Міністерство освіти і науки України
Національний університет водного господарства
та природокористування
Кафедра філософії та культурології

06-07-253М

МЕТОДИЧНІ ВКАЗІВКИ

до практичних занять
з навчальної дисципліни
«Інформаційна безпека»
для здобувачів вищої освіти другого (магістерського) рівня
за освітньо-професійною програмою
«Соціальний менеджмент та інформаційна культура»
спеціальності 028 «Менеджмент соціокультурної діяльності»
денної та заочної форм навчання

Рекомендовано науково-
методичною радою
з якості ННІЕМ
Протокол № 1
від 4 вересня 2024 р.

Рівне – 2024

Методичні вказівки до практичних занять самостійної роботи з навчальної дисципліни «Інформаційна безпека» для здобувачів вищої освіти другого (магістерського) рівня за освітньо-професійною програмою «Соціальний менеджмент та інформаційна культура» спеціальності 028 «Менеджмент соціокультурної діяльності» денної та заочної форм навчання. [Електронне видання] / Рейнська В. Б. – Рівне : НУВГП, 2024. – 48 с.

Укладач: Рейнська В. Б., к.е.н., доцент кафедри філософії та культурології.

Відповідальний за випуск: Шадюк Т. А., к.філос.н., доцент кафедри філософії та культурології, завідувач кафедри філософії та культурології.

Керівник групи забезпечення спеціальності: Шадюк Т. А., к.філос.н., доцент кафедри філософії та культурології.

Зміст

Вступ

Навчальна дисципліна «Інформаційна безпека» є складовою частиною фахового вибору студентів за спеціальністю 028 «Менеджмент соціокультурної діяльності».

Метою навчальної дисципліни є формування у здобувачів вищої освіти теоретичних знань та практичних навичок щодо забезпечення інформаційної безпеки національних інтересів у будь-якій сфері життєдіяльності суспільства.

- Основними завданнями навчальної дисципліни є визначення концептуальних засад, принципів, форм та методів забезпечення інформаційної безпеки;
- ознайомлення з ключовими загрозами інформаційної безпеки, основами управління інформаційною безпекою;

формування навичок використання основ теорії і практики інформаційної безпеки у публічному управлінні

Курс забезпечує студентів спеціальними знаннями з культурно-дозвіллєвої діяльності, сприяє осмисленню та засвоєнню студентами сутності, структури, рівнів, функцій, форм та концепцій дозвілля; допомагає сформувати навички організації дозвіллєвої діяльності серед різних верств населення.

Студент повинен знати:

- етимологію та семантику основних категорій дисципліни;
- феноменологічну та соціально-культурну сутність і значимість дозвілля;
- напрямки розвитку гуманітаристики дозвілля;
- історичні аспекти формування дозвіллєвої діяльності;
- форми і концепції дозвіллєвої діяльності;
- специфіку та технології організації масових, групових та індивідуальних форм дозвіллєвої діяльності.

Студент повинен уміти:

- аргументувати ціннісну основу дозвіллєвої діяльності;

- здійснювати пошук інформативних джерел з дисципліни: підручників, монографій, статей, а також відео-матеріалів;
- писати есе за заданим планом;
- реферувати оригінальні наукові тексти, аналізувати відео-матеріали на тематику дисципліни;
- складати плани-проєкти різних форм індивідуального, масового і групового дозвілля;
- реалізовувати плани-проєкти із фото-відео-фіксацією процесуальності та результатів;
- застосовувати інновації та сучасні технології для ефективної організації роботи у сфері культурно-дозвіллєвої діяльності.

Загальні положення

Оскільки освітня компонента "Інформаційна безпека" повинна формувати у студента навички критичного мислення та практичного застосування знань у сфері захисту інформації, враховуючи швидкий розвиток цифрових технологій та загрози, що з ними пов'язані, освоєння змісту цієї дисципліни вимагатиме активної участі в лекційних та практичних заняттях, глибокого аналізу спеціалізованої літератури, дослідження актуальних матеріалів у мережі Інтернет, а також самостійної роботи над практичними завданнями та кейсами, які відображають реальні виклики у сфері інформаційної безпеки.

Методичні поради по підготовці до практичних занять:

Практичні заняття є ключовим елементом роботи студентів у процесі вивчення дисципліни «Інформаційна безпека». Після прослуховування лекцій студент готується до практичної роботи відповідно до плану виконання практичної роботи за даною темою. У підготовці він повинен

використовувати як основну, так і додаткову літературу, а також досліджувати матеріали з відкритих інтернет-джерел.

Глибшому вивченню певних питань сприяють практичні завдання, що мають різні рівні складності і є сучасними та релевантними. Виконуючи ці завдання, студенти можуть продемонструвати свої аналітичні здібності, розвивати критичне мислення та здобувати нові компетенції в сфері інформаційної безпеки. Це формує комплексний підхід до аналізу загроз і розробки методів захисту інформації в умовах динамічно змінюваного цифрового середовища.

Компетентності:

ІК. Здатність розв'язувати складні задачі і проблеми в сфері менеджменту соціокультурної діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

ЗК1. Здатність спілкуватися іноземною мовою.

ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

СК5. Здатність організовувати та реалізовувати науково-дослідні, науково-виробничі, соціокультурні проекти.

СК13. Здатність здійснювати аналітичну оцінку інформаційного простору соціокультурної сфери, використовувати SMM та SEO технології, а також знання з інформаційної безпеки.

Програмні результати:

ПР1. Відшуковувати, аналізувати та оцінювати інформацію, необхідну для постановки і вирішення як професійних завдань, так і особистісного розвитку.

ПР5. Використовувати міждисциплінарний підхід до вирішення складних задач і проблем соціокультурної діяльності.

ПР12. Збирати необхідні дані з різних джерел, обробляти і аналізувати їх практичні результати із застосуванням сучасних методів та спеціалізованого програмного забезпечення

Методи оцінювання знань

Для оцінювання рівня засвоєння навчального матеріалу студентами застосовуються наступні методи:

- оцінка за участь у практичних заняттях;
- виконання практичних завдань;
- оцінка за активність на лекціях;
- тестування після завершення кожного змістовного модуля;
- оцінка за самостійну роботу;
- підсумковий контроль (залік).

Для діагностики знань використовується кредитно-модульна система зі 100-бальною шкалою оцінювання.

Оформлення звіту з практичних робіт

Складання звіту про проведені дослідження є найважливішим етапом виконання практичної роботи. За кожною виконаною роботою в текстовому редакторі складають звіт, керуючись наступними положеннями:

- Зазначити назву і порядковий номер практичної роботи, а також стисло сформулювати мету роботи;
- Схеми і графіки креслити з дотриманням прийнятих стандартних умов позначень;
- Звіт за кожною практичною роботою повинен містити основні висновки. У заголовку звіту вказують номер роботи та її повне найменування. Під час складання звіту потрібно стисло описати мету роботи, її зміст, вказати використані апаратуру та обладнання.
- Під час виконання практичної роботи необхідно суворо дотримуватися правил техніки безпеки.

Усі практичні роботи висилаються на перевірку

викладачеві виключно через навчальну платформу Moodle за посиланням https://exam.nuwm.edu.ua/course/view.php?id=6107

Критерії оцінювання робіт

Оцінку «відмінно» ставлять, якщо студент виконав роботу в повному обсязі з дотриманням необхідної послідовності дій; у «Звіті до практичних робіт» правильно виконує всі записи, таблиці, малюнки, креслення, графіки, обчислення; правильно виконує аналіз помилок.

Оцінку «добре» ставлять, якщо студент виконав вимоги до оцінки «відмінно», але допущено 2-3 недоліки.

Оцінку «задовільно» ставлять, якщо студент виконав роботу не повністю, але обсяг виконаної частини такий, що дає змогу одержати правильні результати та висновки; під час проведення роботи було допущено помилки.

Оцінку «незадовільно» ставлять, якщо студент виконав роботу не повністю або обсяг виконаної частини роботи не дає змоги зробити належних висновків.

Шкала оцінювання навчальних досягнень студентів

Вид заняття	Бали
1. Поточна складова оцінювання	
1.1. Практична робота 1. Інформація як товар та об'єкт безпеки.	6
1.2. Практична робота 2. Виявлення шкідливих програм для ПК і мобільних пристроїв.	9
1.3. Практична робота 3. Основні завдання Центру протидії дезінформації.	9
1.4. Практична робота 4. Реалізація єдиної інформаційної політики в умовах воєнного стану.	9
1.5. Практична робота 5. Реалізація методів Забезпечення інформаційної безпеки.	9
1.6. Практична робота 6. Алгоритми побудови системи	9

захисту інформації.	
1.7. Практична робота 7. Аудит інформаційної безпеки електронної комерції та комунікаційю	9
Всього поточна складова оцінювання:	**60**
2. Модульна складова оцінювання	
2.1. Модульний контроль №1	20
2.2. Модульний контроль №2	20
Всього підсумкова складова оцінювання:	**40**
Разом:	**100**

*Підсумковий контроль (залік) у тестовій формі складається у ННЦНО через навчальну платформу Moodle за умови скасування модульних контролів МК1 і МК2.

