МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Сумська філія

Кафедра соціально-економічних дисциплін

ТЕКСТ ЛЕКЦІЇ

з навчальної дисципліни «Інформаційне забезпечення професійної діяльності»
обов'язкових компонент
освітньої програми першого (бакалаврського) рівня вищої освіти

081 Право (право)

за темою – «Захист даних у мережі. Електронний цифровий підпис»

Суми 2024

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 14.08.2024 № 8

СХВАЛЕНО
Вченою радою Сумської філії
Харківського національного
університету внутрішніх справ
Протокол від 08.07.2024 № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з гуманітарних та
соціально-економічних дисциплін
Протокол від 13.08.2024 № 7

Розглянуто на засіданні кафедри соціально-економічних дисциплін

Протокол від 25.06.2024 № 23

Розробник:
Доцент кафедри соціально-економічних дисциплін Сумської філії ХНУВС, кандидат економічних наук, доцент Виганяйло С.М.

Рецензенти:
1. Доцент кафедри протидії кіберзлочинності, факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ, канд.пед.наук, доцент Тетяна Петрівна Колісник
2. Доцент кафедри кібернетики та інформатики СНАУ, канд.екон.наук, доцент Олександр Борисович В'юненко

План лекції

1. Комп'ютерні віруси, приклади їх шкідливої дії. Екранування програмне („брандмауер"). Характеристика комп'ютерних злочинів. Криптографічний захист. Сметричне та асиметричне шифрування.
2. Електронний документ – поняття та складові частини, властивості. Електронний цифровий підпис – поняття, складові частини. Накладання ЕЦП. Суб'єкти правових відносин у сфері послуг ЕЦП. Процедури використання ЕЦП. Криптографічна непохитність електронного цифрового підпису.
3. Конфіденційне листування електронною поштою. Створення пари ключів. Збереження файлів ключів. Шифрування файлів на комп'ютері. Розшифрування файлу. Пересилання ключа (3 способи). Одержання ключів. Імпорт ключа.

Рекомендована література:

Нормативні документи

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40-41. – ст. 379 URL: **https://zakon.rada.gov.ua/laws/show/580-19**
2. Закон України "Про захист персональних даних" від 01.06.2010 за 2297-VI. URL: **https://zakon.rada.gov.ua/laws/show/2297-17**
3. Про захист інформації в інформаційно-телекомунікаційних системах.

   Закон України URL: **https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80**
4. Про затвердження Положення про інформаційно-телекомунікаційну систему "Інформаційний портал Національної поліції України": Наказ МВС України від 03.08.2017 № 676 URL: **https://zakon.rada.gov.ua/laws/show/z1059-17**
5. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів: Постанова КМУ від 14 листопада 2018 р. № 1024 URL: **https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF**

Основна

1. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. Харків: ХНУВС, 2021. 110 с. URL: **http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11258/Informatsiine%20zabezpechennia%20profesiinoi%20diialnosti_Vyhaniailo_2021.pdf?sequence=1&isAllowed=y**
2. Клімушин, П. С. Інформаційні системи та технології в економіці : навчальний посібник / П. С. Клімушин, О. В. Орлов, А. О. Серенок; Нац. акад. держ. управління при Президентові України, Харк. регіон. ін-т держ. управління. - Харків : Вид-во ХарРІ НАДУ "Магістр", 2011. - 448 с. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/4730
3. Сезонова, І. К. Інформатика для правоохоронців: навч. посіб. / І. К. Сезонова; МВС України, Харк. нац. ун-т внутр. справ. - Харків, 2015. – 182 с. URL: **http://dspace.univd.edu.ua/xmlui/handle/123456789/1311**

