

УДК 004.738.5:343.97

Шевченко В. В.
Національний педагогічний університет
імені М. П. Драгоманова

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ ПІДВИЩЕНОЇ ІНТЕРНЕТ-ЗЛОЧИННОСТІ

У статті йдеться про вплив інтернет-технологій, а також інтернет-зособів, на соціально-економічний процес інформаційного суспільства, зокрема на систему інформаційного захисту даних установи чи організації в умовах підвищеної інтернет-злочинності.

Ефективне впровадження різноманітних засобів захисту, і перш за все інформаційних і комунікаційних, позитивно впливають на всю систему захисту інформації.

Ключові слова: інформаційні технології, ЕОМ, ІТ, інформаційна грамотність, системи захисту та інтернет-злочинність.

Спочатку система інформаційної безпеки розроблялася для потреб військових. Стратегічні дані, що стосуються обороноздатності, були настільки важливі, що їх витік міг призвести до величезних людських втрат. Відповідно, комп'ютерно-інформаційна безпека звернулася до досвіду криптографії, тобто шифрування. З'являлися кріптошрифти і спеціальні програми, що дають змогу автоматизувати процес шифрування та дешифрування.

Пізніше, коли необхідність захисту інформації поширилася на інші сфери, стало зрозуміло, що іноді шифрування сильно ускладнює та уповільнює передачу і використання даних. А з розвитком комп'ютерних мереж і систем стали з'являтися інші завдання та вимоги.

З часом з'явилася класифікація таємниць, які потребують спеціалізованої системи захисту. На сьогодні вони включають шість категорій: державна, комерційна, банківська, професійна, службова таємниця та персональні дані. Зрозуміло, що для різних галузей і типів підприємств пріоритетними виявляються одна чи дві категорії. Виробництву, пов'язаному з наукою, наприклад, вкрай важливо запобігти витоку планів, нових розробок та випробувань.

Фахівці вважають, що сьогодні, на відміну від минулих десятиліть, більше уваги приділяється двом речам: доступності та цілісності інформації. Доступність означає той факт, що кожен користувач може в будь-який час зажадати необхідний сервіс і працювати в ньому без ускладнень. З другого боку – під час зберігання і передачі інформація повинна залишатися цілісною та незмінною. Особливо актуальним це є для банків, де важливо не допустити зміни реквізитів, приписування зайвих нуликів. Водночас

провайдерам або операторам зв'язку абсолютно необхідно зберігати доступність і безвідмовність роботи інформаційних систем (сервера, вузла зв'язку), тому що саме це є основою успіху.

Отже, сучасний захист інформації – це пошук оптимального співвідношення між доступністю і безпекою. Або, інакше кажучи, це постійна боротьба з дурістю користувачів та інтелектом хакерів.

Існує кілька міфів про те, хто найбільше робить замах на чужу інформацію. Наприклад, дещо перебільшують шанси нападу хакерів. Це, мовляв, такі моторні хлопці, які тільки й роблять, що крадуть гроші з банківських рахунків і руйнують національні системи безпеки. Від них і варто всіляко захищатися. Насправді хакери беруть не числом, а вмінням. А статистика говорить, що 70-80% комп'ютерних злочинів скоюються працюючими або звільненими співробітниками, тобто всередині компаній. Іноді люди, що володіють великими повноваженнями, паролями і доступом до інформації, не можуть здолати спокуси скористатися цими перевагами. А ті, кого звільнили, таким чином мають намір помститися фірмі, відділу або особисто звільнити керівника, звісно віртуально за допомогою мережі Інтернет.

Що ж до хакерів, то сьогодні багато хто з них абсолютно легально займаються тестуванням нових програм захисту. Власне, тестування полягає в тому, що програму намагаються зламати і спостерігають за її "реакцією". Саме це породжує на Заході найсерйозніші складнощі у взаєминах з нашою державою.

За твердженням західних фахівців, витік 20% комерційної інформації в 60 випадках зі 100 призводить до банкрутства фірми. Жодна, навіть процвітаюча, фірма не проіснує більше трьох діб, якщо її інформація, що складає комерційну таємницю, стане відомою. Таким чином, економічна та інформаційна безпека виявляються тісно взаємозалежними.

Справа в тому, що в 1998 році в США був прийнятий один із найбільш спірних та гучних законів – DCMA (Digital Millennium Copyright Act) – "Акт про авторські права в цифровому віці". Він заборонив обходити захист від копіювання та поширювати пристрої, які можна використовувати для порушення авторських прав. Причому покарання за цим законом здійснюється навіть у тому випадку, коли зловмисник не зробив нічого, крім самого взлому, не завдавши при цьому матеріального збитку.

Після того як фахівець перевіряє надійність захисту програмного забезпечення і публікує інформацію про її слабкі місця, його можуть притягнути до відповідальності за порушення закону "Про авторські права".

