Міністерство освіти і науки України
Вищий приватний навчальний заклад
міжнародний економіко-гуманітарний
університет імені академіка Степана
Дем'янчука

А.В.Погребняк

ТЕХНОЛОГІЇ КОМП'ЮТЕРНОЇ БЕЗПЕКИ

КНИГА 3

Науковий керівник:
Р.М.Літнарович, доцент,к.т.н.

Рівне – 2011 р.

УДК 614.2 Погребняк А.В. Технології комп'ютерної безпеки. Монографія. МЕГУ, Рівне, 2011.-117 с. Pogrebnyak A.V. Technologies of computer safety. Monograph. IEGU, Rivne, 2011.-117 p.

Рецензенти: В.Г.Бурачек, доктор технічних наук, професор
Є.С. Парняков, доктор технічних наук, професор
В.О.Боровий , доктор технічних наук, професор
Відповідальний за випуск: Й.В. Джунь, доктор фізико-математичних наук, професор

Послідовно розглядаються основні поняття побудови сучасних технологій комп'ютерної безпеки. Монографія містить актуальний матеріал довідково-аналітичного характеру по наступних темах: основи безпеки даних в комп'ютерних системах, ідентифікація і аутентифікація користувачів, захист даних від несанкціонованого доступу, основи захисту даних від комп'ютерних вірусів, основи криптографії, криптографічні методи захисту інформації, стандарти захисту інформації.
Ключові слова: комп'ютерна безпека, інформаційна безпека, захист, інформація.

Последовательно рассматриваются основные понятия построения современных технологий компьютерной безопасности. Монография содержит актуальный материал справочно аналитического характера по следующим темам: основы безопасности данных в компьютерных системах, идентификация и аутентификация пользователей, защита данных от несанкционированного доступа, основы защиты данных от компьютерных вирусов, основы криптографии, криптографические методы защиты информации, стандарты защиты информации.
Ключевые слова: компьютерная безопасность, информационная безопасность, защита, информация.

The basic concepts of construction of modern technologies of computer safety are consistently examined. A monograph contains aktual material certificate analytical character on the followings themes: bases of safety of information in the computer systems, authentication and authentification of users, protection of data from an unauthorized division, bases of protection of data from computer viruses, bases of cryptography, cryptographic methods of priv, standards of priv.
Keywords: computer safety, informative safety, defence, information

Андрій Володимирович Погребняк,
спеціаліст системотехнік, магістрант
інформаційних технологій

Зміст

Вступ

Проблеми інформаційної безпеки України в сучасних умовах є надзвичайно актуальними і вимагають поглибленого вивчення. Ця робота здійснюється в межах вивчення загальних проблем національної безпеки.

Термін "безпека" розуміють як стан захищеності життєво важливих інтересів особи, суспільства, держави від внутрішніх та зовнішніх загроз. Але його зміст у науковому розумінні ще повною мірою не визначений. Сьогодні точиться дискусія навколо цього питання, зокрема навколо оцінки критеріїв безпеки, характеристик вірогідних небезпек та їх структури або принципів побудови системи забезпечення національної безпеки.

Водночас менеджери відчувають певний дефіцит у спеціальній літературі з питань правового висвітлення сучасних проблем інформаційного права. Незважаючи на вихід у світ окремих вдалих видань і наукових статей, висвітлені ці проблеми лише загалом. Крім того, у сучасній науковій і навчальній літературі нерідко "не завжди адекватно" відображені проблеми правового забезпечення інформаційних процесів або недостатньо фактичного матеріалу.

При аналізі проблем інформаційної безпеки у методологічному плані найбільш важливим є:

визначення та обґрунтування понятійного апарату;

налагодження структурно-функціональних зв'язків базових понять та розробка на цій основі відповідних нормативно-правових засад системи інформаційної безпеки;

удосконалення системи управління інформаційною безпекою на державному та місцевому рівнях;

визначення критеріїв ефективності функціонування системи інформаційної безпеки в різних сферах життя та діяльності суспільства (політичній, економічній, науки і техніки, духовній тощо).

Актуальність теми. Загалом система інформаційної безпеки має відбивати стан захищеності національних інтересів саме в інформаційній сфері від зовнішніх та внутрішніх загроз як для самої держави або суспільства, так і для конкретної людини.

Система інформаційної безпеки є одночасно й елементом у системі вищого рівня — міжнародного, національного, місцевого. Але сьогодні низка підсистем, які входять до цієї макросистеми, ще не вивчені на належному рівні, а також не мають комплексного, системного дослідження з виходом на сучасні конструкції та пропозиції. Це стосується проблем інформаційної безпеки в Україні.

Вивчення науково-теоретичних та практичних проблем інформаційної безпеки дозволить визначити та розв'язати завдання щодо створення системи інформаційної безпеки, які б функціонували ефективно.

Мета даної роботиполягає у визначенні заходів забезпечення інформаційної безпеки у політичній, економічній, наукці і техніці, правоохоронній сферах тощо.

Головним завданням автор ставить визначення національних інтересів у інформаційній сфері, виявлення загроз таким інтересам, їхню класифікацію, пошук та надання оптимальних засобів, які дозволяють забезпечити створення стійкої системи інформаційної безпеки в Україні.

За об'єкт дослідження взято систему інформаційної безпеки як підсистему в системі національної безпеки; сукупність

явищ, процесів, правовідносин, захист яких є метою та головним змістом діяльності державних інститутів. А предметом дослідження є характеристика елементів, критеріїв та заходів забезпечення системи інформаційної безпеки.

Під час дослідження з огляду на мету і сформульоване завдання, а також об'єкт та предмет дослідження, використовувалися загальнонаукові та спеціальні методи пізнання: метод дедукції, індукції, емпіричний, комплексний, порівняльний тощо.

1. ІНФОРМАЦІЙНА БЕЗПЕКА

1.1. Визначення інформаційної безпеки

Поняття інформаційної безпеки, залежно від його використання, розглядається у декількох ракурсах.

У найзагальнішому випадку інформаційна безпека — це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Під інформаційним середовищем [information environment] розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні предметні частини:
створення і розповсюдження вихідної та похідної

інформації;
формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;
споживання інформації;

та дві забезпечувальні предметні частини:
створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;
створення і застосування засобів і механізмів інформаційної безпеки.

Більш розгорнуте формулювання інформаційної безпеки — це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок — обґрунтованість рішень та дій, що приймаються.

В залежності від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати наступним чином
як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;
інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
інформаційних прав і свобод людини і громадянина.

В інформаційному праві інформаційна безпека — це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво

важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

1.2.Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері

Відповідно до усталених поглядів, інтереси особистості в інформаційній сфері полягають:
в реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку;
у захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають:
у забезпеченні інтересів особистості в цій сфері;
у зміцненні демократії;
у створення правової соціальної держави;
у досягненні та підтриманні суспільного спокою;
у духовному відновленні держави.

Інтереси держави в інформаційній сфері полягають у створенні умов:
для гармонійного розвитку державної інформаційної інфраструктури;
для реалізації конституційних прав і свобод людини та громадянина в галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

1.3.Види, об'єкти та суб'єкти інформаційної безпеки

Об'єктами інформаційної безпеки [information security object] можуть бути: свідомість, психіка людей; інформаційні системи різного масштабу і різного призначення. До соціальних об'єктів інформаційної безпеки звичайно відносять особистість, колектив, суспільство, державу, світове товариство.

До суб'єктів інформаційної безпеки [information security subject] відносяться:
держава, що здійснює свої функції через відповідні органи;
громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства.

Інформаційна безпека особистості — це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ і т. ін.

Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи і т. ін.) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси і т. ін.) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Концепція інформаційної безпеки держави — це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення.

В концепції інформаційної безпеки держави:
проводиться системна класифікація дестабілізуючих факторів і інформаційних загроз безпеці особистості,

суспільства і держави;
обґрунтовуються основні положення з організації забезпечення інформаційної безпеки держави;
розробляються пропозиції по способах і формах забезпечення інформаційної безпеки.

1.4.Дестабілізуючі фактори інформаційної безпеки

Дестабілізуючі фактори [destabilizing factor] — явища та процеси природного і штучного походження, що породжують інформаційні загрози.

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їхні об'єднання. До найбільш сильних із них відносяться ворожі держави або коаліції ворожих держав, в яких для формування інформаційних загроз створюються і функціонують спеціальні органи і служби.

Особливу групу джерел складають інформаційні системи і засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей і інших причин.

Джерелом дестабілізуючих факторів може бути також природне середовище. Кожному джерелу властиві певні види дестабілізуючих факторів, які можна представити двома групами: міждержавні дестабілізуючі фактори і внутрішньодержавні дестабілізуючі фактори.

Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них

відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації, а також фабрикування, розповсюдження і впровадження дезінформації.

До внутрішньодержавних дестабілізуючих факторів відносять:
правовий вакуум у більшості питань забезпечення інформаційної безпеки;
навмисне або ненавмисне порушення законодавства з питань інформаційної безпеки;
політичні конфлікти;
зловмисні дії злочинних елементів або груп;
відмови, збої, технічні помилки інформаційних систем (засобів);
природні явища (процеси), що ускладнюють одержання, передачу, прийом і зберігання інформації або руйнують інформаційні системи.

Міждержавні дестабілізуючі фактори — це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії і т. ін.)

1.5 Класифікація загроз інформаційній безпеці

Загрози інформаційній безпеці [information security threat] — сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи:
загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи

їхнього формування і використання);
загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т. ін.).

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні .

Під політичними факторами загроз інформаційній безпеці розуміють:
зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;
інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;
становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;
знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;
порушення інформаційних зв'язків унаслідок утворення на території колишнього СРСР нових держав;
прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;
низька загальна правова та інформаційна культура сторін.

Основними економічними факторами загроз безпеці

інформації є:
перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур — виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;
критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;
розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:
недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;
недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;
широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;
зростання обсягів інформації, яка передається відкритими каналами зв'язку;
загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

Ієрархічна класифікація загроз інформаційній безпеці.

Глобальні фактори загроз інформаційній безпеці:
недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації, розповсюдження інформації та нових інформаційних технологій;

діяльність іноземних розвідувальних та спеціальних служб;
діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави;
злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:
використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації;
невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;
відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій;
недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;
розвиток зарубіжних технічних засобів розвідки, та промислового шпигунства, що дозволяє одержати несанкціонований доступ до конфіденційної інформації, у тому числі такої що складає державну таємницю;
зростання злочинності в інформаційній сфері;
використання старих методів та засобів захисту національних інформаційних мереж, широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку;
відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці:
перехоплення електронних випромінювань;
застосування підслуховуючих пристроїв або закладок;
дистанційне фотографування;

розкрадання носіїв інформації та промислових відходів;
копіювання носіїв інформації з подоланням заходів захисту;
незаконне приєднання до апаратури та ліній зв'язку;
упровадження та використання комп'ютерних вірусів і т. ін..

1.6 **Джерела загроз інформаційній безпеці**

Виходячи з визначення загроз інформаційній безпеці, можна виділити декілька основних джерел загроз, які можуть торкатися інтересів особистості, суспільства і держави.

Джерела загроз інформаційній безпеці особистості

Інтереси особистості, які необхідно охороняти в інформаційному суспільстві, полягають насамперед у реальному забезпеченні конституційних прав і свобод людини і громадянина на доступ до відкритої інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, а також у захисту інформації, що забезпечує особисту безпеку, духовний та інтелектуальний розвиток.

Найбільш небезпечним джерелом загроз цим інтересам вважається суттєве розширення можливості маніпулювання свідомістю людини за рахунок формування навкруг неї індивідуального "віртуального інформаційного простору", а також можливість використання технологій впливу на її психічну діяльність.

Важливою особливістю способу життя людини в інформаційному суспільстві є суттєве скорочення "інформаційних" відстаней (часу доступу до необхідної інформації), що веде до появи нових можливостей — як з

формування особистості, та і з реалізації її потенціалу. Людство впритул підходить до рубежів, за якими інформаційна інфраструктура стає, по суті, основним джерелом інформації для людини, здійснює безпосередній вплив на її психічну діяльність, на формування її соціальної поведінки.

Проблема формування розумових потреб і мотивації соціальної поведінки поки не має загального вирішення навіть для індустріального суспільства і ще більше ускладнюється стосовно інформаційного суспільства. Вона є однією з найбільш складних у сучасній психологічній науці.

В цілому структура споживчо-мотиваційної сфери особистості утворюється базовими потребами, зумовленими його генотипом (у їжі, особистій безпеці, потреба у продовження роду, довголітті, а також потребами у спілкуванні з іншими людьми), похідними потребами, що формуються діючою системою виховання. Способи і форми задоволення цих потреб у значній мірі залежать від інформації і знань, що одержуються з навколишнього світу і, зокрема, надходять через інформаційну інфраструктуру. Спрямованість використання одержаної інформації і результати, що одержуються, визначаються, насамперед, особою людини та її духовним потенціалом.

Складність процедур, що реалізуються в сучасних технологіях доступу до необхідних інформаційних ресурсів, критично збільшують залежність окремої людини від інших людей, які здійснюють розробку інформаційних технологій, визначення алгоритмів пошуку необхідної інформації, її попередньої обробки, приведення до виду, зручного для сприйняття, доведення до споживача. По суті, ці люди формують для людини інформаційний фон його життя, визначають умови, в яких він живе і діє, вирішує свої

життєві проблеми. Саме тому вважається виключно важливим забезпечити безпеку взаємодії людини з інформаційною структурою.

Іншим небезпечним джерелом загроз інтересам особистості є використання на шкоду її інтересам персональних даних, що нагромаджуються різноманітними структурами, в тому числі органами державної влади, а також розширення можливості прихованого збирання інформації, що складає його особисту і сімейну таємницю, відомості про її приватне життя.

Це зумовлено, у першу чергу, труднощами реалізації механізмів охорони цих відомостей, подальшими досягненнями у мікромініатюризації засобів прихованого збирання і передавання інформації.

Інтереси суспільства, що вступило у стадію постіндустріального розвитку, полягають у захисті життєво важливих інтересів у цій сфері, забезпечення реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення демократії, досягнення і підтримування суспільної злагоди, підвищення творчої активності населення.

Одним із джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж зв'язку критично важливих інфраструктур забезпечення життя суспільства.

Ці загрози можуть проявлятися і вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов техніки і програмного забезпечення, шкідливого впливу зі сторони злочинних структур і кримінальних елементів. Об'єктами реалізації таких структур можуть виступати системи енергетичної, транспортної, трубопровідної і деяких інших інфраструктур.

Небезпечним джерелом загроз виступає можливість концентрації засобів масової інформації (ЗМІ) в руках невеликої групи власників.

Ці загрози можуть проявлятися у вигляді маніпуляції суспільною думкою по відношенню до тих чи інших суспільно значимих подій, а також руйнування моральних устоїв суспільства шляхом нав'язування чужорідних цінностей.

Нарешті, небезпечним джерелом загроз є розширення масштабів вітчизняної і міжнародної комп'ютерної злочинності.

Ці загрози можуть проявлятися у вигляді спроб здійснення шахрайських операції з використанням глобальних або вітчизняних інформаційно-телекомунікаційних систем, відмивання фінансових коштів, одержаних протиправним шляхом, одержання неправомірного доступу до фінансової, банківської та іншої інформації, яка може бути використаною з корисливою метою.

Джерела загроз інформаційній безпеці держави

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства.

У першу чергу загрози інтересам держави також можуть проявлятися у вигляді отримання протиправного доступу до

відомостей, що складають державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки державі.

Проте найбільш небезпечними джерелами загроз інтересам держави в інформаційному суспільстві може стати неконтрольоване розповсюдження інформаційної зброї та розгортання гонки озброєнь у цій галузі, спроби реалізації концепції ведення інформаційних війн.

Поняття інформаційної зброї визначається як сукупність засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційну сферу протилежної сторони з метою руйнування її інформаційної інфраструктури, системи управління державою, зниження духовного потенціалу суспільства.

Серед найбільш серйозних завдань, які можуть вирішуватися за допомогою сучасної інформаційної зброї, можна виділити наступні:

створення атмосфери бездуховності та аморальності, негативного відношення до культурної спадщини противника;

маніпулювання суспільною свідомістю та політичною орієнтацією соціальних груп населення держави з метою створення політичної напруги та хаосу;

дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємного знищення;

зниження інформаційного забезпечення влади та управління, інспірація помилкових управлінських рішень;

дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

провокування соціальних, політичних, національних і релігійних сутичок;

ініціювання страйків, масових заворушень та інших акцій економічного протесту;

ускладнення прийняття органами важливих рішень;

підрив міжнародного авторитету держави, її співробітництва з іншими країнами;

нанесення втрат життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

Руйнівний вплив інформаційної зброї в інформаційному суспільстві може бути більш потужним та ефективним, ніж це уявляється зараз. Це є особливо небезпечним в умовах існування майже монопольного положення компаній невеликої кількості країн на ринку інформаційних продуктів, оскільки це здатне спровокувати бажання використати наявну перевагу для досягнення тієї чи іншої політичної мети.

1.7 .Основні принципи забезпечення захисту інформації

Забезпечення інформаційної безпеки — це сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації.

Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації і об'єднання, що мають відповідні повноваження, — у відповідності із законодавством. В основу забезпечення інформаційної безпеки держави повинні бути покладені наступні принципи:

законність, дотримання балансу інтересів особистості, суспільства і держави;

взаємна відповідальність суб'єктів забезпечення інформаційної безпеки;

інтеграція систем національної і міжнародної безпеки.

Специфічними принципами забезпечення інформаційної безпеки є:
превентивний характер проведення її заходів по відношенню до заходів інших видів безпеки;
адекватна інформованість об'єктів безпеки, в тому числі і міжнародних.

Превентивність (лат. praeventio від praevenio — "попереджую") зумовлена властивою людині послідовністю виконання операцій, що складає будь-яку елементарну дію. Усе починається з приймання (добування) інформації, а закінчується активною дією: реакцією на одержану інформацію. Оскільки це справедливо по відношенню до будь-якого виду діяльності, то можна стверджувати, що даний принцип є загальним, і його дія розповсюджується на всі сфери безпеки особистості, суспільства та держави.

Адекватна інформованість об'єктів безпеки означає, що всі вони мають право володіти інформацією про явища і процеси, що їх цікавлять, яке обмежене тільки законодавчо з метою охорони особистої, сімейної, професійної, комерційної та державної таємниці, а також моралі]

Права та свободи суспільства в питаннях пошуку, володіння та розповсюдження інформації повинні регулюватися законодавчими актами, які видаються, щодо специфіки діяльності суспільних об'єднань та організацій або змісту інформації. Наприклад, адекватна інформованість суспільства про його матеріальні цінності досягається у сфері нормотворчості та право-застосування законодавства про захист комерційної таємниці. Права та свободи суспільства в духовній сфері повинні захищати законодавчі акти, які визначають порядок освіти та функціонування освітніх, просвітницьких, культурних, релігійних організацій, а також засобів масової інформації.