Допоміжна

1. Вишня В. Б. Основи інформаційної безпеки: навч. посіб. / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро: ДДУВС, 2020. 128 с. URL: **http://er.dduvs.in.ua/handle/123456789/4206**
2. Заплотинський Б.А. Інформаційні технології в юридичній діяльності. Посібник. Київський інститут інтелектуальної власності та права НУ "Одеська юридична академія", кафедра інформаційно-аналітичної та інноваційної діяльності, 2018.–108с.
3. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. – 132 с. URL: **http://dspace.univd.edu.ua/xmlui/handle/123456789/9984 http://dspace.onua.edu.ua/bitstream/handle/11300/11095/%D0%86%D0%A2%20%D0%B2%20%D0%AE%D0%94%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf?sequence=1&isAllowed=y**
4. Інформаційне забезпечення юридичної діяльності : підручник / В.Б. Вишня, Л.В. Рибальченко, О.О. Косиченко та ін.; за заг. ред. В.Б. Вишні; МВС України, Дніпропетр. держ. ун-т внутр. справ.- Дніпро : ДДУВС, 2019.- 227 с. URL:**http://er.dduvs.in.ua/handle/123456789/3718**
5. Інформаційне забезпечення діяльності Національної поліції України: зб. законодавчих та нормативних документів / уклад.:В.Б. Вишня та ін. Дніпро: ДДУВС, 2016. 476 с. URL: **http://er.dduvs.in.ua/handle/123456789/2043**
6. Кормич Б.А., Федотов О.П., Аверочкіна Т.В. Правове регулювання інформаційної діяльності: навчально-методичний. Одеська юридична академія. 2018. 150 с. URL:https://pidruchniki.com/15931106/politologiya/pravove_regulyuvannya_informatsiynoyi_sferi_ukrayini
7. Краснобрижий І.В. Інформаційне забезпечення професійної діяльності : навч. посіб. Уклад: І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро : ДДУВС, 2018. 220 с. URL: http://er.dduvs.in.ua/handle/123456789/2046
8. Методичні рекомендації щодо використання комп'ютерної програми «Навчальний ЄРДР» (для ролі «курсант») / [Розроб. Коршенко В. А., Демидов З. Г., Колмик О. О., Абламський С. Є.]; МВС України, Харків. нац. ун-т внутр. справ, Наук.-досл. лаб. з проблем розвитку інформац. технологій, Каф. крим. процесу та організації досуд. слідства ф-ту № 1. - Харків: ХНУВС, 2019. - 30 с. URL: **http://dspace.univd.edu.ua/xmlui/handle/123456789/6675**
9. Мордвинцев М. В. Використання автоматизованих систем відеодокументування переміщень об'єкта для протидії торгівлі людьми / М. В. Мордвинцев, О. В. Хлєстков, С. П. Ницюк // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 23 листоп. 2018 р.). – Дніпро: Дніпропетр. держ. ун-т внутріш. справ, 2018. – С. 52-54. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/3953
10. Наказ МВС "Про затвердження Положення про Інтегровану інформаційно-пошукову систему ОВС України" від 12.10.2009 за № 436.

URL: **http://tranzit.ltd.ua/nakaz/**

11. Наказ МВС “Про затвердження Положення про систему Інтернет у телекомунікаційній мережі Національної поліції України” від 22.02.2017 № 141. URL: **http://tranzit.ltd.ua/nakaz/**
12. Нелюбов В.О., Куруца О.С. Основи інформатики. Microsoft Word 2016: електронний навчальний посібник. Ужгород: ДВНЗ УжНУ, 2018. 96 с. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/18659
13. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 р. № 2155-VIII. URL: **http://zakon2.rada.gov.ua/laws/show/2155-19/page**
14. Проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції : методичні рекомендації / О.О. Акімова, О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков, Ю.І. Тюря. Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2017. 37 с.
    URL:**https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/eib2.pdf**

Інформаційні ресурси в Інтернеті

1. **http://www.nau.kiev.ua**
2. **http://www.liga.kiev.ua**
3. **http://www.informjustr.kiev.ua**
4. http://www.rada.gov.ua
5. https://zakon.rada.gov.ua
   http://www.president.gov.ua

Текст лекції

1. Комп'ютерні віруси, приклади їх шкідливої дії. Екранування програмне („брандмауер”). Характеристика комп'ютерних злочинів. Криптографічний захист. Сметричне та асиметричне шифрування.

Комп'ютерні віруси — це спеціально створені і, як правило, невеличкі програми, здатні заражати інші програми включенням до них своєї, можливо модифікованої, копії (яка зберігає здатність до подальшого розмноження). Програма, заражена комп'ютерним вірусом, може бути автоматично створеною «троянською» програмою, прихованим модулем якої є тіло комп'ютерного вірусу.