Плани практичних занять

ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАЦЙНА БЕЗПЕКА. ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Практична робота № 1

Інформація як товар і об'єкт безпеки. Програмне та апаратне забезпечення локальних мереж. Захист інформації.

1. Мета роботи: вивчити поняття, пов'язані з програмним та апаратним забезпеченням комп'ютерних мереж; виробити практичні навички обміну файлами між користувачами локальної комп'ютерної мережі.

2 Обладнання, прилади, апаратура, матеріали: персональний комп'ютер, що входить до складу локальної мережі.

3. Теоретичні основи

Особливості інформації як товару та медіа споживання.

Загальне зростання інформаційних потреб і збільшення потоків інформації в сучасному суспільстві, в його суспільній сфері та в державних інститутах посилюють значення інформації як товару. У медіабізнесі та інших культурних індустріях цей вміст - контент, втілений на тому чи іншому матеріальному носії, в тій чи іншій видовій та жанровій формах. Динамічний розвиток інформаційного сектору і зростаючий його внесок у створення національного багатства призводить до подальшого структурування і розвитку галузей, пов'язаних з інформаційними послугами, зокрема культурних індустрій і медіабізнесу. Підтвердженням тому стають прогресуюча капіталізація в цих галузях, зростання вартості нематеріальних активів за рахунок інтелектуальної власності на продукти креативної практики і творчої діяльності в рекламі (оцінка брендів) і медіабізнесі.

У більшості сегментів інформаційного ринку виробництво та реалізація інформаційного продукту поєднуються з наданням інформаційних послуг. Зокрема, так відбувається в індустрії ЗМІ, яка продукує контент (зміст) як товар для медіаринку, і діє на ринку рекламних послуг, забезпечуючи доступ до аудиторії ЗМІ для рекламодавців, у підсумку формуючи здвоєний ринок взаємопов'язаних товарів і послуг. На цьому ринку рекламних послуг редакція (або рекламне агентство, або інформаційне агентство) монетизує свою можливість доступу до цільової споживчої аудиторії, надаючи такий доступ рекламодавцям

Але основою інформаційного ринку все ж таки залишається виробництво і поширення контенту, змісту. Низка ключових особливостей інформаційного товару

принципово відрізняють його від інших товарів і накладають відбиток на його споживання.

Насамперед, під час споживання інформація не зникає, її можна відтворити і використати багаторазово. Ця багаторазовість не змінює контент.

Але «моральний знос» інформаційного продукту пов'язаний із втратою актуальності та затребуваності. Зміна споживчої вартості цього товару може бути невизначеною і непередбачуваною, інтенсивним розвитком спеціалізованих медіа за професійною, корпоративною ознакою або «за інтересами», глобальною міграцією споживачів до Інтернету, розвитком дедалі більш універсальних цифрових ґаджетів-носіїв або пристроїв для доступу до контенту. Б. М'єж виокремлює такі суттєві чинники сучасного медіаспоживання: індивідуалізація та диференціація, медіатизація (проникнення комунікацій та медіа в усі аспекти повсякденного соціального життя і відносин), диґіталізація в різноманітних сферах, часто під впливом ініціатив влади та бізнесу (електронний документообіг, робота з громадянами через Інтернет і створення «електронного уряду», зростання обсягу комерційних і банківських операцій у мережі), що додатково посилює застосування цифрових технологій у медіа та комунікаціях.

Не викликає сумнівів той факт, що як вітчизняні, так і зарубіжні вчені доволі нерівномірно вивчають окремі сегменти інформаційного ринку та його середовища. Сьогодні економіка інформаційних бізнесів, засоби зв'язку та Інтернет розглядаються деколи набагато глибше, ніж, наприклад, проблеми виходу на зовнішні ринки продуктів книговидання, друкованих та електронних ЗМІ; сьогодні медіаспоживання вивчають насамперед через потребу надати інструмент для вимірювань аудиторії в інтересах рекламного бізнесу. При цьому дослідники нерідко перебільшують значення технологічних інновацій, які ведуть до зміни матеріального носія, але мало змінюють зміст, текстову та візуальну основу

як «традиційних» медіа, так і книжкових видань. Захоплюючись технологічністю та візуалізацією контенту, часто не беруть до уваги базові чинники, що приваблюють аудиторію саме до тексту (сюжетність, наративність, потреба у сприйнятті «історії з деталями», драматургія тексту, його комплексне поєднання з іншими засобами передавання інформації, які створюють можливість якнайкращого розуміння та пояснення змісту).

Глибинний зміст і зміст контенту насправді не дуже змінюються. Але час не чекає, як не чекає і покупець: він готовий здійснити придбання або залишитися в лавах аудиторії медіа, якщо йому буде запропоновано зміст у новій, сучасній формі, адаптований до нових носіїв інформації.

Основні поняття комп'ютерних мереж

Передача інформації між комп'ютерами існує з самого моменту виникнення ЕОМ. Вона дає змогу організувати спільну роботу окремих комп'ютерів, розв'язувати одне завдання за допомогою кількох комп'ютерів, спільно використовувати ресурси та розв'язувати безліч інших проблем.

Під комп'ютерною мережею розуміють комплекс апаратних і програмних засобів, призначених для обміну інформацією та доступу користувачів до єдиних ресурсів мережі.

Основне призначення комп'ютерних мереж - забезпечити спільний доступ користувачів до інформації (баз даних, документів тощо) і ресурсів (жорстких дисків, принтерів, накопичувачів CD-ROM, модемів, виходу в глобальну мережу тощо).

Абоненти мережі - об'єкти, що генерують або споживають інформацію.

Абонентами мережі можуть бути окремі ЕОМ, промислові роботи, верстати з ЧПУ (верстати з числовим програмним управлінням) тощо. Будь-який абонент мережі підключений до станції.

Станція - апаратура, яка виконує функції, пов'язані з передачею і прийомом інформації.

Для організації взаємодії абонентів і станції необхідне фізичне передавальне середовище.

Фізичне передавальне середовище - лінії зв'язку або простір, у якому поширюються електричні сигнали, і апаратура передачі даних.

Однією з основних характеристик ліній або каналів зв'язку є швидкість передачі даних (пропускна здатність).

Швидкість передачі даних - кількість біт інформації, що передається за одиницю часу.

Зазвичай швидкість передавання даних вимірюється в бітах за секунду (біт/с) і кратних одиницях Кбіт/с і Мбіт/с.

Співвідношення між одиницями вимірювання: 1 Кбіт/с =1024 біт/с; 1 Мбіт/с =1024 Кбіт/с; 1 Гбіт/с =1024 Мбіт/с.

На базі фізичного передавального середовища будується комунікаційна мережа. Таким чином, комп'ютерна мережа - це сукупність абонентських систем і комунікаційної мережі.

За типом використовуваних ЕОМ виділяють однорідні та неоднорідні мережі. У неоднорідних мережах містяться програмно несумісні комп'ютери.

За територіальною ознакою мережі поділяють на локальні та глобальні.

Локальні мережі (LAN, Local Area Network) об'єднують абонентів, розташованих у межах невеликої території, зазвичай не більше ніж 2-2.5 км.

Локальні комп'ютерні мережі дають змогу організувати роботу окремих підприємств і установ, зокрема й освітніх, розв'язати завдання організації доступу до загальних технічних та інформаційних ресурсів.

Глобальні мережі (WAN, Wide Area Network) об'єднують абонентів, розташованих один від одного на значних відстанях: у різних районах міста, у різних містах, країнах, на різних континентах (наприклад, мережа Інтернет).

Взаємодія між абонентами такої мережі може

здійснюватися на базі телефонних ліній зв'язку, радіозв'язку та систем супутникового зв'язку. Глобальні комп'ютерні мережі дадуть змогу розв'язати проблему об'єднання інформаційних ресурсів усього людства та організації доступу до цих ресурсів.

Основні компоненти комунікаційної мережі:

-передавач;

-приймач;

-повідомлення (цифрові дані певного формату: файл бази даних, таблиця, відповідь на запит, текст або зображення);

-передавання (фізичне передавальне середовище та спеціальна апаратура, що забезпечує передавання інформації).

