Література:
Інформатика 10(11) кл. Й.Я. Ривкінд
Інформатика 11 кл. В.Руденко

№ урока	Дата	Тема урока	Домашнє завдання
1	19.10.20	**Тема 1**.Інформаційні технології в суспільстві. Основні поняття інформатики .Сучасні інформаційні технології та системи.	Інформатика 10(11) кл. Й.Я. Ривкінд Стор.5. Відповісти на питання на стор.6
2	19.10.20	Проблеми інформаційної безпеки	Інформатика 10(11) кл. Й.Я. Ривкінд. Стор.10 Відповісти на питання .
3	21.10.20	Навчання в Інтернеті	Інформатика 10(11) кл. Й.Я. Ривкінд Стор.15 Дайте відповіді на запитання стор.18
4	21.10.20	Комп'ютерно - орієнтовані засоби діяльності	Інформатика 10(11) кл. Й.Я. Ривкінд стор.18 - 22 Дайте відповіді на запитання і виконайте завдання в кінці теми.
5	26.10.29	Інтернет - комерція Електронне урядування.	Інформатика 10(11) кл. Й.Я. Ривкінд Стор.23 Дайте відповіді на запитання і виконайте завдання в кінці теми
6	26.10.29	Штучний інтелект.Інтернет речей. Smart-технології	Інформатика 10(11) кл. Й.Я. Ривкінд Стор.29
7	28.10.20	Тематичне оцінювання.	Інформатика 10(11) кл. Й.Я. Ривкінд. Надати конспект з виконаними завданнями для перевірки
8	28.10.20	Поняття бази даних і системи управління базами даних.	Інформатика 11 кл. В.Руденко стор.4 - 6 Дайте відповіді на запитання і виконайте завдання в кінці теми.
9	02.11.20	Поняття моделі	Інформатика 11 кл.

		даних	В.Руденко Стор.7 - 10 Дайте відповіді на запитання і виконайте завдання в кінці теми.
10	02.11.20	Основні відомості про системи управління базами даних Access.	Інформатика 11 кл. В.Руденко Стор.11 - 13 Дайте відповіді на запитання і виконайте завдання в кінці теми.
11	04.11.20	Створення й введення структури таблиць	Інформатика 11 кл. В.Руденко Стор.14 - 18 Дайте відповіді на запитання і виконайте завдання в кінці теми.
12	09.11.20	Ключові поля,індекси,зв'язування таблиць.	Інформатика 11 кл. В.Руденко Стор.19 - 22 Дайте відповіді на запитання і виконайте завдання в кінці теми.
13	11.11.20	Ведення ,пошук і редагування даних у таблиці	Інформатика 11 кл. В.Руденко Стор.23 - 25 Дайте відповіді на запитання і виконайте завдання в кінці теми.
14	11.11.20	Сортування і фільтрування записів.операції над таблицями.	Інформатика 11 кл. В.Руденко Стор.26 - 28 Дайте відповіді на запитання і виконайте завдання в кінці теми.
15	16.11.20	Загальні відомості про запити.	Інформатика 11 кл. В.Руденко Стор.29 - 31 Дайте відповіді на запитання і виконайте завдання в кінці теми
16	16.11.20	Запити на вибірку даних.	Інформатика 11 кл. В.Руденко Стор.32-34 Дайте відповіді на запитання і виконайте завдання в кінці теми
17	18.11.20	Запити з функціями і з полями,що обчислюються	Інформатика 11 кл. В.Руденко Стор.35 - 38 Дайте відповіді на запитання і виконайте завдання в кінці теми
18	18.11.20	Запити з	Інформатика 11 кл.

		параметрами.Перехресні запити.	В.Руденко Стор.39-41 Дайте відповіді на запитання і виконайте завдання в кінці тем
19	23.11.20	Створення інтерфейсу користувача для введення даних у базу даних.	Інформатика 11 кл. В.Руденко Стор.42-44 Дайте відповіді на запитання і виконайте завдання в кінці теми
20	23.11.20	Основи мови запитів SQl.Імпорт і експорт об'єктів баз даних.	Інформатика 11 кл. В.Руденко Стор.45- 51 Дайте відповіді на запитання і виконайте завдання в кінці тем
21	25.11.20	Тематичне оцінювання. Урок підсумок.	Повторення всього матеріалу .
Дистанційне навчання з 07.10.21			
6	13.10.21	Основні ненавмисні і навмисні штучні загрози. Технічні засоби добування інформації.	Загрози, які можуть завдати шкоди інформаційній безпеці організації, можна розділити на кілька категорій . 1) До дій, що здійснюються авторизованими користувачами, належать: цілеспрямована крадіжка або знищення даних на робочій станції чи сервері; пошкодження даних користувачами в результаті необережних дій. 2) Дії хакерів: Хакер — кваліфікований IT-фахівець, який знається на комп'ютерних системах і втручається в роботу комп'ютера, щоб без відома власника дізнатися деякі особисті відомості або пошкодити дані, що зберігаються в комп'ютері. Їхні мотиви можуть бути різними: помста, самовираження (дехто робить це задля розваги, інші — щоб показати свою кваліфікацію), винагорода. Останнім часом поняття «хакер» використовується для визначення мережевих зломщиків, розробників

			комп’ютерних вірусів й інших кіберзлочинців. У багатьох країнах злом комп’ютерних систем, розкрадання інформаційних даних, створення та поширення комп’ютерних вірусів і шкідливого програмного забезпечення переслідується законодавством. 3) Окрема категорія електронних методів впливу — комп’ютерні віруси та інші шкідливі програми (Malware). Вони становлять реальну небезпеку, широко використовуючи комп’ютерні мережі, Інтернет й електронну пошту. 4) DoS-атакою, або DDos-атакою (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack — атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні) - напад на комп’ютерну систему з наміром зробити комп’ютерні ресурси недоступними користувачам, для яких комп’ютерна система була призначена. 5) Спам — небажані рекламні електронні листи, повідомлення на форумах, телефонні дзвінки чи текстові повідомлення, що надходять без згоди користувача.Не будучи джерелом прямої загрози, небажана кореспонденція збільшує навантаження на поштові сервери, створює додатковий трафік, засмічує поштову скриньку користувача, веде до втрати робочого часу і тим самим наносить значні фінансові втрати. Зловмисники стали використовувати так звані спамерські технології масового розповсюдження, щоб примусити користувача відкрити лист, перейти по посиланню з листа на якийсь інтернет-

			ресурс. Отже, можливості фільтрації спаму важливі не лише самі по собі, але і для протидії інтернет-шахрайству і розповсюдженню шкідливих програм. 6) Фішинг — один з найпопулярніших і прибуткових (для тих, хто його реалізує) видів атак. Сценарій атак фішингу: зловмисник створює сайт, який у точності копіює дизайн і можливості сайта будь-якого банку,інтернет-магазину або платіжної системи. Далі він замовляє спам-розсилку листів, у яких переконує своїх жертв зайти за посиланням на сайт і заповнити будь-яку форму з внесенням персональних даних. Здебільшого причиною запиту даних зазначається повідомлення про збій в інформаційній системі й загрозу блокування профілю користувача, якщо не буде надано дані. Мета — збір конфіденційної інформації — паролі, коди тощо. 7) Кардинг - У зв'язку з появою кредитних карт, електронних грошей і можливістю їхнього використання через Інтернет інтернет-шахрайство стало одним з найбільш поширених злочинів. 8) Інтернет шахрайство 9) бот-мережі (botnet) – це мережа пов'язаних між собою вірусом комп'ютерів, які керуються зловмисниками з командного центру. 10) «крадіжка особистості» (Identity Theft) **Домашнє завдання** . 1. Створити спільну презентацію про загрози,використовуючи можливості Google Диску. 2.Дайте відповіді на питання: • На які види поділяються загрози інформаційній безпеці залежно від обсягів завданих збитків? • На які види поділяються загрози інформаційній безпеці залежно від результатів шкідливих дій?

			• Які чинники можуть становити загрозу комп'ютеру? Опрацювати конспект та перегляньте стор.11 Відповісти на питання в кінці теми. **Інформатика 10(11) кл. Й.Я.Ривкінд**
7	20.10.21	Інструктаж БЖД.. Практична робота №1 "Використання програмних засобів для тестування та очищення операційної системи від вірусів та шкідливого програмного забезпечення..	Однією з небезпечних загроз є витік інформації технічними каналами і добування інформації програмними засобами. Технічні і програмні засоби добування необхідної інформації - це подолання системи захисту, обмеження або заборона доступу до них посадових осіб, дезорганізації роботи технічних засобів, вивід з ладу комунікаційних і комп'ютерних мереж, усього високотехнологічного забезпечення функціонування системи управління. Спроба одержати несанкціонований доступ до комп'ютерної мережі з метою ознайомитися з нею, залишити інформацію, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як «комп'ютерне піратство». Способи несанкціонованого доступу до інформації здійснюються шляхом: 1.Застосування засобів прослуховування, фото, відеоапаратури, підкуп осіб, використання «троянських» програм; 2) Використання недоліків мови програмування і недоліків в операційної системи, крадіжка носіїв інформації, копіювання інформації; 3) Отримання захищених даних за допомогою запитів дозволу, реквізитів розмежування доступу, таємних паролів. Технічні засоби істотно розширюють і доповнюють можливості людини з добування інформації, забезпечуючи:

			а) знімання інформації з носіїв, які недоступні органам почуттів людини; б) добування інформації без порушення кордонів контрольованої зони; в) передачу інформації практично в реальному масштабі часу в будь-яку точку земної кулі; г) аналіз і обробку інформації в обсязі і за час, недосяжних людині; д) консервацію і як завгодно довгий зберігання видобутої інформації. Технічні засоби добування інформації та їх класифікація (схема в презентації) До технічних і програмних засобів ведення інформаційної боротьби відносять : • комп'ютерний вірус (КВ)- спеціальна програма, що впроваджується в “чуже електронне середовище”. КВ спроможний передаватися по лініях зв'язку і мережам обміну інформацією, проникати в електронні телефонні станції і системи управління. У заданий час або по сигналу КВ стирає інформацію , що зберігається в БД, або довільно змінює її. • логічна бомба (ЛБ)- так звана програмна закладка, що завчасно впроваджується в інформаційні системи і мережі. ЛБ по сигналу, або у встановлений час, приводиться в дію, стираючи або перекручуючи інформацію в інформаційних ресурсах і виводить їх з ладу; • ”троянський кінь” (різновид ЛБ)- програма, що дозволяє здійснювати схований, несанкціонований доступ до інформаційних ресурсів для добування даних; • засоби впровадження КВ і ЛБ в інформаційні ресурси ОУ і керування ними на відстані. Для цих засобів найбільш вразливими є інформаційні ресурси виявлення і управління, що постійно діють у встановлених режимах реального часу.