Для більшості комп'ютерних вірусів, так само, як для біологічних, характерний певний інкубаційний період, упродовж якого виконувані вірусом несанкціоновані дії обмежуються зараженням інших програм. Інфікуючи програми або носії, віруси можуть поширюватися від однієї програми до іншої, що робить комп'ютерні віруси небезпечнішими порівняно з іншими методами комп'ютерного вандалізму. Операційна система типу MS-DOS, що відрізняється практично повною відсутністю захисту від несанкціонованих дій, полегшує розробку вірусів. Однак комп'ютерні віруси не є програмами, що використовують помилки або недоліки конкретної ОС. Для забезпечення їхнього функціонування цілком достатньо звичайних операцій, використовуваних більшістю «нормальних» програм. Тому принципово не може існувати універсального методу, що захищає ОС від поширення будь-якого вірусу. Проте можна значно ускладнити завдання створення і поширення комп'ютерних вірусів, застосовуючи спеціальні методи в ОС та використовуючи додаткові резидентні і нерезидентні програмні засоби захисту.

Наслідки дії комп'ютерних вірусів:

1) відмова системи у виконанні певної функції (наприклад, блокування вірусом RC-1701 завантаження програми з захищеної від запису дискети), виконання дій, не передбачених програмою (наприклад, зміна даних у будь-якому файлі);

2) руйнування окремих файлів, керуючих блоків або усієї файлової системи (форматування диска, видалення файла тощо);

3) видача помилкових, дратівливих повідомлень (наприклад: «Скажи «бебе»);

4) створення звукових або візуальних ефектів (наприклад, падіння літер у вірусі RC-1701, уповільнене виконання програми у вірусі RCE-1913, програвання мелодії в RCE-1805 або поява на екрані рухомого ромбика у BxI-IC тощо);

5) ініціювання помилок або збоїв у програмі чи ОС (наприклад, переповнення стека);

6) перезавантаження або «зависання» операційної системи;

7) блокування доступу до системних ресурсів (розростання заражених файлів за рахунок їх багаторазового повторного зараження;

8) неможливість передавання зараженій програмі параметрів, уповільнення роботи комп'ютера шляхом виконання пустого циклу з кількох команд після кожного переривання таймера);

9) імітація збоїв апаратури (перетворення частини кластерів на псевдозбійні на дискеті або вінчестері, «зависання» комп'ютера через якийсь час після перезавантаження ОС);

10) прискорення зношування обладнання або спроби його псування.

Збитки, яких завдають віруси, можуть мати катастрофічний характер (знищення вінчестера), якщо в них тривалий «інкубаційний період». Або навпаки: вірус може спричиняти незначні ушко

дження даних, які набагато складніше виявити. Через це дії таких вірусів набагато небезпечніші, ніж масове руйнування даних.

Найбільш незахищена частина файлової системи типу MS-DOS − таблиця розміщення файлів. Якщо вона зруйнована, то ОС не може визначити місцезнаходження файла, хоча самі файли не ушкоджено. Вірус може також виконувати формалізацію деяких ділянок диска, які містять системні дані. Тому необхідно часто дублювати керуючі дані файлової системи на іншу, заздалегідь відому ділянку диска або на дискету. Для цього можна використовувати, наприклад, утиліти Нортон. На комп'ютерах типу АТ дані про конфігурацію системи (тип установленого вінчестера тощо) зберігаються в невеличкій енергонезалежній пам'яті (CMOS). Знищення вмісту CMOS-пам'яті унеможливлює завантаження з вінчестера. Відновлення CMOS-пам'яті потребує знання всіх технічних даних про вінчестер. Тому цей тип пам'яті також є потенційним об'єктом атаки вірусу.

Комп'ютерні віруси «безсмертні» і можуть необмежений час зберігатися в різних архівах. Навіть цілком «знищені» віруси можуть зберегтися в будь-якому архівному файлі й випадково або навмисно «реанімуватися» через багато місяців або навіть років після їхнього першого виявлення і знищення. Отже, після появи певного вірусу необхідно вжити спеціальних заходів для запобігання повторним зараженням. Тут можна діяти в двох напрямках:

знайти першоджерело зараження, розробити або установити програми, що ускладнюють (пильнуючи) чи роблять неможливим вакцинуючи) розмноження вірусу.

Далеко не всі ушкодження файлової системи, несправність вінчестера або обладнання спричинені вірусами. Наприклад, деякі типи вінчестерів мають низьку надійність і псуються без втручання вірусів. Є комп'ютери, які можна завантажити тільки після прогрівання, через деякий час. Існують дисководи, що не тільки фрезерують дискети, а й під час запису іноді стирають таблицю розміщення файлів, причому відновити її за допомогою утиліт Нортон не вдається. Багато комп'ютерів і без вірусів регулярно «зависають». Однак є тенденція атрибутувати будь-яке ушкодження даних у присутності комп'ютерних вірусів.