В основі прав і свобод держави у сфері її інформованості з питань світової політики, економіки, науки, ресурсів, екології, оборони і т.ін. лежать діючі норми та принципи міждержавного права. Головним слід вважати принцип рівної безпеки. Стосовно до інформаційної сфери можна говорити про його трансформацію в принцип адекватної інформованості держав світового співтовариства, який передбачає право кожної держави на інформаційну безпеку, забезпечення інформаційної безпеки усіх членів співтовариства в рівній мірі, врахування інтересів усіх сторін без будь-якої дискримінації, виключення односторонніх переваг, відмова від дій, що наносять шкоду іншій державі.

Законодавча база, яка визначає перелік відомостей, що віднесені до державної таємниці, механізм та порядок її захисту повинні розроблюватися, виходячи із наведеного принципу, а також багатосторонніх угод держав, які входять до міжнародної системи інформаційної безпеки. Формування останньої буде, очевидно, справою далекої перспективи, яка ознаменує собою вищий рівень прояву довіри та зацікавленості держав світового співтовариства в забезпеченні виконання на практиці принципу адекватної інформованості. Така система повинна стати підсистемою у системі колективної безпеки.

1.8.Система забезпечення інформаційної безпеки держави

Державна система забезпечення інформаційної безпеки країни [government system of national information security] являє собою організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави в правовій державі. Основними

завданнями такої системи є:
виявлення і прогнозування дестабілізуючих факторів і інформацій них загроз життєво важливим інтересам особистості, суспільства та держави;
здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;
створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки.

На теперішній час окремі елементи системи інформаційної безпеки створені та функціонують (органи зовнішньої розвідки, інформаційні служби різноманітних міністерств, система технічного та криптографічного захисту інформації держави і т. н.). Проте для їхнього функціонування ще недостатня правова база. Зміст діяльності органів інформаційної безпеки також ще не в повній мірі відповідає покладеним на них завданням. Це пояснюється в першу чергу недостатнім опрацюванням питань, що стосуються форм і способів забезпечення інформаційної безпеки.

1.9. Основні форми і способи забезпечення інформаційної безпеки держави

Форми і способи забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави. Тому необхідне чітке юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки.

Найважливіша вимога до обґрунтування способів, форм і механізмів їхньої реалізації полягає в абсолютному верховенстві права у будь-якій, в тому числі і політичній діяльності. У свою чергу, кожний суб'єкт інформаційного процесу повинен мати відповідну правову свідомість, бути законослухняним, добре уявляти наслідки свої дій для інших суб'єктів та міру відповідальності на випадок порушення їхніх життєво важливих інтересів. Це є принциповим, оскільки застосування тих чи інших форм і способів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу. У першому випадку забезпечення інформаційної безпеки здійснюється відповідно у формах інформаційного патронату та інформаційної кооперації, у другому — у формі інформаційного протиборства .

Інформаційний патронат [information patronage] (лат. patronatys від patronys — "захисник") — форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) і власне захист життєво важливих інтересів цих осіб від інформаційних загроз або, як ще кажуть, — інформаційний захист.

При цьому інформаційне забезпечення інформаційної безпеки [information support of information security] включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхню обробку, обмін інформацією між органами керування і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контррозвідува-льної, оперативно-

розшукової і оперативно-інформаційної діяльності.

Інформаційний захист [infosecurity] досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки.

Інформаційна кооперація [information cooperation] (лат. cooperatio, від coopero — "співробітничаю") — форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі і інформаційні загрози та захист від них доступними законними способами і засобами.

Для конкретної особистості такими способами і засобами можуть бути:
судовий захист прав і свобод у використанні інформації;
адміністративний захист її життєво важливих інтересів у інформованості з боку територіальних або відомчих органів інформаційної безпеки;
автономний захист своїх прав і свобод в основному із застосуванням технічних засобів захисту, особистої, сімейної і професійної таємниці.

Це ж характерно і для суспільних об'єднань, організацій (підприємств). Разом із тим, при наявності у них власних органів інформаційної безпеки, їхні можливості у сфері автономного захисту суттєво розширюються[15, с. 220-225].
Висновки

Отже, державна політика забезпечення інформаційної безпеки України визначає головні напрями діяльності органів державної влади України, закріплює права та

обов'язки щодо захисту інтересів України і ґрунтуються на дотриманні балансу інтересів особи, суспільства і держави в інформаційній сфері.

1. Державна політика забезпечення інформаційної безпеки України ґрунтується на таких принципах:
дотримання Конституції України, законодавства України, загальновизнаних принципів і норм міжнародного права при здійсненні діяльності із забезпечення інформаційної безпеки України;
відкритості у реалізації функцій органів державної влади України і суспільних об'єднань, що передбачає інформування суспільства про їхню діяльність з огляду на обмеження, встановлені законодавством України;
правової рівноправності всіх учасників процесу інформаційної взаємодії незалежно від їхнього політичного, соціального та економічного статусу, що ґрунтується на конституційному праві громадян на вільний пошук, одержання, передачу, виробництво і розповсюдження інформації будь-яким законним способом;
пріоритетного розвитку вітчизняних сучасних інформаційних і телекомунікаційних технологій, виробництво технічних і програмних засобів, здатних забезпечити вдосконалення національних телекомунікаційних мереж, підключення їх до глобальних інформаційних мереж з метою забезпечення інтересів України.

2. Вдосконалення правових механізмів регулювання суспільних відносин, що виникають в інформаційній сфері, є пріоритетним напрямом державної політики у сфері забезпечення інформаційної безпеки України, передбачає:
оцінку ефективності застосування чинних законодавчих та інших нормативних правових актів в інформаційній сфері й вироблення програми їх удосконалення;
створення організаційно-правових механізмів забезпечення

інформаційної безпеки;

визначення правового статусу всіх суб'єктів відносин в інформаційній сфері, в т.ч. користувачів інформаційних і телекомунікаційних систем, та встановлення їхньої відповідальності за дотримання законодавства України в даній сфері;

створення системи збору й аналізу даних про джерела загроз інформаційній безпеці України, а також про наслідки їх здійснення;

розробку нормативних правових актів, що обумовлюють організацію наслідків і процедуру судового розгляду по фактах протиправних дій в інформаційній сфері, а також порядок ліквідації наслідків цих протиправних дій;

подальше вдосконалення фабул складів правопорушень і злочинів;

вдосконалення системи підготовки кадрів, використовуваних у галузі забезпечення інформаційної безпеки України.

3. Правове забезпечення інформаційної безпеки України має ґрунтуватися насамперед на дотриманні принципів законності, балансу інтересів громадян, суспільства і держави в інформаційній сфері:

дотримання принципу законності вимагає від органів державної влади України при вирішенні конфліктів, що виникають в інформаційній сфері, неухильно керуватися законодавчими та іншими нормативно-правовими актами, що регулюють відносини у цій сфері;

дотримання принципу балансу інтересів громадян, суспільства і держави в інформаційній сфері передбачає законодавче закріплення пріоритету цих інтересів у різних галузях життя та діяльності суспільства, а також використання форм суспільного контролю діяльності органів державної влади України. Реалізація гарантій конституційних прав і свобод людини і громадянина, що стосується діяльності в інформаційній сфері, є

найважливішим завданням держави в галузі інформаційної безпеки.

2.БОРОТЬБА З КОМП'ЮТЕРНИМИ ЗЛОЧИНАМИ

З того часу коли у 1988 році вірус-черв'як (Morris Worm) паралізував половину комп'ютерів, що працювали у мережі Internet , Internet залишається не тільки засобом передачі інформації в науковій, оборонній та інших сферах, але й став глобальною електронною мережею, яка порушує усі аспекти нашого життя як дома, так і на роботі.

Стрімкий розвиток інформаційних технологій, розширення виробництва технічних засобів і сфери застосування комп'ютерної техніки, а головне - наявність людського фактора у виді задоволення власних амбіцій чи з корисливою метою породили новий вид суспільно небезпечних діянь, у яких неправомірно використовується комп'ютерна інформація або вона сама стає об'єктом зазіхання. Подібно багатьом революційним технологіям глобальна мережа Internet несе із собою величезний потенціал як для прогресу так і для зловживань.

Як стало відомо, терористичний акт у США, який 11 вересня 2001р. зруйнував обидва 110-поверхових хмарочоси Всесвітнього торгового центру у Нью-Йорку, супроводжувався вчиненням комп'ютерного злочину. За повідомленням телекомпанії CNN, терористична атака проти США стала можливою завдяки виведенню з ладу супутникової системи NASA. Таким чином, терористична

група, що підготувала масовану атаку на США, мала у своєму розпорядженні не тільки висококласних камікадзе, але і хакерів найвищої кваліфікації.

Атаки у мережі, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, корпоративне шпигунство та поширення дитячої порнографії - ось тільки деякі зі злочинів, що вчиняються у мережі Internet. Такі протиправні діяння, вже сьогодні складають для нашої держави, як і для багатьох інших країн світу, певну суспільну небезпеку, реально загрожуючи інформаційній безпеці – складовій національної безпеки. Національна інфраструктура держави вже сьогодні щільно пов'язана з використанням сучасних комп'ютерних технологій. Щоденна діяльність банківських та енергетичних систем, керування повітряним рухом, транспортна мережа, навіть швидка медична допомога перебувають у повній залежності від надійної і безпечної роботи автоматизованих електронно-обчислювальних систем.

Не треба бути пророком, щоб прогнозувати подальше зростання залежності життєдіяльності національної інфраструктури від процесів інформатизації та входження України в єдиний інформаційний простір, поширення криміногенних процесів, пов'язаних з протиправним використанням комп'ютерних технологій.

Кіберзлочинність - це явище міжнародного значення, рівень якої знаходиться у прямій залежності від рівня розвитку та впровадження сучасних комп'ютерних технологій, мереж їх загального користування та доступу до них. Таким чином, стрімкий розвиток інформатизації в Україні несе за собою потенційну можливість використання комп'ютерних технологій з корисливих та інших мотивів, що певною мірою ставить під загрозу національну безпеку

держави.

Всебічний аналіз вітчизняного законодавства, яке регулює суспільні інформаційні відносини в Україні, дозволяє стверджувати, що наша держава, поряд із заходами стимулювання розвитку інфраструктури на основі новітніх технологій, вживає необхідні заходи щодо протидії комп'ютерної злочинності. Прикладом цьому може служити Указ Президента від 31 липня 2000 року Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в України , а також Розділ 16. "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж" прийнятого нещодавно нового Кримінального кодексу України .

Разом з тим, є ще багато не врегульованих проблем, які не дають можливості ефективно протидіяти правопорушенням, що вчиняються у сфері використання комп'ютерних технологій.

Вітчизняна та світова практика свідчить, що число клієнтів Internet продовжує бурхливо зростати, а разом з цим зростає і кількість атак, яких щодня зазнають комп'ютерні системи із зовнішнього середовища. За статистикою Американського Інституту Комп'ютерної Безпеки (Computer Security Institute) збитки від злочинів, що вчиняються за допомогою комп'ютерних технологій, з кожним роком зростають. Так сукупний збиток від таких злочинів у США за 5 років з 1997 р. по 2001 р. склав вже біліше 1 млрд. дол. США. За даними експертів тільки у 2000 році втрати комерційних структур через Internet склали понад 1,6 трильйони доларів .

Основною метою кіберзлочинця є комп'ютерна система, яка керує різноманітними процесами, і інформація, що

циркулює в них. На відміну від звичайного злочинця, що діє в реальному світі, кіберзлочинець не використовує традиційну зброю - ніж і пістолет Його арсенал – інформаційна зброя, всі інструменти, що використовуються для проникнення у мережі, злому і модифікації програмного забезпечення, несанкціонованого одержання інформації або блокування роботи комп'ютерних систем. До зброї кіберзлочинця можна додати: комп'ютерні віруси, програмні закладки, різноманітні види віддалених атак, що дозволяють отримати несанкціонований доступ до комп'ютерної системи. У арсеналі сучасних комп'ютерних злочинців не лише традиційні засоби, а й найсучасніша інформаційна зброя та обладнання, яке дає можливість вчиняти злочини проти любої країни світу, тому ця проблема вже давно перетнула кордони держав і стала проблемою міжнародного масштабу.

Разом з поширенням впровадження сучасних інформаційних технологій в Україні постійно зростає загроза як для державних комп'ютерних систем, так і для приватних організацій та окремих громадян. Особливої актуальності проблема кіберзлочинності набула в наш час. Соціологічні опитування в різних країнах, і насамперед, у високорозвинених, показують, що кіберзлочинність посідає одне з чільних місць серед тих проблем, які турбують людей. Більше того, на думку фахівців, сьогодні це явище становить значно серйознішу небезпеку ніж 5 років тому в силу використання зі злочинною метою новітніх інформаційних технологій, а також зростаючої уразливості сучасного індустріального суспільства. Незважаючи на зусилля держав, які спрямовані на боротьбу з кіберзлочинами, їх кількість у світі не зменшується, а, навпаки, постійно зростає

Жодна держава сьогодні не здатна протистояти цьому злу самостійно. Нагальною є потреба активізації міжнародного

співробітництва у цій сфері. Вагоме місце у такому співробітництві належить, безумовно, міжнародно-правовим механізмам регулювання. Але, зважаючи на те, що в сучасних умовах значна частка засобів боротьби з кіберзлочинами, як і з іншими злочинами міжнародного характеру, належить до внутрішньої компетенції кожної окремої держави, необхідно паралельно розвивати й національне законодавство спрямоване на боротьбу з комп'ютерними злочинами, узгоджуючи його з нормами міжнародного права та спираючись на існуючий світовий позитивний досвід.

Відсутність ефективних механізмів боротьби з кіберзлочинами визначається сьогодні як одна із загроз національній безпеці нашої держави. За таких обставин Україна, як незалежна демократична держава, не може стояти осторонь від проблем протидії комп'ютерної злочинності і, зокрема, його транснаціональних форм.

Зараз триває процес реформування правової системи України. Саме цим, у першу чергу, обумовлюється актуальність питань, які розглядаються у цій статті, оскільки аналіз основних проблем боротьби з кіберзлочинами сприятиме формуванню та реалізації на практиці концепції нового Українського інформаційного законодавства, а також розробки та впровадженню термінових, ефективних заходів протидії негативним процесам інформатизації, пов'язаних з комп'ютерною злочинністю.

Розглянемо типові категорії кіберзлочинів та ті негативні наслідки, з якими суспільство зіткнулося вже сьогодні.

Інсайдери (Insiders) - особи, що мають доступ до внутрішньої інформації. Вони частіше всього настроєні

негативно проти своїх роботодавців, інсайдер (працюючий або звільнений співробітник компанії) є потенційним злочинцем. Адже співробітник знайомий із тонкощами комп'ютерної системи компанії, що дозволяє йому одержати необмежений доступ з метою пошкодження системи, або з метою незаконного заволодіння інформацією, яка є власністю компанії.

Як приклад можна привести випадок, коли Національна бібліотека медичної літератури (National Library of Medicine – NLM) у США, до якої звертаються сотні тисяч практикуючих лікарів і спеціалістів в області медицини з усього світу для одержання самої свіжої інформації про захворювання, лікування, медикаменти і дозування, піддалася нападу з боку інсайдера. Інсайдер виконав несанкціонований доступ до головної системи захисту інформації, завантаживши сотні файлів, включаючи файли першорядної важливості, що відносилися до категорії "швидка допомога", і файли програмного забезпечення, що забезпечували безперебійну роботу системи. Ці порушення призвели до значних негативних наслідків у роботі цілої системи та збитків у розмірі 25 тис. доларів. Розслідування, проведено ФБР США, встановило особу злочинця, якою виявився Монтгомері Джон Грей (Montgomery Johns Gray), який був програмістом NLM і чий доступ у комп'ютерну систему був анульований компанією після його звільнення. Він вчинив злом через "чорний вхід", який він створив у програмному коді. Йому було пред'явлено ордер на обшук його комп'ютера, і за загрозу суспільній безпеці він був заарештований ФБР.

Хакери (Hackers) також складають велику небезпеку. Іноді вони зламують мережі просто заради гострих відчуттів або заради завоювання авторитету в хакерських колах. Але не рідко, вони зламують системи і з метою фінансової наживи та інших злодіянь. Як правило, хакери –

прекрасні знавці інформаційної техніки, які мають неординарні здібності, тому їм не складно маніпулювати комп'ютерними системами на відстані: вони несанкціоновано перекачують тексти і протоколи з World Wide Web на сайти комп'ютера жертви. Злочини, при яких відбувається блокування обслуговування (DDOS атака), – ще один доказ того, що економічний саботаж цілком можливий при використанні належних та доступних програмних інструментів у мережі Internet.

Останнім часом спостерігається зростання політично мотивованих атак на вебсайти і сервери електронної пошти, котрі за прийомами виконання дублюють "хакерство". У таких випадках група або окремі суб'єкти перенавантажують сервери електронної пошти, або стирають вебсайти для передачі політичних повідомлень. Хоч такі види порушень не призводять до пошкодження операційних систем або мережі, проте вони стають причиною збоїв роботи електронної пошти, що призводить до великих грошових витрат та блокування доступу абонентів до вебсайтів, на яких знаходиться цінна інформація. Так у 1996 році, був вчинений несанкціонований доступ до комп'ютерної системи вебсайту Міністерства юстиції США. Зловмисники знищили зміст більш 200 каталогів та розмістили сторінки з зображенням Адольфа Гітлера, свастику, сцени порнографічного характеру, тощо.

Творці вірусних програм (Virus Writers). Ще одним видом комп'ютерної злочинності є протиправне пошкодження комп'ютерної системи або мережі з метою порушення функціонування комп'ютерів або глобальних телекомунікаційних систем за допомогою вірусів. Творці таких програм складають на сьогоднішній день серйозну загрозу для користувачів. Існує дуже багато комп'ютерних вірусів таких як, наприклад, Melissa Macro Virus,

Explore.Zip Worm, CIH (Chernobyl) Virus та ін. Не так давно на одній із Українських атомних станцій вірус знищив базу данник енергетичних потужностей АЕС. Аварії не сталося тільки через те, що вірус потрапив лише в систему, що дублює основну. Збитки ж завдані вірусом "I love you" по всьому світі рахують на мільярди доларів .

Кримінальні угруповання. Останнім часом спостерігається тенденція росту вчинення комп'ютерних злочинів кримінальними групами, що діють з метою викрадання грошових коштів, частіше всього з банківських установ.

Як приклад можна навести кримінальну справу Володимира Л. Левіна та його численних спільників, котрі незаконно здійснили переказ більш 10 млн. доларів із рахунків трьох постійних клієнтів Сіті-банку на рахунки у банках Каліфорнії, Фінляндії, Німеччини, Нідерландів, Швейцарії та Ізраїлю з червня по жовтень 1994 року. Левін, інженер-програміст з Росії, вчинив більш 40 зломів центральної банківської електронної системи платежів, використовуючи персональний комп'ютер і вкрадені ним паролі та ідентифікаційні номери. Співробітники російської телефонної компанії, що працювали із Сіті-банком, змогли простежити шлях від джерела несанкціонованих грошових переказів до спільника Левіна у Санкт-Петербурзі (Росія). Сам Левін був заарештований у березні 1995 року в Лондоні, а в потім виданий правоохоронним органам США. 24 лютого 1998 року він був засуджений до трьох років тюремного ув'язнення і відшкодування збитку Сіті-банку у розмірі 240 тис. доларів. Четверо спільників Левіна теж були заарештовані, але не були видані США. Сіті-банк зміг відшкодувати із 10 млн. украдених в нього коштів лише 9 млн. 600 тис. доларів .

