

Урок №10. Правові основи забезпечення безпеки інформаційних технологій. Відповідальність за порушення у сфері захисту інформації та неправомірного використання автоматизованих систем

Вивчення нового матеріалу

Пригадаймо основні види захисту інформації

- **Морально-етичні засоби** реалізуються у вигляді норм поведінки особи в інформаційному просторі.
- **Правові засоби** встановлюють правила користування інформацією та відповідальність користувачів за їх порушення.
- **Адміністративні (організаційні) засоби** регламентують порядок взаємодії користувачів з інформаційними системами.
- **Технічні (фізичні) засоби** забезпечують захист від несанкціонованого доступу, пошкодження інформаційної системи тощо.
- **Програмні засоби** забезпечують захист інформаційної системи від комп'ютерних вірусів, ідентифікацію користувачів тощо.

Морально-етичні засоби захисту включають всілякі норми поведінки (які традиційно склалися раніше). Вони складаються в міру поширення ІС та ІТ в країні і в світі або спеціально розробляються. Морально-етичні норми можуть бути неписані (наприклад, чесність) або оформлені в якийсь звід (статут) правил чи приписів. Ці норми, як правило, не є законодавчо затвердженими, але оскільки їх недотримання призводить до падіння престижу організації, вони вважаються обов'язковими для виконання. Характерним прикладом таких приписів є Кодекс професійної поведінки членів Асоціації користувачів ПК США.

Морально-етичні правила інформаційної безпеки

Використовуйте тільки ліцензоване програмне забезпечення

- Робіть посилання на використані ресурси.
- Використовуйте антивірусні програми.
- Створюйте надійні паролі під час реєстрації акаунтів.
- Не розголошуйте приватну інформацію стороннім особам.
- Обмежуйте доступ сторонніх осіб до комп'ютера.
- Не відкривайте листи й файли, отримані від незнайомих людей.

Комп'ютерна етика займається дослідженням поведінки людей, що використовують комп'ютер, на основі чого виробляються відповідні моральні приписи й своєрідні норми етики. Саме вживання терміну «комп'ютерна етика» досить умовне, ця дисципліна дуже молода, вона з'явилася на межі 70-х - 80-х рр. ХХ сторіччя, і поряд з нею вживаються такі терміни, як «інформаційна етика», «кіберетика».

Принципи комп'ютерної етики:

- **privacy (таємниця приватного життя)** — право людини на автономію й волю в приватному житті, право на захист від вторгнення в неї органів влади й інших людей;

- **accuracy (точність)** — дотримання норм, пов'язаних з точним виконанням інструкцій для експлуатації систем і обробки інформації, чесним і соціально-відповідальним відношенням до своїх обов'язків;
- **property (приватна власність)** — недоторканність приватної власності — основа майнового порядку в економіці. Проходження цьому принципу означає дотримання права власності на інформацію й норми авторського права;
- **accessibility (доступність)** — право громадян на інформацію, її доступність у будь-який час і в будь-якому місці.

Чинне законодавство визначає як життєво важливі інтереси особи в інформаційній сфері України наступні:

- 1) забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;
- 2) недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних;
- 3) захищеність від негативного інформаційно-психологічного впливу.

Проблеми захисту від інформації суттєво складніші за проблеми захисту інформації, оскільки загрози від інформації надзвичайно різноманітні, їх вплив не завжди очевидний, він здійснюється навмисно, витончено і підступно, а відвернення цих загроз і нейтралізація вимагають різноманітних неординарних дій. Інформаційні загрози є складним ієрархічним утворенням із множиною різнорівневих зв'язків, їх вплив на людину комплексний і різноманітний.

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.

Фактично сфера безпеки інформації – не захист інформації, а захист прав власності на неї.

Інформаційна інфраструктура – сукупність організаційних структур і систем, які забезпечують функціонування та розвиток інформаційного простору, засобів інформаційної взаємодії та доступу користувачів до інформаційних ресурсів.

Забезпечення інформаційної безпеки – діяльність, спрямована на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці України.

Кібернетична безпека (кібербезпека) – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі; **кіберпростір** – середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем.

Кіберзлочин – суспільно небезпечне винне діяння у кіберпросторі, передбачене чинним законодавством України про кримінальну відповідальність.

Кібертероризм – терористична діяльність у кіберпросторі або з його використанням.

Державна інформаційна політика – це діяльність держави, спрямована на формування та регулювання середовища, в якому задовольняються інформаційно-комунікативні потреби громадян України, суспільства і держави.