Складність опису різних засобів захисту від комп'ютерних вірусів і часте дублювання цих засобів роблять актуальним питання про класифікацію комп'ютерних вірусів. Ця класифікація має сприяти однозначному опису не тільки відомих вірусів, а й їх нових різновидів за обмеженою кількістю порівняно простих ознак. Пропонуємо класифікацію, у якій ім'я вірусу складається з літерного префікса, цифрового кореня і, можливо, літерного суфікса. Префікс характеризує середовище розмноження вірусу.

У 1990 р. існувало чотири основних типи комп'ютерних вірусів:

1) ті, що розміщуються в бут-секторі і збійних секторах на диску (тип B, бутові віруси);

2) у файлах типу .com (тип C, файлові віруси);

3) у файлах типу .exe (тип E, файлові віруси);

4) ті, що передаються по мережі (тип N, чи так звані мережеві віруси).

Цифровий корінь характеризує довжину вірусу. Для комп'ютерних вірусів типу C, E і CE (файлових вірусів) він відповідає збільшенню довжини файла під час зараження. Це збільшення для низки файлових вірусів є нестабільним і залежить як від типу файла (.com або .exe), так і від довжини файла, що заражається (наприклад, після дописування свого тіла в кінець файла, що заражається, деякі віруси вирівнюють початок свого тіла на початок параграфа, тобто на зсув, кратний 16). У цьому разі за цифровий корінь беруть мінімальну довжину збільшення. Для вірусів типу B як апроксимацію довжини беруть кількість використовуваних секторів, помножену на 512 (довжину сектора).

Комп'ютерні віруси також поділяються на резиденті й нерезидентні. Нерезидентні віруси отримують керування після завантаження в пам'ять зараженої програми, а потім шукають файл-жертву, використовуючи PATH чи іншу інформацію, і заражають цей файл. Потім керування повертається зараженій програмі, і після закінчення її роботи пам'ять комп'ютера звільняється від вірусу. На відміну від них, резидентні віруси після завантаження в пам'ять і передачі керування зараженій програмі перехоплюють низку переривань і залишаються в пам'яті резидентними. Отримавши керування після переривання, вони виконують певні дії (наприклад, заражають кожну програму, що запускається, заражають .exe і .com файли тощо). Для класифікації таких вірусів використовують суфікс R.

Структурно віруси можна подати у вигляді двох частин: голови і хвоста. Головою називається частина вірусу, яка першою отримує керування, хвостом − його частина, розміщена окремо від голови.

Часто вірус складається з однієї голови (більшість файлових вірусів). Такі віруси називаються несегментованими. На відміну від них, сегментовані віруси мають хвіст і якоюсь мірою аналогічні до оверлейних файлів. Прикладом сегментованих вірусів є бутові віруси, хоча можлива й реалізація сегментованих файлових вірусів.

Отже, спочатку з'явилися файлові віруси, за ними завантажувальні, а потім, з появою вірусів, які самі шифрувалися, вірусологія стала розвиватися шаленими темпами, як і віруси. Фахівці вже називали їх поліморфними вірусами (напевне, серед читачів знайдеться хоча б один, хто пам'ятає вірус Фантом, через який «захворіли» комп'ютери в середині 90-х років).

Але перед тим як перейти до класифікації, давайте з'ясуємо, яку дефініцію вірусу дають класики. Наприклад, всесвітньо відомий американський розробник програмного забезпечення для комп'ютерних мереж, зокрема міжнародних, як от Novell, − програміст Пітер Дайсон (Peter Dyson) дав таке означення вірусу:

«Вірус − це програма, призначенням якої є порушення роботи комп'ютерної системи без відома користувача цієї системи. Вірус може приєднувати сам себе до іншої програми, таблиці розділів або до завантажувального сектора диска та активізуватися за певних ситуацій або комбінації певних ситуацій».

Що таке комбінація певних ситуацій, можна продемонструвати на прикладі поведінки вірусу Ієрусалим (цей приклад уже став класичним, майже всі вірусологи наводять його, тому не будемо порушувати традиції).

Отже, вірус Ієрусалим уперше було зафіксовано у 1988 р. в мережі одного з ізраїльських університетів. Вірус виявляв себе так: на екрані монітора з'являлися чорні квадрати, уповільнювалася робота комп'ютера, тобто вірус викликав лише роздратованість користувачів, але якщо програма, яка була інфікована цим вірусом, завантажувалася в оперативну пам'ять комп'ютера саме у п'ятницю 13-го, то вірус знищував кожну активну в цей момент програму.