Терористи. Терористичні організації все частіше використовують нові інформаційні технології та Internet з

злочинними намірами, поповнення коштів, проведення пропаганди або передачі секретної інформації. Директор ЦРУ США Джордж Тенет, виступаючи з проблем світових загроз, заявив, що терористичні угруповання (Hizbollah, HAMAS, the Abu Nidal organization і Bin Laden's al Qa'ida) використовують комп'ютерні файли, електронну пошту та шифрування (криптографію та стеганографію) для підтримки своєї протиправної діяльності. Хоча терористи ще не застосовували кіберзброю по призначенню, але вони використовують нові інформаційні технології і досягнення комп'ютерного прогресу – це вже сигнал про небезпеку. Кібертероризм, під яким розуміється використання сучасних інформаційних технологій і в першу чергу Internet, коли така зброя застосовується з метою пошкодження важливих державних інфраструктур (таких як енергетична, транспортна, урядова) – у недалекому майбутньому може стати реальною загрозою для національної безпеки нашої держави.

Іноземні розвідувальні служби. Не дивно, що іноземні спецслужби вже давно використовують кібероснащення як один з засобів здійснення своєї шпигунської діяльності, як зручний засіб одержання доступу до державних секретів і конфеденційної інформації іншої держави. На жаль деякі держави вже розробляють доктрину ведення війни електронними засобами, для цього створюються комп'ютерні програми і розробляється відповідне обладнання.

У розглянутих видах кіберзлочинів комп'ютери використовуються як знаряддя і як мета злочину, але комп'ютери знайшли застосування в більш традиційних категоріях злочинів.

Шахрайство в (за допомогою) Internet. Використання Internet з метою шахрайства є, мабуть, сьогодні одним із

найпоширеніших видів кіберзлочинів, з яким вже зіштовхнулися як приватні так і державні структури усього світу. Тому дуже важливо, щоб правоохоронні органи вивчили природу цих злочинів і боролися б із зловмисниками їх же зброєю – Internet. Internet – це досконалий інструмент у руках шахраїв завдяки наявності величезної аудиторії користувачів і можливості зберігання анонімності. Маючи певний досвід, будь-хто, знаходячись у своїй власній квартир або офісі, може знайти ефективний засіб обману через Internet, а сама глобальна інформаційна мережа стала благодатним середовищем для розвитку різноманітного роду злочинності. За даними Північноамериканської Асоціації (North American Securities Administrators Association) збитки від шахрайств через Internet у США, складають приблизно 10 млрд. доларів щорічно (1 млн. доларів в годину) . Характерним прикладом таких злочинів може бути випадок, коли 7 квітня 1999 року відвідувачі сайту фінансових новин компанії “Yahoo,Inc”, виявили сенсаційне повідомлення. Оголошення, передане по електронній пошті у розділі "Buyout News", повідомляло, що телекомунікаційна компанія “PairGain” в м.Тьюстині, Каліфорнія, переходить у володіння однієї з ізраїльських компаній, також повідомлялося, що подробиці угоди можна дізнатися на вебсайті Bloomberg News Service. Ця новина поширилася з неймовірною швидкістю і акції компанії, що продавалися, злетіли в ціні більш, ніж на 30 %. Обсяг продаж зріс майже в 7 разів. Проблема була тільки в тому, що угода – це обман, і вебсайт, на якому з'явилася ця інформація, не був Bloomberg's-вебсайтом, а був теж підробкою. Коли істина виявилася, ціни на акції різко впали, що призвело до великих фінансових втрат багатьох вкладників, які купили акції по штучно завищених цінах .

Права інтелектуальної власності. Інтелектуальна власність –

це рушійна сила світового економічного прогресу у новому 21 столітті. Неліцензійна продукція (піратство) загрожує економіці та суспільній безпеці тому, що здебільшого не відповідає ніяким стандартам якості. Зростаючий відсоток випуску низькоякісної піратської продукції зачепив і мережу Internet, де створено десятки тисяч вебсайтів виключно для поширення піратських матеріалів. Сьогодні вживаються заходи щодо охорони інтелектуальної власності в Україні з метою забезпечення конституційних прав громадян на захист інтелектуальної власності, сприятливих умов для створення об’єктів інтелектуальної власності .

Як висновок, хочеться ще раз підкреслити, що проблема боротьби з комп’ютерними злочинами – це комплексна проблема. Злочини у галузі використання інформаційних технологій не піддаються результативному розслідуванню тими засобами і заходами, що були ефективні у минулому столітті, коли інформатизація нашого суспільства тільки починалась. Закони повинні сьогодні відповідати тим вимогам, що пред’являє сучасний рівень розвитку технологій, щоб відправлення правосуддя відбувалося у незалежності від того, чи був такий злочин вчинений за допомогою звичайних засобів або персонального засобу супутникового зв’язку та мережі Internet.

Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Не секрет, що взаємодія відповідних органів на сьогоднішній день в основному зводиться до епізодичного обміну інформацією щодо ситуації у сфері комп’ютерних злочинів, ознайомленням з наказами, положеннями та інструкціями. На жаль, ще немає самого головного - цілісної державної системи відстеження обстановки у сфері забезпечення інформаційної безпеки

щодо прийняття рішень по виявленню і протидії комп'ютерним злочинам. Відсутній також і механізм ефективної взаємодії правоохоронної системи України з правоохоронними органами закордонних країн, що здійснюють боротьбу з комп'ютерними злочинами. Більше того, вирішення цієї проблеми, неможливе без забезпечення висококваліфікованими кадрами. На жаль, на сьогоднішній день правоохоронні органи, суди і прокуратури ще не мають у своєму розпорядженні достатню кількість фахівців, здатних оперативно виявляти та розслідувати комп'ютерні злочини. Тому створення цілісної системи навчання, підготовки і перепідготовки фахівців щодо боротьби з комп'ютерними правопорушеннями є ,на наш погляд, одним з головних завдань сьогодення.

З зазначеним напрямком тісно пов'язана проблема удосконалення нормативно-правової бази, недостатня розвиненість якої поки не дозволяє належною мірою протистояти кримінальним діям у сфері комп'ютерної інформації.

Карні санкції на національному та міжнародному рівні ще не забезпечують надійного захисту від комп'ютерної злочинності по двох причинах: перша - відсутність в існуючих законах чіткої класифікації комп'ютерних злочинів; друга - складність тлумачення та застосування статей законів, що обмежують дії правоохоронних органів. Для ефективної боротьби з кіберзлочинами, треба дати оцінку, чи відповідають зміни процесуальних норм ведення розслідування і переслідування у судовому порядку вимогам часу. Рівень злочинності в мережі Internet зростає настільки й з такою швидкістю, що законодавство просто не встигає за розвитком технологій.

Введення в дію з 1 вересня 2001 р. нового Кримінального кодексу України, прийняття до кінця 2001 року, нового

Кримінально-процесуального кодексу України, а також приєднання України до Страсбургської Конвенції щодо попередження кіберзлочинів (Draft Convention on Cyber-crime) дуже важливий крок у вирішенні цих проблем та надання необхідних і ефективних кримінально-правових та процесуальних механізмів, спрямованих проти загрози поширення кіберзлочинів у сферах державного та приватного сектору економіки нашої держави.

Нарешті, задачею виняткової важливості для побудови національної системи боротьби з правопорушеннями, у сфері використання комп'ютерних технологій є проведення науково-дослідних робіт по вирішенню проблем попередження та розслідування кіберзлочинів та залучення у цю роботу широкого кола науковців та громадськості. Саме на це і спрямована діяльність відомого, як на Україні, так і за її межами, Центру дослідження проблем комп'ютерної злочинності, який функціонує на базі Web сайту www.crime-research.org. У липні місяці 2001 р. Центр дослідження проблем комп'ютерної злочинності увійшов до складу партнерів Національного центу підвищення кваліфікації фахівців у галузі боротьби з кіберзлочинами (National Cybercrime Training Partnership) - проекту, створеному під патронажем Міністерства Юстиції США з метою організації співробітництва з партнерами у рамках програми боротьби зі злочинністю в галузі високих технологій та був прийнятий до Міжнародної Асоціації Дослідників Злочинності - The International Association of Crime Analysts (I.A.C.A.).

Термін "кіберзлочин" молодий і утворений сполученням двох слів: кіберпростір і злочин. Термін кіберпростір (у вітчизняній літературі частіше зустрічаються терміни "віртуальний простір" або "віртуальний світ") позначає інформаційний простір, що моделюється за допомогою комп'ютера, в якому існують визначеного роду об'єкти або символьне уявлення інформації - місце, де діють

комп’ютерні програми і переміщуються дані. Використання цього терміну поширене у світовій науковій літературі та вживається автором не як юридична категорія, а як визначення соціального та технічного феномену. Термін “кіберзлочини” у подальшому використовуватиметься і як синонім термінів “транснаціональні комп’ютерні злочини”, “злочини, що вчиняються за допомогою мережі Internet”. Під терміном “кіберзлочини”, будемо розуміти соціальне явище, що являє собою навмисну мотивовану атаку з використанням мережі Internet на інформацію в комп’ютерній системі, програми або дані, що чиниться окремою особою або угрупуваннями, яке має суспільну небезпеку для суспільного ладу України, його політичної й економічної системи, власності, особі, політичним, трудовим, майновим та іншім правам і свободам громадян.

3. Інформація

3.1 Інформація як об’єкт захисту

Широке використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, її користувачів, інформаційних ресурсів, каналів передачі даних від злочинних зазіхань зловмисників.

Концентрація інформації в комп'ютерах (аналогічно концентрації готівки в банках) змушує одних усе більш підсилювати пошуки шляхів доступу до інформації, а інших, відповідно, підсилювати контроль над нею з метою захисту.

Складність створення системи захисту інформації визначається тим, що дані можуть бути викрадені з комп'ютера (скопійовані), одночасно залишаючись на місці. Цінність деяких даних полягає у володінні ними, а не в їх знищенні або зміні.

Забезпечення безпеки інформації - справа дорога, і не стільки через витрати на закупівлю або установку різних технічних або програмних засобів, скільки через те, що важко кваліфіковано визначити межі розумної безпеки і відповідної підтримки системи в працездатному стані.

Об'єктами зазіхань можуть бути як самі матеріальні технічні засоби (комп'ютери і периферія), так і програмне забезпечення і бази даних.

Кожен збій роботи комп'ютерної мережі - це не тільки моральний збиток для працівників підприємства і мережевих адміністраторів. В міру розвитку технологій електронних платежів, «безпаперового» документообігу серйозний збій локальних мереж може паралізувати роботу цілих підприємств, що приведе до відчутних збитків. Не випадково захист даних у комп'ютерних мережах стає однією із найгостріших проблем.

Забезпечення безпеки інформації в комп'ютерних мережах припускає створення перешкод для будь-яких несанкціонованих спроб розкрадання або модифікації даних, переданих у мережі. При цьому дуже важливо зберегти такі властивості інформації, як:

· доступність,

· цілісність,

· конфіденційність

Доступність інформації - здатність забезпечувати своєчасний і безперешкодний доступ користувачів до інформації, яка їх цікавить.

Цілісність інформації полягає в її існуванні в неспотвореному вигляді (незмінному стосовно деякого фіксованого її стану).

Конфіденційність - це властивість, що вказує на необхідність введення обмежень доступу до даної інформації для визначеного кола користувачів.

Для того, щоб правильно оцінити можливий реальний збиток від втрати інформації, що зберігається на комп'ютері, необхідно знати, які загрози при цьому можуть виникнути і які адекватні заходи для її захисту необхідно приймати.

3.2 Характеристика загроз безпеки інформації

Неправомірне перекручування, фальсифікація, знищення або розголошення конфіденційної інформації може нанести серйозні, а іноді й непоправні матеріальні або моральні втрати. У цьому випадку, досить важливим є забезпечення безпеки інформації без збитку для інтересів тих, кому вона призначена.

Щоб забезпечити гарантований захист інформації в комп'ютерних системах обробки даних, потрібно насамперед сформулювати мету захисту інформації і визначити перелік необхідних заходів, які забезпечують захист. Для цього необхідно, в першу чергу, розглянути і систематизувати всі можливі фактори (загрози), що можуть привести до втрати або перекручування вихідної інформації.

Під загрозою безпеки комп'ютерної системи розуміється подія (вплив), що у випадку своєї реалізації стане причиною порушення цілісності інформації, її втрати або заміни. Загрози можуть бути як випадковими, так і навмисними.

До випадкових загроз відносяться:

1. помилки обслуговуючого персоналу і користувачів;

2. втрата інформації, обумовлена неправильним збереженням архівних даних;

3. випадкове знищення або зміна даних;

4. збої устаткування і електроживлення;

5. збої кабельної системи;

6. перебої електроживлення;

7. збої дискових систем;

8. збої систем архівування даних;

9. збої роботи серверів, робочих станцій, мережевих карт і т.д.;

10. некоректна робота програмного забезпечення;

11. зміна даних при помилках у програмному забезпеченні;

12. зараження системи комп'ютерними вірусами;

13. несанкціонований доступ;

14. випадкове ознайомлення з конфіденційною інформацією сторонніх осіб.

Найчастіше збиток наноситься не через чийсь злий намір, а просто через елементарні помилки користувачів, що випадково псують або видаляють дані, життєво важливі для системи. У зв'язку з цим, крім контролю доступу, необхідним елементом захисту комп’ютерної інформації є

розмежування повноважень користувачів. Крім того, ймовірність помилок обслуговуючого персоналу і користувачів мережі може бути значно зменшена, якщо їх правильно навчати і, крім того, періодично контролювати їх дії зі сторони, наприклад, адміністратора мережі.

Надійний засіб запобігання втрат інформації при короткочасному відключенні електроенергії - установка джерел безперебійного живлення (UPS). Різні по своїх технічних і споживчих характеристиках, подібні пристрої можуть забезпечити живлення всієї локальної мережі або окремого комп'ютера упродовж часу, достатнього для відновлення подачі напруги або для збереження інформації на магнітних носіях. Більшість UPS виконують функції ще і стабілізатора напруги, що є додатковим захистом від стрибків напруги в мережі. Багато сучасних мережевих пристроїв (сервери, концентратори і ін.) оснащені власними дубльованими системами електроживлення.

Основний, найбільш розповсюджений, метод захисту інформації і устаткування від стихійних лих (пожеж, землетрусів, повеней і т.п.) полягає в створенні і збереженні архівних копій даних.

Особливістю комп'ютерних технологій є те, що безпомилкових програм, у принципі, не буває. Якщо проект практично в будь-якій області техніки можна виконати з величезним запасом надійності, то в області програмування така надійність досить умовна, а іноді майже недосяжна. І це стосується не тільки окремих програм, але і цілого ряду програмних продуктів фірм, відомих в усім світі.

Через недоліки в програмних продуктах Microsoft, зв'язаних із забезпеченням безпеки даних у мережі Internet, «хакери» можуть захоплювати особисті ключі шифрів користувачів і діяти від їх імені.

На сьогоднішній день більше половини користувачів випробували «на собі» дію вірусів. Найбільш розповсюдженим методом захисту від вірусів дотепер залишається використання різних антивірусних програм.

Рівень зазначених загроз значною мірою знижується за рахунок підвищення кваліфікації обслуговуючого персоналу і користувачів, а також надійності апаратно-програмних і технічних засобів.

Однак найбільш небезпечним джерелом загроз інформації є навмисні дії зловмисників.

Стандартність архітектурних принципів побудови устаткування і програм забезпечує порівняно легкий доступ професіонала до інформації, що знаходиться в персональному комп'ютері. Обмеження доступу до ПК шляхом введення кодів не гарантує стовідсотковий захист інформації.

Включити комп'ютер і зняти код доступу до системи не викликає особливих утруднень: досить відключити акумулятор на материнській платі. На деяких моделях материнських плат для цього передбачений спеціальний перемикач. Також у кожного виготовлювача програми BIOS (AMI, AWARD і ін.) є коди, що мають пріоритет перед будь-якими кодами користувачів, набравши які можна одержати доступ до системи. У крайньому випадку, можна вкрасти системний блок комп'ютера або витягти жорсткий диск і вже в спокійній обстановці одержати доступ до необхідної інформації.

Загрози, що навмисно створюються зловмисником або групою осіб (навмисні загрози), заслуговують більш детального аналізу, тому що часто носять витончений

характер і приводять до важких наслідків. Тому розглянемо їх докладно.

До навмисних загроз відносяться:

· несанкціонований доступ до інформації і мережевих ресурсів;

· розкриття і модифікація даних і програм, їх копіювання;

· розкриття, модифікація або підміна трафіка обчислювальної мережі;

· розробка і поширення комп'ютерних вірусів, введення в програмне забезпечення логічних бомб;

· крадіжка магнітних носіїв і розрахункових документів;

· руйнування архівної інформації або навмисне її знищення;

· фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому;

· перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку тощо.

Виділяють три основних види загроз безпеки: загрози розкриття, цілісності і відмови в обслуговуванні (рис. 1.1).

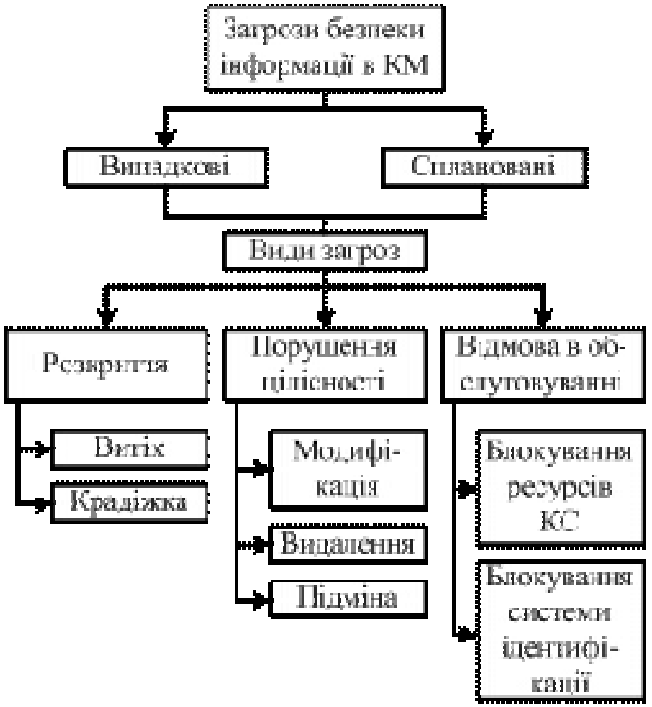


Рис. 1.1 Види загроз безпеки інформації в комп'ютерних мережах

Загроза розкриття полягає в тім, що інформація стає відомою тому, кому не потрібно її знати. Іноді замість слова «розкриття» використовуються терміни «крадіжка» або «витік».