Топологія локальних мереж

Під топологією комп'ютерної мережі зазвичай розуміють фізичне розташування комп'ютерів мережі відносно один одного і спосіб з'єднання їх лініями.

Топологія визначає вимоги до обладнання, тип використовуваного кабелю, методи управління обміном, надійність роботи, можливість розширення мережі. Існує три основні види топології мережі: шина, зірка і кільце.

Рис.1.1. Топологія Шина.

Шина (bus), за якої всі комп'ютери паралельно підключаються до однієї лінії зв'язку, і інформація від кожного комп'ютера одночасно передається до всіх інших комп'ютерів. Відповідно до цієї топології створюється одноранговa мережа. При такому з'єднанні комп'ютери можуть передавати інформацію тільки по черзі, оскільки лінія зв'язку єдина.

Переваги:

-простота додавання нових вузлів у мережу (це можливо навіть під час роботи мережі);

-мережа продовжує функціонувати, навіть якщо окремі комп'ютери вийшли з ладу;

-недороге мережеве обладнання завдяки широкому поширенню такої топології.

Недоліки:

-складність мережевого обладнання;

- складність діагностики несправності мережевого обладнання через те, що всі адаптери ввімкнені паралельно;

-обрив кабелю тягне за собою вихід з ладу всієї мережі;

-обмеження на максимальну довжину ліній зв'язку через те, що сигнали під час передачі послаблюються і ніяк не відновлюються.

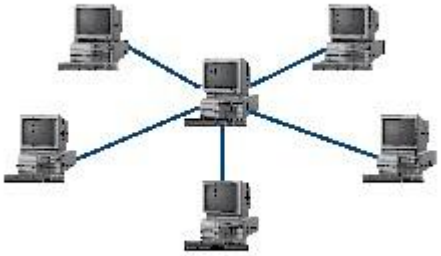

Рис.1.2. Топологія Зірка.

Зірка **(**star), за якої до одного центрального комп'ютера приєднуються решта периферійних комп'ютерів, причому кожен з них використовує свою окрему лінію зв'язку. Весь обмін інформацією йде виключно через центральний комп'ютер, на який лягає дуже велике навантаження, тому він призначений тільки для обслуговування мережі.

Переваги:

-вихід з ладу периферійного комп'ютера жодним чином не позначається на функціонуванні частини мережі, що

залишилася;

-простота використовуваного мережевого обладнання;

-всі точки підключення зібрані в одному місці, що дає змогу легко контролювати роботу мережі, локалізувати несправності мережі шляхом відключення від центру тих чи інших периферійних пристроїв;

-не відбувається загасання сигналів. Недоліки:

-вихід з ладу центрального комп'ютера робить мережу повністю непрацездатною;

-жорстке обмеження кількості периферійних комп'ютерів;

-значна витрата кабелю

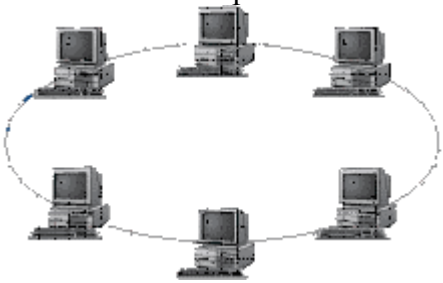

Рис.1.3. Топологія Кільце

Кільце (ring), за якого кожен комп'ютер передає інформацію завжди тільки одному комп'ютеру, наступному в ланцюжку, а отримує інформацію тільки від попереднього в ланцюжку комп'ютера, і цей ланцюжок замкнутий. Особливістю кільця є те, що кожен комп'ютер відновлює сигнал, який до нього надходить, тому загасання сигналу в усьому кільці не має жодного значення, важливим є тільки загасання між сусідніми комп'ютерами.

Переваги:

-легко під'єднати нові вузли, хоча для цього потрібно призупинити роботу мережі;

-велика кількість вузлів, яку можна під'єднати до мережі (понад 1000);

-висока стійкість до перевантажень.

Недоліки:

-вихід з ладу хоча б одного комп'ютера порушує роботу мережі;

-обрив кабелю хоча б в одному місці порушує роботу мережі.

В окремих випадках при конструюванні мережі використовують комбіновану топологію. Наприклад, дерево (tree)- комбінація кількох зірок.

Кожен комп'ютер, який функціонує в локальній мережі, повинен мати мережевий адаптер (мережеву карту). Функцією мережевого адаптера є передача і приймання сигналів, що поширюються по кабелях зв'язку. Крім того, комп'ютер має бути оснащений мережевою операційною системою .

Під час конструювання мереж використовують такі види кабелів:

Рис.1.4. Неекранована кручена пара.

Максимальна відстань, на якій можуть бути розташовані комп'ютери, з'єднані цим кабелем, сягає 90 м. Швидкість передачі інформації від 10 до 155 Мбіт/с; екранована кручена пара. Швидкість передачі інформації 16 Мбіт/с на відстань до 300 м.

Рис.1.5. Коаксіальний кабель.

Відрізняється вищою механічною міцністю, перешкодозахищеністю і дає змогу передавати інформацію на відстань до 2000 м зі швидкістю 2-44 Мбіт/с;

Рис.1.6. Волоконно-оптичний кабель.

Ідеальне передавальне середовище, він не схильний до

дії електромагнітних полів, дає змогу передавати інформацію на відстань до 10 000 м зі швидкістю до 10 Гбіт/с.

Поняття про глобальні мережі

Глобальна мережа - це об'єднання комп'ютерів, розташованих на віддаленій відстані, для спільного використання світових інформаційних ресурсів. На сьогодні їх налічується у світі понад 200. З них найвідомішою є мережа, у глобальних мережах немає будь-якого єдиного центру управління. Основу мережі складають десятки і сотні тисяч комп'ютерів, з'єднаних тими чи іншими каналами зв'язку. Кожен комп'ютер має унікальний ідентифікатор, що дає змогу «прокласти до нього маршрут» для доставки інформації. Зазвичай у глобальній мережі об'єднуються комп'ютери, що працюють за різними правилами (мають різну архітектуру, системне програмне забезпечення тощо). Тому для передавання інформації з одного виду мереж в інший використовуються шлюзи.

Шлюзи (gateway) - це пристрої (комп'ютери), що слугують для об'єднання мереж із абсолютно різними протоколами обміну.

Протокол обміну - це набір правил (угода, стандарт), що визначає принципи обміну даними між різними комп'ютерами в мережі.

Протоколи умовно поділяють на базові (нижчого рівня), що відповідають за передачу інформації будь-якого типу, і прикладні (вищого рівня), що відповідають за функціонування спеціалізованих служб.

Головний комп'ютер мережі, який надає доступ до спільної бази даних, забезпечує спільне використання пристроїв введення-виведення та взаємодії користувачів називається сервером.

Комп'ютер мережі, який тільки використовує мережеві ресурси, але сам свої ресурси в мережу не віддає, називається клієнтом (часто його ще називають робочою станцією).

Для роботи в глобальній мережі користувачеві

необхідно мати відповідне апаратне та програмне забезпечення.

Програмне забезпечення можна розділити на два класи:

- програми-сервери, які розміщуються на вузлі мережі, що обслуговує комп'ютер користувача;

- програми-клієнти, що розміщені на комп'ютері користувача і користуються послугами сервера.

Глобальні мережі надають користувачам різноманітні послуги: електронна пошта, віддалений доступ до будь-якого комп'ютера мережі, пошук даних і програм тощо.

4. Завдання

Завдання 1.

1 Створіть на локальному диску Z аудиторії папку під іменем Пошта_1 (цифра в імені відповідає номеру вашого комп'ютера).

2 За допомогою текстового редактора Word або WordPad створіть лист до одногрупників.

3 Збережіть цей текст у папці Пошта_1 свого комп'ютера у файлі лист1.doc, де 1 - номер комп'ютера.

4 Відкрийте папку іншого комп'ютера, наприклад, Пошта_2, і скопіюйте в неї файл лист1 зі своєї папки Пошта_1.

5 У своїй папці Пошта_1 прочитайте листи від інших користувачів, наприклад лист2. Допишіть у них свою відповідь.

6. Перейменуйте файл лист2 .doc на файл лист2_відповідь1.doc 7. перемістіть файл лист2_відповідь1.doc до папки Пошта _2 і видаліть його зі своєї папки.

8. Далі повторіть п.2-4 для інших комп'ютерів.

9 Прочитайте повідомлення від інших користувачів у своїй папці та повторіть для них дії п.5-8.

