УДК 004.056
© Антоненко О. В.

УДОСКОНАЛЕННЯ ЗМІСТУ НАВЧАННЯ З ЗАХИСТУ ІНФОРМАЦІЇ

Постановка проблеми. Примітна особливість нинішнього періоду – перехід від постіндустріального суспільства до інформаційного, в якому інформація стає більш важливим ресурсом, ніж матеріальні або енергетичні ресурси.

Ми живемо у світі інформації. За всіх часів перевагу мали ті, хто володів найбільш точною й вагомою інформацією, тим більше, якщо це стосувалося інформації про своїх суперників. Це підтверджується й тим, що державні й комерційні секрети, а отже, і полювання за ними, їх добування виникли на зорі людського суспільства, коли з'явилися держави, розвивалася торгівля між ними.

Інформація – відомості про осіб, факти, події, явища і процеси незалежно від форми їх представлення.

Поняття «інформація» сьогодні вживається досить широко й різнобічно. Важко знайти таку галузь знань, де б воно не використовувалося. Величезні інформаційні потоки буквально захльостують людей. Обсяг наукових знань, наприклад, за оцінками фахівців, подвоюється кожні п'ять років.

Проблема захисту інформації від несанкціонованого доступу до неї виникла давно, з тієї пори, коли людині через певні причини не хотілося ділитися нею. З розвитком людського суспільства, появою приватної власності, державного ладу, боротьбою за владу й подальшим розширенням масштабів людської діяльності інформація починає набувати ціну. Коштовною стає та інформація, володіння якою дозволить її існуючому й потенційному власникам отримати певну користь: матеріальну, політичну, військову тощо.

Із переходом на використання технічних засобів зв'язку інформація починає зазнавати впливу випадкових процесів: несправностей і збоїв устаткування, помилок операторів тощо, які могли призвести до помилок та навіть руйнування, а також створити передумови доступу до неї сторонніх осіб. Із подальшим ускладненням і широким поширенням технічних засобів зв'язку зросли можливості для несанкціонованого доступу до інформації.

Збільшення обсягів інформації, необхідність зосередження її в єдиних базах даних, автоматизація обміну інформацією на великих відстанях, розширення кола користувачів і збільшення кількості технічних засобів і зв'язків в автоматизованих системах керування й обробки даних стало передумовою виникнення складних автоматизованих систем (САС).

Із появою САС керування, пов'язаних з автоматизованим введенням, зберіганням, обробкою й виведенням інформації, проблема її захисту здобуває ще більшого значення.

Аналіз останніх досліджень і публікацій. Сучасні дослідження проблеми забезпечення безпеки комп'ютерних систем ведуться як у напрямку розкриття природи явища, що полягає в порушенні цілісності й конфіденційності інформації, дезорганізації роботи комп'ютерної системи, так і в напряму розробки конкретних практичних методів і засобів їх захисту. Серйозно вивчається статистика порушень, причини, що їх викликають, особистості порушників, суть прийомів і засобів які застосовуються порушниками, які використовують при цьому недоліки систем і засобів їх захисту, обставини, при яких було виявлене порушення та інші питання.

Проведений аналіз останніх досліджень і публікацій в галузі захисту інформації показав актуальність проведення даної роботи, що викликана відсутністю необхідних методичних і науково-технічних основ забезпечення захисту інформації в сучасних умовах інформаційного суспільства. Є вагомі підстави вважати, що відсутність певних критеріїв та класифікації об’єктів та шляхів реалізації погроз безпеки інформації, а також організаційні заходи й апаратно-програмні засоби захисту, які застосовуються сьогодні у вітчизняних системах обробки інформації, не можуть забезпечити достатній ступінь безпеки інформації і суб'єктів, які беруть участь в процесі інформаційної взаємодії, і не здатні в необхідному

ступені протистояти різного роду впливам та погрозам, метою яких є доступ до конфіденційної інформації й дезорганізація роботи автоматизованих комп'ютерних систем.

Постановка завдання. Одним із найважливіших аспектів проблеми забезпечення безпеки комп'ютерних систем є виявлення, аналіз і класифікація можливих об'єктів та шляхів реалізації загроз безпеки, тобто можливих каналів несанкціонованого доступу до системи з метою порушення її робочого стану або доступу до критичної інформації.