Загроза порушення цілісності - будь-яка навмисна зміна (модифікація або навіть видалення) даних, що зберігаються в обчислювальній системі або передаються з однієї системи в іншу. Звичайно вважається, що загрозі розкриття піддаються в більшому ступені державні структури, а загрозі порушення цілісності - ділові або комерційні.

Загроза відмови в обслуговуванні виникає всякий раз, коли в результаті певних дій блокується доступ до деякого ресурсу обчислювальної системи.

3.3 Несанкціонований доступ до інформації і його мета

Спосіб несанкціонованого доступу (НСД) - це сукупність прийомів і порядок дій з метою одержання (добування) інформації, що охороняється, незаконним протиправним шляхом і забезпечення можливості впливати на цю інформацію (наприклад: підмінити, знищити і т.п.).

При здійсненні несанкціонованого доступу, зловмисник переслідує три мети:

· одержати необхідну інформацію для конкурентної боротьби;

· мати можливість вносити зміни в інформаційні потоки конкурента у відповідності зі своїми інтересами;

· завдати шкоди конкурентові шляхом знищення матеріалу інформаційних цінностей.

Повний обсяг даних про діяльність конкурента не може бути отриманий тільки яким-небудь одним з можливих способів доступу до інформації. Від мети залежить як вибір способів дій, так і кількісний і якісний склад сил і засобів добування інформації.

3.4 Порушники безпеки інформації

Спроба одержати несанкціонований доступ до комп'ютерної мережі з метою ознайомитися з нею, залишити інформацію, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як «комп'ютерне піратство».

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.

У залежності від мотивів, мети і методів, дії порушників безпеки інформації можна розділити на чотири категорії:

· шукачі пригод;

· ідейні «хакери»;

· «хакери»-професіонали;

· ненадійні (неблагополучні) співробітники.

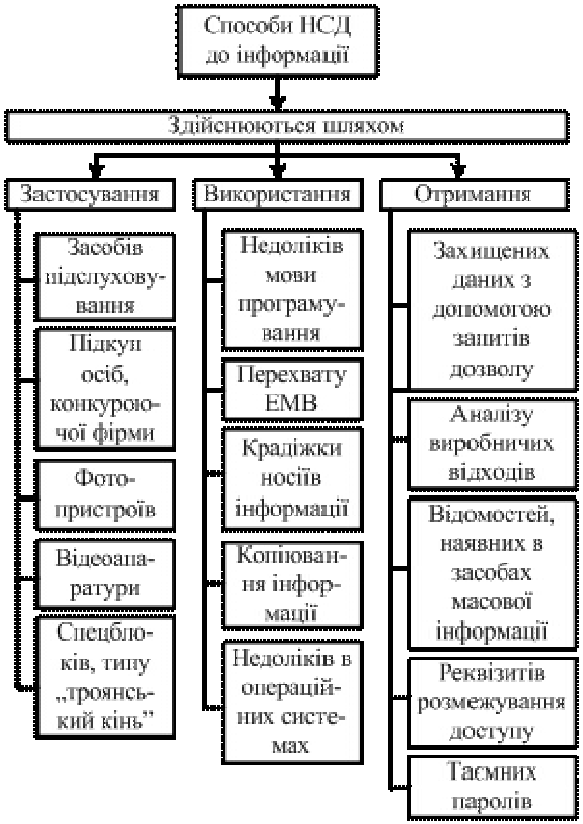


Рис. 1.2 Способи НСД до конфіденційної інформації

Шукач пригод, як правило, студент або старшокласник, і в нього рідко є продуманий план атаки. Він вибирає мету випадковим чином і звичайно відступає, зіштовхнувшись зі складнощами. 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 Web-сервера або, у більш рідких випадках, блокування роботи ресурсу, що атакується. У порівнянні із шукачем пригод, ідейний «хакер» розповідає про успішні атаки набагато більш широкої аудиторії, звичайно розміщаючи інформацію на хакерському Web-вузлі.

«Хакер»-професіонал має чіткий план дій і націлюється на визначені ресурси. Його атаки добре продумані і звичайно здійснюються в 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 в 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 переборювати 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. Однак, у цьому випадку, небезпека його несанкціонованого доступу до корпоративним даних набагато вища, ніж будь-якого іншого зловмисника.

Перераховані категорії порушників безпеки інформації можна згрупувати по їхній кваліфікації: початківець (шукач пригод), фахівець (ідейний «хакер», ненадійний

співробітник), професіонал («хакер»-професіонал). А якщо з цими групами зіставити мотиви порушення безпеки і технічну оснащеність кожної групи, то можна одержати узагальнену модель порушника безпеки інформації, як це показано на рис. 1.3.

Порушник безпеки інформація, як правило, будучи фахівцем визначеної кваліфікації, намагається довідатися все про комп'ютерні системи і мережі, зокрема, про засоби їх захисту. Тому модель порушника визначає:

· категорії осіб, у числі яких може виявитися порушник;

· можливі цілі порушника і їх градації по ступені важливості і небезпеки;

· припущення про його кваліфікації;

· оцінка його технічної озброєності;

· обмеження і припущення про характер його дій.

Діапазон спонукальних мотивів одержання доступу до системи досить широкий: від бажання випробувати емоційний підйом під час гри з комп'ютером до відчуття влади над ненависним менеджером. Займаються цим не тільки новачки, що бажають побавитися, але і професійні програмісти. Паролі вони добувають, або в результаті підбору або здогадування, або шляхом обміну з іншими «хакерами».

Частина з них, однак, починає не тільки переглядати файли, але і виявляти інтерес саме до їх змісту, а це вже являє серйозну загрозу, оскільки в даному випадку важко відрізнити звичайну цікавість від злочинних дій.

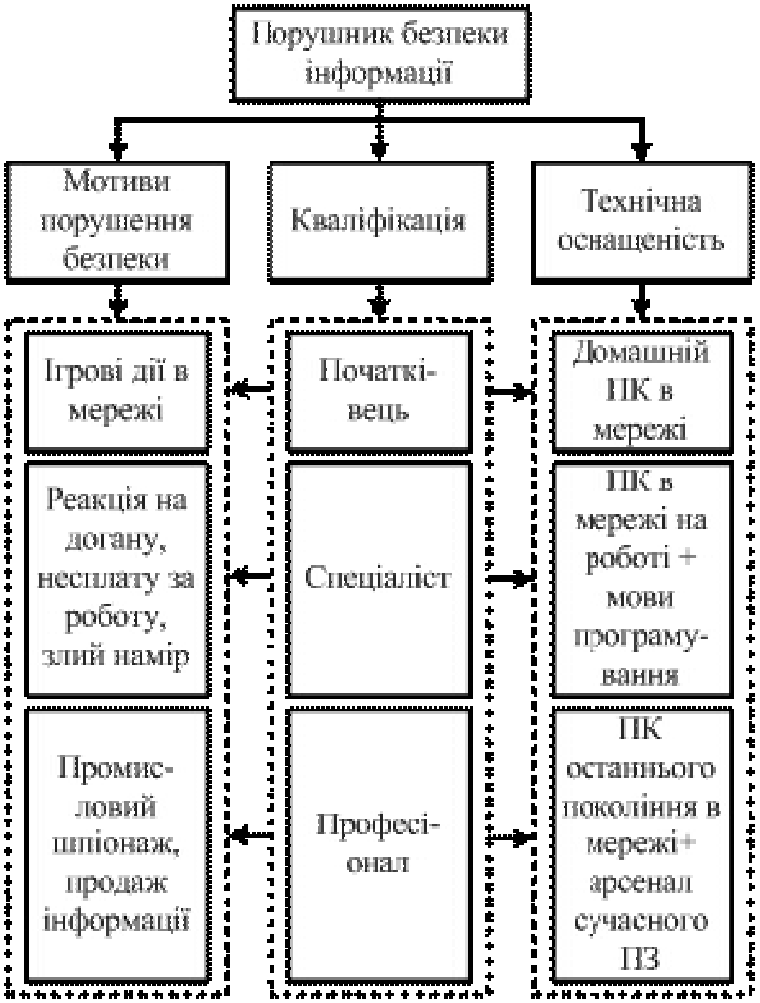


Рис. 1.3 Модель порушника безпеки інформації.

Донедавна викликали занепокоєння випадки, коли незадоволені керівником службовці, зловживаючи своїм положенням, псували системи, допускаючи до них

сторонніх або залишаючи системи без догляду в робочому стані. Спонукальними мотивами таких дій є:

· реакція на догану або зауваження з боку керівника;

· невдоволення тим, що фірма не оплатила понаднормові години роботи (хоча найчастіше понаднормова робота виникає через неефективне використання робочого часу);

· злий намір у якості, наприклад, реваншу з метою послабити фірму як конкурента якої-небудь новоствореної фірми.

Професійні «хакери» - це комп'ютерні фанати, що прекрасно знають обчислювальну техніку і системи зв'язку. Вони затратили масу часу на обмірковування способів проникнення в системи і ще більше, експериментуючи із самими системами. Для входження в систему професіонали найчастіше використовують деяку систематичність та експерименти, а не розраховують на удачу або інтуїцію. Їх мета - виявити і перебороти захист, вивчити можливості обчислювальної установки і потім вийти з неї, довівши можливість досягнення своєї мети.

До категорії хакерів-професіоналів звичайно відносять наступних осіб:

· таких, що входять у злочинні угруповання, які переслідують політичні цілі;

· прагнучих одержати інформацію з метою промислового шпигунства;

· «хакер» або угруповання «хакерів», що прагнуть до наживи.

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.

4. Криптографія

4.1 Термінологія

Тривалий час під криптографією розумілось лише шифрування — процес перетворення звичайної інформації (відкритого тексту) в незрозуміле «сміття» (тобто, шифротекст). Дешифрування — це зворотній процес відтворення інформації із шифротексту. Шифром називається пара алгоритмів шифрування/дешифрування. Дія шифру керується як алгоритмами, та, в кожному випадку, ключем. Ключ — це секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення. Ключі мають велику важливість, оскільки без змінних ключів алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків. Історично склалось так, що шифри часто використовуються для шифрування та дешифрування, без виконання додаткових процедур, таких як аутенифікація або перевірка цілісності.

В англійській мові слова криптографії та криптології інколи мають однакове значення, в той час, як деколи під криптографією може розумітись використання та дослідження технологій шифрування, а під криптологією — дослідження криптографії та криптології.

Дослідження характеристик мов, що мають будь-яке відношення до криптології, таких як частоти появи певних літер, комбінацій літер, загальні шаблони, тощо, називається криптолінгвістикою.

4.2 Історія криптографії

На фото показано сучасну реконструкцію шифра «скітало», що використовувався в Давній Греції, ймовірно був першим пристроєм для шифрування.

До нашого часу, криптографія займалася виключно забезпеченням конфіденційності повідомлень (тобто шифруванням) — перетворенням повідомлень із зрозумілої форми в незрозумілу і зворотнє відновлення на стороні одержувача, роблячи його неможливим для прочитання для того, хто перехопив або підслухав без секретного знання (а саме ключа, необхідного для дешифровки повідомлення). В останні десятиліття сфера застосування криптографії розширилася і включає не лише таємну передачу повідомлень, але і методи перевірки цілісності повідомлень, ідентифікування відправника/одержувача (аутентифікація), цифрові підписи, інтерактивні підтвердження, та технології безпечного спілкування, тощо.

Найперші форми тайнопису вимагали не більше ніж аналог олівця та паперу, оскільки в ті часи більшість людей не могли читати. Поширення писемності, або писемності серед ворогів, викликало потребу саме в криптографії. Основними типами класичних шифрів є перестановочні шифри, які змінюють порядок літер в повідомленні, та підстановочні шифри, які систематично замінюють літери або групи літер

іншими літерами або групами літер. Прості варіанти обох типів пропонували слабкий захист від досвідчених супротивників. Одним із ранніх підстановочних шифрів був шифр Цезаря, в якому кожна літера в повідомленні замінювалась літерою через декілька позицій із абетки. Цей шифр отримав ім'я Юлія Цезаря, який його використовував, зі зсувом в 3 позиції, для спілкування з генералами під час військових кампаній, подібно до коду EXCESS-3 в булевій алгебрі.

Шляхом застосування шифрування намагаються зберегти зміст спілкування в таємниці, подібно до шпигунів, військових лідерів, та дипломатів. Зберіглися також відомості про деякі з ранніх єврейських шифрів. Застосування криптографії радиться в Камасутрі як спосіб спілкування закоханих без ризику незручного викриття. Стеганографія (тобто, приховування факту наявності повідомлення взагалі) також була розроблена в давні часи. Зокрема, Геродот приховав повідомлення — татуювання на поголеній голові раба — під новим волоссям. До сучасних прикладів стеганографії належать невидимі чорнила, мікрокрапки, цифрові водяні знаки, що застосовуються для приховування інформації.

Шифротексти, отримані від класичних шифрів (та деяких сучасних), завжди видають деяку статистичну інформацію про текст повідомлення, що може бути використано для зламу. Після відкриття частотного аналізу (можливо, арабським вченим аль-Кінді) в 9-тому столітті, майже всі такі шифри стали більш-менш легко зламними досвідченим фахівцем. Класичні шифри зберігли популярність, в основному, у вигляді головоломок (див. криптограмма). Майже всі шифри залишались беззахисними перед криптоаналізом з використанням частотного аналізу до винаходу поліалфавітного шифру, швидше за все, Альберта Леоном-Баттіста приблизно в 1467 році (хоча, існують

свідчення того, що знання про такі шифри існували серед арабських вчених). Винахід Альберті полягав в тому, щоб використовувати різні шифри (наприклад, алфавіти підстановки) для різних частин повідомлення. Йому також належить винахід того, що може вважатись першим шифрувальним приладом: колесо, що частково реалізовувало його винахід (див. Шифрувальний диск Альберті). В поліалфавітному шифрі Віженера (англ. Vigenère cipher), алгоритм шифрування використовує ключове слово, яке керує підстановкою літер в залежності від того, яка літера ключового слова використовується. В середині 1800-тих, Чарльз Беббідж показав, що поліалфавітні шифри цього типу залишились частово беззахисними перед частотним аналізом.

Енігма, автомат, варіанти якого використовувались німецькими військовими починаючи з другої половини 1920-тих і до кінця Другої світової війни. Цей автомат реалізовував складний електро-механічний поліафавітний шифр для захисту таємних повідомлень. Злам шифру Енігми в Бюро Шифрів (Biuro Szyfrów), та, слід за цим, дешифрування повідомлень в Блетчі Парк (англ. Bletchley Park), було важливим чинником перемоги Союзників у війні.

Хоча частотний аналіз є потужною та загальною технікою, шифрування, на практиці, часто було ефективним; багато із

криптоаналітиків не знали цю техніку. Дешифрування повідомлень без частотного аналізу практично означало необхідність знання використаного шифру, спонукаючи, таким чином, до шпигунства, підкупу, крадіжок, зрад, тощо для отримання алгоритму. Згодом, в 19-тому столітті, було визнано, що збереження алгоритму шифрування в таємниці не забезпечує захист від зламу; насправді, було встановлено, що будь-яка адекватна криптографічна схема залишається у безпеці, навіть за умови доступу сторонніх. Збереження в таємниці ключа має бути достатньою умовою захисту інформації нормальним шифром. Цей фундаментальний принцип було вперше проголошено в 1883 Огюстом Керкгофсом, і загальновідомий як принцип Керкгоффза; різкіший варіант озвучив Клод Шеннон як максиму Шеннона — ворог знає систему.

Було створено різні механічні прилади та інструменти для допомоги в шифруванні. Одним з найперших є скітала в стародавній Греції, палиця, що, як вважається, використовувалась Спартанцями в якості перестановочного шифру. В середньовіччя, було винайдено інші засоби, такі як дірочний шифр, що також використовувася для часткової стеганографії. Разом із винаходом поліалфавітних шифрів, було розроблено досконаліші засоби, такі як власний винахід Альберті шифрувальний диск, табула ректа Йогана Тритеміуса, та мультициліндр Томаса Джефферсона (повторно винайдений Базерієсом приблизно в 1900 році). Декілька механічних шифрувально/дешифрувальних приладів було створено на початку 20-го століття і багато запатентовано, серед них роторні машини — найвідомішою серед них є Енігма, автомат, що використовувася Німеччиною з кінця 20-тих і до кінця Другої світової війни. Шифри, реалізовані прикладами покращених варіантів цих схем призвели до істотного підвищення криптоаналітичної складності після Другої світової війни..[Поява цифрових комп'ютерів та електроніки після Другої світової війни

зробило можливим появу складніших шифрів. Більше того, комп'ютери дозволяли шифрувати будь-які дані, які можна представити в комп'ютері у двійковому виді, на відміну від класичних шифрів, які розроблялись для шифрування письмових текстів. Це зробило непридатними для застосування лінгвістичні підходи в криптоаналізі. Багато комп'ютерних шифрів можна характеризувати за їхньою роботою з послідовностями бінарних бітів (інколи в блоках або групах), на відміну від класичних та механічних схем, які, зазвичай, працюють безпосередньо з літерами. Однак, комп'ютери також знайшли застосування у криптоаналізі, що, в певній мірі, компенсувало підвищення складності шифрів. Тим не менше, гарні сучасні шифри залшались попереду криптоаналізу; як правило, використання якісних шифрів дуже ефективне (тобто, швидке і вимагає небагато ресурсів), в той час як злам цих шифрів потребує набагато більших зусиль ніж раніше, що робить криптоаналіз настільки неефективним та непрактичним, що злам стає практично неможливим.

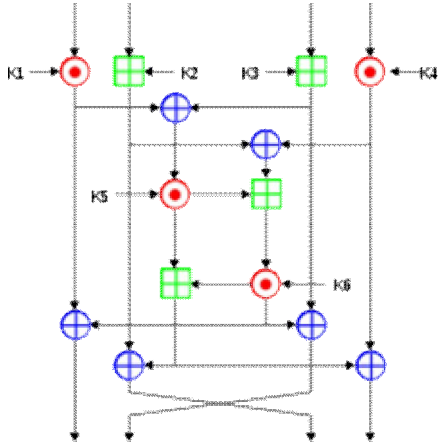
Широкі академічні дослідження криптографії з'явились порівняно нещодавно — починаючи з середини 1970-тих, разом із появою відкритої специфікації стандарту DES (Data Encryption Standard) Національного Бюро Стандартів США, публікацій Діффі-Хелмана та оприлюдненням алгоритму RSA. Відтоді, криптографія перетворилась на загальнопоширений інструмент для передачі даних, в комп'ютерних мережах, та захисті інформації взагалі. Сучасний рівень безпеки багатьох криптографічних методів базується на складності деяких обчислювальних проблем, таких як розклад цілих чисел, або проблеми з дискретними логарифмами. В багатьох випадках, існують докази безпечності криптографічних методів лише за умови неможливості ефективного розв'язання певної обчислювальної проблеми.За одним суттєвим винятком — схема одноразових блокнотів.