Було зафіксовано також вірус Тайвань (1998 р.), дія якого, залежно від поточної дати, могла бути або непомітною, або дуже агресивною. Вірус міг навіть знищити дані у флеш-BIOS, чого було достатньо, щоб змусити користувача замінити материнську плату. А це у грошовому еквіваленті те саме, що купити новий комп'ютер.

Отже, зрозуміло, що не можна одразу визначити міру шкідливості вірусу. Це справа фахівців. Але знати типи вірусів, які можуть загрожувати комп'ютеру, необхідно кожному користувачу.

Сучасні фахівці, зокрема Євген Касперський, поділяють комп'ютерні віруси на такі типи:

файлові; бутові; поліморфні; макровіруси; невидимі; резидентні; хробаки; мережеві.

Вірусологи поділяють віруси не тільки на типи, а й на класи за такими властивостями: середовище розповсюдження вірусу; операційна система, в якій він може існувати; ступінь агресивних дій та особливості алгоритму роботи вірусу (див. таблицю).

Методи захисту від комп’ютерних вірусів

Щодо профілактики зараження вірусами, то тут немає особливих таємниць: здоровий глузд завжди підкаже кожному користувачу, як діяти. Адже правила «гігієни» в комп'ютерному світі дуже схожі на загальнолюдські.

Правила такі:

• бажано мати власний комп'ютер;

• обов'язково встановіть антивірусні програми;

• не забувайте оновлювати антивірусні програми;

• конфіденційну та важливу інформацію дублюйте на зовнішні носії та зберігайте їх окремо від комп'ютера;

• уникайте використання чужих дискет, а якщо все-таки доводиться це робити, обов'язково слід перевіряти таку дискету на наявність вірусів;

• закривайте дискету на запис, якщо вам доводиться переносити таким чином інформацію на інші комп'ютери;

• не користуйтеся піратськими компакт-дисками, пам'ятайте, що вони також можуть містити віруси (особливо, якщо це ігри);

• під час використання електронної пошти не забувайте перевіряти всі отримані листи на наявність вірусів;

• фільтруйте отриману пошту від зайвого спаму, не відкривайте листів від підозрілих адресатів, особливо якщо там є заархівоване вкладення розміром близько 40 кБ (вилучайте такі листи);

• якщо доводиться «скачувати» інформацію з Інтернету, також не забувайте користуватися антивірусом;

• без зайвої потреби не бувайте в Інтернеті. Пам'ятайте: нині існує не тільки безліч вірусів, а й багато програм віддаленого керування комп'ютерами. Завжди знайдуться ті, хто захоче «покопирсатися» у вашому комп'ютері. Пам'ятайте також, що користування Інтернетом не безкоштовне.

Набагато ефективніше вжити заходів, що запобігають враженню комп'ютерними вірусами, ніж витрачати час і кошти на подолання наслідків їх руйнівної дії.

Пропонуємо таку схему антивірусного захисту:

1. Не використовувати програми з незареєстрованими авторськими правами

2. Обмежити доступ до ПК випадковим користувачам, користуючись організаційними і технічними заходами.

3. Систематично створювати архівні та резервні копії інформації, що зберігається на дисках ПК.

4. Періодично здійснювати перевірку інформації на наявність вірусів за допомогою антивірусних сканерів.

5. Відключити завантаження з флоппі-диска і CD-ROM в установках BIOS.

6.Пам'ятайте, що випадковий флоппі-диск є вірогідним джерелом зараження вашого ПК − перед кожним використанням перевіряйте всі диски.

7. За допомогою firewall обмежувати доступ користувачів до небезпечних зон мережі Internet.

8. Системний адміністратор повинен періодично проводити інструктаж користувачів про систему захисту і боротьби з вірусами, пояснювати юридичну відповідальність за написання і розповсюдження комп'ютерних вірусів, пошкодження комп'ютерних систем і комунікацій.

9. Головний захист − компетентність всіх користувачів у питаннях антивірусного захисту.

Проблеми захисту інформації в сучасних системах

Проблема інформаційної безпеки набуває стратегічного значення. Нині практично всі комерційні організації мають автоматизований банк даних з усіх аспектів і напрямків. Як вважають західні фахівці, витік навіть 20 % комерційної інформації в 60 % випадків призводить до банкрутства фірми. Жодна, навіть успішна, фірма США не проіснує більше трьох діб, якщо її конфіденційна інформація, що становить комерційну таємницю, стане відомою конкурентам.