Виклад основного матеріалу. XXI сторіччя безсумнівно є одним з поворотних етапів у житті людства. Людство захоплене технікою й уже навряд чи відмовиться від зручностей, наданих нею. Уже багатьма забуте відвідування бібліотеки, спілкування з друзями біля багаття, звичайна пошта з конвертами й листоношами – на зміну всьому цьому прийшов кіберпростір – електронні бібліотеки й бази даних, чати й форуми користувачів, електронна пошта з приголомшуючою швидкістю доставки (до декількох хвилин без залежності від відстані) і дуже високою надійністю. Важко уявити собі існування сучасного суспільства без комп'ютера, здатного багаторазово підвищити продуктивність праці й передати будь-яку інформацію.

Цим кіберпростором став Інтернет – не тільки всесвітнє сховище даних, у якому кожний обов'язково знайде саме те, що йому потрібно, а також цілий світ всіляких розваг на будь-який смак. Ще одне виняткове призначення Інтернету – передача інформації, наприклад, за допомогою електронної пошти. У цьому плані він унікальний. Немає інших настільки розгалужених поштових мереж. Доставка кореспонденції відбувається тут майже миттєво, на заздрість традиційним службам XX ст. І, нарешті, повідомлення можна отримувати, перебуваючи фізично де завгодно, був би комп'ютер.

Інтернет – це всесвітня "мережа-мереж", що використовує для взаємодії стек протоколів TCP/IP (Transmission Control Protocol/Internet Protocol). Інтернет був створений для полегшення взаємодії між організаціями, що виконують урядові замовлення. У 80-ті роки до нього підключилися навчальні заклади, урядові агентства, комерційні фірми й міжнародні організації. В 90-ті роки Інтернет набуває феноменальної популярності. Зараз до Інтернету приєднані більше трильйону користувачів.

Хоча підключення до Інтернету й надає величезні переваги через доступ до колосального обсягу інформації, воно ж є небезпечним для сайтів із низьким рівнем безпеки. Інтернет страждає від серйозних проблем із безпекою, які, якщо їх ігнорувати, можуть призвести до катастрофи.

Є в Інтернеті й недолік – загроза інформації з боку зловмисників, половина з яких діє просто з бажання комусь нашкодити або довести що-небудь світові. Гірше й небезпечніше, якщо ваша інформація представляє для когось практичний інтерес, наприклад, ділова переписка.

Інтернет – це важливий ресурс, що змінив стиль діяльності багатьох людей і організацій. Проте Інтернет страждає від серйозних і широко розповсюджених проблем із безпекою. Багато організацій було атаковано або зондовано зловмисниками, в результаті чого вони зазнали великих фінансових втрат і позбавилися свого престижу. В деяких випадках організації були змушені тимчасово відключитися від Інтернету й зазнали значних втрат задля усунення проблем із конфігураціями хостів і мереж. Сайти, які не інформовані або ігнорують ці проблеми, ризикують зазнати мережної атаки зловмисниками. Навіть ті сайти, які впровадили в себе заходи щодо забезпечення безпеки, піддаються тим самим небезпекам через появу нових уразливих місць у мережних програмах і наполегливості деяких зловмисників. Що ж може зробити з інформацією зловмисник?

По-перше, просто її прочитати (і використовувати потім вам на шкоду), що називається порушенням конфіденційності інформації.

По-друге, змінити вміст або привласнити собі авторство повідомлення, що є порушенням цілісності інформації. Класичний приклад порушення цілісності – додавання зайвого нуля в платіжному документі, а це зовсім неприпустимо.

Перераховані вище дії здійснюють зловмисники, яких у кіберпросторі називають

хакерами. Дослідження показали, що хакерами найчастіше стають:

- чоловіки;
- у віці від 16 до 35 років;
- самотні;
- з освітою;
- технічно грамотні.

Хакери мають чітке уявлення про роботу комп'ютерів і мереж, про те, які протоколи використовуються для виконання системних операцій.

Але найбільшої шкоди кіберпростору завдають комп'ютерні віруси. До основних технічних феноменів XXI століття відносяться, на мій погляд, грандіозний прогрес систем зв'язку й передачі інформації й, звичайно ж, приголомшуючий розвиток мікро- і макрокомп'ютерів.

