доступу, як правило, застосовується у комерційному секторі, тому що її реалізація відповідає вимогам комерційних організацій з розподілу доступу та підзвітності.

Мандатний спосіб керування доступом характеризується сукупністю правил надання доступу, заданих на множині атрибутів безпеки об'єктів і суб'єктів системи, наприклад, залежно від мітки конфіденційності інформації та рівня допуску користувача. Для застосування даної політики необхідно виконання таких умов:

- наявність засобів надійної ідентифікації усіх об'єктів і суб'єктів системи;
- кожен об'єкт повинен мати мітку конфіденційності, що визначає цінність інформації, яка міститься в ньому;
- кожен суб'єкт повинен мати певний рівень допуску, що характеризує максимальне значення мітки конфіденційної інформації об'єктів, до яких цей суб'єкт має доступ.

Найбільш захищеними стають об’єкти з високими значеннями мітки конфіденційності. Регулювання доступу суб’єктів системи до об’єктів з різними рівнями конфіденційності унеможливлює відплив інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування проникнень з нижніх рівнів на верхні.

Шифр Скітала

Найстаріші з відомих засобів шифрування повідомлень засновані на використанні шифру Скітала, магічних і полібіанських квадратів.

Шифр Скітала базується на використанні найпростішої шифрувальної таблиці у вигляді прямокутника (таблиця 1). Букви відкритого тексту заносяться до таблиці по рядках (наприклад: криптографічний шифр), а зчитуються (шифрований текст) по стовпцях (наприклад: ргчширнипаифтфйр).

Таблиця 1 – Шифр Скітала

к	р	и	п	т
о	г	р	а	ф
і	ч	н	и	й
	ш	и	ф	р

Магічні квадрати

Магічними квадратами називаються квадратні таблиці із вписаними до них клітинок послідовними натуральними числами, починаючи з 1, які в сумі по кожному стовпцю, кожному рядку і кожній діагоналі дають одне і те саме число.

Магічні квадрати широко застосовувалися для передачі секретної інформації. При шифруванні вихідне повідомлення вписувалося у квадрат за наведеною в ньому нумерацією, після чого шифрограма виписувалась по рядках. Кількість можливих магічних квадратів (ключів) швидко зростає зі збільшенням їхнього розміру. Так, існує лише один магічний квадрат розміром 3х3, якщо не брати до уваги його повороти. Магічних квадратів 4х4 налічується вже 880, а розміром 5х5 – близько 250000. Тому магічні квадрати великих розмірів могли бути хорошою основою для надійної системи шифрування того часу, тому що ручне

перебирання всіх варіантів ключа для цього шифру було немислиме.

Розглянемо квадрат розміром 4х4 (таблиця 2). До нього вписуються числа від 1 до 16. Його магія полягає в тому, що сума чисел по рядках, стовпцях і повних діагоналях дорівнює одному й тому числу – 34.

Таблиця 2 – Магічний квадрат 4х4

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Шифрування за магічним квадратом виконується таким чином. Наприклад, потрібно зашифрувати фразу «шифрований текст ...» (таблиця 3). Букви цієї фрази вписуються послідовно до квадрата згідно з записаними до нього числами: позиція букви в тексті відповідає порядковому числу. У порожніх клітинах ставиться крапка або будь-яка буква.

Таблиця 3 – Приклад шифрування за допомогою магічного квадрата

16 с	3 ф	2 и	13 т
5 о	10 й	11	8 н
9 и	6 в	7 а	12 н
4 р	15 к	14 е	1 ш

Після цього шифрований текст записується в рядок (зчитування проводиться зліва направо зверху вниз, по рядках) – «сфитой ниванркеш».

Полібіанські квадрати

Шифр винайдено грецьким державним діячем, полководцем і істориком Полібієм (203-120 рр. до н. е.). Стосовно кирилиці та індійських (арабських) цифр суть шифрування полягала в такому.

У квадрат 6х6 виписуються букви (не обов'язково в алфавітному порядку) (таблиця 4).

Таблиця 4 – Шифрозаміни для полібіанського квадрата

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	-	-	-

Буква, що шифрується, замінюється на координати квадрата (рядок-стовпець), в якому вона записана. Наприклад, якщо вихідне повідомлення «студент», то шифрограма – «41 42 43 15 16 33 42».