Завдання 2. Розв'яжіть задачу.

Максимальна швидкість передачі даних у локальній мережі 100 Мбіт/с. Скільки сторінок тексту можна передати за

1 сек, якщо 1 сторінка тексту містить 50 рядків і на кожному рядку 70 символів.

5. Зміст звіту

Звіт повинен містити:

1. Назву роботи.
2. Мету роботи.
3. Завдання та його розв'язання.
4. Висновок щодо роботи.
5. Перелік використаних джерел.

6. Контрольні запитання

1. Назвіть особливості сучасного інформаційного суспільства.
2. Які елементи інформаційної інфраструктури Ви знаєте?
3. Що розуміється під загрозою безпеці інформації?
4. У чому відмінності понять інформаційний ресурс, продукт і послуга?
5. Як визначається ціна інформаційного продукту?
6. Що таке конфіденційність, цілісність і доступність інформації?
7. Яка інформація компанії не може бути віднесена до комерційної таємниці?
8. Що таке персональні дані?
9. Укажіть основне призначення комп'ютерної мережі.
10. Вкажіть об'єкт, який є абонентом мережі.
11. Назвіть основну характеристику каналів зв'язку.
12. Що таке локальна мережа, глобальна мережа?
13. Що розуміється під топологією локальної мережі?
14. Які існують види топології локальної мережі?
15. Охарактеризуйте коротко топологію «шина», «зірка», «кільце».
16. Що таке протокол обміну?

Практична робота № 2

Виявлення шкідливих програм для ПК і мобільних пристроїв

Захист інформації, антивірусний захист. Експлуатаційні вимоги до комп'ютерного робочого місця. Профілактичні заходи для комп'ютерного робочого місця відповідно до його комплектації для професійної діяльності.

1. Мета роботи: виробити практичні навички роботи з антивірусними програмами, навички правильної роботи з комп'ютером.

2 Обладнання, прилади, апаратура, матеріали: персональний комп'ютер, антивірусна програма.

3. Теоретичні основи

Віруси. Антивірусне програмне забезпечення

Комп'ютерний вірус - програма, здатна мимоволі впроваджуватися і впроваджувати свої копії в інші програми, файли, системні області комп'ютера і в обчислювальні мережі, з метою створення всіляких перешкод роботі на комп'ютері.

Ознаки зараження:

- припинення роботи або неправильна робота раніше функціонуючих програм
- повільна робота комп'ютера -невозможность завантаження ОС
- зникнення файлів і каталогів або спотворення їхнього вмісту зміна розмірів файлів та їхнього часу модифікації
- зменшення розміру оперативної пам'яті
- непередбачувані повідомлення, зображення і звукові сигнали часті збої і зависання комп'ютера та ін.

Класифікація комп'ютерних вірусів За середовищем існування:

- мережеві - поширюються різними комп'ютерними мережами; файлові - впроваджуються у виконувані модулі (COM, EXE);
- завантажувальні - впроваджуються в завантажувальні сектори диска або сектори, що містять програму завантаження диска;
- файлово-завантажувальні - впроваджуються і в

завантажувальні сектори, і у виконувані модулі.

За способом зараження:

- резидентні - під час зараження залишає в оперативній пам'яті комп'ютера свою резидентну частину, яка потім перехоплює звернення ОС до об'єктів зараження;
- нерезидентні - не заражають оперативну пам'ять і активні обмежений час

За впливом:

- безпечні - не заважають роботі комп'ютера, але зменшують обсяг вільної оперативної пам'яті та пам'яті на дисках;
- небезпечні - призводять до різних порушень у роботі комп'ютера;
- дуже небезпечні - можуть призводити до втрати програм, даних, стирання інформації в системних областях дисків.

За особливостями алгоритму:

- паразити - змінюють вміст файлів і секторів, легко виявляються;
- хробаки - обчислюють адреси мережевих комп'ютерів і надсилають за ними свої копії;
- стелси - перехоплюють звернення ОС до уражених файлів і секторів і підставляють замість них чисті області;
- мутанти - містять алгоритм шифрування-дешифрування, жодна з копій не схожа на іншу;
- трояни - не здатні до саморозповсюдження, але маскуючись під корисну програму, руйнують завантажувальний сектор і файлову систему.

Основні заходи щодо захисту від вірусів:

- оснастіть свій комп'ютер однією із сучасних антивірусних програм: Doctor Web, Norton Antivirus, AVP;
- постійно оновлюйте антивірусні бази;
- робіть архівні копії цінної для Вас інформації (гнучкі диски, CD).

Класифікація антивірусного програмного забезпечення

-□□ Сканери (детектори). Принцип роботи антивірусних сканерів заснований на перевірці файлів, секторів і системної пам'яті та пошуку в них відомих і нових (невідомих сканеру) вірусів.

-□□ Монітори. Це цілий клас антивірусів, які постійно перебувають в оперативній пам'яті комп'ютера і відстежують усі підозрілі дії, що виконуються іншими програмами. За допомогою монітора можна зупинити розповсюдження вірусу на ранній стадії.

-□□ Ревізори. Програми-ревізори спочатку запам'ятовують у спеціальних файлах образи головного завантажувального запису, завантажувальних секторів логічних дисків, інформацію про структуру каталогів, іноді - обсяг встановленої оперативної пам'яті. Програми-ревізори спочатку запам'ятовують у спеціальних файлах образи головного завантажувального запису, завантажувальних секторів логічних дисків, інформацію про структуру каталогів, іноді об'єм встановленої оперативної пам'яті. Для визначення наявності вірусу в системі програми-ревізори перевіряють створені ними образи і проводять порівняння з поточним станом.

4. Завдання

Завдання 1. Оновіть через Інтернет антивірусну програму, встановлену на Вашому комп'ютері. Виконайте перевірку папки «Мої документи» на віруси. Дати характеристику цієї програми.

5. Зміст звіту

Звіт повинен містити:

1. Назву роботи.
2. Мету роботи.
3. Завдання та його розв'язання.
4. Висновок щодо роботи.
5. Перелік використаних джерел.

6. Контрольні запитання

1. Що таке вірус?
2. Дайте класифікацію вірусів.
3. Для чого потрібні антивірусні програми?
4. Дайте їхню класифікацію

Практична робота № 3

Основні завдання Центру протидії дезінформації.

1. Мета роботи: визначити основні функції та завдання Центру протидії дезінформації.

2 Обладнання, прилади, апаратура, матеріали: персональний комп'ютер, браузер.

3. Теоретичні основи

В сучасних умовах війни 18.03.2022 р. прийнято рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного ст ану», в якому визначено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки» [10]. Наразі в Україні функціонує також Центр протидії дезінформації пр и РНБО України, на сайті якого можна ознайомитись з актуальною інфо рмацією та подіями в цій сфері.

Центр протидії дезінформації (далі – Центр) є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року "Про створення Центру протидії дезінформації", уведеного в дію Указом Президента України від 19 березня 2021 року № 106. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніп улювання громадською думкою. У своїй діяльності висвітлює тенденції з інформування стану військової справи, ОПК, боротьби зі злочинністю та

корупцією, зовнішньої та внутрішньої політики, економіки, об'єктів кр итичної інфраструктури, екології, охорони здоров'я, соціальної сфери, формування суспільної свідомості, науково-технологічного напряму тощо. Основна увага зосереджена на протидії поширенню неправдивої інформації та боротьбі з інформаційним тероризмом. Центр функціонує відповідно до Конституції і законів України, актів Президента України та Кабінету Міністрів України, міжнародних договорів України, цього П оложення, а також розпоряджень Секретаря Ради національної безпеки і оборони України.