			• ”нейтралізатори текстових програм,” це програми, що забезпечують невиявлення випадкових і навмисних хиб програмного забезпечення; • засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах ; Шкідливе ПЗ Зловмисний програмний засіб або зловмисне програмне забезпечення (англ. Malware - скорочення від malicious - зловмисний і software - програмне забезпечення) — програма, створена зі злими намірами. До зловмисних програмних засобів належать віруси, рекламне ПЗ, хробаки, троянці, руткіти, клавіатурні логери, дозвонювачі, шпигунські програмні засоби, здирницькі програми, шкідливі плаґіни та інше зловмисне програмне забезпечення. Класифікація: За видом програмного забезпечення - програми, що вимагають програм-носіїв - люки; - логічні бомби; - троянські коні; - віруси. - програми, що є незалежними. - черв’яки, - зомбі; - утиліти прихованого адміністрування; - програми-крадії паролів; - “intended”-віруси; - конструктори вірусів; - поліморфік-генератори. За наявністю матеріальної вигоди • що не приносять пряму матеріальну вигоду тому, хто розробив (встановив) шкідливу програму: • хуліганство, жарт; • самоствердження, прагнення довести свою кваліфікацію; • що приносять пряму матеріальну вигоду зловмисникові: • крадіжка конфіденційної інформації, включаючи діставання доступу до

			систем банк-клієнт, отримання PIN кодів кредитних карток і таке інше; • отримання контролю над віддаленими комп'ютерними системами з метою розповсюдження спаму з численних комп'ютерів-зомбі; За метою розробки • програмне забезпечення, яке з самого початку розроблялося спеціально для забезпечення несанкціонованого доступу до інформації, що зберігається на ПК з метою спричинення шкоди (збитку) власникові інформації і/або власникові ПК. • програмне забезпечення, яке з самого початку не розроблялися спеціально для забезпечення діставання несанкціонованого доступу до інформації. Різновиди шкідливих програм: Люк (trapdoor) – це прихована, недокументована точка входу в програмний модуль, яка дозволяє кожному, хто про неї знає, отримати доступ до програми в обхід звичайних процедур, призначених для забезпечення безпеки КС. Люк вставляється в програму в більшості випадків на етапі налагодження для полегшення роботи – даний модуль можна буде викликати в різних місцях, що дозволяє налагоджувати окремі його частини незалежно одна від одної. Логічна бомба – це код, що поміщається в деяку легальну програму. Він влаштований таким чином, що при певних умовах “вибухає”. Умовою для включення логічної бомби може бути наявність або відсутність деяких файлів, певний день тижня або певна дата, а також запуск додатку певним користувачем.

			Хробаки – вид вірусів, які проникають на комп'ютер-жертву без участі користувача. Хробаки використовують так звані «дірки» (уразливості) у програмному забезпеченні операційних систем, щоб проникнути на комп'ютер. Вразливості – це помилки і недоробки в програмному забезпеченні, які дозволяють віддалено завантажити і машинний код, в результаті чого вірус- хробак потрапляє в операційну систему і, як правило, починає дії по зараженню інших комп'ютерів через локальну мережу або Інтернет. Зловмисники використовують заражені комп'ютери користувачів для розсилки спаму або для DDoS-атак. Так само як для вірусів, життєвий цикл хробаків можна розділити на певні стадії: 1. Проникнення в систему 2. Активація 3. Пошук "жертв" 4. Підготовка копій 5. Поширення копій На етапі проникнення в систему хробаки діляться переважно по типах використовуваних протоколів: • Мережні хробаки - чирви, що використають для поширення протоколи Інтернет і локальні мережі. Звичайно цей тип хробаків поширюється з використанням неправильної обробки деякими додатками базових пакетів стека протоколів tcp/ip • Поштові хробаки - чирви, що поширюються у форматі повідомлень електронної пошти • IRC-хробаки - хробаки, що поширюються по каналах IRC (Internet Relay Chat)

			• P2P-хробаки - чирви, що поширюються за допомогою пірінгових (peer-to-peer) файлообмінних мереж • IM-хробаки - хробаки, що використають для поширення системи миттєвого обміну повідомленнями (IM, Instant Messenger - ICQ, MSN Messenger, AIM й ін.) Аналогічно, хробаки можуть міняти тему й текст інфікованого повідомлення, ім'я, розширення й навіть формат вкладеного файлу - виконує модуль, що, може бути прикладений як є або в заархівованому виді. Віруси – трояни Троян (троянський кінь) — тип шкідливих програм, основною метою яких є шкідливий вплив стосовно комп'ютерної системи. Трояни відрізняються відсутністю механізму створення власних копій. Деякі трояни здатні до автономного подолання систем захисту КС, з метою проникнення й зараження системи. У загальному випадку, троян попадає в систему разом з вірусом або хробаком, у результаті необачних дій користувача або ж активних дій зловмисника. У силу відсутності в троянів функцій розмноження й поширення, їхній життєвий цикл украй короткий - усього три стадії: • Проникнення на комп'ютер • Активація • Виконання закладених функцій Троян може тривалий час непомітно перебувати в пам'яті комп'ютера, ніяк не видаючи своєї присутності, доти, поки не буде виявлений антивірусними засобами. Способи проникнення на комп'ютер користувача трояни вирішують звичайно

			одним із двох наступних методів. Маскування — троян видає себе за корисний додаток, що користувач самостійно завантажує з Інтернет і запускає. Іноді користувач виключається із цього процесу за рахунок розміщення на Web- сторінці спеціального скрипта, що використовуючи діри в браузері автоматично ініціює завантаження й запуск трояна. До даної групи шкідливих програм відносять: - програми-вандали, - «дроппери» вірусів, - «злі жарти», - деякі види програм-люків; - деякі логічні бомби, - програми вгадування паролів; - програми прихованого адміністрування. Зомбі - це програма, яка приховано під'єднується до інших підключених в Інтернет комп'ютерів, а потім використовує цей комп'ютер для запуску атак, що ускладнює відстеження шляхів до розробника програми-зомбі. "Жадібні" програми (greedy program). - це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використовувати його. Доступ таких програм до ресурсів системи призводить до порушення її доступності для інших програм. Захоплювачі паролів - це спеціально призначені програми для крадіжки паролів. Утиліти схованого адміністрування (backdoor) Цей вид шкідливого програмного забезпечення у деяких випадках можна віднести до групи троянських коней. Вони по своїй суті є досить могутніми утилітами віддаленого

			адміністрування комп'ютерів у мережі Під час запуску троянська програма встановлює себе в системі і потім стежить за нею, при цьому користувачу не видається ніяких повідомлень про дії такого трояна в системі. (**Інструктаж з правил техніки безпеки).** **Завдання 1**. Знайдіть відомості в Інтернеті та складіть список з 10 найбільш небезпечних комп'ютерних вірусів. Визначте, з якою метою вони були створені. Подайте знайдені відомості в текстовому документі у зручному вигляді **Завдання 2**. Виконайте інтерактивну вправу **https://learningapps.org/7076420** Домашнє завдання 1) Опрацювати конспект 2) Ознайомитися з інформацією про віруси і шкідливі програми на сайті Zillya! (вірусна енциклопедія) Дослідити типи шкідливих програм (virus Trojan, Backdoor, Dropper, Downloader, Tool, Adware, Dialer, Worm, Exploit, Rootkit), скористайтеся даними на сайті Zillya! (вірусна енциклопедія) Творче завдання: Засобами редактора презентацій створіть ілюстрований інтерактивний словник термінів, які виникають при захисті від можливих загроз користувача Інтернету. Передбачте, що користувач може обирати термін у списку та переходити на сторінку із тлумаченням терміна. На такій сторінці може бути ілюстрація, що відображає зміст терміна, корисне посилання на ресурс в Інтернеті, де можна детальніше ознайомитися з поняттям..
8	27.10.21	Тематичне оцінювання	Підготуватися до контрольної роботи Контрольна робота по темі : "Основи безпеки інформаційних технологій." Контрольні запитання на стор.14

			Інформатика 10(11) кл. Й.Я.Ривкінд 1.• На які види поділяються загрози інформаційній безпеці залежно від обсягів завданих збитків? • На які види поділяються загрози інформаційній безпеці залежно від результатів шкідливих дій? • Які чинники можуть становити загрозу комп'ютеру?
9	03.11.21	Об'єкти захисту,види заходів протидії загрозам безпеки.Переваги та недоліки різних видів заходів захисту.	В основі комплексу заходів щодо інформаційної безпеки повинна бути стратегія захисту інформації. У ній визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи захисту. Найважливішою особливістю загальної стратегії інформаційного захисту є дослідження системи безпеки. Можна виділити два основних напрямки: • аналіз засобів захисту; • визначення факту вторгнення. На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації, а далі – політика безпеки інформації Розробку концепції захисту рекомендується проводити в три етапи: I етап – визначення цінності об'єкта захисту інформації. II етап – аналіз потенційних дій зловмисників III етап – оцінка надійності встановлених засобів захисту інформації на об'єкті. На першому етапі повинна бути чітко визначена цільова установка захисту, тобто які реальні цінності, виробничі процеси, програми, масиви даних необхідно захищати. На цьому етапі доцільно диференціювати за значимістю окремі об'єкти, що вимагають захисту, та, у відповідності до цього, встановлення ступенів захисту об'єктів і елементів технічного і програмного забезпечення ІАС (файлів, програм, пакетів дисків, ПЕОМ в цілому). Об'єктом спільного використання є пам'ять, пристрої введення-виведення (наприклад, диски, принтеры), програми, дані. На другому етапі повинен бути проведений аналіз злочинних дій,