Одним із суттєвих недоліків шифрів однозначної заміни є те, що їх легко відкрити. При розтині шифрограми використовуються різні прийоми, які навіть при відсутності потужних обчислювальних засобів дозволяють домогтися позитивного результату. Один з таких прийомів базується на тому, що в шифрограмі залишається інформація про частоту букв вихідного тексту. Якщо у відкритому повідомленні часто зустрічається будь-яка буква, то в зашифрованому повідомленні також часто буде зустрічатися відповідний їй символ. Для різних мов світу існують подібні таблиці. Так, наприклад, нижче наведено таблицю для букв кирилиці (таблиця 5).

Таблиця 5 – Частота появи букв кирилиці в текстах

Номер п/п	Буква	Частота, %	Номер п/п	Буква	Частота, %
1	О	10.97	18	Ь	1.74
2	Е	8.45	19	Г	1.70
3	А	8.01	20	З	1.65
4	И	7.35	21	Б	1.59
5	Н	6.70	22	Ч	1.44

Існують подібні таблиці для пар букв (біграм). Наприклад, часто зустрічаються біграми є «по», «но», «ст», «па», «ен» і т. д.

Інший прийом розкриття шифрограми заснований на виключенні можливих поєднань букв. Наприклад, в текстах (якщо вони написані без орфографічних помилок) не можна зустріти поєднання «чя», «щш», «ь'» і т. п.

Поліграмні шифри

Шифр Playfair (з англ. «чесна гра») став першим літерним біграмним шифром; був призначений для забезпечення секретності телеграфного зв'язку.

Він передбачає шифрування пар символів (біграм). Таким чином, цей шифр більш стійкий до злому в порівнянні з шифром простої заміни, бо важко виконати частотний аналіз; може бути проведений, але не для 26 можливих символів (латинський алфавіт), а для 26 х 26 = 676 можливих біграм. Аналіз частоти біграмм можливий, але є значно важчим і вимагає набагато більшого обсягу зашифрованого тексту.

Для шифрування повідомлення необхідно розбити його на біграми (групи з двох символів), при цьому якщо в біграмі зустрінуться два однакових символи, то між ними додається заздалегідь обумовлений допоміжний символ (в оригіналі – X, для кирилиці – Я). Наприклад, «зашифроване повідомлення» стає «за ши фр ов ан еп ов ід ом ле ня ня». Для формування ключової таблиці вибирається гасло і далі вона заповнюється шляхом вписування букв алфавіту, що залишилися. Нижче наведено ключову таблицю для гасла «Футбол» (таблиця 6).

Таблиця 6 – Ключова таблиця для шифру Playfair

Ф	У	Т	Б	О	Л
А	В	Г	Д	Е	Є
Ж	З	И	Ї	Й	К
Л	М	Н	П	Р	С
Х	Ц	Ч	Ш	Щ	Ь
Ю	Я	‘	-	1	2

Потім, керуючись такими правилами, виконується зашифрування пар символів вихідного тексту.

1 Якщо символи біграми вихідного тексту зустрічаються в одному рядку, то вони заміщуються на символи, розташовані в найближчих стовпцях праворуч від відповідних символів. Якщо символ є останнім в рядку, то він замінюється на перший символ цього ж рядка.

2 Якщо символи біграми вихідного тексту зустрічаються в одному стовпці, то вони перетворюються у символи того ж стовпця, що знаходяться безпосередньо під ними. Якщо символ є нижнім у стовпці, то він замінюється на перший символ цього ж стовпця.

3 Якщо символи біграми вихідного тексту знаходяться в різних стовпцях і різних рядках, то вони замінюються на символи, що знаходяться в тих же рядках, але відповідають іншим кутам прямокутника.

Приклад шифрування:

- біграма «за» формує прямокутник – замінюється на «вж»;
- біграма «ти» знаходиться в одному стовпці – замінюється на «гн»;
- біграма «ве» знаходиться в одному рядку – замінюється на «гє».

Для розшифрування необхідно використовувати інверсію цих правил, відкидаючи символи Я (або Х), якщо вони не несуть сенсу в початковому повідомленні.