Основними завданнями Центру є:

1) проведення аналізу та моніторингу подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі;

2) виявлення та вивчення поточних і прогнозованих загроз інформаційній безпеці України, чинників, які впливають на їх формування, пр огнозування та оцінка наслідків для безпеки національних інтересів України;

3) забезпечення Ради національної безпеки і оборони України, Голови Ради національної безпеки і оборони України інформаційно-аналітичними матеріалами з питань забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії проп аганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

4) підготовка та внесення Раді національної безпеки і оборони України, Голові Ради національної безпеки і оборони України пропозицій щодо: визначення концептуальних підходів у сфері протидії дезінформації та деструктивним інформаційним впливам і кампаніям; координації діяльності та взаємодії органів виконавчої влади з питань національної безпеки в інформаційній сфері, забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і

кампаніям, запобігання спробам маніпулювання громадською думкою; здійснення системних заходів, спрямованих на п осилення спроможностей суб'єктів сектору безпеки та оборони, інших де ржавних органів задля забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою, розвитку національної інфраструктури у відповідній сфері; удосконалення системи правового та наукового забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

5) участь у розбудові системи стратегічних комунікацій, організації та координації заходів щодо її розвитку;

6) участь у розробленні та реалізації Стратегії інформаційної безпеки України, здійсненні аналізу стану її реалізації, зокрема з питань ефекти вності заходів щодо протидії дезінформації;

7) участь у створенні інтегрованої системи оцінки інформаційних з агроз та оперативного реагування на них;

8) розроблення методології виявлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру;

9) сприяння взаємодії держави та інституцій громадянського суспільства щодо протидії дезінформації та деструктивним інформаційним впливам і кампаніям, організація та участь в інформаційнопросвітницьких заходах з питань підвищення медіа-грамотності суспільства;

10) вивчення, узагальнення й аналіз досвіду інших держав і міжнародних організацій з протидії дезінформації та підготовка проп озицій щодо його використання в Україні;

11) бере участь у визначенні пріоритетів залучення міжнародної те хнічної допомоги з питань забезпечення

інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, дестру ктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

Сьогодні Центр активно залучений у протидії російській агресії. Його пріоритетами є: оперативне інформування населення; розкриття дезінформації та маніпуляцій; забезпечення інформаційної безпеки; б оротьба з інформаційним тероризмом. Як один із результатів роботи, фахівцями центру було розроблено освітній курс «Дезінfакеція твого інфопростору».

4. Завдання

Ознайомтеся із структурою сайту Центру протидії дезінформації: https://cpd.gov.ua/. Прочитайте 3-4 аналітичні звіти, випущені на початку створення Центру та 2-3 звіти за останні два місіці. Проаналізуйте та порівняйте масштаби та тематику дезінформації ворожої держави.

5. Зміст звіту

Звіт повинен містити:

1. Назву роботи.
2. Мету роботи.
3. Завдання та його розв'язання.
4. Висновок щодо роботи.
5. Перелік використаних джерел.

6. Контрольні запитання.

Назвіть та охарактеризуйте:

Список TikTok-каналів поширення ворожої пропаганди

Список інструментів поширення ворожої дезінформації

Список безпечних каналів отримання інформації

Топ проросійських наративів у світових ЗМІ

Практична робота № 4

Реалізація єдиної інформаційної політики в умовах воєнного стану.

1. Мета роботи: закріплення знань основного понятійного апарату, що використовується в галузі захисту інформації, формування навичок роботи з нормативними документами з досліджуваного питання.

2. Обладнання, прилади, апаратура, матеріали: навчальний персональний комп'ютер, браузер.

3. Теоретичні основи

Концепція інформаційної безпеки України (далі - Концепція) спрямована на створення передумов для розвитку такого потенціалу інформаційної сфери України, за якого забезпечується її випереджальний розвиток, а зовнішні негативні впливи не створюють реальних небезпек національній інформаційній безпеці держави. Ключове завдання системи інформаційної безпеки - забезпечити сталість такого розвитку, не допускаючи негативних впливів з боку сторонніх суб'єктів.

Реалізація на практиці такого підходу до інформаційної безпеки держави може здійснюватися виключно за участю всіх внутрішніх суб'єктів інформаційних відносин та за умов ефективної взаємодії держави з громадянським суспільством, приватним сектором та окремими громадянами в інтересах ефективного розвитку інформаційної сфери та спільного захисту такого розвитку від зовнішніх загроз.

Систему захисту інформації (СЗІ) у найзагальнішому вигляді може бути визначено як організовану сукупність усіх засобів, методів і заходів, що виділяються (передбачаються) на об'єкті інформатизації (ОІ) для розв'язання в ній обраних завдань із захисту. Введенням поняття СЗЗІ визначається той факт, що всі ресурси, які виділяються для захисту інформації, повинні об'єднуватися в єдину, цілісну систему, яка є функціонально самостійною підсистемою будь-якого ОІ. Таким чином, найважливішою концептуальною вимогою до ЗЗІ є вимога адаптованості, тобто здатності до цілеспрямованого пристосування при зміні структури, технологічних схем або умов функціонування ОІ. Важливість

вимоги адаптованості зумовлюється, з одного боку, можливістю змінюватися переліченим чинникам, а з іншого - відношенням процесів захисту інформації до слабоструктурованих, тобто таких, що мають високий рівень невизначеності. Управління ж слабоструктурованими процесами може бути ефективним лише за умови адаптованості системи управління. Крім загальної концептуальної вимоги, до ЗЗІ висувається ще ціла низка конкретніших, цільових вимог, які можна розділити на:

- функціональні;
- ергономічні;
- економічні;
- технічні;
- організаційні.

Сформована до теперішнього часу система включає такий перелік загальнометодологічних принципів:

- концептуальна єдність;
- адекватність вимогам;
- гнучкість (адаптованість);
- функціональна самостійність;
- зручність використання;
- мінімізація прав, що надаються;
- повнота контролю;
- адекватність реагування;
- економічність.

Концептуальна єдність означає, що архітектура, технологія, організація та забезпечення функціонування як СЗІ загалом, так і складових її компонентів повинні розглядатися та реалізовуватися в суворій відповідності до основних положень єдиної концепції захисту інформації. Адекватність вимогам означає, що СЗІ повинна будуватися в суворій відповідності до вимог до захисту, які, у свою чергу, визначаються категорією відповідного об'єкта і значеннями параметрів, що впливають на захист інформації.

Гнучкість (адаптованість) системи захисту означає таку побудову і таку організацію її функціонування, за яких функції захисту здійснювалися б досить ефективно в разі зміни в деякому діапазоні структури ОІ, технологічних схем або умов функціонування будь-яких її компонентів. Функціональна самостійність передбачає, що СЗЗІ має бути самостійною забезпечувальною підсистемою системи оброблення інформації та під час здійснення функцій захисту не повинна залежати від інших підсистем. Зручність використання означає, що СЗЗІ не повинна створювати додаткових незручностей для користувачів і персоналу ОІ. Мінімізація прав, що надаються, означає, що кожному користувачеві і кожній особі зі складу персоналу ОІ повинні надаватися лише ті повноваження на доступ до ресурсів ОІ та інформації, що міститься в ній, які йому справді потрібні для виконання своїх функцій у процесі автоматизованого опрацювання інформації. При цьому права, що надаються, мають бути визначені та затверджені завчасно в установленому порядку. Повнота контролю передбачає, що всі процедури автоматизованого опрацювання інформації, що захищається, повинні контролюватися системою захисту в повному обсязі, причому основні результати контролю повинні фіксуватися в спеціальних реєстраційних журналах. Активність реагування означає, що СЗІ повинна реагувати на будь-які спроби несанкціонованих дій. Характер реагування може бути різним і включає: прохання повторити дію; вимкнення структурного елемента, з якого здійснено несанкціоновану дію; виключення порушника з числа зареєстрованих користувачів; подання спеціального сигналу тощо. Економічність СЗІ означає, що за умови дотримання основних вимог усіх попередніх принципів витрати на СЗІ мають бути мінімальними.

Практичне завдання

Необхідно запропонувати аналіз збільшення захищеності об'єкта захисту інформації за такими розділами:

1. Визначити вимоги до захисту інформації

2. Класифікувати автоматизовану систему

3. Визначити фактори, що впливають на необхідний рівень захисту інформації

4. Обрати або розробити способи та засоби захисту інформації

5. Побудувати архітектуру систем захисту інформації

6. Сформулювати рекомендації щодо збільшення рівня захищеності

5. Зміст звіту

Звіт повинен містити:

1. Назву роботи.

2. Мету роботи.

3. Завдання та його розв'язання.

4. Висновок щодо роботи.

5. Перелік використаних джерел.

6. Контрольні питання

Ознайомитися із проектами законів про наступні державні програми:

− Державна програма розвитку інформаційного простору України;

− Державна програма доступу до мережі Інтернет;

− Державна програма підтримки вітчизняного ІТ-виробництва;

− Державна програма з питань іномовлення та представлення України в міжнародному інформаційному просторі;

− Державна програма з питань єдиної офіційної комунікативної політики;

− Державна програма розвитку державно-приватного партнерства в інформаційній сфері;

− Державна програма захисту культурних та інформаційних потреб громадян України;

− Державна програма забезпечення кібернетичної безпеки України

− Державна програма підготовки і перепідготовки спеціалістів з інформаційної безпеки;

− Державна програма наукового та моніторингового забезпечення інформаційної сфери.

ЗМІСТОВИЙ МОДУЛЬ 2. МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Практична робота № 5.