Зрозуміло, щоб сьогодні проникнути в інформаційне поле якого-небудь підприємства, установи або людини, абсолютно необов'язково зламувати двері або встановлювати спеціальні "жучки". Експерти кажуть: "Повністю захищений комп'ютер – це той, який стоїть під замком у сейфі в

броньованій кімнаті і не включений навіть в розетку”. Зловмисники використовують найпростіші програми – віруси – програми типу “троянський кінь” (встановлюються на комп’ютер, при цьому досить легко крадуть всі паролі, дають змогу переглядати вміст екрану, перехоплювати всі повідомлення та інформацію, змінювати файли тощо). Модними стали також атаки під назвою “відмова в обслуговуванні”, які виводять з ладу цілі вузли мережі. При цьому робота вузла стає неможливою протягом декількох хвилин або навіть годин. Зрозуміло, що подібні зупинки приносять величезні збитки.

Злочинна практика диктує принципи роботи фахівця із захисту інформації. Все менше він займається фізичною безпекою (пропускним режимом, відеоспостереженням і т.д.) і все більше – мережевою і комп’ютерною. Існує принципова схема, за якою будується алгоритм роботи такого фахівця.

По-перше, він проводить інформаційне обстеження й аналіз. Це найважливіший етап, в результаті якого з’являється так звана “модель порушника”: хто, навіщо і як може порушувати безпеку. Щоб грамотно провести обстеження, професіонал повинен знати основні напрямки економічного і соціального розвитку галузі, перспективи, спеціалізацію й особливості установи, специфіку роботи конкурентів, деталі проходження інформації по підрозділах, знати кадрові проблеми і бути в курсі “підводних течій та каменів” у колективі.

На другому етапі розробляються внутрішні організаційно-правові документи, які максимально впорядковують інформаційні потоки. Зрозуміло, що тут необхідні додаткові знання: законодавства і права, основ організації, планування та управління установою, діловодства тощо.

Далі фахівець із захисту інформації керує роботою з закупівлі, встановлення та налаштування засобів і механізмів захисту. І тут йому не обійтися без серйозної підготовки в сфері інформаційних технологій та програмування, квантової і оптичної електроніки, радіоелектроніки, криптографічних методів захисту, безпеки життєдіяльності.

І, нарешті, на наступному етапі необхідно підтримувати, оновлювати, модернізувати створену систему безпеки. Найбільші банки, наприклад, змінюють програмне забезпечення, яке відповідає за захист, приблизно раз на півроку. У відділах, які займаються безпекою, працюють, як правило, найбільш досвідчені програмісти, які постійно проходять навчання, переатестацію та отримують додаткову кваліфікацію.

Попит на висококваліфікованих фахівців із захисту інформації зростає досить швидко. Якщо кілька років тому керівники багатьох невеликих фірм були спантеличені переважно фізичною безпекою, то з кожним роком збільшується потреба в технічно грамотних, всебічно підготовлених професіоналах у сфері комп’ютерного захисту.

Відповідно, збільшується конкурс на факультети, які випускають подібних фахівців, зростає заробітна плата (керівник відділу інформаційного захисту невеликої організації отримує в середньому близько \$ 2,5 тис.).

Для побудови найнадійнішої системи захисту необхідно виявити можливі загрози безпеці інформації, оцінити їх наслідки, визначити необхідні заходи і засоби захисту й оцінити при цьому їх ефективність, що вимагає великого професіоналізму, майстерності та часу.

При розробці складних автоматизованих систем захисту інформації збільшується кількість схемних, системотехнічних, структурних, алгоритмічних програмних помилок. На їх збільшення в процесі проектування впливає багато інших факторів: кваліфікація розробників, умови їх роботи, наявність досвіду та ін. До помилок людини як ланки системи потрібно відносити помилки людини як джерела інформації, людини-оператора, помилкові дії обслуговуючого персоналу та помилки людини, як ланки, яка приймає рішення. Помилки людини можуть ділитися на логічні (неправильно прийняте рішення), сенсорні (неправильне сприйняття оператором інформації) або моторні (неправильна реалізація рішення). Інтенсивність помилок людини може коливатися в широких межах: від 1-2% до 15-40% і вище від загальної кількості операцій, які виконуються при вирішенні задачі. Хоча людина як елемент системи має, порівняно з технічними засобами, свої переваги, їй водночас притаманний ряд недоліків, основними з яких є: стомлюваність, чутливість до змін навколишнього середовища, залежність якості роботи від фізичного стану, емоційність тощо.

Умисні загрози пов'язані з діями людини, причинами яких можуть бути певне невдоволення своєю життєвою ситуацією чи матеріальний інтерес або проста розвага з самоствердженням своїх здібностей, як у хакерів тощо. Слід зазначити, що вивчення мотивів поведінки порушника не є метою статті. Потенційні загрози з цього боку розглядаються тільки в технічному аспекті.