ПРАКТИЧНЕ ЗАНЯТТЯ 4
Шифри перестановки

Мета заняття – ознайомлення з основами підходу до шифрування інформації за допомогою алгоритмів перестановок; вивчення варіантів застосування відомого алгоритму шифрування за допомогою шифру Цезаря.

Завдання і порядок виконання

1 Вивчити теоретичний матеріал.

2 Підготувати відповіді на контрольні запитання.

3 Вивчити принцип побудови і технологію застосування шифру Цезаря. Виконати завдання з шифрування, проаналізувати й обговорити складність використання і розкриття шифру Цезаря.

4 Вивчити принцип побудови і технологію застосування шифру простої одинарної перестановки. Виконати завдання з шифрування, проаналізувати й обговорити складність використання і розкриття шифру та.

5 Вивчити принцип побудови і технологію застосування шифру блочної одинарної перестановки. Виконати завдання з шифрування, проаналізувати й обговорити складність використання і розкриття шифру.

6 Вивчити принцип побудови і технологію застосування шифру табличної маршрутної перестановки. Виконати завдання з шифрування, проаналізувати й обговорити складність використання і розкриття шифру.

Контрольні запитання

1 Яким чином виконується шифрування повідомлень за шифром Цезаря? Складіть і поясніть алгоритм дій для використання шифру Цезаря.

2 Яким чином виконується шифрування повідомлень за шифром простої одинарної перестановки?

3 Яким чином виконується шифрування повідомлень за шифром блочної одинарної перестановки?

4 Яким чином виконується шифрування повідомлень за шифром табличної маршрутної перестановки?

Зміст звіту

1 Назва заняття, визначення мети.

2 Стислий зміст теоретичного матеріалу та відповіді на контрольні запитання.

3 Результати виконання завдання: вихідне повідомлення, алгоритм шифрування, зашифроване повідомлення.

4 Висновки до заняття.

Навчальний матеріал

Шифри заміни

При шифруванні заміною (підстановкою) символи вихідного пакета замінюються символами того самого або іншого алфавіту за заздалегідь установленим правилом. Залежно від того

використовується один або кілька алфавітів, розрізняють просту (одноалфавітну) заміну й багатоалфавітну.

Відкритий текст x_0, x_1... x_{n-1} шифрується заміною за допомогою ключа $k = \{\pi_0, \pi_1..., \pi_{n-1}\}$, в результаті чого до каналу зв'язку надходить шифротекст y_0, y_1, ..y_{n-1} , тобто

$$(y_0, y_1, ..y_{n-1}) = Ek(x_0, x_1... x_{n-1}). \quad (1)$$

Якщо для шифрування кожного символу x_i, i=0, n-1, використовується той самий ключ, то має місце проста заміна, тобто π_i = const.

Коли ж $y_i = \pi_i(x_i)$, тобто π_i = var, то йдеться про багатоалфавітну заміну.

Класичний приклад простої заміни – шифр Цезаря. Шифрування виконується відповідно до такого правила:

$$y_i = Eк(x_i); \quad 0 \le i \le n-1 \quad (2)$$

$$Eк: t \rightarrow (t+к) \bmod m, \ 0 \le до < m \quad (3)$$

де t – числовий код символу вихідного тексту;

t+к – числовий код символу шифротексту;

m – кількість символів алфавіту.

У цьому випадку має місце сімейство одноалфавітних замін для обраних значень ключа k.

Розвитком шифрування за Цезарем є використання афінних шифрів.

Криптоперетворення в цьому випадку має такий вигляд:

$$E_{a,b}: t \rightarrow (at+b) \bmod m, \quad (4)$$

де a, b – цілі числа; 0 <a, b <m; НОД (a, m) = 1.

Слід зазначити, що вимога взаємної простоти чисел a та m є умовою того, що $E_{a,b}(t)$ є взаємно однозначним відображенням на множині Z_m.

Основні недоліки шифрів простої заміни:

- відсутність маскування частоти появи букв вихідного алфавіту;
- мала кількість ключів.

Внаслідок цього шифри простої заміни легко розкриваються і сьогодні у чистому вигляді не застосовуються.

