Урок № *1 Інформаційна безпека 10(11) клас вибірковий модуль*

Тема. Основні поняття в області безпеки інформаційних технологій. Місце і роль автоматизованих систем в управлінні бізнес-процесами

«Хто володіє інформацією – той володіє світом» – це банальна фраза, відома, напевно, навіть дітям. Як ви розумієте цей вислів?

Вже не можна собі уявити світ без інформаційних технологій, персональних комп'ютерів, глобальних комп'ютерних мереж та мобільного зв'язку. В даний час інформаційні системи та інформаційно-телекомунікаційні мережі підтримують різноманітні сервіси та обробляють дані в таких кількостях, які важко було собі уявити ще кілька років тому. Їх функціонування необхідне для роботи дуже багатьох інфраструктур, наприклад, комунальні або електричні мережі, органи державного та регіонального управління, різноманітні організацій тощо.

Інформаційний ресурс є сьогодні таким же багатством, як корисні копалини, виробничі і людські ресурси, і також як вони підлягає захисту від різного роду посягань, зловживань і злочинів.

Розвиток ІТ впливає і на зростання злочинності в мережі. Постійно виявляються нові вразливі місця в програмному забезпеченні, створюються нові комп'ютерні віруси. У таких умовах системи інформаційної безпеки повинні уміти протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, атакам автоматизованим і скоординованим.

Отже, тема нашого уроку «Основні поняття в області безпеки інформаційних технологій. Місце і роль автоматизованих систем в управлінні бізнес-процесами»

Давайте перевіримо, що ви знаєте про інформаційну безпеку, пройдіть он-лайн тестування за посиланням. https://onlinetestpad.com/ua/test/79462-osnovi-D1%96nformac%D1%96jnoi-bezpeki-test1

З якими поняттями ви вже знайомі? Які нові терміни ви зустрічали в тесті?

Вивчення нового матеріалу

Як тільки на Землі з'явилися люди, вони почали збирати, осмислювати, обробляти, зберігати і передавати різноманітну інформацію. Людство постійно має справу з інформацією. Перш ніж говорити про інформаційну безпеку необхідно визначитися з поняттям "інформація".

Точного наукового визначення поняття "інформація" немає. Під інформацією розуміють відомості про об'єкти, процеси та явища.

Інформація – данні про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього представлення. Відомо, що інформація може мати різну форму, зокрема, дані, закладені в комп'ютерах, листи, пам'ятні записи, досьє, формули, креслення, діаграми, моделі продукції і прототипи, дисертації, судові документи й ін.

У *галузі інформаційних систем* рекомендується таке означення інформації:

Інформація – це відомості, які є об'єктом зберігання, передавання і оброблення.

Оскільки інформація представляє інтерес для різних категорій користувачів, то основним призначенням інформації є її використання.

Як і всякий продукт, інформація має споживачів, що потребують її, і тому володіє певними споживчими якостями, а також має і своїх власників або виробників.

Інформаційні ресурси – це окремі документи та масиви документів, представлені самостійно або в інформаційних системах (бібліотеках, архівах, фондах, базах даних та інших ІС).

Інформаційні ресурси можна класифікувати:

- *за видом інформації* – правові, науково-технічні, політичні, фінансово-економічні, статистичні, метрологічні, соціальні, персональні, медичні, про надзвичайні ситуації та т.п.;

- *за режимом доступу* – відкриті, обмеженого доступу, державна таємниця, конфіденційна інформація, комерційна таємниця, професійна таємниця, службова таємниця, особиста (персональна) таємниця;
- *за формою власності* – державні, муніципальні, регіональні, приватні, колективні;
- *за видом носія* – на папері (документи, листи, медичні карти, телефонні довідники організацій, чернетки і т.п.), в пам'яті комп'ютера, в каналі зв'язку, на дисках та інших носіях.

Інформація, що захищається, — це інформація, що є предметом власності якого-небудь суб'єкта (держави, відомства, групи осіб або окремого громадянина) і підлягає захисту відповідно до вимог правових документів або вимог, які встановлюються власником інформації.

Види інформації, які підлягають захисту

1) Інформація з обмеженим доступом - інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами.
2) Таємна інформація - інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.
3) Конфіденційна інформація - інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними.

Під ***доступом до інформації*** розуміється ознайомлення з інформацією, її обробка, зокрема копіювання, модифікація або знищення інформації. Розрізняють санкціонований і несанкціонований доступ до інформації.

Санкціонований доступ до інформації – це доступ до об'єктів, програм і даних користувачів, що мають право виконувати певні дії, а також права користувачів на використання ресурсів і послуг. Цей доступ не порушує встановлені правила розмежування доступу.

Несанкціонований доступ (НСД) до інформації характеризується порушенням встановлених правил розмежування доступу. Це найбільш поширений вид комп'ютерних порушень. Дане поняття також пов'язане з поширенням різного роду комп'ютерних вірусів.

Захист інформації – це комплекс заходів, направлених на забезпечення інформаційної безпеки.

Захищеною вважають інформацію, не зазнала незаконних змін у процесі передачі, зберігання та збереження, не змінила такі властивості, як достовірність, повнота і цілісність даних.