Разом із пам'яттю про історію криптографії, розробники криптографічних алгоритмів та систем також мають брати до уваги майбутній поступ технологій в своїх розробках. Наприклад, постійне підвищення обчислювальної потужності комп'ютерів розширило поле для атак грубої сили. Тому, відповідно і оновлюються стандарти в сенсі вибору довжини ключа. Можливі наслідки розвитку квантових комп'ютерів вже враховуються деякими розробниками криптографічних систем; анонсована поява малих реалізацій цих комп'ютерів робить важливою попередню підготовку.

Взагалі кажучи, до початку 20-го століття, криптографія, в основному, була пов'язанна з лінгвістичними схемами. Після того, як основний акцент було зміщено, зараз криптографія інтенсивно використовує математичний апарат, включно з теорією інформації, теорією обчислювальної складності, статистики, комбінаторики, абстрактної алгебри та теорії чисел. Криптографія є також відгалуженням інженерії, але не звичним, оскільки вона має справу з активним, розумним та винахідливим супротивником; більшість інших видів інженерних наук мають справу з нейтральними силами природи. Існують дослідження з приводу взаємозв'язків між криптографічними проблемами та квантовою фізикою.

4.3 Сучасна криптографія

4.3.1 Симетричне шифрування



Один із циклів (із 8.5) запатентованого блочного шифру IDEA, що використовується в деяких версіях PGP для високошвидкісного шифрування, зокрема, електронної пошти.

До алгоритмів симетричного шифрування належать методи шифрування, в яких і відправник, і отримувач повідомлення мають однаковий ключ (або, менш поширено, ключі різні але споріднені та легко обчислюються). Ці алгоритми шифрування були єдиними загально відомими до липня 1976.

Сучасні дослідження симетричних алгоритмів шифрування зосереджено, в основному, навколо блочних та потокових алгоритмів шифрування та їхньому застосуванні. Блочний шифр подібний до поліалфавітного шифру Альберті: блочні

шифри отримують фрагмент відкритого тексту та ключ, і видають на виході шифротекст такого самого розміру. Оскільки повідомлення зазвичай довші за один блок, потрібен деякий метод склеювання послідовних блоків. Було розроблено декілька методів, що відрізняються в різних аспектах. Вони є режимами дії блочних шифрів та мають обережно обиратись під час застосування блочного шифру в криптосистемі.

Шифри Data Encryption Standard (DES) та Advanced Encryption Standard (AES) є стандартами блочних шифрів затверджених урядом США (однак, стандартизацію DES було скасовано після прийняття стандарту AES).[9] Не зважаючи на те, що стандарт DES було визнано застарілим, він (та особливо його все ще дійсний варіант triple-DES) залишається досить популярним; він використовується в багатьох випадках, від шифрування в банкоматах до забезпечення приватності електронного листування[11] та безпечному доступі до віддалених терміналів. Було також розроблено багато інших шифрів різної якості. Багато з них було зламано.

Потокові шифри, на відміну від блочних, створюють ключ довільної довжини, що накладається на відкритий текст побітово або політерно, в дечому подібно до одноразової дошки. В потокових шифрах, потік шифротексту обчислюється на основі внутрішнього стану алгоритму, який змінюється протягом його дії. Зміна стану керується ключем, та, в деяких алгоритмах, ще і потоком відкритого тексту. RC4 є прикладом добре відомого, та широко розповсюдженого потокового шифру.

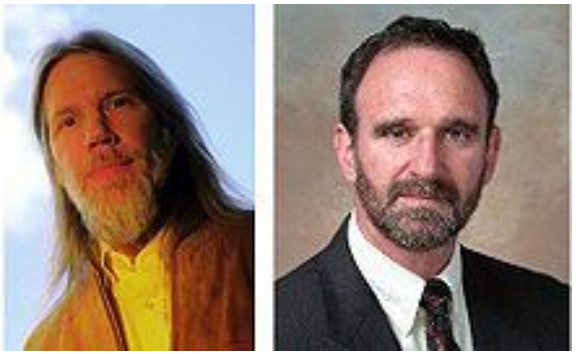
Криптографічні хешувальні функції (англ. cryptographic hash functions, або англ. message digest functions) не обов'язково використовують ключі, але часто використовуються і є важливим класом криптографічних

алгоритмів. Ці функції отримують дані (часто, ціле повідомлення), та обчислюють коротке, фіксованого розміру число (хеш). Гарні хешувальні функції створені таким чином, що дуже важко знайти колізії (два відкритих тексти, що мають однакове значення хешу).

Коди аутентифікації повідомлень (англ. Message authentication code, MAC) подібні до криптографічних хешувальних функцій, за виключенням того, що вони використовують секретний ключ для аутентифікації значення хешу при отриманні повідомлення. Ці функції пропонують захист проти атак на прості хешувальні функції.

4.3.2 Асиметричне шифрування

На відміну від симетричних, асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний. При цьому, не зважаючи на пов'язаність відкритого та секретного ключа в парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим.



Вітфілд Діффі та Мартін Хелман, автори першої доповіді про асиметричні алгоритми шифрування.

В асиметричних криптосистемах, відкритий ключ може вільно розповсюджуватись, в той час як приватний ключ має зберігатись в таємниці. Зазвичай, відкритий ключ використовується для шифрування, в той час як приватний (секретний) ключ використовується для дешифрування. Діффі та Хелман показали, що криптографія з відкритим ключем можлива за умови використання протоколу обміну ключами Діффі-Хелмана.

Іконка з замком в браузері Firefox, має показувати, що сторінку було відправлено через канал захищений SSL або TLS. Однак, подібна іконка не є гарантією безпеки; будь-який зламаний браузер може заводити користувачів в оману показуючи таку іконку в той час, як сторінка передається без захисту SSL або TLS.

4.3.3 Шифрування і розшифрування

Інформація, що може бути прочитана, осмислена і зрозуміла без яких-небудь спеціальних заходів, називається відкритим текстом (plaintext, clear text). Метод перекручування відкритого тексту таким чином, щоб сховати його суть, називається шифруванням (encryption або enciphering). Шифрування відкритого тексту приводить до його перетворення в незрозумілу абракадабру, іменовану шифртекстом (ciphertext). Шифрування дозволяє сховати інформацію від тих, для кого вона не призначається, незважаючи на те, що вони можуть бачити сам шифртекст. Протилежний процес перетворення шифртекста в його вихідний вид називається розшифруванням (decryption або deciphering).

4.3.4 Стійка криптографія

«У світі розрізняють два типи критографії: криптографія, що перешкодить вашій молодшій сестрі читати ваші файли,

і криптографія, що перешкодить читати ваші файли урядам великих країн. Ми будемо розглядати криптографію другого типу.»

Криптографія може бути стійкою, а може бути і слабкою, як описано в приведеному прикладі. Криптографічна стійкість виміряється тим, скільки знадобиться часу і ресурсів, щоб із шифртекста відновити вихідний відкритий текст. Результатом стійкої криптографії є шифртекст, який винятково складно зламати без володіння визначеними інструментами дешифрування. Але наскільки складно? Використовуючи весь обчислювальний потенціал сучасної цивілізації — навіть мільярд комп'ютерів, що виконують мільярд операцій у секунду — неможливо дешифрувати результат стійкої криптографії до кінця існування Всесвіту.

Хтось може вирішити, що стійка криптографія зможе устояти навіть проти самого серйозного криптоаналітика. Але хто про це говорить? Ніким не доведене, що краще шифрування, доступне сьогодні, зможе вистояти проти обчислювальних можливостей комп'ютерів, доступних завтра. Проте, стійка криптографія, задіяна в PGP, — краща на сьогоднішній день.

4.4 Дія криптографії

Криптографічний алгоритм, або шифр, — це математична формула, що описує процеси шифрування і розшифрування. Щоб зашифрувати відкритий текст, криптоалгоритм працює в сполученні з ключем — словом, числом або фразою. Те саме повідомлення одним алгоритмом, але різними ключами буде перетворюватися в різний шифртекст. Захищеність шифртекста цілком залежить від двох речей: стійкості криптоалгоритму і таємності ключа. Криптоалгоритм плюс усілякі ключі і протоколи, що

приводять їх у дію, складають криптосистему. PGP — це криптосистема.

У традиційній криптографії, також називаної шифруванням таємним, або симетричним, той самий ключ використовується як для шифрування, так і для розшифрування даних. Data Encryption Standart (DES) — приклад симетричного алгоритму, що широко застосовувався на Заході з 70-х років у банківській і комерційних сферах. В даний час його переміняє Advanced Encryption Standard (AES). Малюнок 2 ілюструє процес симетричного шифрування.

4.5 Шифр Цезаря

Юлій Цезар не довіряв гінцям. Тому, відправляючи листа своїм генералам, він замінював кожну букву A у своєму повідомленні на D, кожну B на E, і т. д. Тільки той, хто знав правило «зсуву на 3» міг розшифрувати його послання.

Украй простий приклад симетричного шифрування — це підставний шифр. Підставний шифр заміняє кожну частину інформації іншою інформацією. Найчастіше це досягається зсувом букв алфавіту. Пари прикладів — це Секретне кільце-декодер капітана Міднайта, що могло бути у вас у дитинстві, і шифр Юлія Цезаря. В обох випадках алгоритм полягає в тому, щоб зрушити алфавіт, а ключ — це число букв, на яке зроблений зсув. Допустимо, якщо ми вирішимо зашифрувати слово «SECRET», використовуючи ключ Цезаря, рівний 3, то зрушимо латинський алфавіт так, щоб він починався з третьої букви (D).

Отже, беручи вихідний варіант
ABCDEFGHIJKLMNOPQRSTUVWXYZ,

і зміщаючи усі на 3, одержуємо

DEFGHIJKLMNOPQRSTUVWXYZABC,

де D=A, E=B, F=C, і т. д.

Використовуючи цю схему, відкритий текст «SECRET» перетворюється в «VHFUHW». Щоб хтось міг відновити вихідний текст, ви повідомляєте йому, що ключ — 3. Очевидно, що за сьогоднішніми мірками це надзвичайно слабкий алгоритм, проте, навіть він допомагав Цезареві. І прекрасно демонструє, як діє симетричне шифрування.

4.6 Симетричне шифрування і керування ключами

Симетричне шифрування має ряд переваг. Перше — швидкість криптографічних операцій. Воно особливо корисно для шифрування даних, що залишаються у вас. Однак, симетричне шифрування, використане саме по собі як засіб захисту коштовних даних, що пересилаються, може виявитися досить витратним просто через складність передачі таємного ключа.

Згадаєте персонажа з вашого улюбленого шпигунського фільму: людина з запечатаним кейсом, пристебнутим наручниками до руки. Як ви вважаєте, що в цьому кейсі? Навряд чи в ньому коди запуску ракет / формула хімічної зброї / плани вторгнення. Імовірніше, там — ключ, що розшифрує секретну інформацію. Для встановлення криптографічного зв'язку за допомогою симетричного алгоритму, відправникові й одержувачеві потрібно попередньо погодити ключ і тримати його в таємниці. Якщо вони знаходяться в географічно вилучених місцях, то повинні вдатися до допомоги довіреного посередника, наприклад, надійного кур'єра, щоб уникнути компрометації ключа в ході транспортування. Зловмисник, що перехопив ключ на шляху, зможе пізніше читати, змінювати і підробляти будь-яку інформацію, зашифровану або завірену

цим ключем. Глобальна проблема симетричних шифрів (від Кільця-декодера капітана Міднайта до DES і AES) складається в складності керування ключами: як ви доставите ключ одержувачеві без ризику, що його перехоплять?

4.7 PGP

PGP поєднує в собі кращі сторони симетричної криптографії і криптографії з відкритим ключем. PGP — це гібридна криптосистема.

Коли користувач зашифровує дані за допомогою PGP, програма для початку їх стискає. Стиск скорочує час модемної передачі і заощаджує дисковий простір, а також, що важливіше, підвищує криптографічну стійкість. Більшість криптоаналітичних техніків засновано на статистичному аналізі шифртекста в пошуках ознак відкритого тексту. Стиск зменшує число таких ознак, що істотно підсилює опірність криптоаналізу.

Потім, PGP створює сеансовий ключ, тобто одноразовий симетричний ключ, застосовуваний тільки для однієї операції. Цей сеансовий ключ являє собою псевдовипадкове число, згенероване від випадкових рухів мишки і натискання клавіш. Сеансовий ключ працює на основі дуже надійного, швидкого симетричного алгоритму, яким PGP зашифровує стиснуте повідомлення; у результаті виходить шифртекст. Як тільки дані зашифровані, сеансовий ключ також шифрується, але уже відкритим ключем одержувача. Цей зашифрований відкритим ключем сеансовий ключ прикріплюється до шифртексту і передається разом з ним одержувачеві.

Розшифрування відбувається в зворотному порядку. PGP одержувача використовує його закритий ключ для витягу

сеансового ключа з повідомлення, яким шифртекст вихідного послання відновлюється у відкритий текст.

Таким чином, комбінація цих двох криптографічних методів поєднує зручність шифрування відкритим ключем зі швидкістю роботи симетричного алгоритму. Симетричне шифрування в тисячі разів швидше асиметричного. Шифрування відкритим ключем, у свою чергу, надає просте рішення проблеми керування ключами і передачі даних. При використовувані їх спільно, швидкість виконання і керування ключами взаємно доповнюються і поліпшуються без якого-небудь збитку безпеки.

4.8 Ключі

Ключ — це деяка величина, що, працюючи в сполученні з криптоалгоритмом, робить визначений шифртекст. Ключі, як правило, — це дуже великі числа. Розмір ключа виміряється в бітах; число, що представляє 2048-бітовий ключ, скажено велике. В асиметричній криптографії, чим більший ключ, тим захищеніший отриманий шифртекст. Однак, розмір асиметричного ключа і розмір симетричного таємного ключа, абсолютно непорівнянні. Симетричний 80-бітовий ключ еквівалентний у стійкості 1024-бітовому відкритому ключеві. Симетричний 128-бітовий ключ приблизно дорівнює 3000-бітовому відкритому. Знову ж, більший ключ — вища надійність, але механізми, що лежать в основі кожного з типів криптографії зовсім різні, і порівнювати їхні ключі в абсолютних величинах неприпустимо.

Незважаючи на те, що ключова пара математично зв'язана, практично неможливо з відкритого ключа обчислити закритий; у той же час, обчислення закритого ключа завжди залишається можливим, якщо мати в розпорядженні достатній час і обчислювальні потужності. От чому

критично важливо створювати ключ вірної довжини: досить великий, щоб був надійним, але досить малий, щоб залишався швидким у роботі. Для цього подумайте й оцініть, хто може спробувати «прочитати ваші файли», наскільки вони можуть бути таємні, скільки часу потрібно для їхнього розшифрування та якими ресурсами.

Більші ключі будуть криптографічно захищені за більший проміжок часу. Якщо те, що треба зашифрувати, повинно зберігатися в таємниці довгі-довгі роки, то, можливо, варто скористатися дуже великим ключем. Хто знає, скільки буде потрібно часу, щоб розкрити ключ, використовуючи завтрашні швидші, ефективніші комп'ютери? Були часи, коли 56-бітовий симетричний ключ DES вважався вкрай надійним.

За сучасними уявленнями 128-бітові симетричні ключі зовсім надійні і не піддані зломові, принаймні сьогодні, поки хтось не побудує функціонуючий квантовий суперкомп'ютер. 256-бітові ключі за оцінками криптологів не можуть бути зламані навіть теоретично і навіть на гіпотетичному квантовому комп'ютері. Саме з цієї причини алгоритм AES підтримує ключі довжиною 128 і 256 біт. Однак історія вчить нас тому, що всі ці запевняння впродовж десятиліть можуть виявитися порожньою балаканиною.

PGP зберігає ключі в зашифрованому виді. Вони утримуються в двох файлах на твердому диску; один файл для відкритих ключів, іншої — для закритих. Ці файли називаються з'єднувальними (keyrings). Використовуючи PGP, Ви, час від часу, будете додавати відкриті ключі своєї кореспонденції на зв'язування відкритих. Ваші закриті ключі знаходяться на зв'язуванні закритих. Якщо ви втратите (видалите) зв'язування закритих ключів, то вже ніяким чином не зможете розшифрувати інформацію,

зашифровану для ключів з цього зв'язування. Отже, збереження пари резервних копій цього файлу є необхідною.

4.9 Цифрові підписи

Додаткова перевага від використання криптосистем з відкритим ключем полягає в тому, що вони надають можливість створення електронних цифрових підписів (ЕЦП). Цифровий підпис дозволяє одержувачеві повідомлення переконатися в автентичності джерела інформації (іншими словами, у тім, хто є автором інформації), а також перевірити, чи була інформація змінена (перекручена), поки знаходилася в шляху. Таким чином, цифровий підпис є засобом авторизації і контролю цілісності даних. Крім того, ЕЦП несе принцип незречення, що означає, що відправник не може відмовитися від факту свого авторства підписаної ним інформації. Ці можливості настільки ж важливі для криптографії, як і таємність.

ЕЦП служить тієї ж мети, що печатка або власноручний автограф на паперовому листі. Однак внаслідок своєї цифрової природи ЕЦП перевершує ручний підпис і печатку в ряді дуже важливих аспектів. Цифровий підпис не тільки підтверджує особистість що підписала, але також допомагає визначити, чи був зміст підписаної інформації змінений. Власноручний підпис і печатка не мають подібної якості, крім того, їх набагато легше підробити. У той же час, ЕЦП аналогічна фізичної печатки в тім плані, що, як печатка може бути проставлена будь-якою людиною, що одержала в розпорядження печатку, так і цифровий підпис може бути згенерована ким завгодно з копією потрібного закритого ключа.

Деякі люди використовують цифровий підпис набагато частіше ніж шифрування. Наприклад, ви можете не

хвилюватися, якщо хтось довідається, що ви тільки що помістили $1000 на свій банківський рахунок, але ви повинні бути абсолютно упевнені, що робили транзакцію через банківського касира. Простий спосіб генерації цифрових підписів показаний на малюнку 6. Замість Шифрування інформації чужим відкритим ключем, ви шифруєте її своїм власним закритим. Якщо інформація може бути розшифрована вашим відкритим ключем, значить її джерелом є ви.

4.10 Хеш-функція

Однак описана вище схема має ряд істотних недоліків. Вона вкрай повільна і робить занадто великий обсяг даних — щонайменше вдвічі більше обсягу вихідної інформації. Поліпшенням такої схеми стає введення в процес перетворення нового компонента — однобічної хеш-функції. Одностороння хеш-функція отримує ввід довільної довжини, називаний прообразом, — у даному випадку, повідомлення будь-якого розміру, хоч тисячі або мільйони біт — і генерує строго залежний від прообразу значення фіксованої довжини, допустимо, 160 біт. Хеш-функція гарантує, що якщо інформація буде будь-як змінена — навіть на один біт, — у результаті вийде зовсім інше хеш-значення.