Для постановки більш конкретного завдання слід проаналізувати об'єкт захисту інформації на предмет введення-виведення, збереження та обробки інформації та можливостей порушника з доступу до інформації за відсутності засобів захисту в певній автоматизованій системі захисту.

Для таких систем в цьому випадку характерні такі штатні канали доступу до інформації:

- термінали користувачів;
- термінал адміністратора системи;
- термінал оператора функціонального контролю;
- засоби відображення інформації;
- засоби документування інформації;

- засоби завантаження програмного забезпечення в обчислювальний комплекс;
- носії інформації (ОЗУ, паперові носії);
- зовнішні канали зв'язку.

Очевидно, що за відсутності законного користувача, контролю і розмежування доступу до термінала кваліфікований порушник легко скористається його функціональними можливостями для несанкціонованого доступу до інформації шляхом введення відповідних запитів або команд. За наявності вільного доступу в приміщення можна візуально спостерігати інформацію на засобах відображення і документування, а на останніх – викрасти паперовий носій, зняти зайву копію, а також викрасти інші носії з інформацією.

Особливу небезпеку становить собою безконтрольне завантаження програмного забезпечення комп'ютера, в якому можуть бути змінені дані, алгоритми або “троянський кінь”, програма, яка виконує додаткові незаконні функції: запис інформації на сторонній носій, її передачу в канали зв'язку іншого абонента обчислювальної мережі, занесення в систему комп'ютерного вірусу тощо. За відсутності розмежування та контролю доступу до технологічної та оперативної інформації доступ до останньої можливий з терміналу функціонального контролю. Небезпечна ситуація, коли порушником є користувач системи, який за своїми функціональними обов'язками має законний доступ до однієї частини інформації, а звертається до іншої за межами своїх повноважень. З боку законного користувача існує багато способів порушити роботу обчислювальної системи, зловживати нею, витягати, модифікувати або знищувати інформацію. З цією метою можуть використовуватися привілейовані команди введення-виведення, відсутність контролю законності запиту і звернень до адрес пам'яті запам'ятовуючих пристроїв тощо. Під час технічного обслуговування (профілактики та ремонту) апаратури може бути виявлена залишкова інформація на магнітних та інших носіях. Стирання інформації звичайними методами при цьому не завжди ефективно. Створення системи контролю і розмежування доступу до інформації на програмному рівні не має сенсу, якщо не контролюється доступ до засобів управління комп'ютера, внутрішнього монтажу апаратури, кабельним з'єднанням.

Порушник може стати незаконним користувачем системи в режимі поділу часу, визначивши порядок роботи законного користувача або працюючи вслід за ним по тих самих лініях зв'язку. Він може також використовувати метод проб і помилок і реалізувати “діри” в операційній системі, прочитати паролі. Без знання паролів він може здійснити “селективне” включення в лінію зв'язку між терміналом і процесором комп'ютера і без переривання роботи законного користувача продовжити її

від його імені.

Процеси обробки, передачі та збереження інформації апаратними засобами автоматизованої системи захисту інформації забезпечуються спрацюванням логічних елементів, побудованих на базі напівпровідникових приладів, виконаних найбільш часто у вигляді інтегральних схем.

Необхідно скласти перелік об'єктів, які підлягають захисту, і суб'єктів, які задіяні в цьому інформаційному просторі і впливатимуть на інформаційний захист системи захисту інформації. При цьому необхідно не просто скласти перелік, а вказати особливості того чи іншого об'єкта, тобто стисло описати його з погляду інформаційної безпеки. Чим докладніше опис на початковому етапі, тим легше надалі випрацьовувати уточнення і будувати остаточну модель захисту інформації.

В и к о р и с т а н а л і т е р а т у р а :

1. <http://tolk.h1.ru/>
2. www.google.com.ua
3. www.nbu.gov.ua
4. www.osvita.org.ua/referat/bga/741-17k

ШЕВЧЕНКО В. В. *Системы защиты информации в условиях растущей интернет-преступности.*

В статье идет речь о влиянии интернет-технологий и методов на социально-экономический процесс информационного общества, в том числе на системы информационной защиты данных учреждения или организации в условиях растущей интернет-преступности.

Эффективное внедрение реализации различных средств, особенно информационно-коммуникационные средства, благоприятно влияют на всю систему защиты информации.

Ключевые слова: *информационные технологии, компьютеры, ИТ, информационная грамотность, защита систем и интернет-преступность.*

SHEVCHENKO V. V. *Information protection systems in conditions of increasing Internet-crime.*

In this article we are talking about the impact of Internet technology and its methods, the socio-economic process information society including the system information data protection agency or organization in conditions of increasing Internet - crime.

Effective implementation of various remedies and, especially information and communication tools, favorably affect the entire system of information protection.

Keywords: *information technology, computers, IT, information literacy, protection systems and Internet-crime.*