Цікаво: У 1988 році американська *Асоціація комп'ютерного обладнання* оголосила 30 листопада Міжнародним днем захисту інформації (ComputerSecurityDay). Було зафіксовано першу масову епідемію хробака, якого назвали за іменем його творця — Морріса.

3. Роль автоматизованих систем в управлінні процесами

Комп'ютери – тільки одна з складових інформаційних систем, і хоча наша увага буде зосереджена в першу чергу на інформації, яка зберігається, обробляється і передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових і, в першу чергу, найслабкішою ланкою, якою в переважній більшості випадків виявляється людина.

Згідно визначення інформаційної безпеки, вона залежить не тільки від комп'ютерів, але і від інфраструктури, що її підтримує, до якої можна віднести системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання інформаційною системою своїх функцій.

Автоматизовані системи (АС) являє собою організаційно-технічну систему, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію.

ОС - сукупність програмно-апаратних засобів, що призначені для обробки інформації

Інформація в АС піддається різним процесам: введення, збереження, обробка, виведення. Найбільш загальними інформаційними процесами, що відбуваються в автоматизованих системах є такі:

- інформаційно-довідкове забезпечення;
- інформаційне забезпечення задач;
- обслуговування інформаційних баз.

Усі вони реалізуються персоналом за допомогою апаратних засобів, ПЗ та інформаційних баз автоматизованих систем.

Прийнято розрізняти два основних напрями ТЗІ в АС — це захист АС і оброблюваної інформації від несанкціонованого доступу та захист інформації від витоку технічними каналами.

- Захищена АС:*АС, що здатна забезпечувати захист інформації, що обробляється, від певних загроз*
- Захист інформації в АС - *діяльність, спрямована на забезпечення безпеки інформації, що обробляють в АС, і АС в цілому, яка дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенціального збитку в результаті реалізації загроз*

- Комплексна система захисту інформації *Захист інформації в АС полягає у створенні й підтриманні у працездатному стані системи заходів як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційний збиток*

Практична робота

Увага! ***Під час роботи з комп'ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.***

Завдання 1. Створіть текстовий документ, що містить відомості про історію розвитку інформаційної безпеки. Подайте знайдені відомості в текстовому документі у зручному вигляді (таблиці, схеми тощо). Розмістіть роботу на Google-диску, наддайте доступ для перегляду і редагування учителю і однокласникам. Перегляньте проектну роботу своїх друзів.

Додатково: Перегляд відео з наступним обговоренням -https://youtu.be/PIZ9NaCB7ZM

Домашнє завдання

1) Опрацювати конспект, створити карту знань до уроку
2) **Он-лайн курс.** Зареєструватися на он-лайн курс «Основи інформаційної безпеки» від антивірусної компанії від антивірусної лабораторії Zillya! Антивірус (zillya.ua/prometheus) за посиланням https://edx.prometheus.org.ua/register#. Ознайомтеся з матеріалами курсу
3) За матеріалами Інтернету підготуйте добірку реальних історій про порушення інформаційної безпеки та наслідки цих дій.

Додаток 1.

Історія розвитку інформаційної безпеки та засобів інформаційних комунікацій можна виділити декілька етапів:

- Іетап — до 1816 року — характеризується використанням природно виникаючих засобів інформаційних комунікацій. В цей період основне завдання інформаційної безпеки полягало в захисті відомостей про події, факти, майно, місцезнаходження і інші дані, що мають для людини особисто або співтовариства, до якого вона належала, життєве значення.
- IIетап — починаючи з 1816 року — пов'язаний з початком використання штучно створюваних технічних засобів електро-радіозв'язку. Для забезпечення скритності і перешкодостійкості радіозв'язку необхідно було використовувати досвід першого періоду інформаційної безпеки на вищому технологічному рівні, а саме застосування перешкодостійкого кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).
- IIIетап — починаючи з 1935 року — пов'язаний з появою засобів радіолокаційігідроакустики. Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, направлених на підвищення захищеності засобів радіолокацій від дії на їхні приймальні пристрої активними маскуючими і пасивними імітуючими радіоелектронними перешкодами.
- IVетап — починаючи з 1946 року — пов'язаний з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися, в основному, методами і способами обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації.
- Vетап — починаючи з 1965 року — обумовлений створенням і розвиткомлокальнихінформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних в локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів.
- VIетап — починаючи з 1973 року — пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Загрози інформаційній безпеці стали набагато серйознішими. Для забезпечення інформаційної безпеки в комп'ютерних системах з безпровідними мережами передачі даних потрібно було розробити нові критерії безпеки. Утворилися співтовариства людей — хакерів, що ставлять собі за мету нанесення збитку інформаційній безпеці окремих користувачів, організацій та країн. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки –найважливішою, обов'язковою складовою національної безпеки. Формується інформаційне право — нова галузь міжнародної правової системи.
- VIIетап — починаючи з 1985 року — пов'язаний із створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення. Можна припустити що черговий етап розвитку інформаційної безпеки, буде пов'язаний з широким використанням надмобільних комунікаційних пристроїв з широким спектром завдань і глобальним охопленням у просторі та часі, забезпечуваним космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросистеми інформаційної безпеки людства під егідою ведучих міжнародних форумів.