Шифр Цезаря

Даний шифр використовувався Гаєм Юлієм Цезарем для секретного листування зі своїми генералами (I ст. до н. е.). Стосовно української мови суть його полягає в такому. Виписується вихідний алфавіт (А, Б, ..., Я), потім під ним – той же алфавіт, але з циклічним зрушенням на 3 букви вліво (таблиця 7).

Таблиця 7 – Шифрозаміни для шифру Цезаря

А	Б	В	Г	Д
Г	Д	Е	Є	Ж

При зашифруванні буква А замінюється буквою Г, Б – на Д і т. д.

Одержувач повідомлення шукає ці букви в нижньому рядку і по буквах над ними відновлює вихідне повідомлення.

Шифри одинарної перестановки

У загальному випадку для даного класу шифрів при шифруванні і дешифруванні використовується таблиця перестановок (таблиця 8).

Таблиця 8

1	2	3	…	n
I_1	I_2	I_3	…	I_n

У першому рядку цієї таблиці вказується позиція символу у вихідному повідомленні, а в другому – його позиція у шифрограмі. Таким чином, максимальна кількість ключів для шифрів перестановки дорівнює n!, де n – довжина повідомлення.

Шифр простої одинарної перестановки

Для шифрування і дешифрування застосовується таблиця перестановок (таблиця 9), аналогічна показаній в таблиці 7.

Таблиця 9 – Перестановки

1	2	3	4	5	6
2	4	1	3	6	5

Наприклад, якщо для шифрування вихідного повідомлення «ФУТБОЛ» використовувати таблицю 6, то шифрограмою буде «ТФБУЛО». Для використання на практиці такий шифр незручний, бо при великих значеннях n доводиться працювати з довгими таблицями і для повідомлень різної довжини необхідно мати свою таблицю перестановок.

Шифр блокової одинарної перестановки

При використанні цього шифру задається таблиця перестановки блока символів, яка послідовно застосовується до тих пір, поки вихідне повідомлення не закінчиться. Якщо вихідне повідомлення не кратне розміром блоку, тоді воно при шифруванні доповнюється довільними символами (таблиця 10).

Таблиця 10 – Перестановки для шифру блокової одинарної перестановки

1	2	3
2	3	1

Для прикладу виберемо розмір блока, що дорівнює 3, і приймемо перестановки, показані в таблиці 7. Вихідне повідомлення – «ФУТБОЛ». В результаті шифрування отримаємо «УТФОЛБ».

Кількість ключів для даного шифру при фіксованому розмірі блока дорівнює m!, де m – розмір блока.

Шифри маршрутної перестановки

Широке поширення отримали шифри перестановки, які використовують деяку геометричну фігуру (плоску або об'ємну).

Перетворення полягають у тому, що у фігуру вихідний текст вписується за одним маршрутом, а виписується за іншим. Деякі з них наводяться нижче.

Шифр табличної маршрутної перестановки

Найбільшого поширення набули шифри маршрутної перестановки, засновані на таблицях. При шифруванні в таку таблицю вписують вихідне повідомлення за певним маршрутом, а виписують (отримують шифрограму) – за іншим. Для даного шифру маршрути вписування і виписування, а також розміри таблиці є ключем.

Наприклад, вихідне повідомлення вписується у прямокутну таблицю розмірами 4х6, маршрут вписування – зліва направо і зверху вниз, маршрут виписування – зверху вниз і зліва направо.

ПРАКТИЧНЕ ЗАНЯТТЯ 5
Шифрування за допомогою методів віженера та гамування

Мета заняття – ознайомлення з основами підходу до шифрування інформації за допомогою алгоритмів багатоалфавітних підстановок; вивчення варіантів застосування алгоритму шифрування повідомлень за допомогою шифру Віженера; ознайомлення з основами побудови та використання гами для шифрування і розшифрування даних.

Завдання і порядок виконання

1 Вивчити теоретичний матеріал.

2 Підготувати відповіді на контрольні запитання.

3 Вивчити принцип побудови і технологію застосування шифру Віженера. Виконати завдання з шифрування, проаналізувати й обговорити складність використання і розкриття шифру Віженера.

4 Вивчити принцип побудови і технологію застосування методу гамування. Виконати завдання з шифрування, проаналізувати й обговорити складність використання шифру.