			що потенційно можуть бути зроблені стосовно об'єкта, що захищається, визначення усіх можливих загроз та каналів витоку інформації. Важливо визначити ступінь реальної небезпеки таких найбільш широко розповсюджених злочинів, як економічне шпигунство, саботаж, крадіжки зі зломом. Потім потрібно проаналізувати найбільш ймовірні дії зловмисників стосовно основних об'єктів, що потребують захисту. Головною метою третього етапу є аналіз обставин, у тому числі місцевих специфічних умов, виробничих процесів, уже встановлених технічних засобів захисту. Визначаються вимоги до системи захисту, здійснюється вибір заходів, методів і засобів захисту інформації та їх впровадження і організація використання. У загальному випадку існують чотири стратегії захисту. 1. Нікого не впускати. Це повна ізоляція. Вона забезпечує найкращий захист, але перешкоджає використанню інформації або послуг від інших, і передачі їх іншим користувачам. Це непрактично для всіх. 2. Не впускати порушників. Програми всередині цього захисту можуть бути легковірними. Це дозволяє зробити електронні цифрові підписи програм і міжмережеві екрани (МЕ). 3. Пустити порушників, але перешкодити їм в заподіянні шкоди. Традиційним способом захисту служить динамічне ПЗ типу sandboxing, що створює в комп'ютері захищений простір (sandbox), в якому може виконуватися підозрілий код, і в типовому випадку використовує контроль доступу до ресурсів, щоб визначити порушення. 4. Захопити порушників і переслідувати їх. Це роблять аудит і силові структури Види заходів протидії загрозам безпеки Всі заходи протидії комп'ютерним злочинам, що безпосередньо забезпечують безпеку інформації, можна підрозділити на: • правові; • організаційно-адміністративні; • інженерно-технічні. До правових заходів варто віднести розробку норм, що встановлюють відповідальність за

			комп'ютерні злочини, захист авторських прав програмістів, удосконалення карного і цивільного законодавства, а також судочинства. До організаційно-адміністративних заходів відносяться: охорона комп'ютерних систем, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією. людиною, наявність плану відновлення працездатності центру після виходу його з ладу, обслуговування обчислювального центру сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення роботи центру, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво), покладання відповідальності на осіб, що повинні забезпечити безпеку центру, вибір місця розташування центру і т.п. До інженерно-технічних заходів можна віднести: 1) захист від несанкціонованого доступу до комп'ютерної системи, 2) резервування важливих комп'ютерних систем, 3) забезпечення захисту від розкрадань і диверсій, 4) резервне електроживлення, розробку і реалізацію спеціальних програмних і апаратних комплексів безпеки тощо. Фізичні засоби містять у собі різні інженерні засоби, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту, що захищають персонал (особисті засоби безпеки), матеріальні засоби і фінанси, інформацію від протиправних дій. До апаратних засобів відносяться прилади, пристрої, пристосування та інші технічні рішення, які використовуються в інтересах забезпечення безпеки. У практиці діяльності будь-якої організації знаходить широке застосування різна апаратура: від телефонного апарату до розроблених автоматизованих інформаційних систем, що забезпечують її виробничу діяльність. Основна задача апаратних засобів - стійка безпека комерційної діяльності. Програмні засоби - це спеціальні програми, програмні комплекси і системи захисту

			інформації в інформаційних системах різного призначення і засобах обробки даних. Криптографічні засоби - ця спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по мережах зв'язку, збереженої та обробленої на комп'ютерах з використанням методів шифрування. Всі заходи являють собою складну систему захисту, визначаються та проводяться в тісному взаємозв’язку на всіх етапах розробки, створення та функціонування ІАС. Основні принципи побудови системи безпеки інформації Загальновідомо, що відділам безпеки, які займаються захистом інформації, протистоять різні організації і зловмисники, як правило, оснащені апаратними засобами доступу до інформації. Виходячи з цього, основу захисту інформації повинні складати принципи, аналогічні принципам отримання інформації, а саме: − безперервність захисту інформації. Характеризується постійною готовністю системи захисту до відбиття загроз інформаційній безпеці в будь-який час; − активність, яка передбачає прогнозування дій зловмисника, розробку і реалізацію випереджаючих захисних заходів; − скритність, що виключає ознайомлення сторонніх осіб із засобами і технологією захисту інформації; − цілеспрямованість, яка передбачає зосередження зусиль щодо запобігання загроз найбільш цінної інформації − комплексне використання різних способів і засобів захисту інформації, що дозволяє компенсувати недоліки одних перевагами інших. При побудові системи захисту інформації потрібно враховувати також наступні принципи: - мінімізація додаткових завдань і вимог до співробітників організації, викликаних заходами щодо захисту інформації; - надійність в роботі технічних засобів системи, що виключає як не реагування на погрози (пропуски загроз) інформаційної безпеки, так і помилкові реакції при

			їх відсутності; - обмежений і контрольований доступ до елементів системи забезпечення інформаційної безпеки; - безперервність роботи системи в будь-яких умовах функціонування об'єкта захисту, в тому числі, наприклад, короткочасному відключенні електроенергії; - адаптованість (пристосовність) системи до змін навколишнього середовища. Система захисту інформації повинна задовольняти такі умови: • охоплювати весь технологічний комплекс інформаційної діяльності; • бути різноманітною за використовуваними засобами, багаторівневою з ієрархічною послідовністю доступу; • бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації; • бути нестандартною, різноманітною. Вибираючи засоби захисту не можна розраховувати на непоінформованість зловмисників щодо її можливостей; • бути простою для технічного обслуговування і зручною для експлуатації користувачами; • бути надійною. Будь-які несправності технічних засобів є причиною появи неконтрольованих каналів витоку інформації; • бути комплексною, мати цілісність, що означає, що жодна її частина не може бути вилучена без втрат для всієї системи. До системи безпеки інформації висуваються також певні вимоги: • чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації; • надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи; • зведення до мінімуму кількості спільних для декількох користувачів засобів захисту; • облік випадків і спроб несанкціонованого доступу до конфіденційної інформації; • забезпечення оцінювання ступеня конфіденційної інформації; • забезпечення контролю цілісності зас обів захисту і негайне реагування на вихід їх з ладу. **Д/З:Створіть текстовий документ, що містить відомості про систему інформаційної безпеки. Подайте**

			знайдені відомості в текстовому документі у зручному вигляді (таблиці, схеми тощо). Розмістіть роботу на Google-диску, надайте доступ, для перегляду і редагування викладачу. Опанувати конспект.
10	10.11.21	Правові основи забезпечення безпеки інформаційних технологій.	**Правові методи** — встановлюють правила користування інформацією та відповідальність користувачів за їх порушення. Це — чинні закони, укази та інші нормативні акти, які регламентують правила користуванняі нформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання інформаційних технологій (IT). Правовий захист інформації (даних) передбачає: • наявність прав на інформацію — сертифікацію, ліцензування, патентування; • реалізацію прав — захист інтелектуальної власності, захист авторських прав; • контроль за процедурами реалізації прав — систему адміністративного, програмного, фізико-технічного захисту інформації. На законодавчому рівні в Україні прийнято кілька законів та видано постанови Кабінету Міністрів щодо забезпечення інформаційної безпеки. Серед них можна назвати: · Закон України «Про інформацію»; · Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»; · Закон України «Про державну таємницю»; · Закон України «Про захист персональних даних» · Постанову Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». У вищезгаданих «Правилах», вказується, зокрема, що: Захисту в системі підлягає: · відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка

			оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами; · конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації»; · службова інформація; · інформація, яка становить державну або іншу передбачену законом таємницю; · інформація, вимога щодо захисту якої встановлена законом. Відкрита інформація під час опрацювання в системі має зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам має бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише користувачі, яким надано відповідні повноваження. В Україні створено Державну службу спеціального зв'язку та захисту інформації України — державний орган спеціального призначення, який опікується питаннями забезпечення формування і реалізації державної політики у сферах захисту державних інформаційно-телекомунікаційних систем, криптографічного й технічного захисту інформації, використання і захисту державних електронних інформаційних ресурсів. Класифікація порушників кібербезпеки Ха́кер (від англ. to hack – рубати) – особливий тип комп'ютерних спеціалістів. Нині так часто помилково називають комп'ютерних хуліганів, тобто тих, хто здійснює неправомірний доступ до комп'ютерів та інформації. Інколи цей термін використовують для позначення спеціалістів взагалі — у тому контексті, що вони мають дуже детальні знання в якихось питаннях, або мають достатньо нестандартне і конструктивне мислення. За однією з легенд,