Комп'ютерні віруси є паразитами стосовно інших комп'ютерних програм. Вони зроблені так, що не можуть жити самостійно. При виконанні програми, в яку впроваджений вірус, виконується код вірусу, що реалізує власні функції. Ці функції зазвичай включають зараження інших програм і поширення на інші диски. Деякі віруси є шкідливими - вони видаляють файли або виводять із ладу систему. Інші віруси не завдають ніякої шкоди, крім поширення самих себе по комп'ютерних системах.

По-перше, комп'ютерні віруси – серйозна й досить помітна проблема, виникнення якої ніхто не очікував. По-друге, комп'ютерні віруси – це перша цілком вдала спроба створити штучне життя. Спроба вдала, але не можна сказати, що корисна, бо сучасні комп'ютерні "мікроорганізми" найбільше нагадують комах-шкідників, що приносять тільки проблеми й неприємності. І, по-третє, тема вірусів стоїть трохи осторонь від усіх інших завдань, розв'язуваних за допомогою комп'ютера. Практично всі проблеми, розв'язувані за допомогою обчислювальної техніки, є продовженням цілеспрямованої боротьби людини з навколишньою природою. А от боротьба з комп'ютерними вірусами є боротьбою людини з людським розумом.

Віруси можна розділити на класи за такими ознаками:

– середовище перебування;

– операційна система (ОС);

– особливості алгоритму роботи;

– деструктивні можливості.

Залежно від ***середовища перебування*** віруси можна розділити на:

– файлові;

– завантажувальні;

– макровіруси;

– мережеві.

Файлові віруси впроваджуються у виконувані файли (найпоширеніший тип вірусів), або створюють файли-двійники (віруси-компаньйони) або використовують особливості організації файлової системи (link-віруси).

Завантажувальні віруси записують себе або в завантажувальний сектор диска (boot-сектор), або в сектор, що містить системний завантажник вінчестера (Master Boot Record), або змінюють покажчик на активний boot-сектор.

Макровіруси заражають файли-документи й електронні таблиці декількох популярних редакторів.

Мережеві віруси використовують для свого поширення протоколи або команди комп'ютерних мереж і електронної пошти.

Існує велика кількість сполучень, наприклад файлово-завантажувальні віруси, що заражають як файли, так і завантажувальні сектори дисків. Такі віруси, як правило, мають досить складний алгоритм роботи, часто застосовують оригінальні методи проникнення в систему, використовують стелс- і поліморфік-технології. Інший приклад такого сполучення – мережевий макровірус, що не тільки заражає документи, які редагуються, але й розсилає

свої копії по електронній пошті.

Заражена операційна система, (точніше ОС, об'єкти якої піддані зараженню) є другим рівнем розподілу вірусів на класи. Кожний файловий або мережевий вірус заражає файли однієї або декількох ОС. Макровіруси заражають файли форматів Word, Excel. Завантажувальні віруси також орієнтовані на конкретні формати розташування системних даних у завантажувальних секторах дисків.

Так хто ж пише віруси? Переважну їх кількість створюють студенти й школярі, які тільки що вивчили мову Асемблер, хочуть спробувати свої сили, але не можуть знайти для них більш гідного застосування. Втішний той факт, що значна частина таких вірусів часто не поширюється, й вони через якийсь час "вмирають" разом із носіями інформації, на яких зберігаються. Такі віруси пишуться, як правило, тільки для самоствердження.

Другу групу становлять також молоді люди (частіше студенти), які ще не повністю опанували мистецтвом програмування, але вже вирішили присвятити себе написанню й поширенню вірусів. Головною причиною, яка штовхає певну категорію людей на написання вірусів, – комплекс неповноцінності, що проявляє себе в комп'ютерному хуліганстві.

З-під пера подібних "умільців" часто виходять або численні модифікації "класичних" вірусів, або віруси вкрай примітивні, з великою кількістю помилок.

З часом багато хто з цих "вірусописьменників" попадають у третю, найнебезпечнішу групу, що створює й запускає в світ "професійні" віруси. Ці дуже ретельно продумані й налагоджені програми створюються професійними, часто досить талановитими програмістами.

На мою думку, причина, що змушує таких людей направляти свої здатності на таку безглузду роботу, все та ж – комплекс неповноцінності, що іноді сполучається з неврівноваженою психікою. Показовий той факт, що подібне "вірусописьменництво" часто поєднується з іншими ззгубними пристрастями.