Контрольні запитання

1 В чому полягає шифрування за методом Віженера?

2 Що таке багатоалфавітна заміна?

3 Чим досягається підвищення криптостійкості багатоалфавітного шифрування?

4 Що таке гамування?

Зміст звіту

1 Назва заняття, визначення мети.

2 Стислий зміст теоретичного матеріалу та відповіді на контрольні запитання.

3 Результати виконання завдання: вихідне повідомлення, алгоритм шифрування, зашифроване повідомлення.

4 Висновки до заняття.

Навчальний матеріал

Використання шифру Віжинера

У випадку багатоалфавітної підстановки для шифрування використовуються кілька алфавітів, які змінюються послідовно й циклічно. Для r-алфавітної підстановки символ x_0 вихідного тексту замінюється символом y_0 з алфавіту Y_0, символ x_i – символом y_i з алфавіту Y_i і т. д. І нарешті символ x_{r-1} замінюється символом y_{r-1} з алфавіту B_{r-1}, а символ x_r – символом y_r, але вже з алфавіту Y_0. Далі цикл повторюється.

Таким чином,

$$(y_0, y_1, ..y_{n-1}) = [\pi_i(x_0), \pi_i(x_1)... \pi_i(x_{n-1})], \qquad (5)$$

де $\pi_i = \pi_i(i \bmod r)$, r – довжина ключової послідовності.

Практичною реалізацією багатоалфавітної заміни є шифри Віженера, одноразова система шифрування й ін. Теоретично доведено, що остання є системою, яка не розкривається, оскільки її шифротекст не містить достатньої інформації для відновлення відкритого тексту. Однак можливості використання одноразової системи обмежені тільки практичними аспектами.

Підвищення криптостійкості багатоалфавітного шифрування пояснюється тим, що забезпечується маскування

природної статистики вихідної мови. Дійсно, один і той самий символ вихідного тексту може бути перетворений у кілька різних символів шифрувальних алфавітів, причому чим більше період, тим вище ступінь захисту вихідного тексту.

Метод багатоалфавітної підстановки Віженера призначений для підвищення безпеки передачі даних, є одним з найбільш поширених, забезпечує прийнятний компроміс між вартістю шифрування і необхідним рівнем захисту інформації.

Суть багатоалфавітних підстановок полягає у послідовній і циклічній зміні алфавітів, які використовуються для шифрування. Кожен наступний знак вихідного повідомлення кодується знаками різних алфавітів, кількість яких пропорційна довжині ключа. Алгоритм шифрування полягає у такому. Ключ, що являє собою деяке слово чи послідовність знаків, підписується під вихідним повідомленням з періодичним повторенням. Цифрові еквіваленти знаків тексту і розташованого під ним ключа додаються і після приведення суми за модулем К дають цифровий еквівалент кожного знака криптограми.

Фактично застосовується формула, в якій значення коефіцієнтів зсуву визначаються цифровими еквівалентами поточних знаків ключа і змінюються з періодом, що дорівнює кількості знаків у ньому. Надійність закриття даних зростає зі збільшенням довжини ключа. Це пояснюється тим, що застосування бататоалфавітних підстановок створює маскування природної частотної статистики вихідного алфавіту. Дійсно, кожен знак цього алфавіту може бути перетворений у декілька (пропорційно довжині ключа) різних знаків шифрувальних алфавітів.

Шифрування методом гамування

Під гамуванням розуміється процес накладення за певним законом гами шифру на вихідний текст. Гама – це псевдовипадкова послідовність чисел, вироблена за певним алгоритмом і призначена для шифрування і розшифрування даних.

Як певний закон накладення гами можна використати додавання по mod m числового еквівалента символу і псевдовипадкового числа гами. Можна також подати вихідний

текст у вигляді блоків, наприклад, по 64 біти, і складати по mod 2 із блоками гами тієї самої довжини.

Криптостійкість шифрування залежить від якості гами, що визначається такими факторами:

- величиною періоду гами;

- непередбачуваністю гами.

Довжиною періоду гами називається мінімальна кількість символів, після якої послідовність цифр у гамі починає повторюватися. Випадковість розподілу символів за періодом означає відсутність закономірностей між появою різних символів у межах періоду.