			слово «hack» уперше стало застосовуватись у Массачусетському технологічному інституті для позначення проекту, який не має видимого практичного значення і виконується виключно заради задоволення від самого процесу роботи. У більш вузькому Хакери (хакери) — це узагальнююча назва людей, які зламують комп'ютерні системи і одержують неправомірний доступ до ресурсів. Для запобігання можливих загроз, фірми повинні не тільки забезпечити захист операційних систем, програмного забезпечення і контроль доступу, але і спробувати виявити категорії порушників і ті методи, які вони використовують. Залежно від мотивів, мети та методів, дії порушників безпеки інформації можна поділити на чотири категорії: • шукачі пригод; • ідейні «хакеры»; • «хакери»-професіонали; • ненадійні (неблагополучні) співробітники Шукач пригод рідко має продуманий план атаки. Він вибирає мету випадковим чином і звичайно відступає, зіштовхнувшись із ускладненнями. Знайшовши діру в системі безпеки, він намагається зібрати закриту інформацію, але практично ніколи не намагається її таємно змінити. Своїми перемогами такий шукач пригод ділиться тільки зі своїми близькими друзями-колегами.Ідейний «хакер» - це той же шукач пригод, але більш майстерний. Він уже вибирає собі конкретні цілі (хости і ресурси) на підставі своїх переконань. Його улюбленим видом атаки є зміна інформаційного наповнення Webсервера або, рідше, блокування роботи ресурсу, що атакується. У порівнянні із шукачем пригод, ідейний «хакер» розповідає про успішні атаки набагато більшій аудиторії, звичайно розміщаючи інформацію на хакерському Webвузлі. «Хакер»-професіонал має чіткий план дій і спрямовує його на визначені ресурси. Його атаки добре продумані і, звичайно, здійснюються у кілька етапів. Спочатку він збирає попередню інформацію (тип ОС, надані сервіси і міри захисту). Потім він складає план атаки з

			урахуванням зібраних даних і підбирає (або навіть розробляє) відповідні інструменти. Далі, провівши атаку, він одержує закриту інформацію і, нарешті, знищує всі сліди своїх дій. Такий професіонал звичайно добре фінансується і може працювати один або у складі команди професіоналів. Ненадійний (неблагополучний) співробітник своїми діями може спричинити стільки ж проблем (буває і більше), скільки промисловий шпигун, до того ж, його присутність звичайно складніше знайти. Крім того, йому доводиться долати не зовнішній захист мережі, а тільки, як правило, менш жорсткіший, внутрішній. Він не такий витончений у способах атаки, як промисловий шпигун, і тому частіше допускає помилки, і тим самим може видати свою присутність. Сьогодні, зі стрімким розвитком Internet, «хакери» стають справжньою загрозою для державних і корпоративних комп'ютерних мереж. Так, за оцінками експертів США, напади «хакерів» на комп'ютери і мережі федеральних державних систем відбуваються в цій країні не рідше 50-ти раз на день. Багато великих компаній і організації піддаються атакам кілька разів у тиждень, а деякі навіть щодня. Виходять такі атаки не завжди ззовні, 70% спроб зловмисного проникнення в комп'ютерні системи мають джерело всередині самої організації. Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: «хакери», «кракери», «пірати», «шкідники». Останнє відрізняє хакерів від професійних зламувачів — кракерів (або «крекерів», не плутати з печивом!), які є серйозними порушниками безпеки, оскільки не мають жодних моральних обмежень.

			Найбільш криміногенною групою є пірати — професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, природно, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може зосередитися на кредитних картках, банківських рахунках, телефонному зв’язку. В усіх випадках мотивація – матеріальні інтереси, а не цікавість чи пустощі. За даними дослідження корпорації IDG у 88 % випадків розкрадання інформації відбувається через працівників фірм і тільки 12 % — через зовнішні проникнення із застосуванням спеціальних засобів. Шкідники (вандали) намагаються реалізувати у кіберпросторі свої патологічні схильності — вони заражають його вірусами, частково або повністю руйнують комп'ютерні системи. Найчастіше вони завдають шкоди без якої-небудь вигоди для себе (крім морального задоволення). Часто спонукальним мотивом є помста. Іноді шкідника надихає масштаб руйнівних наслідків, значно більший за можливі позитивні успіхи від аналогічних зусиль. Експериментатори («піонери») - найчастіше це молоді люди, які під час освоєння інструментальних та інформаційних ресурсів Мережі і власного комп'ютера бажають вчитися тільки на власних помилках, відштовхуючись від того, «як не можна». **Домашнє завдання** 1) Опрацювати конспект 2) Створіть інформаційний бюлетень із правилами комп’ютерного етикету.

			3)Розмістіть роботу на Google-диску, надайте доступ, для перегляду викладачу. 4)Дайте відповіді на питання: 4.1Які розрізняють етичні та правові основи захисту даних? 4.2. Що таке інформаційна етика? 4.3.Чи існує “хакерська” етика? В чому вона полягає?
11	11.11.21	**Ідентифікація та автентифікація користувачів. Розмежування доступу зареєстрованих користувачів до ресурсів автоматизованих систем. Реєстрація та оперативне оповіщення про події безпеки**	**інформаційні технології ТНЕУрматика 11** **Вивчення нового матеріалу** **Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу і захисту інформації від витоку технічними каналами.** **Під НСД мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розуміються канали сторонніх електромагнітних випромінювань і наведень, акустичні канали, оптичні канали й ін.** **Захист від НСД може здійснюватися в різних складових інформаційної системи: на прикладному і програмному рівні, на апаратному та на мережевому рівні.** **Для захисту інформації на рівні прикладного та системного ПЗ використовуються:** **• системи розмежування доступу до інформації;** **• системи ідентифікації;** **• системи аудиту та моніторингу;** **• системи антивірусного захисту.** **Для захисту інформації на рівні апаратного забезпечення використовуються: апаратні ключі; системи сигналізації; засоби блокування пристроїв та**

			інтерфейс вводу-виводу інформації. **Розглянемо методи, що забезпечують санкціонованим особам доступ до об'єктів та інформаційних ресурсів. До них відносять аутентифікацію та ідентифікацію користувачів.** **Аутентифікація - це метод незалежного від джерела інформації встановлення автентичності інформації на основі перевірки достовірності її внутрішньої структури ("це той, ким назвався?").** **Авторизація - в інформаційних технологіях це надання певних повноважень особі або групі осіб на виконання деяких дій в системі обробки даних. ("Чи має право виконувати цю діяльність?"). За допомогою авторизації встановлюються і реалізуються права доступу до ресурсів.** **Ідентифікація - це метод порівняння предметів або осіб за їх характеристиками, шляхом розпізнавання з предметів або документів, визначення повноважень, пов'язаних з доступом осіб в приміщення, до документів і т.д. ("Це той, ким назвався і має право виконувати цю діяльність?").** **Що таке ідентифікація?** **Ідентифікація - посвідчення або підтвердження автентичності особи або будь-якої інстанції при їх зверненні до захищеної обчислювальної системи, забезпечує перевірку достовірності партнерів по спілкуванню і перевірку достовірності джерела даних** **Ідентифікація - це процедура розпізнавання суб'єкта за його ідентифікатором (простіше кажучи, це визначення імені, логіна або номера).** **Ідентифікація виконується при спробі увійти в будь-яку систему (наприклад, в операційну систему або в сервіс електронної пошти). Мета ідентифікації — перевірити, чи відомий**

			індивід системі. Ідентифікатором може бути: номер телефону, номер паспорта, e-mail, номер сторінки в соціальній мережі і т.д. Коли нам дзвонять з невідомого номера, що ми робимо? Запитуємо "Хто це", тобто дізнаємося ім'я. Ім'я в даному випадку і є ідентифікатор, а відповідь вашого співрозмовника - це буде ідентифікація. Що таке аутентифікація? Після ідентифікації проводиться аутентифікація - це процедура перевірки автентичності (перевірка справжності). Це процес розпізнавання користувача системи і надання йому певних прав та повноважень. Його суть — визначити, чи справді індивід є тією особою, якою він або вона себе називає. Аутентифікація (authentification) - це процес перевірки облікових даних користувача (зазвичай імені та пароля). Іншими словами введені облікові дані звіряються з даними, що зберігаються в базі даних (користувача перевіряють за допомогою пароля, лист перевіряють по електронного підпису і т.д.) Способи Автентифікації ✓ Парольна (здійснюється на основі володіння користувачем певної конфіденційної інформації) ✓ Біометрична (основана на унікальності певних антропометричних характеристик людини) Щоб визначити чиюсь справжність, можна скористатися трьома факторами: • Пароль - то, що ми знаємо (слово, PIN-код, код для замка, графічний ключ): об’єкт може продемонструвати знання якого-небудь загального для сторін секрету • Пристрій - то, що ми маємо (пластикова карта, ключ від замка, USB-ключ)

			• Біометрика - то, що є частиною нас (відбиток пальця, портрет, сітківка ока) **Парольна аутентичність** **Більшість мережевих систем на даний час продовжують використовувати парольну аутентифікацію, оскільки вона простіше і дешевше. Перевірка автентичності користувача звичайно здійснюється операційною системою. Користувач ідентифікується своїм ім'ям, а засобом аутентифікації служить пароль.** **Конструкція пароля: Для розумної ефективності паролі повинні складатися не менше ніж з 6-8 символів, не бути легко згадувані і змінюватися не рідше, ніж кожні 90 днів.** **Чим довше пароль, тим більше складнощів для зловмисника, щоб його вгадати або обчислити. Можна стверджувати, що збільшення довжини пароля тільки на один символ помітно збільшує безпечний час: якщо очікуваний безпечний час для пароля з трьох символів становить близько трьох місяців, безпечний час для пароля з чотирьох символів становить сімдесят вісім місяців.** **Так само важлива форма пароля. Користувач повинен бути в змозі впевнено його пам'ятати (і не відчувати незручностей від неможливості його записувати), але пароль також повинен бути дуже складним для вгадування іншими. Телефонний номер шкільної подруги або назва вулиці – приклади правильних форм.** **Біометрична аутентифікація** **Системи біометричного захисту використовують унікальні для кожної людини вимірювані характеристики для перевірки особи індивіда.** **Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів.**