Трохи окремо розташована четверта група авторів вірусів – "дослідники". Ця група складається з досить кмітливих програмістів, які займаються винаходом принципово нових методів зараження, приховання, протидії антивірусам і т.д. Вони ж придумують способи впровадження в нові ОС (операційні системи), конструктори вірусів і поліморфік-генератори. Ці програмісти пишуть віруси не заради вірусів, а скоріше заради дослідження потенціалу "комп'ютерної фауни".

Часто автори подібних вірусів не запускають свої творіння в життя, однак дуже активно пропагандують свої ідеї через численні електронні видання, присвячені створенню вірусів. При цьому небезпека від таких "дослідницьких" вірусів не падає, тому що, потрапивши в руки "професіоналів" із третьої групи, нові ідеї дуже швидко реалізуються в нових вірусах.

Способи протидії комп'ютерним вірусам можна розділити на кілька груп:

– профілактика вірусного зараження й зменшення передбачуваного збитку від такого зараження;

– використання антивірусних програм, зокрема для знешкодження й видалення відомого вірусу;

– виявлення й видалення невідомого вірусу.

Одним з основних методів боротьби з вірусами є, як і в медицині, своєчасна профілактика. Комп'ютерна профілактика припускає дотримання деяких правил, що дозволяють значно знизити ймовірність зараження вірусом і втрати будь-яких даних.

Для того, щоб визначити основні правила комп'ютерної гігієни, необхідно з'ясувати основні шляхи проникнення вірусу в комп'ютер і комп'ютерні мережі.

Основним джерелом вірусів на сьогоднішній день є глобальна мережа Internet. Найбільше число заражень вірусом відбувається при обміні листами у форматах Word. Користувач зараженого макровірусом редактору, сам того не підозрюючи, розсилає заражені листи адресатам, а вони, у свою чергу, відправляють нові заражені листи тощо.

Припустимо, що користувач веде переписку з п'ятьма адресатами, кожний з яких

також листується з п'ятьма адресатами. Після посилки зараженого листа всі п'ять комп'ютерів, що отримали його, виявляються зараженими. Потім із кожного знову зараженого комп'ютера відправляється ще п'ять листів: один іде назад на вже заражений комп'ютер, а чотири – до нових адресатів.

Файл-сервери загального користування й електронні конференції також виступають одним з основних джерел поширення вірусів. Практично щотижня приходить повідомлення про те, що який-небудь користувач заразив свій комп'ютер вірусом, що був знятий з ftp-сервера або з якої-небудь електронної конференції.

При цьому часто заражені файли "вкладаються" автором вірусу на декілька або розсилаються по декількох конференціях одночасно, і ці файли маскуються під нові версії якого-небудь ПО (іноді під нові версії антивірусів).

У випадку масового розсилання вірусу по файл-серверах ураженими практично одночасно можуть виявитися тисячі комп'ютерів, однак у більшості випадків "вкладаються" DOS- або Windows-віруси, швидкість поширення яких у сучасних умовах значно нижче, ніж макровірусів. Із цієї причини подібні інциденти практично ніколи не закінчуються масовими епідеміями, чого не можна сказати про макровіруси.

Третій шлях швидкого зараження – локальні мережі. Якщо не вживати необхідних заходів захисту, то заражена робоча станція при вході в мережу заражає один або кілька службових файлів на сервері. Наступного дня користувачі при вході в мережу запускають заражені файли із сервера, й у такий спосіб вірус одержує доступ на незаражені станції.

Замість службового файлу може також виступати різне ПЗ (програмне забезпечення), встановлене на сервері, стандартні документи-шаблони або таблиці, які використовуються у фірмі тощо.

Нелегальні копії програмного забезпечення є однією з основних зон ризику. Часто піратські копії на дискетах і навіть на CD-ROM містять файли, заражені найрізноманітнішими типами вірусів.

Небезпеку представляють також комп'ютери, встановлені в навчальних закладах. Якщо один зі студентів приніс на своїх носіях інформації вірус і заразив який-небудь навчальний комп'ютер, то чергову "заразу" при завантаженні даних із цього ПК (персонального комп’ютеру) одержать і носії всіх інших студентів, що працюють на цьому комп'ютері.

Те ж саме стосується й домашніх комп'ютерів, якщо на них працює більше одного користувача. Нерідкі ситуації, коли діти-студенти, працюючи на багатокористувальницькому комп'ютері в навчальному закладі, перетаскують звідти вірус на домашній комп'ютер, у результаті чого останній попадає в комп'ютерну мережу фірми, де працюють батьки.

