**Міністерство освіти та науки України**

**Київський національний торговельно - економічний університет**

**Факультет інформаційних технологій**

**Кафедра інженерії програмного забезпечення та кібербезпеки**

**ПРАКТИЧНА РОБОТА № 1**

**З ДИСЦИПЛІНИ**

**«Безпека інформаційних систем»**

**НА ТЕМУ:**

ПОНЯТТЯ ЗАХИСТУ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. КРИТЕРІЇ ОЦІНКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ.

**Виконала:** студентка ФІТ

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Лахно Валерiй Анатолiйович

Київ 2023

**Практична робота №1**

Тема: «Поняття захисту інформації та інформаційної безпеки. Критерії оцінки інформаційної безпеки. Аспекти захисту інформації»

Мета: ознайомитися з базовими поняттями захисту інформації, інформаційної безпеки, властивостями інформації, аспектами захисту інформації та критеріями оцінки інформаційної безпеки.

1. За допомогою пошукової системи Google було знайдено такі закони, укази президента, постанови, положення, що стосуються захисту інформації та інформаційної безпеки:
   1. Закон України «Про інформацію»
   2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
   3. Закон України «Про державну таємницю»
   4. Закон України «Про захист персональних даних»;
   5. Закон України «Про доступ до публічної інформації»;
   6. Закон України «Про основні засади забезпечення кібербезпеки України»;
   7. Указ Президента України від 27.09.1999 № 1229 «Про Положення про технічний захист інформації в Україні»;
   8. постанова Кабінету Міністрів України від 03.09.2014 № 411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України»;
   9. постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;
   10. постанова Кабінету Міністрів України від 16.11.2002 № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах»;
   11. постанова Кабінету Міністрів України від 12.04.2002 № 522 «Про затвердження Порядку підключення до глобальних мереж передачі даних»;
   12. постанова Кабінету Міністрів України від 13.03.2002 № 281 «Про деякі питання захисту інформації, охорона якої забезпечується державою»;
   13. постанова Кабінету Міністрів України від 16.02.1998 № 180 «Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційно-телекомунікаційних та інформаційних системах»;
   14. постанова Кабінету Міністрів України від 08.10.1997 № 1126 «Про затвердження Концепції технічного захисту інформації в Україні»;
   15. наказ Адміністрації Держспецзв’язку від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», зареєстрований в Міністерстві юстиції України 28.01.2015 за № 90/26535;
2. На офіційному сайті Верховної ради «Законодавство України» (http://zakon2.rada.gov.ua/laws) було знайдено Закон України «Про інформацію».

***Основні терміни:***

документ - матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

суб'єкт владних повноважень - орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

***Основні види інформації:***

За змістом інформація поділяється на такі види:

* інформація про фізичну особу - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;
* інформація довідково-енциклопедичного характеру - систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище;
* інформація про стан довкілля (екологічна інформація);
* інформація про товар (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги);
* науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
* податкова інформація - сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України;
* правова інформація - будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо;
* статистична інформація - документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства;
* соціологічна інформація - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо;
* критична технологічна інформація - дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об’єктів критичної інфраструктури;
* інші види інформації.

***Основні аспекти відповідальності за порушення законодавства про інформацію:***

Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України.

Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

Ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень.

У разі якщо порушенням права на свободу інформації особі завдано матеріальної чи моральної шкоди, вона має право на її відшкодування за рішенням суду.

1. На офіційному сайті Верховної ради «Законодавство України» (http://zakon2.rada.gov.ua/laws) було знайдено Закон України «Про захист інформації в інформаційно-телекомунікаційних системах.

***Основні терміни:***

блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

володілець інформації - фізична або юридична особа, якій належать права на інформацію;

власник системи - фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-комунікаційна система - сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

електронна комунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації;

резервна копія державних інформаційних ресурсів - копія інформації, яка міститься в державних інформаційних ресурсах, що перебувають у володінні або розпорядженні органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, державних підприємств, установ та організацій, та є критичною для їх сталого функціонування, створюється, записується, обробляється або зберігається у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів з метою подальшого відновлення цієї інформації.

***Об’єктами захисту в системі*** є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

***Суб’єктами відносин,*** пов'язаних із захистом інформації в системах, є:

* володільці інформації;
* власники системи;
* користувачі;
* спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи.

***Умови обробки інформації в системі:***

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

***Повноваження державних органів у сфері захисту інформації в системах:***

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

* розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;
* визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
* організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;
* здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
* здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

***Основні аспекти відповідальності за порушення законодавства про захист інформації в системах:***

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

**Висновок:** заходи, спрямовані на захист інформаційної безпеки України, є важливими інтересами держави. Проблеми інформаційної безпеки згідно з українським законодавством мають розв’язуватись так:

* створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
* підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;
* вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії кіберзлочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
* розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

**Контрольні питання:**

* 1. Інформаційна безпека - це сукупність заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в інформаційних системах.
  2. Захист інформації - це сукупність технічних, організаційних і юридичних заходів, спрямованих на забезпечення безпеки інформації в інформаційних системах.
  3. Основні властивості інформації:
     + Конфіденційність
     + Цілісність
     + Доступність
  4. Основні аспекти захисту інформації та інформаційної безпеки:
     + Конфіденційність — захист від несанкціонованого ознайомлення з інформацією.
     + Цілісність — захист інформації від несанкціонованої модифікації.
     + Доступність — захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані, так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.
  5. Загрози безпеки інформації відповідно до властивостей:
     + Конфіденційності - несанкціонований доступ, витік інформації.
     + Цілісності - випадкові чи навмисні зміни, втрата даних.
     + Доступності - атаки на сервіси, перевантаження ресурсів.
  6. Базові поняття інформаційної безпеки:
     + Інформаційна безпека (information security) — збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність
  7. Шляхи забезпечення інформаційної безпеки:
     + створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
     + підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;
     + вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії кіберзлочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
     + розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.
  8. Основні критерії інформаційної безпеки:
     + Конфіденційність - збереження від несанкціонованого доступу.
     + Цілісність - забезпечення невідмінності інформації.
     + Доступність - готовність для використання в момент потреби.
     + Законодавчі вимоги до інформаційної безпеки:
     + Закони та нормативні акти, які регулюють захист інформації в різних сферах.
  9. Законодавчі вимоги до інформаційної безпеки:

Законодавчі вимоги - це нормативно-правові акти, прийняті на рівні держави, які регулюють питання захисту інформації. Ці вимоги визначають правила та обов'язки щодо збереження конфіденційності, цілісності та доступності інформації. Зазвичай це включає в себе вимоги до захисту персональних даних, обмеження доступу до конфіденційної інформації, а також встановлення відповідальності за порушення правил захисту.

* 1. Модель тріади СІА:

Модель тріади СІА є концепцією, яка визначає три основні властивості інформації, що підлягають захисту:

* Конфіденційність (C - Confidentiality): Гарантує, що інформація доступна лише тим особам або системам, які мають право отримати доступ.
* Цілісність (I - Integrity): Забезпечує невідмінність та непереборність інформації. Це означає, що інформація не повинна бути змінена несанкціоновано.
* Доступність (A - Availability): Забезпечує готовність інформації для використання в момент потреби. Інформація повинна бути доступною для користувачів, які мають на це право.

Ця модель є основою для розуміння та реалізації політик і заходів інформаційної безпеки в організаціях.