			До біометричних засобів захисту інформації відносять системи аутендифікації за: **✓ Параметрами голосу.** **✓ Візерунком райдужної оболонки ока і карта сітчатки ока.** **✓ Рисами обличчя.** **✓ Формою долоні.** **✓ Відбитками пальців.** **✓ Формою і спосібом підпису.** **Біометричні системи складаються з двох частин: апаратних засобів і спеціалізованого програмного забезпечення.** **Для того, щоб біометрична система змогла надалі аудентифікувати користувача, в ній необхідно спочатку зареєструвати відомості про його ідентифікатори. Під час процедури реєстрації в базу даних системи заносяться характеристики користувачів, необхідні для встановлення їх автентичності.** **Апаратні засоби включають в себе біометричні сканери і термінали. Вони фіксують той чи інший біометричний параметр (відбиток пальця, райдужну оболонку очей, малюнок вен на долоні або пальці) і перетворять отриману інформацію в цифрову модель, доступну комп'ютера. А програмні засоби ці дані обробляють, співвідносять з базою даних і виносять рішення, хто постав перед сканером.** **• Аутентифікація по райдужній оболонці ока** **Райдужна оболонка ока є унікальною для кожної людини біометричної характеристикою.** **Зображення ока виділяється з зображення особи і на нього накладається спеціальна маска штрих-кодів. Результатом є матриця, індивідуальна для кожної людини.** **• Аутентифікація по зображенню особи**

			Для ідентифікації особи часто використовуються технології розпізнавання по обличчю. Розпізнавання людини відбувається на відстані. Ідентифікаційні ознаки враховують форму особи, його колір, а також колір волосся. До важливих ознак можна віднести також координати точок особи в місцях, відповідних зміні контрасту (брови, очі, ніс, вуха, рот і овал). Алгоритм функціонування системи розпізнавання: Зображення особи зчитується звичайною відеокамерою і аналізується. Програмне забезпечення порівнює введений портрет з еталоном, що зберігаються. Важливо також те, що біометричні системи цього класу здатні виконувати безперервну аутентифікацію користувача комп'ютера протягом всього сеансу його роботи • Аутентифікація по долоні руки. У біометриці з метою ідентифікації використовується проста геометрія руки - розміри і форма, а також деякі інформаційні знаки на тильній стороні руки (образи на згинах між фалангами пальців, візерунки розташування кровоносних судин). Сканери ідентифікації по долоні руки встановлені в деяких аеропортах, банках і на атомних електростанціях. Метод розпізнавання геометрію кисті руки заснований на аналізі тривимірного зображення кисті. Однак форма кисті руки також є параметром, який досить сильно схильний до змін в часі, а крім того, вимагає сканерів великого розміру, що веде до подорожчання системи • Аутентифікація за відбитками пальців

			Оптичні сканери зчитування відбитків пальців встановлюються на ноутбуки, миші, клавіатури, флеш-диски, а також застосовуються у вигляді окремих зовнішніх пристроїв і терміналів (наприклад, в аеропортах і банках) .Якщо візерунок відбитка пальця не збігається з візерунком допущеного до інформації користувача, то доступ до інформації неможливий **• Аутентифікація по характеристикам мови** **Ідентифікація людини по голосу - один з традиційних способів розпізнавання, інтерес до цього методу пов'язаний і з прогнозами впровадження голосових інтерфейсів в операційні системи.** **Що таке авторизація? Коли визначили ідентифікатор, перевірили справжність, вже можна надати і доступ, тобто, виконати авторизацію. Авторизація - це надання доступу до будь-якого ресурсу (наприклад, до електронної пошти).** **• Чим відрізняється авторизація від аутентифікації?** **Ідентифікація – це процедура розпізнавання суб'єкта за його ідентифікатором. Мета аутентифікації — перевірити, чи відомий індивід системі, наприклад перевіркою пароля, а авторизація полягає в наданні користувачеві доступу до певних ресурсів залежно від його особи, тобто після аутентифікації.** **Автентифікація — це процес доказу об’єктом своєї дійсності системі.** **Ідентифікація — це процес визначення прав об’єкта стосовно системи.** **Авторизація — це процес доказу дій об’єкта стосовно системи або інших об’єктів.** **Засоби ідентифікації й авторизації часто реалізуються в**

			одній підсистемі. Перші дозволяють визначити приналежність того чи іншого ресурсу мережі об'єкта, а другі реалізують механізм причетності, у результаті чого об'єкт не зможе довести, що не робив спроби обігу або впливу на ресурс. Такі засоби контролюють доступ об'єктів до ресурсів системи, надаючи кожному об'єкту саме ті права, які йому були визначені відповідальною особою. **Завдання 1. Ознайомитися з основними правилами кіберзахисту та правилами створення надійного пароля на сайті https://cyberukraine.in.ua/ (#ПарольГраєРоль)** **Завдання 2. Здійсніть перевірку пароля на сайті Проверка пароля - Zillya! https://zillya.ua/ru/check-password** **Обговорюємо .** **1. Вкажіть переваги і недоліки біометричної системи захисту даних** **2. Чому біометричні системи захисту інформації є найбільш надійними?** **3. Як ви думаєте, які недоліки ідентифікації людей за характеристиками голосу? Наведіть приклади застосування даного методу ідентифікації.** **4. Чому райдужка краще за інших біометричних технологій?** **5. Вкажіть проблеми ідентифікації особистості по обличчю.** **Працюємо в парах. Які умови дозволяють не встановлювати пароль на комп'ютері?** **Домашнє завдання** **1) Опрацювати конспект, відповісти на запитання.** **2). Виконайте завдання 1.2.** **3) Знайдіть означення та пояснити термін "двоетапна аутентифікація»** **4)За матеріалами Інтернету підготуйте бюлетень "Як придумати надійний пароль і де його зберігати".**

			5). Розмістіть роботу на Google-диску, надайте доступ, для перегляду і редагування викладачу.
12	11.11.21	**Криптографічні методи захисту інформації**	**Основи криптографії** **Одним з найбільш відомих способів захисту інформації є її кодування (шифрування, криптографія). Воно не рятує від фізичних впливів, але в решті випадків служить надійним засобом.** **Криптографія – це прикладна наука, яка використовує найсучасніші досягнення фундаментальних наук і, в першу чергу, математики. З іншого боку, всі конкретні завдання криптографії істотно залежать від рівня розвитку техніки і технології, від застосовуваних засобів зв'язку і способів передавання інформації. Розвинулась дана наука з практичної потреби передавати важливі відомості найнадійнішим чином.** **Криптографія (від грецького kryptos - прихований і graphein - писати) - наука про математичні методи забезпечення конфіденційності і автентичності інформації.** **Криптографія займається методами перетворення інформації, які б не дозволили зловмиснику витягти її з повідомлень, що перехоплюються. При цьому по каналу зв'язку передається вже не сама інформація, що захищається, а результат її перетворення за допомогою шифру, і для зловмисника виникає складне завдання розкриття шифру.** **Тобто, криптографія повинна забезпечити такий захист інформації, що навіть у випадку її перехоплення сторонніми особами й обробки будь-якими способами з використанням**

			комп'ютерів і останніх досягнень науки і техніки вона не повинна бути дешифрована протягом декількох десятків років. **Вона вважається потужним засобом забезпечення конфіденційності і контролю цілісності інформації. Поки альтернативи методам криптографії немає** **В криптографії застосовуються такі поняття:** **Зашифрування – це процес перетворення інформації, при якому її зміст стає незрозумілим для суб'єктів, що не мають відповідних повноважень** **Результат зашифрування інформації називають шифротекстом або криптограмою.Розшифрування - процес перетворення зашифрованої інформації у придатну для читання інформацію.** ***Сукупність процесів зашифрування і розшифрування називають шифруванням.*** **Відкритий текст - початкове повідомлення, яке повинен захистити криптограф.** **Кодування - заміна логічних (смислових) елементів, наприклад, слів.** **Дія криптографії** **Криптографічний алгоритм, або шифр, — це математична формула, що описує процеси шифрування і розшифрування. Щоб зашифрувати відкритий текст, криптоалгоритм працює в сполученні з ключем (секретним параметром) — словом, числом або фразою. Те саме повідомлення одним алгоритмом, але різними ключами буде перетворюватися в різний шифртекст. Ключ забезпечує конфіденційність шифротексту.** **Знання ключа шифрування дозволяє виконати правильне розшифрування шифротексту.** **Дешифрування (розкриття шифру) – процес одержання інформації із шифротексту без знання застосованого ключа.**

			Захищеність шифртекста цілком залежить від двох речей: стійкості криптоалгоритму і таємності ключа. **Стійкість (криптостійкість) - здатність шифру протистояти будь-яким атакам на нього (спробам розшифрувати перехоплене повідомлення, розкрити ключ шифру або порушити цілісність, достовірність інформації.** **Стійкість конкретного шифру оцінюється тільки шляхом усіляких спроб його розкриття і залежить від кваліфікації криптоаналітиків, що атакують шифр.** **Криптоалгоритм плюс усілякі ключі і протоколи, що приводять їх у дію, складають криптосистему. PGP — це криптосистема.** **Криптологія – наука, що складається із двох галузей: криптографії і криптоаналізу.** **Криптографія – наука про способи перетворення (шифрування) інформації з метою її захисту від незаконних користувачів.** **Криптоаналіз – наука (і практика її застосування) про методи і способи розкриття шифрів.** **Співвідношення криптографії й криптоаналізу очевидне: криптографія – це захист, тобто розробка шифрів, а криптоаналіз – це напад, тобто атака на шифри. Однак ці дві дисципліни пов'язані між собою – не буває гарних криптографів, що не володіють методами криптоаналізу.** **«У світі розрізняють два типи криптографії: криптографія, що перешкодить вашій молодшій сестрі читати ваші файли, і криптографія, що перешкодить читати ваші файли урядам великих країн. Ми будемо розглядати криптографію другого типу.»**

			Криптографія може бути стійкою, а може бути і слабкою, як описано в приведеному прикладі. Криптографічна стійкість виміряється тим, скільки знадобиться часу і ресурсів, щоб із шифртекста відновити вихідний відкритий текст. **Криптографічні методи захисту інформації - це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення.** **На практиці для шифрування інформації використовують методи *симетричного і асиметричного шифрування.*** **Метод симетричного шифрування передбачає використання одного і того ж ключа, що зберігається у секреті, для за шифрування і для розшифрування даних.** **В асиметричній криптографії для зашифровування даних використовується один ключ, а для розшифровування — інший ключ (звідси і назва — асиметричні). Чим більший ключ (число), тим найбільш захищений отриманий шифртекст.** **Переглянути відео «Як працює шифрування?» (про симетричне і асиметричне шифрування) https://www.youtube.com/watch?v=89JyxcVn0lE** **Отже, криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді програм або пакетів програм.** **Д/З:** **Опрацювати конспект**