Найбільш ефективні в боротьбі з комп'ютерними вірусами антивірусні програми. Однак відразу хотілося б відзначити, що не існує антивірусів, що гарантують стовідсотковий захист від вірусів, і заяви про існування таких систем можна розцінити або як несумлінну рекламу, або як непрофесіоналізм. Таких систем не існує, оскільки на будь-який алгоритм антивірусу завжди можна запропонувати контралгоритм вірусу, невидимого для цього антивірусу. До того ж, неможливість існування абсолютного антивірусу була доведена математично на основі теорії кінцевих автоматів, автор доказу – Фред Коєн.

Висновки. Безперечно, процес захисту інформації від вірусів та хакерів у сучасному кіберпросторі передбачає велику роботу. По-перше, у вихованні комп’ютерно-грамотної людини, ціннісного ставлення до будь-якої інформації, до оволодіння сучасними технологіями її захисту. По-друге, в розробці та впровадженні нових більш жорстких умов використання електронної інформації та створенню абсолютно захищеної комп’ютерної системи.

Постає питання: хто буде створювати таку систему? Водночас виникає безліч нових питань: а хто буде навчати цьому, хто буде стежити за виконанням усіх умов безпеки, хто буде виховувати в користувачів комп’ютерну грамотність та етикет? Мабуть відповідь така

– хакери! Бо вони краще за всіх володіють знаннями про кіберпостір, це їх віртуальне життя.

Перспективи подальших досліджень. Існує ще багато питань, пов'язаних із психологічними та моральними аспектами, що стосуються захисту інформаційного простору, які постійно потребують аналізу та діагностики. Саме вирішення цих питань і є метою нашого подальшого дослідження.

Список використаних джерел

1. Галатенко В. А. Основы информационной безопасности / В. А. Галатенко. – 4-е изд. М. : ИНТУИТ. ру, 2008. - 208 с. – Сер. : Основы информационных технологий.
2. Галатенко В. А. Стандарты информационной безопасности / В. А. Галатенко. - 2-е изд. – М. : ИНТУИТ.ру, 2005. - 264 с. – Сер. : Основы информационных технологий.
3. Савельев М. Защита информации в корпоративных сетях / М. Савельев // Мир связи. Connect. – 2004. – № 9.
4. Панасенко С. П. Защита информации в компьютерных сетях / С. П. Панасенко // Мир ПК. – 2002. – № 4.
5. Мэйволд Э. Безопасность сетей : практическое пособие / Э. Мэйволд. – М. : Эком, 2006. – 528 с. – (Сер. : Шаг за шагом.)
6. Avolio F. A Network Perimeter With Secure Internet Access / F. Avolio, M. Ranum // Internet Society Symposium on Network and Distributed System Security / Internet Society, February 2-4, 1994. – P. 109–119.
7. Lincoln D. Stein. The World Wide Web Security FAQ [Electronic recource] / Lincoln D. Stein. – Access mode: http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html
8. NIST Special Publication 800-12, An Introduction to Computer Security : The NIST Handbook.
9. Holbrook P. Site Security handbook [Elecronic resource] / P. Holbrook, J. Reynolds.– Access mode : ftp://nic.ddn.mil/rfc/rfc1244.txt.

Антоненко О. В.

Удосконалення змісту навчання з захисту інформації

Розглянуто проблеми безпеки в комп'ютерних системах і мережах. Розглянуто типи зловмисників у комп'ютерному світі та основні види вірусів, які становлять загрозу всьому кіберпростору.

Ключові слова: об'єкти, шляхи, реалізація погроз, безпека інформації, комп'ютерні системи, мережі, вірус.

Антоненко А. В.

Усовершенствование содержания обучения по защите информации

Рассмотрена проблема безопасности в компьютерных системах и сетях. Описаны типы преступников в компьютерном мире и основные виды вирусов, которые представляют угрозу киберпространству.

Ключевые слова: объекты, пути, реализация угроз, безопасность информации, компьютерные системы, сети, вирус.

A. Antonenko

Improving Contents of Teaching Information Protection

The issue of safety of computer systems and networks is considered. Types of criminal in the computer world are described ass well as main kinds of viruses that threaten the cyberspace.

Key words: objects, ways, realization of threats, information safety, computer systems, networks, virus.

Стаття надійшла до редакції 15.12.2011 р.