Урок № 6

Тема. Правові основи забезпечення безпеки інформаційних технологій.

Мета:

- ✓ ***навчальна:*** ознайомити з етичними та правовими основами захисту даних, основними нормативно-правові документи України у сфері ІБ, категорії порушників інформаційної безпеки;

ХІД УРОКУ.

Актуалізація опорних знань

1. Які є види захисту інформації?
2. Які заходи відносяться до організаційних? Технічних? Програмних?
3. Пригадайте, що таке інтелектуальна власність, авторське право, плагіат?

Виконайте інтерактивну вправу https://learningapps.org/2613055 «Особиста і публічна інформація»

Інформація, головний ресурс і цінність сучасного суспільства одночасно є засобом та об'єктом скоєння неетичних, протиправних дій і кримінальних злочинів.

Сьогодні в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях ухвалено спеціальні закони щодо комп'ютерних злочинів, і вони постійно доповнюються. Загальною тенденцією є підвищення жорсткості кримінальних законів щодо осіб, які скоїли комп'ютерні злочини. Існують також як неписані морально-етичні норми, так і оформлені в деякий статут, як, наприклад, Кодекс професійної поведінки членів Асоціації користувачів комп'ютерів США.

Разом із тим важливо, щоб із розвитком інформаційних технологій забезпечувалося дотримання прав людини стосовно захисту авторських прав, інтелектуальної власності та безпеки. Сьогодні ми розглянемо на уроці всі ці аспекти.

Вивчення нового матеріалу

Пояснення вчителя з елементами демонстрування презентації

(використовується проектор)

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні.

Програмні засоби — забезпечують захист інформаційної системи від комп'ютерних вірусів, ідентифікацію користувачів тощо.

Технічні засоби — забезпечують захист від несанкціонованого доступу, пошкодження інформаційної системи тощо.

Адміністративні методи — регламентують порядок взаємодії користувачів з інформаційними системами.

Морально-етичні засоби — реалізуються у вигляді норм поведінки особи в інформаційному просторі: соціальна й персональна відповідальність, рівноправність партнерів по комунікації, точне й сумлінне виконання обов'язків тощо.

Інформаційна етика розглядає проблеми власності, доступу, безпеки й спільності інформації. У світі складаються певні морально-етичні норми поведінки користувачів, наприклад, не втручатися в роботу інших користувачів мереж; не використовувати файли, не призначені для вільного використання; не використовувати комп'ютер для розповсюдження неправдивої інформації та ін.

Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни. Морально-етичні норми бувають як неписаними, так й оформленими в деякий статут.

Поряд із загальнолюдськими етичними нормами є такі **базові права**, як:

- загальнодоступність — гарантує право на комунікацію й передбачає доступність державних інформаційних ресурсів;
- таємниця приватного життя — дотримання конфіденційності довірених даних;
- недоторканність приватної власності — основа майнового порядку, дотримання права власності на дані й норм авторського права.

Правові методи — встановлюють правила користування інформацією та відповідальність користувачів за їх порушення. Це — чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання інформаційних технологій (ІТ).
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 декілька 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 (хекери) — це узагальнююча назва людей, які зламують комп'ютерні системи і одержують неправомочний 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 «хакери»;
- «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». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією у цій групі є гра. З експериментаторів виходять професіонали високого класу, зокрема і законослухняні

IV. Формування практичних умінь і навичок

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

Завдання 1. Виконайте інтерактивну вправу «Інформаційна етика» за посиланням http://LearningApps.org/watch?v=p502ii7et16

Завдання 2. Ознайомитися з інформацією на сайті кіберполіції України (підсумки 2017 року і новини) https://cyberpolice.gov.ua/articles/

V. Підсумок уроку

Працюємо в парах.

1) Які розрізняють етичні та правові основи захисту даних?
2) Що таке інформаційна етика? Чи існує "хакерська" етика? В чому вона полягає?

VI. Домашнє завдання

3) Опрацювати конспект
4) Створіть інформаційний бюлетень із правилами комп'ютерного етикету. Розмісіть роботу на Google-диску, наддайте доступ, для перегляду і редагування учителю і 2 однокласникам. Перегляньте проектну роботу своїх друзів. Додайте коментарі. Порівняйте змістовну частину і оформлення. Оцініть власну роботу і переглянуті роботи.