Дослідження показало, що найретельніше захищають бази даних, а найнезахищенішими є системи електронної пошти. У своїх регулярних оглядах web-серверів служба Netcraft із тривогою зазначає, що нині Інтернет атакують так часто, як ніколи раніше. Всі експерти, аналітики та спеціалізовані IT-фірми в один голос б'ють тривогу щодо стану справ із гарантуванням безпеки корпоративних сайтів та інформаційних мереж.

За даними Celent Communications, витрати компаній, які займаються торгівлею в Інтернеті, на гарантування власної та клієнтської безпеки мають зрости з 730 млн. доларів у 2002 р. до 2,6 млрд. доларів у 2006 р.

Сьогодні великим і малим підприємствам та організаціям необхідні доступні за ціною засоби безпеки. Практично до кінця 90-х років персоні-фікація користувача виконувалася способом вказівки його мережевого імені й

пароля. Потрібно зазначити, що подібного підходу, як і раніше, дотримуються в багатьох установах і організаціях. Небезпека, пов'язана з використанням пароля, добре відома: його можна забути, зберегти в невідповідному місці або просто вкрасти. Деякі користувачі навіть записують пароль на папері і тримають ці записи поруч зі своїми робочими станціями. За повідомленням IT-груп багатьох компаній, до 50% дзвінків у службу підтримки пов'язані з забутими паролями, або з паролями, що втратили силу.

Втім, у деяких випадках, коли до безпеки системи не пред'являють особливих вимог, такий підхід цілком виправданий. Однак у міру розвитку комп'ютерних мереж і розширення сфер автоматизації цінність інформації неухильно зростає. Державні секрети, наукомісткі ноу-хау, комерційні, юридичні і лікарські таємниці все частіше довіряються комп'ютеру, що, як правило, підключений до локальних і корпоративних мереж.

Однак варто зазначити, що, оскільки вимоги різних корпоративних інфраструктур до безпеки неоднакові, то наявні рішення в більшості випадків не є універсальними і не виправдовують чекань клієнтів.

Поширення на робочих місцях багатокористувацьких обчислювальних систем, засобів комп'ютерних комунікацій для зберігання та опрацювання інформації вимагає від кожного, хто використовує названі засоби, елементарних вмінь і навичок захисту конфіденційної інформації підприємства, особистої інформацію від викрадення, вилучення, спотворення. Питання забезпечення захисту інформаційних систем досить серйозні і складні, але нехтувати ними при вивченні інформатики у шкільному курсі не можна.

Доцільно навести означення інформаційних технологій як сукупність методів і технічних засобів збирання, організації, зберігання, опрацювання, подання, передавання, захисту інформації, що розширює знання людей і розвиває їхні можливості управлінням технічними і соціальними процесами. За означенням однією складовою інформаційної технології є забезпечення захисту інформації.

Як театр починається з роздягалки, так використання обчислювальної системи починається з операційної системи і саме від ОС залежить наскільки надійно буде захищена збережувана інформація. Насамперед необхідно звернути увагу, що не існує ідеального захисту на всі випадки життя. При практичній реалізації заходів щодо захисту системи необхідно враховувати, що це є цілий комплекс який складається з:

1) забезпечення фізичної безпеки комп'ютера;

2)забезпечення локального захисту системи від втручання несанкціонованих користувачів та неправомірних дій легальних користувачів.

3) забезпечення захисту під час роботи в мережі.

Забезпечення фізичної безпеки комп 'ютера

При забезпеченні фізичної безпеки комп'ютера необхідно чітко визначити коло фізичних осіб, що можуть мати до системи, права надані їм для роботи, які вирішують завдання, наявність сигналізації в приміщенні де знаходиться комп'ютер, адже якщо викрадуть комп'ютер то у зловмисника можуть опинитися файли паролів, структура і адресація мережі, що зробить прозорим проникнення в мережу організації.

Забезпечення локального захисту системи Одним із методів забезпечення локального захисту є автентифікація користувачів перед початком роботи,

введення реєстраційної імені та пароля. Необхідно звернути увагу на правила вибору пароля, для зменшення ймовірності його підбору:

1) не можна використовувати власні імена дружини, дітей, батьків, сестер, братів;

2) невикористовуйте в якості пароля номер паспорта, машини, телефону;

3) не використовуйте як пароль повторюючі символи на зразок 44444, ggggg;

4) довжина пароля повинна бути не меншою 4 символів, оптимально 6.