Інтелектуальна власність (англ. *intellectual property*) — результат інтелектуальної, творчої діяльності однієї людини (автора, виконавця, винахідника та інш.) або кількох осіб.

Право інтелектуальної власності — у найширшому розумінні означає закріплені законом права на результат інтелектуальної діяльності в промисловій, науковій, художній, виробничій та інших галузях.

До порушення права інтелектуальної власності відносяться:

- піратство
- плагіат
- несумлінна реєстрація
- недобросовісна конкуренція
- підроблення та зміна інформації
- Розмиття торговельної марки.

В Україні прийнято низку законів та постанов щодо забезпечення інформаційної безпеки:

- «Про захист інформації в інформаційно-телекомунікаційних системах»;
- «Про державну таємницю»;
- «Про захист персональних даних»;
- «Про авторське право і суміжні права» та ін.

Незаконне втручання в роботу комп'ютерів і мереж, а також розповсюдження вірусів тягне за собою кримінальну відповідальність (ст. 361 Кримінального кодексу України).

Закон України «Про доступ до публічної інформації».

- Метою цього Закону є забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації.
- Публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами **владних повноважень** своїх обов'язків.
- Публічна інформація є відкритою, крім випадків, встановлених законом.
- Інформацією з обмеженим доступом є конфіденційна, таємна, службова.

Закон України «Про захист персональних даних».

- Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.
- *Обробка персональних даних* - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.
- *Персональні дані* - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Закон України «Про авторське право і суміжні права»

- Цей Закон охороняє особисті немайнові та майнові права авторів та їх правонаступників, пов'язані зі створенням та використанням творів науки, літератури і мистецтва - авторське право, і права виконавців, виробників фонограм і відеогам та організацій мовлення - суміжні права.
- Автор - фізична особа, яка своєю творчою працею створила твір.
- Оприлюднення (розкриття публіці) твору - здійснена за згодою автора чи іншого суб'єкта авторського права і (або) суміжних прав дія, що вперше робить твір доступним для публіки шляхом опублікування, публічного виконання, публічного показу, публічної демонстрації, публічного сповіщення тощо.

Кодекс України про адміністративні правопорушення.

Стаття 188-39. Порушення законодавства у сфері захисту персональних даних.

Неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей - тягнуть за собою накладення штрафу на громадян від 100 до 200 неоподаткованих мінімумів доходів громадян і на посадових осіб, громадян - суб'єктів підприємницької діяльності - від 200 до 400 неоподаткованих мінімумів доходів громадян.

Кримінальний кодекс України

Стаття 182. Порушення недоторканності приватного життя.

Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, караються штрафом від 500 до 1000 неоподаткованих мінімумів доходів громадян або виправними роботами на строк до 2 років, або арештом на строк до 6 місяців, або обмеженням волі на строк до 3 років.

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, карається штрафом від 600 до тисячі неоподаткованих мінімумів доходів громадян або обмеженням волі на строк від 2 до 5 років, або позбавленням волі на строк до 3 років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 2 років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, караються штрафом від 500 до 1000 неоподаткованих мінімумів доходів громадян або позбавленням волі на строк до 2 років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Несанкціоновані зміна, знищення або блокування інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, караються штрафом від 600 до 1000 неоподаткованих мінімумів доходів громадян або виправними роботами на строк до 2 років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

Найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту.

Хакери (хекери) — це узагальнююча назва людей, які зламують комп'ютерні системи. Часто цей термін застосовується і до «програмістів-маніяків» — 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 розумінні слово «хакер» позначає тих, хто одержує неправомірний доступ до ресурсів ІС тільки для самоствердження (див. приклад). 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 гатунку, 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.

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.

Слід також зупинитись ще на одній групі, яка посідає проміжне місце між хакерами і недосвідченими користувачами (до речі, ненавмисні дії останніх можуть призвести до не менш тяжких наслідків, ніж сплановані атаки професіоналів). Ідеться про **експериментаторів («піонерів»)**. 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». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією у цій групі є гра. З експериментаторів виходять професіонали високого класу, зокрема й законослухняні.

- **Практичне завдання**

Докладно опрацювати Кримінальний кодекс України:

стаття 182

стаття 361

стаття 361-2

стаття 362

Визначити перелік правопорушень, кримінальну відповідальність, повторне правопорушення і покарання.

Результат оформити в Google-презентацію (1 слайд -1 стаття).