			1) Перегляд відео про історію криптографію «Еволюція криптографії» https://www.youtube.com/watch?v=M9W4QpqQ5Ps **2) Підготувати повідомлення про шифрувальну машину Енігма, шифрування RSA.** **3) Дослідити , як криптографія застосовується у крипто валюті.**
13	17.11.21	Керування механізмами захисту. Виявлення атак.Захист периметра комп'ютерних мереж.	Процес виявлення атак є процесом оцінки підозрілих дій, які відбуваються в корпоративный мережі. Інакше кажучи, виявлення атак (intrusion detection) це процес ідентифікації й реагування на підозрілу діяльність, спрямовану на обчислювальні або мережні ресурси. Основні підходи до виявлення атак практично не змінилися за останню чверть століття, і, незважаючи на гучні заяви розробників, можна з упевненістю стверджувати, що виявлення атак базується або на методах сигнатурного аналізу, або на методах виявлення аномалій. Можливо також спільне використання зазначених вище методів. Існує кілька способів класифікації систем виявлення атак, кожен з яких заснований на різних характеристиках: • Спосіб контролю за системою (поділяються на network-based, host-based і applicationbased). • Спосіб аналізу. (частина системи визначення проникнення, яка аналізує події, отримані з джерела інформації, і приймає рішення, чи відбувається проникнення). Способами аналізу є виявлення зловживань (misuse detection) та виявлення аномалій (anomaly detection). • Затримка в часі між отриманням інформації з джерела та її аналізом і прийняттям рішення. Залежно від затримки в часі, системи виявлення атак діляться на interval-based (або пакетний режим) і real-time.

			Механізми виявлення атак, застосовувані в сучасних системах виявлення атак IDS (Intrusion Detection System), засновані на декількох загальних методах. Класифікація систем виявлення атак може бути виконана за декількома ознаками: • за способом реагування; розрізняють пасивні й активні IDS. Пасивні IDS просто фіксують факт атаки, записують дані у файл журналу й видають попередження. Активні IDS намагаються протидіяти атаці. • за способом виявлення атаки; За способом виявлення атаки системи IDS прийнято ділити на дві категорії: виявлення аномального поводження (anomaly-based); виявлення зловживань (misuse detection або signature-based). Аномальне поводження користувача (тобто атака або яка-небудь ворожа дія) часте проявляється як відхилення від нормального поводження. Прикладом аномального поводження може служити велика кількість з'єднань за короткий проміжок часу, високе завантаження центрального процесора й т.ін. Однак аномальне поводження не завжди є атакою. Наприклад, одночасну посилку великої кількості запитів від адміністратора мережі система виявлення атак може ідентифікувати як атаку типу "відмова в обслуговуванні" (denial of service). • за способом збору інформації про атаку. Аналіз активності Статичні і динамічні IDS Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе ПО, помилки в конфігураціях і т. д. Статичні IDS перевіряють версії

			прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів. Статичні IDS виявляють сліди вторгнення. Динамічні IDS здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Динамічні IDS реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи. Мережеві IDS Мережеві IDS (англ. Network-based IDS, NIDS) розташовуються в стратегічному місці або у таких місцях мережі, де можливий контроль трафіку всіх пристроїв у мережі. Вони здійснюють контроль всього трафіку даних всієї підмережі та порівнюють трафік, який передається у підмережі з бібліотекою відомих атак. Як тільки розпізнана атака або визначено відхилення у поведінці, відразу надсилається попередження адміністратору. Хостові IDS IDS, які встановлюються на хості і виявляють зловмисні дії на ньому називаються хостовими або системними IDS. Экспертные системи. Експертна система складається з набору правил, які охоплюють знання людини-експерта. Використання експертних систем являє собою розповсюджений метод виявлення атак, при якому інформація про атаки формулюється у вигляді правил. Ці правила можуть бути записані, наприклад, у вигляді послідовності дій або сигнатури. При виконанні кожного із цих правил приймається рішення про наявність несанкціонованої діяльності. Важливим

			достоїнством такого підходу є практично повна відсутність фіктивних тривог. Сигнатурний аналіз заснований на припущенні, що сценарій атаки відомий і спроба її реалізації може бути виявлена в журналах реєстрації подій або шляхом аналізу мережевого Домашнє завдання 1) Опрацювати конспект, 2) За матеріалами Інтернету підготуйте доповідь «Які є види мережевих атак?». Розмістіть роботу на Google-диску, надайте доступ, для перегляду викладачу
14	18.11.21	Міжнародні стандарти інформаційної безпеки.	**Стандарти кібербезпек**и – це методи, що зазвичай викладені в опублікованих матеріалах, які намагаються захистити кібернетичне середовище користувача чи організації. Це середовище включає в себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, інформацію в режимі зберігання або транзиту, програми, служби та системи, які можуть бути безпосередньо або опосередковано підключені до мереж. Основна мета — знизити ризики, включаючи попередження або пом'якшення кібер- атак. Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології. **Міжнародні стандарти** BS 7799-1: 2005 — Британський стандарт BS 7799 перша частина. BS 7799 Частина 1 — Кодекс практики управління інформаційною безпекою (Практичні правила управління інформаційної безпеки) описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду в цій області . Цей документ служить практичним керівництвом по створенню СУІБ BS 7799-2: 2005 — Британський стандарт BS 7799 друга частина стандарту. BS 7799

			Частина 2 — Управління інформаційною безпекою — специфікація систем управління інформаційною безпекою (Специфікація системи управління інформаційної безпеки) визначає специфікацію СУИБ. Втора частина стандарту використовується як критерії при проведенні офіційної процедури сертифікації СУІБ організації. BS 7799-3: 2006 — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт в області управління ризиками інформаційної безпеки ISO/IEC 17799: 2005 — «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005. ISO/IEC 27000 — Словарь і визначення. ISO/IEC 27001 — «Інформаційні технології — Методи забезпечення безпеки — Системы управління інформаційної безпеки — Требования». Міжнародний стандарт, базувався на BS 7799-2: 2005. ISO/IEC 27002 — Зараз: ISO/IEC 17799: 2005. «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Дата выхода — 2007 год. ISO/IEC 27005 — Зараз: BS 7799-3: 2006 — Руководство по управлению рисками ИБ. Німецьке агентство з інформаційної безпеки. Інструкція з захисту базової лінії — стандартні гарантії безпеки (керівництво по базовому рівню захисту інформаційних технологій). Д/З: 1.Стандарти кібербезпеки – це методи… 2.Основна мета Стандартів кібербезпеки.
15	24.11.21	Тематичне оцінювання по темі: "Забезпечення безпеки інформаційних технологій"	Підготуватися до КР: 1. Які ви знаєте криптографічні методи захисту інформації? 2.Криптографія − це прикладна наука, яка.... 3.Сукупність процесів зашифрування і розшифрування. 4.Стандарти кібербезпеки − це методи, що.. 5.Виявлення атак (intrusion detection) це процес - ... 6.Основні підходи до виявлення атак. 7.Для захисту інформації на рівні прикладного та системного ПЗ використовуються: (перерахуйте) 8.Криптографічні методи захисту інформації це...

			9. Які є методи, що забезпечують санкціонованим особам доступ до об'єктів та інформаційних ресурсів? 10.Криптографічний алгоритм, або шифр, — це …
16	25.11.21	Проблеми забезпечення безпеки в комп'ютерних системах і мережах.Типова корпоративна мережа.Заходи захисту мереж.	**Проблеми забезпечення безпеки в комп'ютерних системах і мережах.** Захист інформації в комп'ютерних системах володіє рядом специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаної з носієм, може легко і швидко копіювати та передаватися по каналах зв'язку. Виникнення глобальних інформаційних мереж типу Internet є важливим досягненням комп'ютерних технологій, однак, з Internet пов'язано безліч комп'ютерних злочинів. Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи: 1) перехоплення інформації – при перехоплені порушується конфіденційність інформації; 2) модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і надсилається адресату; 3) підміна авторства інформації. Ця проблема може мати серйозні наслідки. Наприклад, хтось може надіслати листа від вашого імені (цей вид обману прийнято називати спуфінга) або Web-сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів. Корпоративна мережа. Корпоративна мережа — це мережа, головним призначенням якої є підтримка роботи конкретного підприємства, що володіє даною мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства. Корпоративна мережа - це складний комплекс взаємозалежних і узгоджено функціонуючих програмних і апаратних компонентів, який забезпечує передачу інформації між різними віддаленими додатками й системами, що використовуються на підприємстві.

