УДК 004.056

ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Іванов Володимир Георгийович

доктор технічних наук, професор,
Національний юридичний університет
імені Ярослава Мудрого,
Україна, м. Харків
e-mail: vladimir-ivanov33@rambler.ru
ORCID: 0000-0001-5619-2839

Анотація. *Запропоновано авторське визначення поняття «інформаційна безпека», розглянуто основні ознаки ефективного функціонування систем інформаційної безпеки. Наведено класифікацію видів загроз порушення інформаційної безпеки і надана їх коротка характеристика. Розглянуто методи захисту від цих загроз.*

Ключові слова: *інформаційна безпека, ефективні ознаки систем безпеки, класифікація загроз безпеки, методи захисту від загроз.*

В сучасному інформаційному суспільстві забезпечення інформаційної безпеки (Далі – ІБ) є перманентним і системним процесом. Саме з огляду на це потребує негайного рішення ряд завдань: наукових, науково-технологічних, політичних, економічних, культурологічних, а так же завдань правового забезпечення ІБ [2–4]. Інформаційна безпека є основною і невід'ємною складовою загальної політики національної безпеки України [1].

Враховуючи наведене, спробуємо надати визначення. Інформаційна безпека – це відсутність можливостей несанкціонованого доступу до інформації з метою її копіювання, поширення, використання, доповнення, знищення, модифікації, блокування, а так само негативного впливу інформації на індивідуальну і суспільну свідомість і психіку людей, тобто стан захищеності інформаційного середовища суспільства, що забезпечує

функціонування і розвиток цього середовища в інтересах громадян, організацій і держави.

Ознаками ефективного функціонування систем ІБ є масштабність і глибина, комплексність (поєднання технічних, правових і організаційних методів і засобів), а також адаптація до агресивного інформаційного середовища. Спробуємо розібратися із тим, за допомогою яких заходів можна покращити захист інформації. Так ІБ підвищується завдяки вжиттю таких технічних заходів: 1) створення апаратно - програмних комплексів захисту, їх постійне оновлення і модифікація, 2) застосування криптографічних засобів захисту інформації при її зберіганні, обробці та передачі, резервуванні особливо важливих комп'ютерних підсистем; захист інформації від витоку технічними каналами; 3) організація обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок; 4) використання конструкцій для захисту від розкрадань, саботажу, диверсій, вибухів; 5) установка резервних систем електроживлення, оснащення приміщень замками, сигналізацією тощо; 6) установка систем аутентифікації з використанням паролів, сертифікатів, методів біометрії і портретної ідентифікації, засобів контролю приміщень на основі систем відеоспостереження. Для надійності забезпечення ІБ стають у нагоді такі правові заходи, як: 1) розробка норм, що встановлюють відповідальність за комп'ютерні злочини; 2) захист авторських прав; 3) удосконалення кримінального й цивільного законодавства, а також судочинства; 4) ліцензування діяльності в галузі захисту інформації. Організаційними заходами є: 1) охорона обчислювального центру; 2) підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною; захист від атак методами соціальної інженерії; 3) наявність плану відновлення працездатності інформаційного центру після виходу його з ладу; 4) організація обслуговування обчислювального центру сторонньою організацією або особами, не зацікавленими в приховуванні фактів порушення роботи центру; правильний розподіл повноважень користувачів

тощо; 5) універсальність засобів захисту від усіх користувачів (у тому числі й вищого керівництва); 6) покладання відповідальності на осіб, які повинні забезпечити безпеку центру, регулярна зміна паролів і ключів, додержання строгого порядку їх зберігання, аналіз журналів реєстрації подій у системі.

Розглянувши заходи, яких вживає держава для захисту інформації, слід розібратися із тим, від чого останню треба захищати.

ОСНОВНІ ВИДИ ПОРУШЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Загроза віддаленого адміністрування. Під віддаленим адмініструванням слід розуміти несанкціоноване управління віддаленим комп'ютером, що дає змогу копіювати і модифікувати наявні на ньому дані, установлювати довільні програми, у тому числі й шкідливі, використовувати чужий комп'ютер для вчинення злочинних дій у мережі від імені його власника. Існує два способи реалізації таких загроз. Так перший передбачає встановлення на комп'ютер "жертви" програми, так званого аналога сервера, з якого зловмисник може створити віддалене з'єднання в той час, коли "жертва" знаходиться в мережі. Програми, що використовуються для цього, називаються троянськими. За своїми ознаками вони значною мірою нагадують комп'ютерні віруси. Другий метод віддаленого адміністрування заснований на використанні слабких місць (помилок), що є в програмному забезпеченні комп'ютерної системи – партнера по зв'язку. Мета цього методу – вийти за межі спілкування з клієнтської (серверної) програми і прямо впливати на операційну систему, щоб через неї одержати доступ до інших програм і даних. Програми, що спрямовані на експлуатацію уразливих місць комп'ютерних систем, називаються експлоітами.