5) найкращий пароль це комбінація букв різного регістру і цифр. Наприклад: 6Kd3rP.

Не можна передавати свої реєстраційні дані, ім'я та пароль, стороннім особам, надавати інформацію про втановлені права доступу до робочих файлів, каталогів, інстальоване програмне забезпечення. Як показує досвід, більшість комп'ютерних злочинів відбувається саме з вини користувачів, які не дотримувалися елементарних правил використання обчислювальної техніки. У більшості ситуацій достатньо заборонити доступ до системи випадкових відвідувачів.

Ще одним засобом захисту локальної системи є встановлення відповідних прав доступу до файлів, каталогів.

Також доцільно розглянути засоби забезпечення безпеки, що надаються системою BIOS, використання паролів при включенні системи і на модифікацію системних параметрів BIOS. Хоча це не є достатньо ефективним заходом, при певних навиках такий пароль легко змінити, але для захисту від ненавмисного втручання може бути цілком достатнім.

Забезпечення захисту під час роботи в мережевому середовищі

Обговорюючи питання захисту необхідно наголосити, що встановлюючи захист не можна забувати, що з кожним бар'єром легальному користувачу буде все важче виконувати свої повсякденні функції. Отже потрібно шукати компроміс, «золоту середину», щоб користувачі могли нормально працювати і зловмисник не міг проникнути в систему. Одним з критеріїв оцінки заходів забезпечення захисту є співвідношення витрат на отримання доступу до інформації і вартістю цієї інформації, якщо витрати на забезпечення захисту значно перевищують цінність інформації, зрозуміло, що організація таких заходів буде недоцільною.

2. Електронний документ – поняття та складові частини, властивості. Електронний цифровий підпис – поняття, складові частини. Накладання ЕЦП. Суб'єкти правових відносин у сфері послуг ЕЦП. Процедури використання ЕЦП. Криптографічна непохитність електронного цифрового підпису.

Інформаційний обмін є необхідним динамічним компонентом кожної соціальної організації. Однією з найбільш роз повсюджених форм інформаційного обміну в установах є доку ментообіг.

Документообіг – комплекс робіт з документами: прийом, реєстрація, розсилка, контроль виконання, формування справ, збереження та повторне використання документації, до відкова робота.

Майже 100% документів установ представлені в електронному виді, тобто є електронним документом.

Електронний документ – це документ, створений за допомогою засобів комп'ютерної обробки інформації, підписаний електронним цифровим підписом (ЕЦП) і збережений на машинному носії у вигляді файла відповідного формату. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою представлення електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною.

Електронний документообіг – сукупність процесів створення, обробки, виправлення, передачі, одержання, збереження, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. Засоби управління документами забезпечують процес створення документів, контролю їх версій, управління доступом до них і їх розповсюдженням у корпоративних мережах, а також здійснюють контроль над потоками документів в організації.

Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством. Це визначено у ст. 9 Закону України «Про електронні документи та електронний документообіг» від 22 травня 2003 р. № 851-IV.

Система автоматизації документообігу – це організаційно-технічна система, що забезпечує процес створення, управління доступом і розповсюдження електронних документів у комп'ютерних мережах, а також забезпечує контроль над потоками документів в організації. Основні принципи електронного документообігу:

- одноразова реєстрація документа;
- можливість паралельного виконання різних операцій з метою скорочення часу руху документів і підвищення оперативності їх виконання;
- безперервність руху документа;
- єдина база документної інформації для централізованого збереження документів і виключення можливості дублювання документів;
- ефективно організована система пошуку документа;
- розвинена система звітності по різних статусах і атрибутах документів, що дозволяє контролювати рух документів у процесах документообігу.

Наприклад, у судовій діяльності використовується автоматизована система документообігу суду. Положення про автоматизовану систему документообігу суду затверджене рішенням Ради суддів України від 26 листопада 2010 р. № 30 щодо впровадження документообігу у судах загальної юрисдикції. Введене у дію з 1 січня 2011 р. Положення визначає порядок функціонування автоматизованої системи документообігу в судах загальної юрисдикції.