			Основними елементами мережі є робочі станції, сервери і комутатори. Основну частину мережі складають робочі станції, які підключені до комутаторів. Комутатори пересилають пакети даних з одного порту в іншій за потрібною адресою. Також в мережі є сервери, що забезпечують роботу робочих станцій в складі мережі. Наявність мережі приводить до вдосконалення комунікацій між співробітниками підприємства, а також його клієнтами і постачальниками. Мережі знижують потребу підприємств в інших формах передачі інформації, таких як телефон або звичайна пошта. Безпе́ка мере́жі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. 3. Мережеві загрози вразливості і атаки Дії, які так або інакше загрожують збереженню, що допускають нанесення збитків інформаційній безпеці підрозділяються на певні категорії. 1. Дії, які здійснюють користувачі, авторизовані в системі. Ця категорія включає: • зловмисні дії користувача з метою крадіжки або повного або часткового знищення даних, що є на сервері або робочій станції компанії • пошкодження наявних даних як результат прояву необережності, халатності у діях користувача. 2. "Електронне" втручання - дії хакерів: • здійснення DOS та dDOS-атак • незаконне проникнення в захищені комп'ютерні мережі; Несанкціоноване проникнення ззовні в захищену мережу тієї або іншої компанії може

			здійснюватися з метою нанесення збитку (знищення, підміна наявних даних), крадіжка інформації, що відноситься до розряду конфіденційною з подальшим її незаконним використанням, розпорядження мережевою інфраструктурою компанії як методом для здійснення атак на інші мережеві вузли, крадіжка грошових коштів з рахунків компанії або окремих користувачів і т.д. Атаки категорії DOS ("Denial of Service") здійснюються ззовні і направлені на мережеві вузли тієї або іншої компанії, які відповідають за її безпечне, ефективне і стабільне функціонування (поштовий, файловий сервер). Зловмисниками організовується масова відправка яких-небудь даних на вибрані вузли, що викликає їх перевантаження, тим самим,виводячи з працездатного стану на деякий час. Подібні атаки можуть обернутися для постраждалої компанії різними порушеннями в здійсненні безперервних бізнес-процесів, втратою клієнтів, а також втратою репутації. Д/З: 1) Опрацювати конспект, 2) За матеріалами Інтернету підготуйте бюлетень на тему: «Історія розвитку програм для захисту інформації”. Розмістіть роботу на Google-диску, надайте доступ, для перегляду і редагування викладачу.
17	02.03.21	Призначення, можливості, і основні захисні механізми між мережевих екранів (брандмауерів). .	**В комп’ютерних системах використовуються такі засоби мережевого захисту інформації:** **1) Брандмауери (або міжмережеві екрани (Firewall)) — для блокування атак, це окремі** **пристрої чи спеціальні програми, які створюють бар’єр між комп’ютером і мережею, між** **внутрішньою локальною мережею організації та Інтернетом.** **Термін брандмауер походить від нім. brand — пожежа та mauer — стіна; його англійський** **еквівалент — firewall, асоціюється з вогнестійкою капітальною стіною, що перешкоджає** **поширенню пожежі. Термін виник приблизно в 1995 р.** **Мережеві екрани керують проходженням мережевого трафіку відповідно до правил**

			(policies) захисту, контролюють трафік, що входить в мережу і що виходить з неї. **За допомогою програм-брандмауерів відслідковуються всі під'єднання й за необхідності** **дозволяється чи блокується доступ до комп'ютера. Використовуючи інтерфейс налаштувань** **профілю доступу міжмережевого екрану, є можливість для кожного користувача створити свій** **профіль, який буде визначати не тільки права доступу цього користувача до мережі Інтернет,** **але і права доступу до цього користувача з Інтернет. Міжмережевий екран може блокувати** **спроби хакерів, вірусів і черв'яків отримати доступ до вашого комп'ютера через Інтернет.** **Добре сконфігурований міжмережевий екран спроможний зупинити більшість відомих** **комп'ютерних атак.** **Як правило, міжмережеві екрани встановлюються на вході мережі і розділяють внутрішні** **(приватні) та зовнішні (загального доступу) мережі.** **2) Іншим пристроєм ефективного захисту в комп'ютерних мережах є маршрутизатор. Він** **здійснює фільтрацію пакетів даних для передачі і, тим самим, з'являється можливість** **заборонити доступ деяким користувачам до певного "хосту", програмно здійснювати** **детальний контроль адрес відправників та одержувачів та інше.** **Міжмережеві екрани працюють з програмами маршрутизації та фільтрами всіх мережевих** **пакетів, щоб визначити, чи можна пропустити інформаційний пакет, а якщо можна, то** **відправити його до певної комп'ютерної служби за призначенням. Для того щоб** **міжмережевий екран міг зроб*ити це, необхідно визначити правила фільтрації. Отже,*** ***міжмережевий екран є немовби віртуальним кордоном*, на якому перевіряється цілісність** **фрагментованих пакетів даних, що передаються, їх відповідність стандарту тощо.** **3) системи виявлення втручань — для виявлення спроб несанкціонованого доступу як**

			ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні». **Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі.** **4) засоби аналізу захищеності — для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації. Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.** **5) засоби створення віртуальних приватних мереж (Virtual Private Network) — для організації захищених каналів передачі даних через незахищене середовище.** **Віртуальні приватні мережі (virtualprivatenetworks, VPN) - територіально розподілені корпоративні мережі, які використовують для зв'язку між окремими сегментами Інтернет.** **Часто корпоративні мережі зв'язують офіси, розкидані в місті, регіоні, країні або всьому світі.** **Провідні постачальники міжмережевих екранів і маршрутизаторів запропонували технологію S/WAN. Протоколи S/WAN допомагають досягти сумісності між маршрутизаторами і брандмауерами різноманітних виробників. Іншими словами, компанії зможуть створювати власні віртуальні приватні мережі (virtualprivatenetworks, VPN) і використовувати Інтернет як альтернативу традиційним каналам зв'язку, які орендуються за високу плату .** **Віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування.** **Засоби захисту VPN - це інтегровані з віртуальними мережами засоби захисту мережі, в**

			цілому, її сегментів та кожного клієнта мережі окремо (захист TCP/IP трафіку, створюваного будь-якими додатками і програмами; захист робочих станцій, серверів WWW, баз даних і додатків; автопроцесингу, трансакцій для фінансових та банківських додатків і платіжних систем). Вони реалізуються в рамках програмно-апаратних рішень VVPN-шлюзів. Серед основних функцій VPN-шлюзів: автентифікація (MD5, SHA1), шифрування (DES, 3DES, AES), тунелювання пакетів даних через IP. Певні шлюзи підтримують також функції firewall. **Однак міжмережеві екрани не є універсальним вирішенням усіх проблем безпеки в Інтернет. Брандмауер може блокувати доступ до комп'ютера вірусів і хробаків, але він не здійснює перевірку на віруси і не здатен забезпечити цілісність даних.** **6) Використання антивірусних засобів вважається необхідною умовою при підключенні до Internet, дозволяє значно знизити втрати інформації в наслідок зараження шкідливими програмами.** **Антивірус - програма, що виявляє або виявляє та знищує комп'ютерні віруси. Мережеві антивіруси - використовують для захисту від вірусів однієї або кількох OS, протоколів та команди комп'ютерних мереж і електронної пошти. Використання автоматизованих засобів перевірки мережі на можливі уразливості в системі захисту та аудиту безпеки корпоративних серверів дозволяє встановити джерела загроз та значно понизити вірогідність ефективних атак на корпоративну мережу або персональний комп'ютер.** **SKIPBridge - система, яка встановлюється на інтерфейсі внутрішня / зовнішня мережа (локальна мережа або комунікаційний провайдер), забезпечує захист (шифрування) трафіка, що направляється з внутрішньої мережі у зовнішню на основі протоколу SKIP, а також фільтрацію і дешифрування трафіка, який поступає із зовнішньої мережі у внутрішню. IP-**

			пакети, що приймаються із зовнішньої мережі, обробляються протоколом SKIP (розшифровуються, фільтруються відкриті пакети в режимі тільки захищеного трафіка, контролюється і забезпечується імітозахист). Пакети, які пройшли фільтрацію SKIP, за допомогою протоколу IP передаються програмному забезпеченню SKIP-Bridge. Програмне забезпечення вирішує завдання адміністративної безпеки (забезпечуючи пакетну фільтрацію), і потім системи SKIPBridge, який маршрутизує пакети на адаптер локальної мережі. **Використання Proxy та анонімних серверів дозволяє залишатись умовно анонімним при діях в мережі Internet та знизити ризики, пов'язані із збиранням та моніторингом мережевої інформації на користь третіх осіб, потоком непотрібної та шкідливої інформації у системі.** **Використання систем обмеження доступу до мережевих ресурсів Internet, використання маршрутизаторів та надійних постачальників мережевих послуг, короткочасного каналу зв'язку дозволяє скоротити збір та моніторинг мережевої інформації на користь третіх осіб, потік непотрібної та шкідливої інформації.** **Захист даних в Інтернеті.** **Для захисту даних під час роботи в Інтернеті доцільно використовувати підключення, захищене шифруванням. Наприклад, за замовчуванням Google шифрує з'єднання з Gmail, атакож при виборі інших сервісів Google, наприклад Google Диск, активується протокол шифрування SSL, який використовується до завершення сеансу роботи.** **Щоб визначити, що сайти захищені, слід звернути увагу на їхню URL-адресу — вона починається з https://. Це, на відміну від протоколу http, — протокол зашифрованого підключення, що забезпечує більш ефективний захист даних. У деяких браузерах поруч із назвою протоколу відображається значок замка, це означає, що з'єднання захищене й більш безпечне.**

			HTTPS (від англ. HyperText Transfer Protocol Secure) — розширення протоколу http для підтримки шифрування з метою підвищення безпеки. **Браундмаєр** **Перш ніж під'єднати комп'ютер до Інтернету, бажано підключити брандмауер. Наприклад, щоб підключити брандмауер в операційній системі Windows 7, треба виконати вказівку Пуск/Панель керування та обрати Брандмауер Windows.** **У вікні, що відкрилося, слід встановити режим Підключено та за необхідності задати додаткові параметри.** **Після встановлення міжмережевого екрана при кожному першому запуску мережевих програм брандмауер видаватиме вікно з попередженням, що деяка програма намагається одержати доступ до мережевого ресурсу.** **Користувачеві пропонується на вибір: одноразово чи назавжди дозволити або заборонити доступ до комп'ютера для обраної програми.** **Крім брандмауера, вбудованого у Windows 7, є багато інших засобів, що мають гнучкі параметри налагодження.** **Поради:** **• Якщо у вас будинку до Інтернету підключено кілька комп'ютерів, або вони з'єднані в мережу, важливо захистити кожен з них. Для захисту мережі слід використовувати апаратний брандмауер (наприклад, маршрутизатор), однак, щоб запобігти поширенню вірусу в самій мережі в разі зараження одного з комп'ютерів, на кожному з них необхідно включити програмний брандмауер.** **• Якщо ваш комп'ютер підключений до корпоративної, шкільної або мережі іншої організації, дотримуйтесь політиці, встановленої адміністратором даної мережі .** **• При використанні комп'ютера вдома, найперший крок, який слід зробити для його захисту , - включити брандмауер.** **За допомогою брандмауера можна запобігти проникненню на комп'ютер хакерів або зловмисних програм (наприклад, хробаків) через мережу або Інтернет. Крім того, брандмауер**