У процесі цифрового підпису PGP обробляє повідомлення криптографічно стійким однобічним хеш-алгоритмом. Ця операція приводить до генерації рядка обмеженої довжини, називаної дайджестом повідомлення (message digest). (Знову ж, будь-яка зміна прообразу приведе до абсолютно іншого дайджесту.) Потім PGP зашифровує отриманий дайджест закритим ключем відправника, створюючи «електронний підпис», і прикріплює її до прообразу. PGP передає ЕЦП разом з вихідним повідомленням. Після одержання повідомлення, адресат за допомогою PGP заново

обчислює дайджест підписаних даних, розшифровує ЕЦП відкритим ключем відправника, тим самим звіряючи, відповідно, цілісність даних і їхнє джерело; якщо обчислений адресатом і отриманий з повідомленням дайджести збігаються, значить інформація після підписання не була змінена. PGP може як зашифрувати саме повідомлення, що підписується, так і не робити цього; підписання відкритого тексту без шифрування корисно в тому випадку, якщо хто-небудь з одержувачів не зацікавлений або не має можливості звірити підпис (допустимо, не має PGP).

Якщо в механізмі формування ЕЦП застосовується стійка однобічна хеш-функція, немає ніякого способу взяти або підпис з одного документа і прикріпити неї до іншого, або ж будь-якимось чином змінити підписане повідомлення. Найменша зміна в підписаному документі буде виявлено в процесі звірення ЕЦП.

ЕЦП відіграють найважливішу роль у посвідченні і запевнянні ключів інших користувачів PGP.

4.11 Цифрові сертифікати

Одна з головних проблем асиметричних криптосистем полягає в тому, що користувачі повинні постійно стежити, чи зашифровують вони повідомлення власними ключами своїх кореспондентів. У середовищі вільного обміну відкритими ключами через суспільні сервери-депозитарії атаки представляють собою серйозну потенційну загрозу. У цьому виді атак зловмисник підсуває користувачеві підроблений ключ з ім'ям передбачуваного адресата; дані зашифровуються підставним ключем, перехоплюються його власником-зловмисником, потрапляючи в чужі руки. У середовищі криптосистем з відкритим ключем критично важливо, щоб ви були абсолютно упевнені, що відкритий

ключ, яким збираєтеся щось зашифрувати — не митецька імітація, а власність вашого кореспондента. Можна попросту шифрувати тільки тими ключами, що були передані вам їхніми власниками з рук у руки на дискетах. Але припустимо, що потрібно зв'язатися з людиною, що живе на іншому краї світу, з яким ви навіть незнайомі; як ви можете бути упевнені, що одержали його справжній ключ?

Цифрові сертифікати ключів спрощують задачу визначення приналежності відкритих ключів передбачуваним власникам. Сертифікат це форма посвідчення. Інші види посвідчень включають ваші права водія, державний паспорт, свідоцтво про народження, і т. д. Кожне з них несе на собі деяку ідентифікуючу вас інформацію і визначений запис, що непідробляється, щоб хтось інший встановив вашу особистість. Деякі сертифікати, такі як паспорт, — самодостатнє підтвердження вашої особистості; буде досить неприємно, якщо хтось викраде його, щоб видати себе за вас.

Цифровий сертифікат у своєму призначенні аналогічний фізичному. Цифровий сертифікат ключа — це інформація, прикріплена до відкритого ключа користувача, що допомагає іншим встановити, чи є ключ справжнім і вірним. Цифрові сертифікати потрібні для того, щоб унеможливити спробу видати ключ однієї людини за ключ іншого.

Цифровий сертифікат складається з трьох компонентів:
відкритого ключа, до якого він прикладений;
даних, або записів сертифіката (зведення про особистості користувача, ім'я, електронна пошта і т. д., а також, у разі необхідності, вказати додаткові обмежуючі зведення : права доступу, робочі ліміти та інше);
однієї або декількох цифрових підписів, «з'єднаних» ключем з сертифікатом.

Ціль ЕЦП на сертифікаті — указати, що зведення сертифіката були завірені довіреною третьою особою або організацією. У той же час цифровий підпис не підтверджує вірогідність сертифіката як цілого; вона є дорученням тільки того, що підписаний запис сертифіката (ідентифікуюча інформація) зв'язані з даним відкритим ключем.

Таким чином, сертифікат, звичайно, — це відкритий ключ із прикріпленими до нього однієї або декількома формами ID плюс оцінка підтвердження від довіреної особи, «єднальна» ID і відкритий ключ.

4.12 Поширення сертифікатів

Сертифікати застосовуються, коли потрібно обмінятися з ким-небудь ключами. Невеликим групам людей, що бідує в захищеному зв'язку, не складе праці просто передати один одному дискети або відправити електронні листи, що містять копії їхніх ключів. Це — ручне поширення відкритих ключів, і воно ефективно тільки до визначеного етапу. Подальше — за межами можливостей даного методу, і тоді виникає необхідність розгортання системи, яка б забезпечувала достатню надійність і безпеку, надавала можливості збереження й обміну ключами, так що колеги, бізнеси-партнери або незнайомці змогли б відправляти один одному зашифровані повідомлення, якщо в тім виникне необхідність. Така система може реалізуватися у формі простого сховища-депозитарію, називаного сервером сертифікатів, або сервером-депозитарієм відкритих ключів, або мати складнішу і комплексну структуру, що припускає додаткові можливості адміністрування ключів, і називану інфраструктурою відкритих ключів (Public Key Infrastructure, PKI).

4.13 Сервери-депозитарії

Сервер-депозитарій, також називаний сервером сертифікатів, або сервером ключів, — це мережна база даних, що дозволяє користувачам залишати і витягати з неї цифрові сертифікати. Сервер ключів також може мати деякі функції адміністрування, що допомагають організації підтримувати свою політику безпеки. Наприклад, на збереження можуть залишатись тільки ключі, що задовольняють визначеним критеріям.

4.14 Інфраструктури відкритих ключів (PKI)

PKI, як і простий сервер-депозитарій, має базу даних для збереження сертифікатів, але, у той же час, надає сервіси і протоколи для керування відкритими ключами. У них входять можливості випуску (видання), відкликання (анулювання) і системи довіри сертифікатів. Головною же особливістю PKI є наявність компонентів, відомих як Центр сертифікації (Certification Authority, CA) і Центр реєстрації (Registration Authority, RA). Центр сертифікації (ЦС) видає цифрові сертифікати і підписує їх своїм закритим ключем. Через важливість своєї ролі, ЦС є головним компонентом інфраструктури PKI. Використовуючи відкритий ключ ЦС, будь-який користувач, що бажає перевірити дійсність конкретного сертифіката, звіряє підпис Центра сертифікації і, отже, засвідчується в цілісності інформації, що утримується в сертифікаті, і, що важливіше, у взаємозв'язку зведень сертифіката і відкритого ключа.

Як правило, Центром реєстрації (ЦР) називається система людей, механізмів і процесів, що служить цілям зарахування нових користувачів у структуру PKI і подальшого адміністрування постійних користувачів

системи. Також ЦР може робити «веттинг» — процедуру перевірки того, чи належить конкретний відкритий ключ передбачуваному власникові.

ЦР — це людське співтовариство: особа, група, департамент, компанія або інша асоціація. З іншого боку, ЦС — звичайно, програма, що видає сертифікати своїм зареєстрованим користувачам. Існують і захищені від злому апаратні реалізації ЦС, споруджені з куленепробивних матеріалів і постачені «червоною кнопкою», що анулює в критичній ситуації усі видані ключі. Роль ЦР-ЦС аналогічна тієї, що виконує державний паспортний відділ: одні його співробітники перевіряють, потрібно чи видача паспорта (робота ЦР), а інші виготовляють сам документ і передають його власникові (робота ЦС). Наявність ЦР для ЦС не обов'язково, але воно забезпечує поділ функцій, що іноді необхідно. Формат сертифікатів Цифровий сертифікат — це набір ідентифікуючих зведень, зв'язаних з відкритим ключем і підписаних довіреною третьою особою, щоб довести їхня дійсність і взаємозв'язку. Сертифікат може бути представлений безліччю різних форматів. PGP підтримує два формати сертифікатів:
Сертифікати OpenPGP (частіше називані просто ключами PGP)
Сертифікати X.509

4.15 Формат сертифікату PGP

Сертифікат PGP містить:
Відкритий ключ власника сертифіката — відкрита частина ключової пари і її алгоритм: RSA v4, RSA Legacy v3, DH або DSA.

Зведення про власника сертифіката — інформація, що ідентифікує особистість користувача: його ім'я, адреса електронної пошти, номер ICQ, фотографія і т. д.
ЕЦП власника сертифіката — підпис ключової пари, зв'язаної із сертифікатом (т.зв. автопідпис).
Період дії сертифіката — дата початку дії сертифіката і дата закінчення його дії; указує на те, коли сертифікат стане недійсним (аналогічно терміну дії посвідчення водія). Якщо ключова пара містить додаткові підключи шифрування, то тут буде зазначений період дії кожного з них .
Кращий алгоритм шифрування — указує на те, зашифровану яким алгоритмом інформацію воліє одержувати власник сертифіката. Підтримуються такі: CAST, AES, IDEA, Triple-DES і Twofish.

Ви можете представити сертифікат PGP у виді відкритого ключа з однієї або декількома прив'язаними до нього «бирками». На цих «бирках» зазначена інформація, що ідентифікує власника ключа, а також підпис цього ключа, що підтверджує, що ключ і ідентифікаційні зведення взаємозалежні. (Цей вид підпису називається автопідписом (self-signature); її містить кожен PGP-сертифікат.)

Унікальний аспект формату сертифікатів PGP у тім, що кожен сертифікат може містити безліч підписів. Будь-яка людина може підписати ідентифікаційно-ключову пару, щоб завірити, покладаючись на своє особисте переконання, що відкритий ключ належить саме зазначеному в ID користувачеві. Якщо пошук на суспільних серверах-депозитаріях, то можете знайти деякі ключі, як, наприклад, що належить авторові PGP Філу Ціммерману, що містять величезну кількість підписів. Деякі PGP-сертифікати складаються з відкритого ключа з декількома «бірками», кожна з яких містить власні зведення, що ідентифікують власника ключа (наприклад, ім'я власника і його робітник e-mail, прізвисько власника і його домашній e-mail,

фотографія власника — усі на одному сертифікаті). Список підписів на кожній з «бірок» може бути різним; підпису вказують на вірогідність визначеної «бірки» і її приналежність відкритому ключеві, а не на те, що всі «бірки» достовірні. (Врахуйте, що «вірогідність» залежить від встоновленого неї : підпису — це думки, і різні люди приділяють різний ступінь уваги перевірці дійсності перед підписанням ключа.)

4.16 Формат сертифіката X.509

X.509 — це інший дуже розповсюджений формат. Усі сертифікати X.509 відповідають міжнародному стандартові ITU-T X.509; у такий спосіб (теоретично), сертифікат X.509, створений для одного додатка, може бути використаний у будь-якому іншому, підтримуючий цей стандарт. На практиці, однак, склалася ситуація, що різні компанії створюють власні розширення для X.509, не усі з яких між собою сумісні. Усякий сертифікат вимагає, щоб хтось завірив взаємозв'язок відкритого ключа й ідентифікуючого власника ключа інформації. Маючи справу з PGP-сертифікатом, кожний може виступати як завіритель зведень, що утримуються в ньому, (за винятком випадків, коли ця можливість навмисно обмежена політикою безпеки). Але у випадку сертифікатів X.509 завірителем може бути тільки Центр сертифікації або хтось, спеціально вповноважений їм на цю роль. (Майте на увазі, що PGP-сертифікати також повною мірою підтримують ієрархічне структурування системи довіри, що використовує ЦС для посвідчення сертифікатів.) Сертифікат X.509 — це набір стандартних полів, що містять зведення про користувача або пристрій, і їх відповідний відкритий ключ. Стандарт X.509 визначає, які зведення входять у сертифікат і як вони кодуються (формат даних).

Сертифікат X.509 містить такі зведення :

Версія X.509 — указує, на основі якої версії стандарту X.509 побудований даний сертифікат, що визначає, яка інформація може в ньому утримуватися.
Відкритий ключ власника сертифіката — відкритий ключ поряд з ідентифікатором використовуваного алгоритму (вказуючим криптосистему, до якої належить даний ключ) і інша інформація про параметри ключа.
Серійний номер сертифіката — організація-видавець сертифіката зобов'язаний привласнити йому унікальний серійним (порядковий) номер для його впізнання серед інших сертифікатів, виданих даною організацією. Ця інформація застосовується в ряді випадків; наприклад, при анулюванні сертифіката, його серійний номер міститься до реєстру анульованих сертифікатів (Certificate Revocation List, CRL).
Унікальний встановлювач власника ключа (або DN, distinguished name — унікальне ім'я) — це ім'я повинне бути унікальному і єдиним у всьому Інтернету . DN складається з декількох підпунктів і може виглядати приблизно так:

CN=Bob Davis, EMAI=bdavis@pgp.com, OU=PGP Engineering, O=PGP Corporation, C=US

(Що позначає Зрозуміле ім'я суб'єкта, Електронну пошту, Підрозділ організації, Організацію і Країну відповідно.)
Період дії сертифіката — дата початку дії сертифіката і дата закінчення його дії; указує на те, коли сертифікат стане недійсний.
Унікальне ім'я видавця — унікальне ім'я організації, що підписав сертифікат. Звичайно, це найменування Центра сертифікації. Використання сертифіката має на увазі довіра організації, його що підписала. (У випадках з кореневими сертифікатами організація, що видала — цей же ЦС — підписує його сама.)
ЕЦП видавця — електронний підпис, створений закритим ключем організації, що видав сертифікат.

Ідентифікатор алгоритму підпису — вказує алгоритм, використаний ЦС для підписання сертифіката.

Існує ряд фундаментальних розходжень між форматами сертифікатів X.509 і PGP:
ви можете особисто створити власний сертифікат PGP; ви повинні запросити й одержати сертифікат X.509 від Центра сертифікації;
сертифікати X.509 містять тільки одне ім'я власника сертифіката;
сертифікати X.509 містять тільки одну ЕЦП, що підтверджує дійсність сертифіката.

Щоб одержати сертифікат X.509, ви повинні попросити ЦС видати його вам. Ви надаєте системі свій відкритий ключ, чим доводите, що володієте відповідно закритим, а також деякі ідентифікуючі ваші зведення . Потім ви электронно підписуєте ці зведення і відправляєте весь пакет — запит сертифіката — у Центр сертифікації. ЦС виконує визначений процес перевірки дійсності наданої інформації і, якщо усе сходиться, створює сертифікат, підписує і повертає вам. Ви можете представити сертифікат X.509, як звичайний паперовий сертифікат або атестат із приклеєним до нього відкритим ключем. На ньому зазначене ваше ім'я, а також деякі зведення про вас, плюс підпис видавця сертифіката.

Імовірно, найбільша користь від сертифікатів X.509, це їхнє застосування у Веб-браузерах.

4.17 Дійсність і довіра

Будь-який користувач у середовищі криптосистем з відкритим ключем ризикує рано або пізно прийняти помилково підроблений ключ (сертифікат) за дійсний.

Вірогідність (дійсність) є в тому, що конкретний відкритий ключ належить передбачуваному власникові, чия ідентифікаційна інформація зазначена в сертифікаті ключа. Дійсність є одним з найважливіших критеріїв у середовищі системи відкритих ключів, де ви повинні визначати автентичність кожного конкретного сертифіката.

Переконавши, що чужий відкритий ключ достовірний (тобто дійсно належить саме передбачуваному власникові), ви можете підписати копію цього ключа на своєму зв'язуванні, чим засвідчите факт, що ви його перевірили і прийняли за достовірний. Якщо захочете, щоб інші знали ваш ступінь довіри цьому сертифікатові, ви можете експортувати свій підтверджуючий підпис на сервер-депозитарій для того, щоб інші могли неї бачити і могли на неї покластися при визначенні дійсності цього ключа.

Деякі компанії вповноважують один або кілька Центрів сертифікації (ЦС) на перевірку дійсності сертифікатів. В організації, що використовує PKI із сертифікатами X.509, задача Центрів реєстрації складається в прийомі запитів на сертифікати, а задача Центрів сертифікації — у видачі сертифікатів кінцевим користувачам: процес відповіді на запит користувача на одержання сертифіката. В організації, що використовує сертифікати PGP без PKI, задача ЦС — у перевірці вірогідності всіх PGP-сертифікатів і підписанні справжніх. Як правило, основна мета ЦС — власним підписом «зв'язати» відкритий ключ з ідентифікаційною інформацією, що утримується в сертифікаті, чим завірити третіх осіб, що були прийняті визначені заходи для встановлення зв'язку між ключем і ідентифікаційними зведеннями.

Центр сертифікації в організації — це камінь системи дійсності і довіри; у деяких організаціях, як, наприклад, у тих, котрі використовують PKI, жоден сертифікат не

вважається справжнім, поки не буде підписаний довіреним ЦС.

4.18 Перевірка дійсності

Один зі способів визначення дійсності сертифіката — деяка механічна процедура. Існує кілька методик її проведення. Наприклад, ви можете попросити свого кореспондента передати копію його відкритого ключа «фізично», тобто вручити на твердому носії — магнітному або оптичному диску тощо Але найчастіше це буває незручно і неефективно.

Інший варіант — звірити відбиток (fingerprints) сертифіката. Наскільки унікальні відбитки пальців людей, настільки ж унікальні і відбитки кожного сертифіката PGP. Відбиток — це хеш-значення сертифіката користувача, що показано як одне з його властивостей. У PGP відбиток може бути представлений або як шестнадцяткове число, або як набір біометричних слів, фонетично чіткого і застосовуваних для спрощення вербальної ідентифікації відбитка.

Ви можете визначити дійсність сертифіката подзвонивши власникові ключа і попросивши його прочитати відбиток з його ключа; вам же потрібно звірити цей відбиток проти того, котрий знаходиться на отриманій вами копії. Такий спосіб допустимо, якщо вам знайомий голос кореспондента, але як ви встановите особистість того, з ким навіть незнайомі? Деякі з цією метою поміщають відбитки ключів на свої візитні картки. Ще один метод визначення дійсності чужого сертифіката — покластися на думку третьої сторони, що вже установила його дійсність.

ЦС, наприклад, відповідає за детальну перевірку приналежності відкритого ключа передбачуваному

власникові перед видачею йому сертифіката. Будь-який користувач, що довіряє ЦС, буде автоматично розцінювати справжніми всі сертифікати, підписані ЦС. Рівнобіжний аспект перевірки дійсності і вірогідності полягає в тому, щоб переконатися, що сертифікат не був анульований (відкликаний).

4.19 Установлення довіри

Ви самі засвідчуєте сертифікати. Але ви також довіряєте людям. Тому ви можете довірити людям і право засвідчувати сертифікати. Як правило, якщо тільки власник сам не вручив вам копію ключа, ви повинні покластися на чиюсь чужу думку про його дійсність.

