Урок 1 «Основні поняття в області безпеки ІТ»

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 розуміютьвідомості 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 підлягаютьзахисту

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*

Питання для самоконтролю

1. Що таке інформація з обмеженим доступом?
2. Яку інформацію називають конфіденційною? Таємною?
3. Що називають доступом до інформації? Які є види доступу?
4. Що таке захист інформації в автоматизованій системі?
5. Опрацювати конспект, створити карту знань до уроку