			запобігатиме надсиланню зловмисних програм із вашого комп'ютера на інші. **У брандмауер Windows вбудований журнал безпеки, який дозволяє фіксувати ір-адреси і інші дані, що відносяться до з'єднань в домашніх і офісною мережах або в Інтернеті. Можна записувати як успішні підключення, так і пропущені пакети. Це дозволяє відстежувати, коли комп'ютер в мережі підключається, наприклад, до web-сайту. Дана можливість за умовчанням відключена (її може включити системний адміністратор).** **Д/З:** ***Опанувати конспект та дати відповіді на запитання та виконайте завдання :*** **1. Які загрози існують під час роботи в Інтернеті?** **2. Яке призначення брандмауера?** **3. Які засоби захисту від інтернет-загроз мають браузери?** ***Завдання* . Навчитися працювати з поштою, брандмауером і на захищених сайтах.** **1) Запустіть текстовий процесор і створіть новий документ.** **2) Визначити, чи увімкнено брандмауер Windows на вашому комп'ютері. Зробіть скріншот вікна налаштування брандмауера та збережіть у створеному документі.** **3) Запустіть браузер та відкрийте один із захищених сайтів. Зробіть скріншот вікна захищеного сайта та збережіть у документі.** **4) Запишіть у документ пояснення, чому, на вашу думку, актуальним є використання захищеного каналу зв'язку.**
18	03.12.21	Політика безпеки при доступі до мережі загального користування.	Із часом до Інтернету під'єднується дедалі більше користувачів. Якщо раніше мережа використовувалась лише в якості середи для передачі файлів та повідомлень електронної пошти, то сьогодні вирішуються складніші завдання розподіленого доступу до ресурсу. Зараз будь-яка людина може отримати доступ до даних, що зберігаються в Інтернеті, або створити свій власний веб-ресурс. Internet, який раніше слугував виключно дослідницьким та учбовим групам, стає все більш популярною у діловому світі. Компанії спокушають швидкість, дешевий глобальний зв'язок, зручність для проведення спільних робіт, доступні програми,

			унікальна база даних мережі. Вони розглядають глобальну мережу, як доповнення до власних локальних мереж. Ці особливості глобальної мережі надають зловмисникам можливість скоєння злочинів в Інтернеті, ускладнюючи їх виявлення й покарання. Зловмисники розміщують шкідливі програми на веб-ресурсах, «маскують» їх під корисне й безкоштовне програмне забезпечення. Тому важливо запобігти небезпеці, уникнути можливих загроз. Саме тому, важливим є захист інформації у всесвітній мережі Internet. Internet, дозволяє значно знизити втрати інформації в наслідок зараження шкідливими програмами. Антивірус - програма, що виявляє або виявляє та знищує комп'ютерні віруси. Мережеві антивіруси - використовують для захисту від вірусів однієї або кількох OS, протоколів та команди комп'ютерних мереж і електронної пошти. Використання автоматизованих засобів перевірки мережі на можливі уразливості в системі захисту та аудиту безпеки корпоративних серверів дозволяє встановити джерела загроз та значно понизити вірогідність ефективних атак на корпоративну мережу або персональний комп'ютер. SKIPBridge - система, яка встановлюється на інтерфейсі внутрішня / зовнішня мережа (локальна мережа або комунікаційний провайдер), забезпечує захист (шифрування) трафіка, що направляється з внутрішньої мережі у зовнішню на основі протоколу SKIP, а також фільтрацію і дешифрування трафіка, який поступає із зовнішньої мережі у внутрішню. IP- пакети, що приймаються із зовнішньої мережі, обробляються протоколом SKIP (розшифровуються, фільтруються відкриті пакети в режимі тільки захищеного трафіка, контролюється і забезпечується імітозахист). Пакети, які пройшли фільтрацію SKIP, за допомогою протоколу IP передаються програмному забезпеченню SKIP-Bridge. Програмне забезпечення вирішує завдання адміністративної безпеки (забезпечуючи пакетну фільтрацію), і потім системи SKIPBridge, який маршрутизує пакети на адаптер локальної мережі. Використання Proxy та анонімних серверів дозволяє залишатись умовно анонімним при діях в мережі Internet та знизити ризики, пов'язані із збиранням та моніторингом мережевої інформації на користь третіх осіб, потоком непотрібної та шкідливої інформації у системі. Використання систем обмеження доступу до мережевих ресурсів Internet, використання

			маршрутизаторів та надійних постачальників мережевих послуг, короткочасного каналу зв'язку дозволяє скоротити збір та моніторинг мережевої інформації на користь третіх осіб, потік непотрібної та шкідливої інформації. Захист даних в Інтернеті. Для захисту даних під час роботи в Інтернеті доцільно використовувати підключення, захищене шифруванням. Наприклад, за замовчуванням Google шифрує з'єднання з Gmail, а також при виборі інших сервісів Google, наприклад Google Диск, активується протокол шифрування SSL, який використовується до завершення сеансу роботи. Щоб визначити, що сайти захищені, слід звернути увагу на їхню URL-адресу — вона починається з https://. Це, на відміну від протоколу http, — протокол зашифрованого підключення, що забезпечує більш ефективний захист даних. У деяких браузерах поруч із назвою протоколу відображається значок замка, це означає, що з'єднання захищене й більш безпечне. HTTPS (від англ. HyperText Transfer Protocol Secure) — розширення протоколу http для підтримки шифрування з метою підвищення безпеки. Д/З: 1.Для захисту даних під час роботи в Інтернеті доцільно використовувати… 2.Антивірус - програма, що виявляє … 3.Мережеві антивіруси - …. 4.Щоб визначити, що сайти захищені, слід звернути увагу НА…..
дистанційне навчання з 01.02.22			
31	03.02.22	Інструктаж БЖД.Практична робота №5.Виконання гіпертекстової розмітки.	Інформатика 11 кл. В.Руденко стор.163, дайте відповіді на запитання та виконайте завдання для самостійного виконання.
32	03.02.22	Каскадні таблиці стилів	Інформатика 11 кл. В.Руденко стор.164 дайте відповіді на запитання та виконайте завдання для самостійного виконання.
33	10.02.22	Проектування та верстка веб - сторінок	Інформатика 11 кл. В.Руденко стор.167 дайте відповіді на запитання та виконайте завдання для самостійного виконання.
34	10.02.22	Адаптивна верстка	Інформатика 11 кл. В.Руденко стор.190

			дайте відповіді на запитання та виконайте завдання для самостійного виконання.
37	17.03.22	(1) Тема:Мультимедіа на веб - сторінках.	Інформатика а 11 кл. В.Руденко стор.193 Відповісти на питання і виконати завдання в кінці теми
38	17.03.22	(2) Тема:Об'єктна модель документа	Інформатика 11 кл. В.Руденко стор.196 Відповісти на питання і виконати завдання в кінці теми
39	24.03.22	(1) Тема:Веб - програмування та інтерактивні сторінки	Інформатика 11 кл. В.Руденко стор.198 Відповісти на питання і виконати завдання в кінці теми
40	24.03.22	(2) Тема:Хостинг Сайта	Інформатика 11 кл. В.Руденко стор.202 Відповісти на питання і виконати завдання в кінці теми
41	31.03.22	(1) Тема:Веб - сервер та база даних	Інформатика 11 кл. В.Руденко стор.203 - 206 Відповісти на питання і виконати завдання в кінці тем
42	31.03.22	(2) Тема:Взаємодія “Клієнт - сервер”	Інформатика 11 кл. В.Руденко стор. - 210 Відповісти на питання і виконати завдання в кінці тем
43	07.04.22	(1) Тема:Валідація сайта та збереження даних форм.	Інформатика 11 кл. В.Руденко стор. - 213 Відповісти на питання і виконати завдання в кінці тем
44	07.04.22	(2) Тема: Прикладний програмний	Інформатика 11 кл. В.Руденко

		інтерфейс	стор. - 216 Відповісти на питання і виконати завдання в кінці тем
45	14.04.22	Тема: (1)Перевірка сайтів на валідність	Інформатика 11 кл. В.Руденко стор. - 215 Відповісти на питання і виконати завдання в кінці тем
46	14.04.22	Тема(2):Інструктаж БЖД. Практична робота №6 Перевірка сайтів на валідність	Інформатика 11 кл. В.Руденко стор. - 215 Відповісти на питання і виконати завдання в кінці тем
47	21.04.22	Тема:Тематичне оцінювання	Повторення всього матеріалу. Запитання для перевірки знань 1.Дайте визначення мультимедіа. 2.Наведіть приклади об'єктів мультимедіа. 3.Що таке формат MIME? 4.Поясніть необхідність конвертації відеофайлів. 5.Які теги для яких форматів використовують? 6.Що таке об'єктна модель документа? 7.Яка організація і чому запропонувала стан-дарт DOM? 8.Як можна представити веб-сторінку? 9.Що таке веб-програмування? 10.Яка мова програмування є базовою у веб-розробці? 11.Наведіть приклади використання JavaScript. 12.Опишіть призначення форм. З яких елементів складається форма? 13.Як досягається інтерактивність сторінок?

			14.Розгляньте такі елементи форми: текстові поля введення (<textarea>), розкривні списки (<select>), кнопки (<button>), прапорці (<input type = "checkbox">), перемикачі (<input type = "radio">). Інформацію про дані елементи оформте у вигляді презентації. *Письмово дайте відповіді на запитання та перешліть викладачу на перевірку.*