4.20 Позначки-поручителі і довірені поручителі

У більшості випадків користувачі цілком покладаються на ЦС у перевірці дійсності сертифікатів. Іншими словами, користувачі переконані, що ЦС провів усю механічну процедуру перевірки за них, і упевнені в його поручительствах за дійсність завірених їм сертифікатів. Така схема працює тільки до деякої межі в кількості користувачів PKI, перейшовши який ЦС не зможе дотримувати колишнього рівня старанності процедури перевірки. У цьому випадку стає необхідним додавання в систему додаткових «поручителів».

ЦС також може бути поручителем (позначкою-представником). Позначка-поручитель не тільки сам завіряє ключі, але надає й іншим особам (організаціям) повноваження запевняння. За аналогією з тим, як король передає свою особисту печатку або факсиміле наближеним радникам, щоб ті могли діяти від його імені, так і позначка-поручитель вповноважує інших діяти як довірених поручителів (довірених представників). Ці довірені

поручителі можуть засвідчувати ключі з тим же результатом, що і позначка-поручитель. Однак, вони не можуть створювати нових довірених поручителів.

«Позначка-поручитель» і «довірений поручитель» — це терміни PGP. У середовищі X.509 позначка-поручитель називається кореневим Центром сертифікації (root CA), а довірені поручителі — підлеглими, або проміжними, Центрами сертифікації (subordinate CAs, intermediate CAs).

Корнєвій ЦС для підписання ключів використовує закритий ключ, зв'язаний з особливим типом сертифіката, називаним кореневим сертифікатом ЦС. Будь-який сертифікат, підписаний кореневим ключем ЦС, стає достовірним будь-якому іншому сертифікатові, підписаному кореневим. Такий процес посвідчення діє навіть для сертифікатів, підписаних іншим ЦС у [зв'язаної] системі — якщо ключ проміжного ЦС підписаний ключем кореневого ЦС, будь-який сертифікат підписаний першим розцінюється вірним у межах ієрархії. Цей процес відстеження уздовж галузей ієрархії того, хто підписав які сертифікати, називається відстеженням шляху, або ланцюга, сертифікатів.

4.21 Моделі відносин довіри

У відносно закритих системах, таких як невеликі організації і фірми, можна без праці відстежити шлях сертифіката назад до кореневого ЦС. Однак, користувачам найчастіше приходиться зв'язуватися з людьми за межами їхнього корпоративного середовища, включаючи і таких, з якими вони колись ніколи не зустрічалися, наприклад, з постачальниками, споживачами, клієнтами й ін. Установлення лінії довіри з тими, хто не був явно засвідчений ЦС, стає непростою задачею.

Організації виходять з однієї з декількох моделей відносин довіри, що диктують користувачам їхньої дії по визначенню дійсності сертифікатів. Існують три різні моделі:
Пряма довіра
Ієрархічна довіра
Мережа довіри (Web of Trust)

4.22 Пряма довіра

Пряма довіра — це найпростіша з моделей відносин довіри. У цій схемі користувач переконаний, що ключ справжній, оскільки точно знає, від кого одержав цей ключ. Усі криптосистеми тією чи іншою мірою використовують цю форму довіри. Наприклад, у веб-браузерах кореневі ключі Центрів сертифікації довіряються прямо, тому що знаходилися в дистрибутиві даного програмного продукту. Якщо й існує який-небудь вид ієрархії, то він поширюється з цих сертифікатів, що прямо довіряються. У PGP користувач, що завіряє ключі самостійно, не прибігаючи до допомоги довірених поручителів, використовує схему прямої довіри.

4.23 Ієрархічна довіра

В ієрархічній системі існує ряд кореневих сертифікатів, від яких розповсюджується довіра. Ці сертифікати можуть або самі завіряти сертифікати кінцевих користувачів, або вони можуть вповноважують інші сертифікати, що будуть завіряти сертифікати користувачів по деякому ланцюзі. Представте, що це велике «дерево» довіри. Дійсність сертифікатів-„листків“ (сертифікатів кінцевих користувачів) визначається відстеженням ланцюжка до їхніх посвідчувачів, а від них уже до посвідчувачів цих посвідчувачів, і так доти, поки не буде знайдений кореневий сертифікат, що довіряється прямо.

4.24 Мережа довіри

Мережа довіри поєднує обидві попередні моделі, також привносячи принцип, що довіра є поняття суб'єктивне (що співвідноситься з життєвим представленням), і ідею про те, що чим більше інформації, тим краще. Таким чином, це накопичувальна модель довіри. Сертифікат може бути довіряємо прямо або довіряємо по деякому ланцюжку, що іде до кореневого сертифіката, що довіряється прямо, (позначці-поручителеві), або може бути завірений групою довірених поручителів.

Можливо, вам знайоме поняття «шість ступенів поділу», що означає, що будь-який індивід може встановити деякий ланцюжок до будь-якого іншого індивіда на планеті, використовуючи шість або менш чоловік як посередників. Це — мережа представників.

Таке ж і представлення PGP про довіру. PGP використовує цифрові підписи як власний вид поручительства. Коли один користувач підписує ключ іншого, він стає поручителем цього ключа (відповідає за дійсність ключа і його приналежність передбачуваному власникові). Цей процес, розширюючи, і утворить мережа довіри.

У середовищі PGP будь-який користувач може виступати як центр сертифікації. Кожен користувач може завірити відкритий ключ іншого користувача. Однак, такий сертифікат буде розцінений справжнім іншим користувачем тільки тоді, коли останній визнає завірителя своїм довіреним поручителем. (Іншими словами, ви довіряєте моїй думці про дійсність інших ключів, тільки якщо вважаєте мене своїм довіреного поручителем. У противному випадку, моя суб'єктивна оцінка дійсності чужих ключів для вас щонайменше неоднозначна.) На

зв'язуванні відкритих ключів кожного користувача утримуються такі показники:
чи вважає користувач визначений ключ справжнім;
рівень довіри, наданий користувачем визначеному ключеві, з яким його власник буде виступати поручителем у дійсності інших ключів.

Ви вказуєте на своїй копії мого ключа, наскільки вагомим вважаєте мою думку про дійсність підписаних мною ключів. Це винятково система репутації: деякі користувачі відомі тим, що ретельно перевіряють ключі і дають гарні підписи, яким люди довіряють як беззастережному показникові дійсності.

4.25 Ступені довіри в PGP

Найвищий рівень довіри — безумовна довіра (Implicit Trust) — це довіра вашій власній ключовій парі. PGP думає, що якщо ви володієте закритим ключем, те повинні довіряти і діям відповідного відкритого. Усі ключі, підписані вашим довір'ям безумовно, для вас вірні і справжні. Існує три ступені довіри, що ви можете привласнити чужому відкритому ключеві:
Повна довіра
Часткова довіра
Немає довіри

Щоб ще більше все заплутати, існує також три рівні дійсності:
Справжній
Можливо справжній
Невизначений

Щоб дати іншому ключеві повноваження поручительства, ви:

Берете справжній ключ, який або підписаний вами, або іншим довіреним поручителем.
Встановлюєте рівень довіри, який, на вашу думку, заслуговує власник.

Для прикладу представимо, що на вашому зв'язуванні є ключ Олесі. Ви визначили дійсність її ключа і, підписуючи його, указуєте на це. Вам відомо, що Олеся — активний прихильник ретельної перевірки чужих ключів. Тому ви наділяєте її Повною довірою, що, фактично, перетворює її в Центр сертифікації: якщо Олеся підпише чужий ключ, він буде вірним на вашому зв'язуванні апріорі.

PGP вимагає одну довіру Цілком або дві довірі частково, щоб встановити ключ як справжній. Метод PGP прирівнювання двох Часткових до одній Повного аналогічний тому, як іноді від вас вимагають два види документів, що засвідчують особистість. Ви можете порахувати Олесю частково надійної, також порахувати Олександра, який частково заслуговує довіри. Є ризик, що кожний з них окремо може випадково підписати липовий ключ, так що ви, імовірно, не станете надавати Повної довіри жодному. Однак, імовірність того, що обоє вони підпишуть той самий липовий ключ, досить мала.

4.26 Анулювання сертифіката

Застосування сертифіката припустиме тільки поки він достовірний. Небезпечно покладатися на те, що сертифікат буде захищений і надійний вічно. У більшості організацій і у всіх PKI сертифікат має обмежений термін «життя». Це звужує період, у який система може виявитися під погрозою, якщо сертифікат буде зламаний.

Таким чином, сертифікат створюється з визначеним заданим періодом вірогідності, що починається з дати створення і закінчується датою витікання (аналогічно терміну придатності харчових продуктів або дії прав водія). Сертифікат може бути використаний протягом усього періоду дії, після закінчення якого перестає бути вірним, оскільки вірогідність його ідентифікаційно-ключової пари більш не може бути гарантована. (Проте, сертифікат як і раніше може застосовуватися для підтвердження інформації, зашифрованої або підписаної їм раніше протягом періоду життя; однак він стає незастосовний для майбутніх криптографічних нестатків.) Але іноді з'являється потреба зробити сертифікат недійсним до закінчення терміну його життя, наприклад, у випадку звільнення власника сертифіката з дійсного місця роботи або коли у власника виникає підозра, що закритий ключ даного сертифіката був зкомпроментований. Такий процес називається відкликанням або анулюванням. Анульований сертифікат набагато підозріліший, ніж минулий. Минулий сертифікат більш непридатний до використання, однак, не несе такої погрози скомпрометованості, як анульований.

Будь-який користувач, що завірив сертифікат (що доручився за взаємозв'язку ключа і зведень сертифіката), у будь-який момент може відкликати з його свій підпис, використовуючи той же закритий ключ, яким неї створював. Відкликаний підпис указує на те, що завіритель рахував, що відкритий ключ і ідентифікаційна інформація більше не зв'язані один з одним, або що відкритий ключ сертифіката (або відповідний закритий) був скомпрометований. Відкликаний підпис має практично таке ж значення, як і анульований сертифікат.

У випадку сертифікатів X.509 відкликаний підпис фактично представляє те саме, що й анульований сертифікат, оскільки взагалі лише один підпис був поручительством дійсності

сертифіката — підпис Центра сертифікації. PGP надає додаткову можливість анулювання всього сертифіката (а не тільки підписів на ньому), якщо ви раптом порахуєте, що він був яким-небудь образом скомпрометований.

Тільки власник сертифіката (власник соотвествующего закритого ключа) або хтось, спеціально уповноважений власником (т.зв. «довірений відмінювач», designated revoker), може анулювати PGP-сертифікат. (Довіреня третій особі функції анулювання досить корисно, тому що втрата пароля до закритого ключа, що найчастіше і є приводом до анулювання, робить виконання цієї процедури самим власником сертифіката неможливої .) Сертифікат X.509 може бути відкликаний тільки його видавцем — ЦС — за запитом власника.

4.27 Повідомлення про анулювання сертифіката

Після анулювання сертифіката украй важливо сповістити всіх потенційних кореспондентів, що він більше не дійсний. Найпростіший спосіб оповіщення в середовищі PGP — це розміщення анульованого сертифіката на сервері-депозитарії; таким чином, усі, хто можуть вирішити зв'язатися з вами, будуть попереджені не використовувати цей відкритий ключ.

У середовищі PKI повідомлення про анулювання сертифікатів здійснюється за допомогою спеціального механізму, називаного реєстром анульованих сертифікатів (Certificate Revocation List, CRL), публікуючого Центром сертифікації. CRL містить датований, завірений список всіх анульованих непрострочених сертифікатів системи. Анульовані сертифікати залишаються в списку тільки до моменту свого фактичного витікання, після чого віддаляються відтіля — це запобігає нескінченному

розростанню списку. ЦС обновляє CRL через регулярні проміжки часу. Теоретично, це повинно звести до мінімуму ризик ненавмисного використання анульованого сертифіката. Хоча, усе-таки залишається імовірність випадкового застосування скомпрометованого сертифіката в тимчасовому проміжку між публікаціями CRL.

4.28 Ключова фраза

Більшість користувачів як знак обмеження доступу до комп'ютера або комп'ютерних ресурсів використовують пароль, що являє собою унікальну послідовність символів, що вводиться як ідентифікаційний код.

PGP використовує ключову фразу щоб зашифрувати ваш закритий ключ. Закритий ключ зберігається на диску, зашифрований хеш-значенням ключової фрази як симетричним таємним ключем. Ви ж використовуєте ключову фразу, щоб розшифрувати і застосовувати закритий ключ. Ключова фраза повинна бути такою, щоб вам було її важко забути, а іншим — здогадатися. Вона повинна бути чимось, вже давно і надійно зберігається в довгостроковій пам'яті вашого мозку, а не придуманим з нуля. Чому? Тому що якщо ви забудете ключову фразу — ви у великому лиху. Закритий ключ абсолютно і зовсім марний без його ключової фрази, і з цим нічого не можна поробити. Пам'ятаєте цитату на початку? PGP — це криптографія, що не дозволить урядам могутніх держав читати ваші файли. І тим більше вона не дозволить читати їх вам. Врахуйте це, якщо раптом вирішите змінити ключову фразу на уривок з анекдоту, який ніколи не могли толком запам'ятати.

4.29 Поділ ключа

Говорять, що секрет — це вже не секрет, коли його знають два чоловіки. Поділ закритого ключа спростовує така думка. Хоча це і практика, що не рекомендується, поділ закритого ключа у визначених ситуаціях буває необхідно. Наприклад, корпоративні ключі підписання (Corporate Signing Keys, CSK) — це особливо важливі закриті ключі, використовувані організацією, наприклад, для запевняння правових документів, особистої інформації співробітників або прес-релізів для посвідчення авторства. У даному випадку буде корисно, щоб кілька членів компанії мало доступ до закритого ключа. Але це буде значити, що кожний із членів команди зможе вільно і повною мірою виступати від імені компанії.

Рішенням подібної проблеми є поділ і розподіл закритого ключа між декількома особами таким чином, що для відновлення його в робочий стан потрібно присутність більше одного або двох хоронителів частин (часток) ключа.

5 . Віруси та антивірусні програми

5.1 Компютерний вірус

Масове використання ПК у мережному режимі, включаючи вихід у глобальну мережу Інтернет, породило проблему зараження їхніми комп'ютерними вірусами.

Комп'ютерним вірусом прийнято називати спеціально написану, звичайно невелику по розмірах програму, здатну мимовільно приєднуватися до інших програм (тобто заражати їх), створювати свої копії (не обов'язково цілком співпадаючі з оригіналом) і впроваджувати їх у файли, системні області комп'ютера й в інші об'єднані з ним комп'ютери з метою порушення нормальної роботи програм, псування файлів і каталогів, створення різних перешкод при роботі на комп'ютері.

Уперше термін «комп'ютерний вірус» ужив співробітник Лехайского університету (США) Ф. Коэн у 1984 р. на 7-й конференції по безпеці інформації, що проходила в США. Однак перше згадування про подібний тип програмах для ЕОМ відноситься до середини минулого сторіччя. Саме тоді американські вчені Джон фон Нейман і Норберт Вінер, займаючись проблемами алгоритмічного забезпечення і програмного керування ЕОМ, відкрили можливість саморозмноження штучних алгоритмічних конструкцій, тобто програмного коду.

Відповідно до підготовленого Російська аналітична центром «Лабораторія Касперського» звіту-огляду вірусної активності за 2002 р. в усьому світі інтенсивність вірусних інцидентів (тобто повідомлень компаній і приватних осіб

про те, що вони піддалися атаці комп'ютерних чи вірусів інших шкідливих кодів) постійно росте. Одночасно збільшується і збиток, нанесений світовому співтовариству цими створюваними людиною програмами. Так, у 2002 р. цей збиток оцінювався майже в 14,5 млрд дол., перевищивши аналогічний показник 2001 р. майже на 10%, а в 2000 р., по підрахунках фахівців, ця цифра була ще вище -17,1 млрд дол.

У 2002 р. було зафіксовано 12 великих і 34 менш значних вірусних епідемій. При цьому, по опублікованим даної (www.messagelabs.com),кількість вірусів, що пересилаються по електронній пошті, за рік виросло в два рази, і нині злобливі коди містяться приблизно в кожнім 200-м листі. Самими шкідливими програмами в 2002 р. виявилися програми «поштові хробаки» (понад 61% від загального числа випадків) і макровіруси Word97 (близько 2%). Ненецікаво, що віруси «поштові хробаки» уперше з'явилися в 1998 р.

Світова практика комп'ютерної вірусології свідчить, що основним джерелом погрози для організацій і приватних осіб залишається електронна пошта. З нею зв'язано понад 96% усіх зареєстрованих у 2002 р. випадків. Через електронну пошту до персональних комп'ютерів добираються не тільки «мережні хробаки», але і звичайні віруси, у тому числі «троянські коні». Через інші служби Інтернету, до приклада через FTP, IRC, відсоток зараження комп'ютерів вірусами складав 2,3%. Більш низок відсоток зараження комп'ютерів вірусами через заражені мобільні нагромаджувачі інформації (флопи-, CD-, магнітооптичні й інші диски).

. Спосіб функціонування більшості вірусів - це така зміна системних файлів комп'ютера, щоб вірус починав свою діяльність при кожнім завантаженні. Деякі віруси інфікують файли завантаження системи, інші спеціалізуються на EXE-, COM- і інших програмних файлах. Усякий раз, коли користувач копіює файли на

гнучкий чи диск посилає інфіковані файли по модему, передана копія вірусу намагається установити себе на новий диск.

Звичайно вірус розробляється так, щоб він з'явився, коли відбувається деяка подія виклику, наприклад п'ятниця 13-і, інша дата, визначене число перезавантажень зараженого чи якогось конкретного додатка, відсоток заповнення твердого диска й ін.

Після того як вірус виконає потрібні йому дії, вона передає керування тій програмі, у якій він знаходиться, і її робота якийсь час не відрізняється від роботи незараженої. Усі дії вірусу можуть виконуватися досить швидко і без видачі яких-небудь повідомлень, тому користувач часто і не зауважує, що комп'ютер працює з «дивинами». До ознак появи вірусу можна віднести:

• уповільнення роботи комп'ютера;

• неможливість завантаження операційної системи;

• часті «зависання» і збої в роботі комп'ютера;

• припинення чи роботи неправильну роботу раніше що успішно функціонували програм;

• збільшення кількості файлів на диску;

• зміна розмірів файлів;

• періодична поява на екрані монітора недоречних повідомлень;

• зменшення обсягу вільної оперативної пам'яті;

• помітне зростання часу доступу до твердого диска;

• зміна дати і часу створення файлів;

• руйнування файлової структури (зникнення файлів, перекручування каталогів і ін.);

• загоряння сигнальної лампочки дисковода, коли до нього немає звертання, і ін.

Треба помітити, що названі симптоми необов'язково викликаються комп'ютерними вірусами, вони можуть бути наслідком інших причин, тому комп'ютер варто періодично діагностувати.

У багатьох країнах діють законодавчі заходи для боротьбі з комп'ютерними злочинами і злочинними діями, розробляються антивірусні програмні засоби, однак кількість нових програмних вірусів зростає. Обличчя, що використовують свої знання і досвід для несанкціонованого доступу до інформаційних і обчислювальних ресурсів, до одержання конфіденційної і секретної інформації, до здійснення шкідливих дій, називають хакерами.