Захист від троянських програм. Для ураження комп'ютера троянською програмою хтось повинний її запустити на цьому комп'ютері. Тому варто обмежити доступ сторонніх осіб до мережних комп'ютерів загальним адміністративним способом (фізичне обмеження доступу, пароль тощо). Звичайний метод установки троянських програм на сторонніх комп'ютерах пов'язаний із психологічним впливом на користувача, а саме

треба умовити користувача зробити це самостійно. Найчастіше використовуються розсилання шкідливих програм у вигляді додатків до повідомлень електронної пошти. У тексті повідомлення вказується, наскільки корисна і вигідна ця програма. Крім електронної пошти, зловмисники поширюють троянські програми через компакт-диски.

Захист від експлуатації помилок у програмному забезпеченні. Цей вид загроз майже небезпечний для клієнтської сторони. Атакам програм – експлоітів переважно піддаються сервери. Стратегія зловмисників реалізується в три етапи.

На першому етапі вони з'ясовують склад програм і устаткування в локальній мережі "жертви". На другому – розшукують інформацію про відомі помилки в даних програмах (про уразливості). На третьому – готують програми – експлоіти (чи використовують раніше підготовлені кимось програми) для експлуатації виявлених уразливостей. Боротьба з цими загрозами може відбуватися на всіх трьох етапах. Адміністрація серверів, насамперед, контролює звертання, мета яких полягає в з'ясуванні програмно-апаратної конфігурації сервера. Це дозволяє поставити порушника на облік задовго до того, як він здійснить реальну атаку.

У найбільш відповідальних випадках використовують спеціально виділені комп'ютери чи програми, що виконують функції міжмережних екранів. Такі засоби також називають брандмауерами. Брандмауер займає положення між комп'ютерами, що захищаються, і зовнішнім світом. Він не дозволяє переглядати ззовні склад програмного забезпечення на сервері і не пропускає несанкціоновані дані і команди. Також адміністрація сервера повинна уважно слідіть за публікаціями в мережі повідомлень про уразливість, виявлену у програмах.

Загроза активного змісту. Активний зміст – це активні об'єкти, вбудовані у веб-сторінки. На відміну від пасивного змісту (текстів, малюнків, аудіокліпів тощо) активні об'єкти містять у собі не тільки дані, а й програмний код, що одержує клієнт веб-сторінки, яка завантажується.

Агресивний програмний код, що потрапив у комп'ютер, здатний поводитися як комп'ютерний вірус чи як агентська програма. Так, він може як руйнувати дані, так і взаємодіяти з віддаленими програмами і таким чином працювати як засіб віддаленого доступу чи готувати ґрунт для його установки.

Захист від активного змісту. Сторона, що захищається, повинна оцінити загрозу для свого комп'ютера і, відповідно, налаштувати браузер так, щоб небезпека була мінімальною. Якщо такі цінні дані чи конфіденційні зведення на комп'ютері не зберігаються, захист можна відключити і переглядати веб-сторінки в тому вигляді, який передбачив їх розробник. Якщо загроза небажана, необхідно виконати налаштування захисту у програмі Internet Explorer у діалоговому вікні «*Параметры безопасности (Сервис/Свойства обозревателя/Безопасность/Другой)*».

Загроза перехоплення чи підміни даних на шляхах транспортування. Із проникненням Інтернету в економіку дуже гостро постала загроза перехоплення чи підміни даних на шляху транспортування. Так, розрахунки електронними платіжними засобами (картками платіжних систем) передбачають відправлення покупцем конфіденційних даних про свою картку продавцю. Якщо ці дані будуть перехоплені на одному з проміжних серверів, немає гарантії, що ними не скористається зловмисник. Крім того, через Інтернет передаються файли програм. Підміна цих файлів під час транспортування може призвести до серйозних негативних наслідків. Одночасно із захистом даних необхідно забезпечити посвідчення (ідентифікацію) партнерів по зв'язку і підтвердження (аутентифікацію) цілісності даних.

Засоби захисту даних на шляхах транспортування. Сьогодні в електронній комерції захищають і аутентифікують дані, а також ідентифікують віддалених партнерів за допомогою криптографічних методів, що технологічно реалізовані в електронному цифровому підписі.

Загроза втручання в особисте життя. В основі цієї загрози лежать комерційні інтереси рекламних організацій. Відвідуючи веб-

сторінки, ми бачимо майже на кожній рекламні оголошення (банери). При їх прийомі браузер установлює зв'язок з їх власником (рекламною системою) і непомітно для користувача реєструється в цій системі. Переходячи від однієї веб-сторінки до іншої, користувач створює свій психологічний портрет (він називається профілем). За характером відвідуваних веб-вузлів і веб-сторінок віддалена служба здатна визначити стать, вік, рівень освіти, рід занять, коло інтересів, рівень добробуту і навіть характер захворювань особи. Досить хоча б один раз зареєструватися десь під своїм ім'ям і прізвищем, і раніше зібрані абстрактні відомості набувають цілком конкретного змісту – так утворюються негласні персональні бази даних на учасників роботи в мережі Internet. Найбільш простим і очевидним джерелом для збору даних про активність клієнтів Internet є маркери "cookie", що працюють у такий спосіб.