Стаття 35 «Автоматизована система документообігу суду» Кримінального процесуального кодексу України, прийнятого у 2012 р., визначає:

1. У суді функціонує автоматизована система документообігу суду, що забезпечує:

1) об’єктивний та неупереджений розподіл матеріалів кримінального провадження між суддями з додержанням принципів черговості та однакової кількості проваджень для кожного судді;

2) визначення присяжних для судового розгляду з числа осіб, які внесені до списку присяжних;

3) надання фізичним та юридичним особам інформації про стан розгляду матеріалів кримінального провадження у порядку, передбаченому цим Кодексом;

4) централізоване збереження текстів вироків, ухвал та інших процесуальних документів;

5) підготовку статистичних даних;

6) реєстрацію вхідної і вихідної кореспонденції та етапів її руху;

7) видачу вироків, ухвал суду та виконавчих документів

на підставі наявних у системі даних;

8) передачу матеріалів до електронного архіву.

3. Конфіденційне листування електронною поштою. Створення пари ключів. Збереження файлів ключів. Шифрування файлів на комп’ютері. Розшифрування файлу. Пересилання ключа (3 способи). Одержання ключів. Імпорт ключа.

Internet, як вже згадувалося, це величезне сховище ін формації. Причому інформацією можуть бути енциклопедичні відомості та цифрові фотографії, статті, відеофільми, електронні книги, ігри, реферати, оголошення про знайомства, постанови уряду та багато іншого.

В основі роботи сучасного Internet – наступні основні сервіси:

- Web-сторінки і Web-сайти
- Електронна пошта (e-mail) – можливість отримувати і відправляти електронні листи
- Списки розсилання (Mailing List). Звичайна електронна пошта припускає наявність двох партнерів по переписуванню. Великий потік поштової інформації на свою адресу можна забезпечити, підписавшись на списки розсилання. Це спеціальні тематичні сервери, на яких збирають інформацію за визначеними темами і переправляють її передплатникам у виді повідомлень електронної пошти. Списки розсилання дозволяють ефективно вирішувати питання регулярної доставки даних.
- IRC. Служба IRC (Internet Relay Chat) призначена для прямого спілкування кількох людей у режимі реального часу. Іноді цю службу називають чат-конференціями чи просто чатом. Повідомлення, що відправляються на сервер, який забезпечує функціонування форуму, негайно транслюється всім користувачам, підключеним до поточної дискусії. На відміну від системи телеконференції, у якій спілкування між учасниками обговорення теми відкрито усьому світу, у системі IRC спілкування відбувається тільки в межах одного каналу, у роботі якого беруть участь звичайно лише кілька людей. Кожен користувач може створити власний канал і запросити в нього учасників бесіди чи приєднатися до одного з відкритих у даний момент каналів.
- Інтернет-пейджери (месенджери) – можливість в реальному часі обмінюватися короткими електронними повідомленнями з користувачами, які в даний момент знаходяться в мережі. Від електронної пошти даний сервіс відрізняється насамперед тим, що в ході спілкування видно, коли

співрозмовник знаходиться на зв'язку. Програми, які забезпечують даний сервіс, називаються ICQ – I seek you – я шукаю тебе.

- Сховища файлів – так звані FTP-сервери. На них розміщуються файли, доступні для скачування.
- Файлообмінні мережі (пірінгові мережі) – це так звані мережі всередині великої мережі Internet, в які об'єднуються користувачі, що пропонують один одному різні файли – відео, музику, програми. Пірінгова мережа P2P (peer-to-peer) передбачає спілкування і передачу файлів між комп'ютерами в мере жі безпосередньо без посередників (проміжних серверів). У багатьох пірінгових мережах можна включитися і скачати з них файли тільки тоді, коли запропонуєте свої для обміну.

Для роботи з P2P необхідна спеціальна програма-клієнт, причому для кожної мережі вона своя. Завантажити файли з пірінгової мережі можна за допомогою Internet-браузера.

Контрольні запитання

1. Історія створення комп'ютерних вірусів.
2. Поясніть процес зараження комп'ютерними вірусами.
3. Перелічіть наслідки дії комп'ютерних вірусів.
4. Перелічіть основні типи комп'ютерних вірусів.
5. Сучасна класифікація комп'ютерних вірусів.
6. Перелічіть "найсвіжіші" комп'ютерні віруси.
7. Методи захисту від комп'ютерних вірусів.
8. Огляд антивірусних програм.
9. Перелічіть основні проблеми захисту інформації.
10. Як забезпечується фізична безпека комп'ютера.
11. Як забезпечити захист під час роботи в мереженому просторі.
12. Правові та етичні питання використання програмного забезпечення.
13. Новітні засоби захисту інформації.