За довжиною періоду розрізняються гами з кінцевим і нескінченним періодом. Якщо довжина періоду гами перевищує довжину шифрованого тексту, гама є істинно випадковою і не використовується для шифрування інших повідомлень, то таке перетворення є абсолютно стійким.

Значний успіх у криптографії пов'язаний з ім'ям американця Г. Вернама. У 1917 р. він, будучи співробітником телеграфної компанії AT & T, запропонував ідею автоматичного шифрування телеграфних повідомлень. Йшлося про своєрідне накладення гами на знаки алфавіту, подані відповідно до телетайпних кодом Бодо п'ятизначними «імпульсними комбінаціями». Наприклад, буква А подається комбінацією («- - - + +»), а комбінація («+ + - + +») – це символ переходу від букв до цифр. На паперовій стрічці, яка використовується при роботі телетайпа, знаку «+» відповідала наявність отворів, а знаку «-» – їхня відсутність. При зчитуванні зі стрічки металеві щупи проходили через отвори, замикали електричний ланцюг і тим самим посилали в лінію імпульс струму.

У 1949 р. Клод Шеннон довів абсолютну стійкість шифру Вернама. При цьому послідовність символів у межах періоду гами (ключа) повинна мати три властивості:

- бути істинно випадковою;

- збігатися за розміром або бути більше заданого відкритого тексту;

- застосовуватися тільки один раз.

Як така гами може бути використана будь-яка послідовність випадкових символів, наприклад, послідовності цифр підстави

натурального логарифму e, числа π і т. п. Звичайно ж, використання загальновідомих e і π зробить передані повідомлення абсолютно захищеними. На практиці використовують довгі випадкові або псевдовипадкові ключі, згенеровані за допомогою спеціальних технічних пристроїв або програмно-апаратних комплексів.

Застосовуються детерміновані алгоритми генерації псевдовипадкових чисел за допомогою функції Random, хеш-функцій або рекурентних формул. Однак слід зазначити, що жоден детермінований алгоритм не може генерувати повністю випадкові числа.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

1 Написати програму, яка шифрує дані за допомогою шифрів Трисемуса та вертикальної перестановки. Програма має шифрувати і розшифровувати текст на двох будь-яких мовах. Під час розшифровування повинні відновлюватися розділові знаки.

2 Написати програму, яка шифрує дані за допомогою шифрів поєднаного та «поворотної решітки». Програма має шифрувати і розшифровувати текст на двох будь-яких мовах. Під час розшифровування повинні відновлюватися розділові знаки.

3 Написати програму, яка шифрує дані за допомогою шифрів Хіла та подвійної перестановки. Програма має шифрувати і розшифровувати текст на двох будь-яких мовах. Під час розшифровування повинні відновлюватися розділові знаки.

4 Написати програму, яка шифрує дані за допомогою шифрів Порти і «Перехрестя». Програма має шифрувати і розшифровувати текст на двох будь-яких мовах. Під час розшифровування повинні відновлюватися розділові знаки.

5 Написати програму, яка виконує шифрування/розшифрування даних методом мережі Фейстеля, блок 128 біт.

6 Написати програму, яка виконує шифрування/розшифрування даних методом ADFGVX.

7 Написати програму, яка виконує шифрування/розшифрування даних методом складання за модулем N (33).

8 Написати програму, яка виконує симетричне шифрування/розшифрування даних з використанням режиму шифрування CBC (WORD).

9 Написати програму, яка виконує симетричне шифрування/розшифрування даних з використанням режиму шифрування ECB (DWORD).

10 Написати програму, яка виконує симетричне шифрування/розшифрування даних з використанням режиму шифрування PCBC (BYTE).

11 Написати програму, яка стискає і розпаковує дані, використовуючи алгоритм RLE першого типу.

12 Написати програму, яка стискає і розпаковує дані, використовуючи алгоритм Шенона-Фанно.

ПИТАННЯ ДЛЯ САМОСТІЙНОЇ ПІДГОТОВКИ ДО МОДУЛЬНОГО КОНТРОЛЮ

1 Дайте визначення захисту інформації.

2 Дайте визначення інформаційної безпеки.