Відповідно до протоколу HTTP браузер може відправити серверу запит на постачання одного веб-ресурсу (документа HTML) і ніяк при цьому серверу не представляється. Іноді доцільно, щоб браузер серверу представлявся. Це корисно для інтернет-магазинів. Сервер може передати браузеру невеликий пакет даних, у яких закодована інформація, потрібна серверу для ідентифікації браузера і налаштування на роботу з ним (доменне ім'я сервера і шлях доступу до веб-сторінки, для якої маркер був створений, а також час дії маркера). Цей пакет тимчасово запам'ятовується в оперативній пам'яті комп'ютера і виконує роль маркера (мітки). Якщо браузер знову звернувся до цього сервера, то він пред'являє йому раніше прийнятий маркер, і сервер відразу "розуміє", з яким клієнтом він має справу.

Маркери можуть бути тимчасовими і постійними. Тимчасовий маркер зберігається в оперативній пам'яті доти, поки браузер працює. По закінченні його роботи всі тимчасові маркери, отримані від серверів, знищуються. Однак сервери залишають не тільки тимчасові, а й постійні маркери. Коли браузер завершує роботу, всі постійні маркери, що накопичилися в оперативній пам'яті, переносяться на твердий диск у вигляді файлів "cookie". Так відбувається маркування жорсткого диска і комп'ютера клієнта. При

виході в Internet маркери зчитуються з жорсткого диска в оперативну пам’ять, звідки браузер пред’являє їх серверам, які їх поставили. Браузер також легально поставляє інформацію з протоколу HTTP: повідомляє свою назву, номер версії, тип операційної системи комп’ютера і URL-адресу веб-сторінки, яку клієнт відвідав останньою.

Фізичної загрози маркери “cookie” комп’ютеру не несуть, оскільки це файли даних, що не є програмним кодом. Однак вони вважаються загрозою через можливість втручання в особисте життя. Нелегальний збір інформації може здійснюватися завдяки тому, що сервер в змозі прочитати не тільки свої маркери, а й ті, які встановили інші сервери. Практика використання маркерів для збору зведень про користувачів Internet в даний час знаходиться під пильною увагою фахівців-правознавців. Сьогодні в деяких країнах розробляються обмеження на використання маркерів “cookie” у зв’язку з тим, що сервер повинний мати об’єктивні засоби ідентифікації правового статусу клієнта, перш ніж розміщати на його комп’ютері маркери.

Захист від втручання в особисте життя. Браузер Internet Explorer має спеціальні налаштування для відключення прийому маркерів “cookie” в діалоговому вікні «*Параметры безопасности»*. Найпростіше захистити папку C:\Windows\Cookies від запису. Час від часу видаляйте вміст папки.

Загроза соціальної інженерії. Це метод маніпуляції людьми або певною людиною (особистістю) з метою отримання від цих людей або конкретної людини доступу до конфіденційної інформації або розголошення цієї інформації. Метод базується на використанні слабких місць людини (людського чинника) і вважається дуже руйнівним. Уся техніка соціальної інженерії грунтується на особливостях ухвалення рішень людьми, що називаються когнітивним базисом. Для проведення своїх атак зловмисники часто експлуатують довірливість, лінь, заздрість, жадібність, люб'язність і навіть ентузіазм користувачів і співробітників організацій. У своєму традиційному вигляді атака на людину зазвичай зводиться до дзвінків по

телефону з метою отримання конфіденційної інформації (як правило, паролів) за допомогою видачі себе за іншу особу. Для захисту користувачів від соціальної інженерії застосовуються як технічні, так і антропогенні засоби. Найпростішими методами антропогенного захисту можна назвати привернення уваги людей до питань безпеки. До технічного захисту належать засоби, що заважають отримати інформацію, і засоби, що заважають скористатися отриманою інформацією.

Список використаної літератури

1. Горбулін В. П. Проблеми захисту інформаційного простору України : монографія / В. П. Горбулін, М. М. Биченок ; Ін-т проблем нац. безпеки. – Київ : Інтертехнологія, 2009. – 136 с.

2. Ліпкан Ю. Є. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / Ю. Є. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – Київ : КНТ, 2006. – 280 с.

3. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. / за заг. ред. В. Г. Іванова. – Харків : Право, 2010. – 208 с.

4. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – Киев : Изд-во Юниор, 2003. – 504 с.

Аннотация. *Предложено современное определение понятия «информационная безопасность» и рассмотрены основные признаки эффективного функционирования систем информационной безопасности. Дана классификация видов угроз нарушения информационной безопасности и их краткая характеристика. Рассмотрены методы защиты от этих угроз.*

Ключевые слова: *информационная безопасность, эффективные признаки систем безопасности, классификация угроз безопасности, методы защиты от угроз.*

Summary. *It is proposed the modern definition of information security concepts and describes the main features of the effective functioning of information security systems. The classification of types of threats to information security violations and their brief characteristics. The methods of protection against these*

threats.

Keywords*: information security, effective signs security systems, classification of security threats, methods of protection against threats.*