Реалізація методів забезпечення інформаційної безпеки

1. Мета роботи: ознайомитися з методами обмеження доступу до інформації.

2. Обладнання, прилади, апаратура, матеріали: навчальний персональний комп'ютер, браузер.

3. Теоретичні основи

Розмежування доступу є досить ефективним засобом попередження можливого збитку внаслідок порушення цілісності або конфіденційності інформації. У тому разі, якщо доступ до самого комп'ютера або до його ресурсів може одержати користувач, який має злий умисел або недостатній рівень підготовки, він може випадково або навмисно спотворити інформацію або знищити її повністю чи частково.

Ця ж обставина може призвести до розкриття закритої інформації або несанкціонованого тиражування відкритої, наприклад, програм, баз даних, різного роду документації, літературних творів тощо на порушення прав власників інформації, авторських прав...

З точки зору розмежування доступу, в інформаційних системах слід розрізняти суб'єкти доступу та об'єкти доступу. До числа суб'єктів доступу можуть увійти або персонал інформаційної системи, або сторонні особи. Об'єктами доступу є апаратно-програмні елементи інформаційних систем. Найчастіше як об'єкти доступу розглядають файли (у тому числі папки і файли програм). Доступ до об'єкта може

розглядатися або як читання (отримання інформації з нього), або як зміна (запис інформації в нього). Тоді види доступу визначаються такими можливими поєднаннями цих операцій:

- ні читання, ні зміна;
- лише читання;
- лише зміна;
- і читання, і зміна.

Очевидно, що відмінність функціональних обов'язків суб'єктів зумовлює необхідність надання їм відповідних видів доступу.

Керування доступом користувачів і глобальними параметрами на членах домену здійснюється на двох рівнях: локальної системи і домену. На окремих комп'ютерах доступ користувачів конфігурують на рівні локальної системи, а одночасно для кількох систем або ресурсів, що входять до домену, - на рівні домену.

Права доступу користувача визначаються керівником організації і прописуються на робочій станції системним адміністратором (адміністратором домену).

Процедура перевірки прав доступу охоплює авторизацію й автентифікацію. Авторизація передбачає перевірку рівня доступу до об'єкта, а аутентифікація - перевірку справжності користувача. Для аутентифікації зазвичай використовуються ім'я користувача (login) і пароль (password). Системний адміністратор здійснює розмежування прав доступу відповідно до заданої системної політики, яка передбачає:

- обмеження на мінімальну довжину, складність і термін дії пароля;
- вимогу унікальності паролів;
- блокування користувача в разі невдалої аутентифікації;
- обмеження часу і місця роботи користувача.

Система розмежування доступу реалізована так, що під час повсякденної роботи користувачі не повинні помічати, що будь-яке звернення до будь-якого об'єкта проходить перевірку на відповідність встановленим правам доступу. Списки прав

доступу можна задавати на кожен документ окремо. Під час створення документа автоматично задається такий доступ на нього, щоб творець мав усі права.

Система розмежування доступу призначена для реалізації визначених адмі-ністратором захисту правил на виконання операцій користувачами над об'єктами сховища.

Система обмеження прав доступу не може дати повної гарантії безпеки інформації. Річ у тім, що зловмисник може отримати або підібрати пароль легального користувача. Крім того, досвідчений фахівець може обійти систему розмежування доступу. Засобом виявлення несанкціонованого доступу до ресурсів слугують системи аудиту, які автоматично фіксують доступ до файлів і папок та системні події.

Моделі розмежування доступу

Найпоширеніші моделі розмежування доступу:

- дискреційна (вибіркова) модель розмежування доступу;
- повноважна (мандатна) модель розмежування доступу.

Дискреційна модель характеризується такими правилами:

- будь-який об'єкт має власника;
- власник має право довільно обмежувати доступ суб'єктів до даного об'єкта;
- для кожного набору суб'єкт - об'єкт - метод право на доступ визначено одно-значно;
- наявність хоча б одного привілейованого користувача (наприклад, адміністратора), який має можливість звертатися до будь-якого об'єкта за допомогою будь-якого методу доступу.

У дискреційній моделі визначення прав доступу зберігається в матриці доступу: у рядках перелічені суб'єкти, а в стовпчиках - об'єкти. У кожній комірці матриці зберігаються права доступу даного суб'єкта до даного об'єкта.

Повноважна модель характеризується такими правилами:

- кожен об'єкт має гриф секретності. Гриф секретності має числове значення: чим воно більше, тим вища секретність об'єкта;

- у кожного суб'єкта доступу є рівень допуску. Допуск до об'єкта в цій моделі суб'єкт отримує тільки в разі, коли у суб'єкта значення рівня допуску не менше значення грифа секретності об'єкта.

Перевага повноважної моделі полягає у відсутності необхідності зберігання великих обсягів інформації про розмежування доступу. Кожним суб'єктом виконується зберігання лише значення свого рівня доступу, а кожним об'єктом - значення свого грифа секретності.

Методи розмежування доступу Види методів розмежування доступу: Розмежування доступу за списками

Суть методу полягає в заданні відповідностей: для кожного користувача задається список ресурсів і права доступу до них або для кожного ресурсу визначається список користувачів і права доступу до цих ресурсів. За допомогою списків можливе встановлення прав із точністю до кожного користувача. Можливий варіант додавання прав або явної заборони доступу. Метод доступу за списками використовується в підсистемах безпеки операційних систем і систем управління базами даних.

Використання матриці встановлення повноважень

Під час використання матриці встановлення повноважень застосовується матриця доступу (таблиця повноважень). У матриці доступу в рядках записуються ідентифікатори суб'єктів, які мають доступ до комп'ютерної системи, а в стовпчиках - об'єкти (ресурси) комп'ютерної системи. У кожній комірці матриці може міститися ім'я і розмір ресурсу, право доступу (читання, запис тощо), посилання на іншу інформаційну структуру, що уточнює права доступу, посилання на програму, що управляє правами доступу тощо. Цей метод є досить зручним, оскільки вся інформація про повноваження зберігається в єдиній таблиці.

Недолік матриці - її можлива громіздкість.

Розмежування доступу за рівнями секретності та категоріями

Розмежування за ступенем секретності поділяється на кілька рівнів. Повноваження кожного користувача можуть бути задані відповідно до максимального рівня секретності, до якого він допущений. При розмежуванні за категоріями задається і контролюється ранг категорії користувачів. Таким чином, усі ресурси комп'ютерної системи розділені за рівнями важливості, причому кожному рівню відповідає категорія користувачів.

Парольне розмежування доступу

Парольне розмежування використовує методи доступу суб'єктів до об'єктів за допомогою пароля. Постійне використання паролів призводить до незручностей для користувачів і тимчасових затримок. З цієї причини методи парольного розмежування використовують у виняткових ситуаціях.

На практиці прийнято поєднувати різні методи розмежувань доступу. Наприклад, перші три методи посилюються парольним захистом. Використання розмежування прав доступу є обов'язковою умовою захищеної інформаційної системи.

4. Завдання

Хід роботи

1 Ознайомитися із засобами розмежування доступу користувачів до папок:

- виконати команду «Загальний доступ і безпека» контекстного меню папки (якщо ця команда недоступна, то вимкнути режим «Використовувати простий загальний доступ до файлів» на вкладці «Вид» вікна властивостей папки) або команду «Властивості»;

- відкрити вкладку «Безпека» і включити до звіту відомості про суб'єктів, яким дозволено доступ до папки і про дозволені для них види доступу;

- за допомогою кнопки «Додатково» відкрити вікно додаткових параметрів безпеки папки (вкладка «Дозволи»);

- включити до звіту відомості про повний набір прав доступу до папки для кожного з наявних у списку суб'єктів;

- відкрити вкладку «Власник», включити у звіт відомості про власника папки і про можливість його зміни звичайним користувачем;

- відкрити папку «Аудит», включити до звіту відомості про призначення параметрів аудиту, що встановлюються на цій вкладці, і про можливість їх встановлення звичайним користувачем;

- закрити вікно додаткових параметрів безпеки.

2. Оволодіти засобами розмежування доступу користувачів до файлів: - виконати команду «Властивості» контекстного меню файлу;

- повторити всі завдання п. 1, але стосовно не папки, а файлу.

3 Освоїти засоби розмежування доступу до принтерів:

- виконати команду «Принтери і факси» меню «Пуск»;

- виконати команду «Властивості» контекстного меню встановленого в системі принтера;

- повторити всі завдання п. 1, але стосовно не папки, а принтера.