3 Хто є суб’єктами інформаційних відносин?

4 Дайте визначення доступності інформації.

5 Дайте визначення цілісності інформації.

6 Дайте визначення конфіденційності інформації.

7 Які засоби захисту інформації відносяться до формальних?

8 Які засоби захисту інформації відносяться до неформальних?

9 Дайте визначення фізичних засобів захисту інформації.

10 Дайте визначення апаратних засобів захисту інформації.

11 Дайте визначення програмних засобів захисту інформації.

12 Дайте визначення законодавчих засобів захисту інформації.

13 Дайте визначення організаційних засобів захисту інформації.

14 Дайте визначення морально-етичних засобів захисту інформації.

15 Які види діяльності відносяться до організаційного захисту інформації?

16 Які принципи відносяться до організаційного захисту інформації?

17 Вкажіть, які ознаки відносяться до організаційного захисту інформації.

18 Які завдання вирішує режимно-секретний відділ підприємства?

19 Які завдання вирішує підрозділ по технічному захисту інформації підприємства?

20 Які завдання вирішує підрозділ криптографічного захисту інформації підприємства?

21 Які завдання вирішує підрозділ охорони та пропускного режиму підприємства?

22 Дайте визначення аутентифікації.

23 Дайте визначення авторизації.

24 Дайте визначення санкціонованого доступу.

25 Дайте визначення несанкціонованого доступу.

26 Дайте визначення загрози безпеці комп'ютерних систем.

27 Дайте визначення атаки комп'ютерних систем.

28 Дайте визначення вразливості комп'ютерних систем.

29 Дайте визначення недоліків захисту комп'ютерних систем.

30 На що спрямовані загрози порушення конфіденційності комп'ютерних систем?

31 На що спрямовані загрози порушення цілісності інформації комп'ютерних систем?

32 На що спрямовані загрози порушення доступності комп'ютерних систем?

33 Які дії відносяться до навмисних?

34 Які дії відносяться до випадкових?

35 Дайте визначення безпеки інформації.

36 В чому полягає сутність захисту інформації?

37 В чому полягає попередження загроз безпеці?

38 В чому полягає виявлення загроз безпеці?

39 В чому полягає знаходження загроз безпеці?

40 В чому полягає припинення або локалізація загроз безпеці?

41 В чому полягає ліквідація наслідків загроз?

42 В чому полягає попередження загроз безпеці?

43 Що відноситься до підтримуючої інфраструктури?

44 Дайте визначення інформаційної загрози.

45 Що відноситься до видів правової (регламентованої законами) інформації?

46 Що відноситься до видів конфіденційної інформації?

47 Що є правом суб’єкта персональних даних?

48 Дайте визначення формальних засобів захисту інформації.

49 Наведіть ознаки неформальних засобів захисту інформації.

50 Які засоби захисту інформації не відносяться до неформальних засобів захисту?

СПИСОК ЛІТЕРАТУРИ

1 Гавловський В. Д., Голубев В. О., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Харків : Фоліо, 2012. 284 с.

2 Нарожний В. В. Цифрові електронно-обчислювальні машини : Конспект лекцій. Харків : УкрДАЗТ, 2010. 105 с.

3 Данько М. І., Меркулов В. С., Гончаров В. О. та ін. Математичні методи та моделі в розрахунках на ЕОМ : навч. посіб. / за заг. ред. М. І. Данька. Харків : УкрДАЗТ, 2008. 172 с.

4 Голубев В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / за заг. ред. Р. А. Калюжного, М. Я. Швеця. Запоріжжя : Просвіта, 2011. 252 с.

5 Комп'ютерна злочинність : навч. посіб. / за ред. П. Д. Біленчука, Б. В. Романюка, В. С. Цимбалюка. Київ, 2014. 240 с.

6 Кузьменко Б. В., Чайковська О. А. Захист інформації. Ч. 2. Програмно-технічні засоби забезпечення інформаційної безпеки. Київ, 2009. 215 с.

7 Пількевич І. А., Лобанчикова Н. М., Молодецька К. В. Захист інформації в автоматизованих системах управління : навч. посіб. Житомир : Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

8 Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. Київ : Видавнича група BHV, 2009. 608 с