4 Опанувати засоби розмежування доступу до розділів реєстру операційної системи:

за допомогою команди «Виконати» меню «Пуск» запустити програму редагування системного реєстру regedit (regedt32);

- за допомогою команди «Дозволи» меню «Правка» редактора реєстру визначити відомості про права доступу користувачів до кореневих розділів реєстру, їхніх власників і параметри політики аудиту;

- включити до звіту відомості про права доступу користувачів до даної папки і про її власника.

5. Зміст звіту

Звіт повинен містити:

1. Назву роботи.
2. Мету роботи.
3. Завдання та його розв'язання.
4. Висновок щодо роботи.
5. Перелік використаних джерел.

6. Контрольні запитання

1. Які основні правила характеризують повноважну модель у контексті розмежування доступу?
2. Як визначається допустимий доступ суб'єкта до об'єкта в повноважній моделі?
3. У чому полягає суть методу розмежування доступу за списками, і де він зазвичай використовується?
4. Як функціонує матриця доступу, і які її переваги та недоліки?
5. Які методи розмежування доступу використовуються у практиці, і чому поєднання різних методів є важливим для захищеної інформаційної системи?

Практична робота № 6.
Алгоритм побудови системи захисту інформації

1. Мета роботи: ознайомитися з механізмами захисту інформації від несанкціонованого копіювання з використанням спеціалізованих програмних засобів.

2 Обладнання, прилади, апаратура, матеріали: персональний компютер, браузер.

3. Теоретичні питання.

1. Поняття системи захисту від несанкціонованого використання та копіювання.
2. Поняття надійності системи захисту від несанкціонованого копіювання.
3. Принципи створення та використання систем захисту від копіювання.

4. Основні вимоги, що висуваються до системи захисту від копіювання.

5. Основні компоненти системи захисту програмних продуктів від несанкціонованого копіювання.

6. Методи, що ускладнюють зчитування скопійованої інформації.

7. Методи, що перешкоджають використанню скопійованої інформації.

8. Основні функції засобів захисту від копіювання.

4. Завдання

Завдання 1. Охарактеризуйте компоненти системи захисту від несанкціонованого копіювання.

Рис.6.1. Система захисту від несанкціонованого копіювання

Завдання 2. Системи захисту від несанкціонованого копіювання можна класифікувати за способом упровадження захисного механізму:

- вбудована впроваджується під час створення програмного продукту;

- пристикувальна підключається до вже готового програмного продукту.

Наведіть переваги та недоліки цих способів впровадження захисного механізму.

Завдання 3. Опишіть основні вимоги, що висуваються до системи захисту від копіювання.

Завдання 4. Загроза несанкціонованого копіювання інформації блокується методами, які можуть бути розподілені за двома групами: методи, що ускладнюють зчитування скопійованої інформації; методи, що перешкоджають використанню інформації.

Наведіть приклади методів кожної групи. Зробіть порівняльний аналіз основних методів захисту від копіювання.

Завдання 5: Відобразіть схематично загальний алгоритм механізму захисту від несанкціонованого використання програм у «чужому» середовищі розміщення.

5. Зміст звіту

Звіт повинен містити:

1. Назву роботи.
2. Мету роботи.
3. Завдання та його розв'язання.
4. Висновок щодо роботи.
5. Перелік використаних джерел.

6. Контрольні запитання

1. Дайте означення системи захисту від несанкціонованого використання та копіювання.
2. Назвіть принципи створення та використання систем захисту від копіювання.
3. Опишіть основні вимоги, що висуваються до системи захисту від копіювання.
4. Охарактеризуйте основні компоненти системи захисту програмних продуктів від несанкціонованого копіювання.

5. Перерахуйте методи, що ускладнюють зчитування скопійованої інформації.
6. Назвіть основні функції засобів захисту від копіювання.

Практична робота № 7. Аудит інформаційної безпеки електроної комерції.

1. Мета роботи вивчення та перевірка сайтів за допомогою сервісів на наявність вразливостей і загроз за допомогою різних інтернет-аудитів.

2 Обладнання, прилади, апаратура, матеріали: персональний компютер, браузер.

3. Теоретичні основи

Аудит безпеки сайту (перевірка сайту на вразливості) - низка процедур, націлених на забезпечення стабільної роботи веб-ресурсу, безпеки даних і зниження ризиків.

Ні для кого не секрет, що економічна ситуація зараз диктує нові правила, зокрема і в конкурентній боротьбі. Якщо раніше «війна технологій», кібершпигунство і деструктивні дії були, в основному, долею великих корпорацій або цілих держав, то тепер ці методи цілком успішно застосовують у малому і середньому бізнесі.

Сайти офлайн-компаній поки залишимо осторонь, а сьогодні поговоримо про комерційні вебсайти, чий основний дохід пов'язаний з інтернет-діяльністю.

Аудит безпеки сайту - це комплекс робіт із виявлення помилок у коді сайту і програмному забезпеченні сервера, скориставшись якими зловмисники можуть атакувати і зламати сайт.

У наш час світова економічна ситуація відбувається в режимі конкурентної боротьби. якщо кілька років тому кібершпигунством і різноманітними атаками займалися величезні корпорації або цілі країни, то зараз ці методи застосовуються і в малому бізнесі.

Аудит безпеки вебсайту - це робота зі знаходження недоліків у коді сайту і всьому програмному забезпеченні

сервера, якими можуть скористатися хакери під час злому сайту. Мотиви злому сайту можуть бути різні. Зловмисники роблять це або за певним замовленням, для пошуку особистої вигоди або просто від нічого робити.

Ризики під час злому сайту просто величезні. Вони безпосередньо впливають на прибутковий дохід фірми. Але є ще й пряма загроза, наприклад, для інтернет-магазинів або електронних бірж. Це велика клієнтська база, яка зберігає в собі логіни, паролі, реквізити банківських карт для повторних покупок. За допомогою цієї інформації шахраї можуть легко виводити кошти з банківських карт звичайних людей.

Інтернет - злодіїв можна поділити на два види. Одні зламують сайт і беруть звідти все, «що погано лежить», інші користуються інформацією у своїх цілях і розміщують несанкціонований спам або рекламу. Якщо своєчасно проводити аудит безпеки, таких неприємностей можна уникнути.

До другої категорії можна віднести зловмисників, які йдуть на конкретну мету. Їм потрібно або отримати дані клієнтів, або знищити сайт повністю. У цьому разі атаки здійснюватимуть із завидною регулярністю, поки хакери не доб'ються бажаного результату, шляхом підбору паролів, логінів, шукатимуть різні вразливості сайту.

Аудит безпеки сайту - спосіб отримання адекватної оцінки ступеня захищеності ресурсів, отримання повної інформації про знайдені вразливості та рекомендації щодо їх усунення. Це безперервний, постійний процес із забезпечення безпеки всіх веб-ресурсів фірми, збереження ділової репутації та забезпечення збереження всіх особистих даних.

Істотно підвищити захищеність сайту може допомогти комплексний аудит безпеки, який зазвичай містить наступні дії:

-пошук вразливостей серверних компонентів;

-пошук вразливостей у веб-оточенні сервера;

-перевірка на віддалене виконання довільного коду;

-перевірка на наявність ін'єкцій (впровадження коду);

-спроби обходу системи аутентифікації веб-ресурсу;

-перевірка веб-ресурсу на наявність «XSS» / «CSRF» вразливостей;

-спроби перехопити привілейовані акаунти (або сесії таких акаунтів);

-спроби здійснити Remote File Inclusion / Local File Inclusion;

- пошук компонентів із відомими вразливостями;

-перевірка на перенаправлення на інші сайти і відкриті редиректи;

-сканування директорій і файлів, використовуючи перебір і «google hack»;

-аналіз пошукових форм, форм реєстрацій, форм авторизації тощо;

-перевірки ресурсу на можливість відкритого отримання конфіденційної та секретної інформації;

-атаки класу «race condition»;

-підбір паролів.

Для великих підприємств не варто чекати нападу шахраїв - потрібно замовити аудит безпеки у професіоналів, які в короткі терміни покажуть вам слабкі місця вашого сайту і забезпечать надійний захист. У нашому ж випадку для приватного використання буде достатньо перевірених онлайн сервісів для перевірки безпеки сайтів.

Розглянемо один із таких сервісів.

Веб-сканер QUTTERA (http://quttera.com).

Виконує пошук шкідливого коду на сторінках, використовуючи безсигнатурний аналіз. Тобто має певну евристику і виконує динамічний аналіз сторінок, що дає змогу виявляти 0-day загрози. З приємних особливостей варто відзначити можливість перевірки одразу кількох сторінок сайту, оскільки перевіряти по одній не завжди ефективно.

Добре виявляє загрози, пов'язані із завантаженням або розміщенням троянів, завірусованих виконуваних файлів.

Орієнтований на західні сайти з їх характерними зараженнями, але часто виручає і під час перевірки заражених сайтів інтернету. Оскільки сервіс безкоштовний, є черга на опрацювання завдань, тому доведеться трохи почекати.

4. Завдання

- вивчити можливості представлених сервісів для проведення аудиту сайтів на безпеку;
- проаналізувати критерії перевірки безпеки інтернет-ресурсів;
- провести аналіз сайту за допомогою наданих двох систем для перевірки аудиту сайтів.

Завдання 1. Знайомство з інтернет сервісами для перевірки безпеки сайту та виявлення критеріїв безпеки за двома запропонованими сервісами.

Знайомство з безплатними сервісами, які допомагають перевірити сайт на шахраїв онлайн. Вони аналізують сайт за посиланням та IP-адресою.

1. Зайдіть на сторінки сервісів: Google Transparency Report, Web Of Trust, Whois, VirusTotal
2. Проведіть перевірку будь-якого інтернет-ресурсу в цих двох сервісах.
3. Виявіть критерії перевірки та оцінювання безпеки цих інтернет-сервісів.
4. Заповніть таблиці за даними сервісами (приклад вище), вкажіть посилання на аналізовані сайти перед таблицею.
5. Зробити висновок за результатами перевірки та вставити у звіт

Таблиця 7.1.

Сервіс	Критерій оцінки безпеки	Отримані дані

5. Зміст звіту

Звіт повинен містити:

1. Назву роботи.
2. Мету роботи.
3. Завдання та його розв'язання.
4. Висновок щодо роботи.
5. Перелік використаних джерел.

6. Контрольні запитання

1. Яким способом можна істотно підвищити безпеку сайту?
2. Як називається робота зі знаходження недоліків у коді сайту та всьому програмному забезпеченні сервера.
3. Які дії включає в себе комплексний аудит?
4. Від якого головного чинника залежить ризик злому сайту?

Методичне забезпечення

1. 06-07-145S Рейнська, В. Б. (2024) Силабус навчальної дисципліни «Інформаційна безпека» для здобувачів вищої освіти ступеня «магістр», які навчаються за освітньо-професійною програмою «Соціальний менеджмент та інформаційна культура» спеціальності 028 «Менеджмент соціокультурної діяльності» галузі знань 02 «Культура і мистецтво». https://ep3.nuwm.edu.ua/view/shufr/06-07-145S.html

Література

Основна:

1. Герман, М. Л. Політика та стратегія державного регулювання інформаційної безпеки. Львів : Видавництво Львівського національного університету, 2017. 275 с.
2. Гончаров П. А. Менеджмент інформаційної безпеки: Основи та практичні аспекти. Львів : Видавництво ЛНУ ім. Івана Франка, 2020. 230 с.

3. ДаниловВ. С. Інформаційна безпека в умовах сучасних загроз. Львів : Видавництво Львівської політехніки, 2018. 256 с.
4. Зубарєв В. В. Організація системи захисту інформації: Теорія і практика. Київ : Видавництво НТУУ «КПІ», 2020. 300 с.
5. Кавун С. В. Інформаційна безпека :навчальний посібник. Харків : Вид. ХНЕУ, 2020. 352 с.
6. Козлов О. А. Теоретичні аспекти інформаційної безпеки. Одеса : Астропринт, 2016. 290 с.
7. Крючков С. В. Державне регулювання у сфері інформаційної безпеки України: Проблеми та рішення. Київ : Центр учбової літератури, 2021. 220 с.
8. Кудрявцев Ю. І. Основи інформаційної безпеки: Теорія та практика. Київ : Техніка, 2017. 320 с.
9. Лебедєв А. С. Управління системами інформаційної безпеки. Київ : Видавничий дім «КНТ», 2022. 270 с.
10. Петренко В. О. Інформаційна безпека України: Виклики та відповіді. Одеса : ОНУ ім. І. І. Мечникова, 2022. 240 с.
11. Романенко О. В. Методологія та практика забезпечення інформаційної безпеки. Київ : Видавництво Національного університету «Київська політехніка», 2021. 250 с.
12. Семенов М. І. Інформаційні загрози та їх класифікація. Харків : Національний технічний університет Харківського політехнічного інституту, 2019. 180 с.
13. Сергієнко В. О. Підходи до забезпечення інформаційної безпеки в умовах воєнного стану. Харків : Видавництво ХНУРЕ, 2023. 260 с.
14. Тимошенко І. В. Принципи та методи забезпечення інформаційної безпеки. Дніпро : Дніпровський національний університет імені Олеся Гончара, 2019. 245 с.
15. Черненко А. В. Теоретичні та практичні аспекти менеджменту інформаційної безпеки. Київ : Видавництво «Міжнародні відносини», 2022. 300 с.
16. Шевченко І. М. Аудит систем інформаційної безпеки. Київ : Видавництво «Юрінком Інтер», 2018. 210 с.

Допоміжна:

17. Богуш В., Бровко В., Настрадін В. Основи кіберпростору, кіберзахисту та кібербезпеки. Видавництво: Ліра-К., 2021. 554 с.
18. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань» : монографія. Київ-Одеса : Фенікс, 2021. 176 с.
19. Інтеграція цифрових технологій в освітній процес: виклики та перспективи : монографія / Саєнко Н. С., Голуб Т. П., Лавриш Ю. Е., Лук'яненко В. В., Литовченко І. М. Видавництво: Центр навчальної літератури, 2022. 220 с.
20. Кулініч О. О. Охорона та захист прав інтелектуальної власності: економіко-правові підходи. Видавництво «Ліра-К», 2019. 276 с.
21. Ланде Д. В. Правові питання конкурентної розвідки. *Інформація і право.* 2020. 2(33). С. 51–68. DOI: https://doi.org/10.37750/2616- 6798.2020.2(33).208089
22. Росс А. Індустрії майбутнього. Видавництво «Наш Формат», 2022. 320 с.

Інформаційні джерела

1. Національний центр кібербезпеки України. Теоретичні аспекти інформаційної безпеки. URL: https://ncc.gov.ua/ (дата звернення: 01.09.2024).
2. Інститут інформаційної безпеки. Теоретичні основи інформаційної безпеки. URL: https://iis.org.ua/theory-information-security (дата звернення: 01.09.2024).
3. Міністерство цифрової трансформації України. Захист інформаційних систем. URL: https://thedigital.gov.ua/ (дата звернення: 01.09.2024).

4. Міністерство культури та інформаційної політики України. URL: https://mkip.gov.ua/
5. Ukrainian Cyber Security Group. Поняття інформаційних загроз. URL: https://ucsg.org.ua/ (дата звернення: 01.09.2024).
6. Центр моніторингу та захисту інформації. Підходи до забезпечення інформаційної безпеки. URL: https://cmpi.gov.ua/ (дата звернення: 01.09.2024).
7. Методи забезпечення інформаційної безпеки. Інтернет-ресурс. URL: https://it-ukraine.org.ua/methods-information-security (дата звернення: 01.09.2024).
8. CyberSecurity in Ukraine. Державне регулювання в умовах воєнного стану. URL: https://cybersecurity.com.ua/ (дата звернення: 01.09.2024).
9. Аудит і безпека інформації. Основи аудиту систем інформаційної безпеки. URL: https://auditinfosec.com.ua/ (дата звернення: 01.09.2024).
10. Інститут безпеки та захисту інформації. Організація системи захисту інформації. URL: https://ibzi.org.ua/ (дата звернення: 01.09.2024).
11. Кібербезпека України. Принципи і методи забезпечення інформаційної безпеки. URL: https://cybersecurity.gov.ua/ (дата звернення: 01.09.2024).
12. Центр інформаційної безпеки. Поняття інформаційних загроз. URL: https://cib.org.ua/ (дата звернення: 01.09.2024).
13. Управління інформаційною безпекою в Україні. Управління та менеджмент систем інформаційної безпеки. URL: https://info-security.ua/ (дата звернення: 01.09.2024).
14. Безпека даних та інформації. Підходи та засоби захисту інформації. URL: https://datasecurity.com.ua/ (дата звернення: 01.09.2024).

15. Безпека інформаційних систем в Україні. Принципи забезпечення безпеки. URL: https://securitysys.org.ua/ (дата звернення: 01.09.2024).
16. Проблеми та рішення в інформаційній безпеці. Менеджмент і аудит систем інформаційної безпеки. URL: https://info-problems.com.ua/ (дата звернення: 01.09.2024).