Діяльність хакерів найчастіше буває соціально небезпечної. У червні 1987 р. спецслужбами ФРН був арештований М. Шпеер, «взломавший» комп'ютерну систему військової бази в Алабамі, що зберігала зведення про боєздатність ракет великої дальності, інформаційну мережу ЦРУ, банк даних Пентагона й інших державних установ. У листопаду 1988 р. аспірант факультету інформатики Корнелського університету (США) Р.Моррис запустив у мережу Інтернет вірус-хробак, названий згодом «вірусом Морриса». Протягом декількох годин програма заразила близько 6000 ЕОМ, у тому числі військової мережі Міністерства оборони США, що працювали під керуванням операційної системи UNIX. Покарання за це діяння в суді було зм'якшено тими доводами, що програма-вірус створювалася для перевірки захисту комп'ютерів, і небажані наслідки виникли через технічну помилку, допущеної автором програми.

У травні 2000 р. вірус за назвою «I love you» (Я тебе люблю), написаний студентом з Філіппін і розповсюджений по електронній пошті, вразив 3,1 млн персональних комп'ютерів у США і країнах Європи. Збиток від цієї витівки для фірм, по оцінках фахівців, склав 8,7 млрд дол., а також приніс масу неприємностей простим користувачам. Зараженими виявилися навіть комп'ютерні системи британського парламенту й американського конгресу.

За даними фахівців в області комп'ютерної економіки, у 2002 р. збиток від комп'ютерних вірусів великого бізнесу (компаній, що входять у список Fortune 500) склав 14,5

млрд дол. Реальні ж збитки з урахуванням інших компаній, державних структур і приватних осіб значно вище.

За більш деталізованою схемою класифікації комп'ютерних зловмисників поділяють на хакерів (hacker), кракерів (cracker) і фрикерів (phracer).

Дії хакерів, чи комп'ютерних хуліганів, можуть наносити істотна шкода власникам комп'ютерів і власникам (творцям) інформаційних ресурсів, тому що приводять до простоїв комп'ютерів, необхідності відновлення зіпсованих даних або до дискредитації юридичних чи фізичних осіб, наприклад, шляхом перекручування інформації на електронних дошках чи оголошень на Web-серверах в Інтернету. Мотиви дій комп'ютерних зловмисників усілякі: прагнення до фінансових придбань; бажання нашкодити і помститися керівництву організації, з якої по тим чи іншим причинам звільнився співробітник; психологічні риси людини (заздрість, марнославство, бажання виявити свою технічну перевагу над іншими, просто хуліганство й ін.).

Основними шляхами зараження комп'ютерів вірусами є знімні диски (дискети і CD-ROM) і комп'ютерні мережі. Зараження твердого диска комп'ютера може відбутися при завантаженні комп'ютера з дискети, що містить вірус. Для посилення безпеки необхідно звертати увага на те, як і відкіля отримана програма (із сумнівного джерела, чи мається наявність сертифіката, чи експлуатувалася раніш і т.д.). Однак головна причина зараження комп'ютерів вірусами - відсутність в операційних системах ефективних засобів захисту інформації від несанкціонованого доступу.

За даними спеціальної літератури, у світовій практиці було зареєстровано близько 70 тис. комп'ютерних вірусів, і щотижня з'являються нові віруси. Одна зі схем класифікації комп'ютерних вірусів представлена на мал. 11.2.

Рис. 11.2. Класифікація комп'ютерних вірусів

У залежності від середовища обитания віруси класифікуються як завантажувальні, файлові, системні, мережні, файлово-загрузоні.

Завантажувальні віруси впроваджуються в завантажувальний сектор чи диска в сектор, що містить програму завантаження системного диска.

Файлові віруси впроваджуються в основному у файли, що виконуються, з розширенням .COM і .EXE.

Системні віруси проникають у системні модулі і драйвери периферійних пристроїв, таблиці розміщення файлів і таблиці розділів.

Мережні віруси живуть у комп'ютерних мережах; файлово-загрузочні (багатофункціональні) уражають

завантажувальні сектори дисків і файли прикладних програм.

По способі зараження середовища обитания віруси підрозділяються на резидентні і на нерезидентні.

Резидентні віруси при зараженні комп'ютера залишають в оперативній пам'яті свою резидентну частина, що потім перехоплює звертання операційної системи до інших об'єктів зараження, впроваджується в них і виконує свої руйнівні дії аж до чи вимикання перезавантаження комп'ютера. Нерезидентні віруси не заражають оперативну пам'ять ПК і є активними обмежений час.

Алгоритмічна особливість побудови вірусів впливає на їхній прояв і функціонування. Так, репликаторні програми завдяки своєму швидкому відтворенню приводять до переповнення основної пам'яті, при цьому знищення програм-реплікаторів ускладнюється, якщо відтворені програми не є точними копіями оригіналу. У комп'ютерних мережах поширені програми-хробаки. Вони обчислюють адреси мережних комп'ютерів і розсилають по цих адресах свої копії, підтримуючи між собою зв'язок. У випадку припинення існування «хробака» на якому-небудь ПК що залишилися відшукують вільний комп'ютер і впроваджують у нього таку ж програму.

«Троянський кінь» - це програма, що, маскуючи під корисну програму, виконує доповнюючі функції, про що користувач і не догадується (наприклад, збирає інформацію про імена і паролі, записуючи їх у спеціальний файл, доступний лише творцю даного вірусу), або руйнує файлову систему.

Логічна бомба - це програма, що вбудовується у великий програмний комплекс. Вона нешкідлива до настання визначеної події, після якого реалізується її логічний механізм. Наприклад, така вірусна програма починає працювати після деякого числа прикладної програми, комплексу, при чи наявності відсутності визначеного чи файлу запису файлу і т.д.

Програми-мутанти, самовідтворюючи, відтворюють копії, що явно відрізняються від оригіналу.

Віруси-невидимки, чи стелс-віруси, перехоплюють звертання операційної системи до уражених файлів і секторів дисків і підставляють замість себе незаражені об'єкти. Такі ' віруси при звертанні до файлів використовують досить оригінальні алгоритми, що дозволяють «обманювати» резидентні антивірусні монітори.

Макровіруси використовують можливості макромов, убудованих в офісні програми обробки даних (текстові редактори, електронні таблиці і т.д.).

По ступені впливу на ресурси комп'ютерних систем і мереж, чи по деструктивних можливостях, виділяються нешкідливі, безпечні, небезпечні і руйнівні віруси.

Нешкідливі віруси не роблять руйнівного впливу на роботу ПК, але можуть переповняти оперативну пам'ять у результаті свого розмноження.

Безпечні віруси не руйнують файли, але зменшують вільну дискову пам'ять, виводять на екран графічні малюнки, створюють звукові ефекти і т.д. Небезпечні віруси нерідко приводять до різних серйозних порушень у роботі комп'ютера; руйнівні - до стирання інформації, повному чи частковому порушенню роботи прикладних програм. Необхідно мати у виді, що будь-який файл, здатний до завантаження і виконання коду програми, є потенційним місцем, куди може упровадитися вірус.

5.2 Антивірусні програми

Масове поширення комп'ютерних вірусів викликало розробку антивірусних програм, що дозволяють виявляти і знищувати віруси, «лікувати» заражені ресурси.

В основі роботи більшості антивірусних програм лежить принцип пошуку сигнатури вірусів. Вірусна сигнатура - це деяка унікальна характеристика вірусної

програми, що видає присутність вірусу в комп'ютерній системі.

Звичайно в антивірусні програми входить періодично обновлювана база даних сигнатур вірусів. Антивірусна програма переглядає комп'ютерну систему, проводячи порівняння і відшукуючи відповідність із сигнатурами в базі даних. Коли програма знаходить відповідність, вона намагається вичистити виявлений вірус.

По методу роботи антивірусні програми підрозділяються на фільтри, ревізора-доктора, детектори, вакцини й ін.

Програми-фільтри, чи «сторожа», постійно знаходяться в оперативній пам'яті, будучи резидентними, і перехоплюють усі запити до операційної системи на виконання підозрілих дій, тобто операцій, використовуваних вірусами для свого розмноження і псування інформаційних і програмних ресурсів у комп'ютері, у тому числі для переформатування твердого диска. Такими діями можуть бути спроби зміни атрибутів файлів, корекції виконува COM- чи Exe-файлов, запису в завантажувальні сектори диска й ін.

При кожнім запиті на таку дію на екран комп'ютера видається повідомлення про те, яке дія викликана і яка програма бажає його виконувати. Користувач у відповідь на це повинен або дозволити виконання дії, або заборонити його. Подібна часто повторювана «настирливість», що дратує користувача, і те, що обсяг оперативної пам'яті зменшується через необхідність постійного перебування в ній «сторожа», є головними недоліками цих програм. До того ж програми-фільтри не «лікують» чи файли диски, для цього необхідно використовувати інші антивірусні програми.

Надійним засобом захисту від вірусів вважаються програми-ревізори. Вони запам'ятовують вихідний стан програм, каталогів і системних областей диска, коли комп'ютер ще не був заражений вірусом, а потім періодично

порівнюють поточне стан з вихідним. При виявленні невідповідностей (по довжині файлу, даті модифікації, коду циклічного контролю файлу й ін.) повідомлення про це видається користувачу.

Програми-доктора не тільки виявляють, але і «лікують» заражені чи програми диски, «выкусывая» із заражених програм тіло вірусу. Програми цього типу поділяються на фаги і поліфаги. Останні служать для виявлення і знищення великої кількості різноманітних вірусів.

Програми-детектори дозволяють виявляти файли, заражені одним чи декількома відомими розроблювачам програм вірусами.

Чи вакцини імунізатори, відносяться до резидентним програм. Вони модифікують програми і диски таким чином, що це не відбивається на роботі програм, але вірус, від якого виробляється вакцинація, вважає їхній уже зараженими і не впроваджується в них.

До дійсного часу закордонними і вітчизняними фірмами і фахівцями розроблена велика кількість антивірусних програм. Багато хто з них, що одержали широке визнання, постійно поповнюються новими засобами для боротьби з вірусами і супроводжуються розроблювачами.

У російських користувачів персональних комп'ютерів відомою популярністю користається антивірусний комплект ЗАТ «Діалог-Наука» - сімейство антивірусних програм Doctor Web.

Комплексний антивірус Doctor Web містить у собі компоненти, що забезпечують різні рівні боротьби з комп'ютерними вірусами :

• для захисту корпоративних мереж;

• для захисту робочих станцій;

• для захисту автономних комп'ютерів (домашнє користування);

• для реалізації спеціалізованих рішень.

Сімейство Doctor Web включає антивіруси для ряду операційних систем, включаючи Windows 95/98/Me/NT/2000/XP, DOS, OS/2, Novell NetWare, Linux, FreeBSD, Solaris (Intel) і ін.

Програма-антивірус Doctor Web призначен для пошуку і виявлення файлових, завантажувальних і файлово-загрузочних вірусів. Особливістю програми є закладені в ній три методи, що дозволяють виявляти віруси: по їх сигнатурі, за допомогою евристичного аналізатора, з використанням емулятора процесора.

Пошук вірусів по сигнатурі (інша назва цього процесу - сканування вірусів) дозволяє дуже швидко знайти набір вірусних зразків, уже відомих розроблювачу антивірусної програми. Використання ж евристичного аналізатора дозволяє виявляти такі віруси, сигнатури яких відсутні в антивірусній базі. Прийом емуляції процесора забезпечує боротьбу зі складними шифрованими і поліморфними вірусами.

Особливою властивістю сімейства програм Doctor Web є модульний принцип побудови, що забезпечує можливість їхньої роботи на різних програмних платформах. Програма включає оболонку, орієнтовану на роботу в конкретному середовищі; ядро, що не залежить від середовища, і вірусну базу, регулярно поповнювану. Така структура дозволяє ті самі файли вірусної бази Doctor Web використовувати для різних програмних платформ, підключати ядро до різних оболонок і додатків, а також реалізувати механізм автоматичного поповнення вірусних баз і відновлення версій оболонки і ядра через мережу Інтернет.

Антивірусний сканер. **Doctor Web** для Windows 95/98/Me/NT/ **2000/XP** перевіряє файли, каталоги і диски комп'ютера на основі установок користувача. Також забезпечується повна перевірка всієї пам'яті комп'ютера, включаючи системну і пам'ять усіх віртуальних машин у середовищі NT/2000/XP. Цей сканер знаходить і

знешкоджує складні з вірусами «троянський кінь» програми, у тому числі «» паролі, щокрадуться, для доступу в Інтернет.

Антивірусна програма SplDer Guard для Windows 95/98/Me/ NT/2000/XP орієнтована на організацію захисту персонального комп'ютера від вірусів і являє собою резидентний сторож, тобто програма постійно знаходиться в пам'яті комп'ютера. Сторож **SplDer** використовує те ж ядро і вірусну базу, що і всі сканери сімейства Doctor Web, але може робити всі перевірки автоматично, не відволікаючи користувача на спеціальні дії по забезпеченню антивірусної безпеки. Програма не тільки виявляє і лікує усі відомі віруси (завантажувальні, файлові, макрокомандні, HTML-віруси), але і здійснює перевірку упакованих файлів і архівів, перевірку і видалення вірусів з оперативної пам'яті.

Вхідна до складу сімейства антивірусна програма Doctor Web для Novell NetWare запускається на сервері модуль, що як завантажується, у середовищі мережної операційної системи Novell NetWare версій від 3.11 до 5.1. Вона дозволяє проводити перевірку томів сервера по заздалегідь заданому розкладі; здійснювати перевірку прихожих на сервер і файлів, що ідуть з його; оповіщати адміністратора про виявлені інфіковані і підозрілі файли, вести протокол перевірки; вибирати тому, каталоги і файли, що підлягають перевірці, і др.

У 2001 р. у сімействі Doctor Web з'явився новий компонент для роботи в середовищі досить мало використовуваних операційних систем Linux, FreeBSD і Solaris, названий програмою-демоном Dr. Web. Зовнішнього антивірусного фільтра, що підключається в якості, ця програма перевіряє минаючі через поштовий сервер повідомлення електронної пошти, а також організує добір «комп'ютерного сміття», виступаючи як спамфильтр.

У листопаду 2002 р. розроблений антивірусний модуль Dr. Web для The Bat! для забезпечення

антивірусного захисту при роботі з поштовими повідомленнями в поштовій програмі The Bat!. Цей модуль дозволяє перевіряти на наявність вірусів вхідну пошту при її одержанні і при відкритті вкладення. При виявленні вірусу модуль у залежності від настроювання в поштовій програмі The Bat! (меню «Властивості», пункт «Антивірусний захист») може зробити одне з наступних дій:

• перемістити лист у спеціальну поштову папку «Карантин» для наступного аналізу;

• спробувати вилікувати заражені частини листа;

• видалити заражені частини з листа;

• видалити лист цілком.

У боротьбі з комп'ютерними вірусами дуже важлива швидкість реакції - чим швидше створюється «вакцина» проти нового вірусу, тим більша кількість комп'ютерів і інформації, що знаходиться на них, удається врятувати. З жовтня 2000 р. доповнення вірусної бази Doctor Web виходять регулярно. При цьому щоденне і щотижневе доповнення доступні на сторінці Web-сервера цієї компанії (www.DialogNauka.ru/dsav/russian/add-on).

З програмою Doctor Web можна працювати як у режимі повноекранного інтерфейсу з використанням меню і діалогових вікон, так і в режимі командного рядка. При роботі в режимі повноекранного інтерфейсу після запуску антивірусної програми користувач використовує необхідні установки через пункти основного меню: Тест Настроювання Доповнення.

Перехід на операційні системи Windows NT/2000 породив проблеми з захистом від вірусів, створюваних спеціально для цього середовища. Крім того, з'явився новий різновид інфекції - макровіруси, «вживляемые» у документи, підготовлювані текстовим процесором Word і електронними таблицями Excel. Відомими антивірусними програмами є AntiViral Toolkit Pro (A VP32), Norton Antivirus Sophos SWEEP, Thunder BYTE Antivirus Utilities і

ін. Ці програми працюють у виді програм-сканерів і проводять антивірусний контроль оперативної пам'яті, папок і дисків, містять алгоритми для розпізнавання нових типів вірусів, дозволяють у процесі перевірки лікувати файли і диски.

Програма AntiViral Toolkit Pro (A VP32) є 32-розрядним додатком, що працює в середовищі Windows NT, має зручний користувальницький інтерфейс, систему допомоги, гнучку систему настроювань, обираних користувачем, розпізнає більш 7 тис. різних вірусів. Для роботи цієї програми комп'ютер повинний мати не менш 4 Мбайт оперативної пам'яті і не менш 2 Мбайт вільного місця на твердому диску. AntiViral Toolkit Pro розпізнає (детектують) і видаляє поліморфні віруси, віруси-мутанти і віруси-невидимки, макровіруси, що заражають документ Word і таблиці Excel, об'єкти Access - «троянські коні».

Важлива особливість цієї програми складається в можливості контролю усіх файлових операцій у системі у фоновому режимі і виявленні вірусів до моменту реального зараження системи, а також у можливості детектирования вірусів усередині архівів формату ZIP, ARJ, ZHA, RAR.

З огляду на розвиток локальних комп'ютерних мереж, електронної пошти і мережі Інтернет і впровадження мережний ОС Windows NT, розроблювачами антивірусних програм розроблені і поставляються на ринок такі програми, як Mail Checker - для перевірки вхідної і вихідної електронної пошти, AntiViral Toolkit Pro для Novell NetWare (A VPN) - для виявлення, лікування, видалення і переміщення в спеціальний каталог уражених вірусом файлів при роботі з мережний ОС Novell NetWare версій 3.x і 4.x.

AVPN працює як антивірусний сканер і фільтр, постійно контролюючи файли, що зберігаються на сервері. У режимі фільтра скануються на наявність відомих файлових вірусів файли, що приходять на сервер і виходять із сервера (у тому числі що запускаються і що зчитуються),

у режимі сканера відбувається негайне чи автоматичне сканування томів сервера.

AVPN має можливість видаляти, переміщати і «лікувати» заражені об'єкти; перевіряти упаковані й архівні файли; детектувати невідомі віруси за допомогою евристичного механізму; перевіряти в режимі сканера вилучені сервери; відключати заражену станцію від мережі і т.д.

Крім того, AVPN легко набудовується для сканування файлів різних типів; має зручну схему поповнення антивірусної бази; посилає повідомлення про зараження сервера вірусом по мережі, електронній пошті і на пейджер; здійснює автоматичне ведення файлу-звіту про виконувані операції і керування програмою з робочої станції.

Література

1. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ – Петербург; Арлит 2002. – 496 с.;

2. Баранов В М. и др. Защита информации в системах и средствах информатизации и связи. Учебное пособие. – СПб.: 1996. – 111 с.

3. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика. – 1997. – 364 с.

Використана література

4. Коваленко Микола Миколайович Комп"ютерні віруси і захист інформації.- К: Наукова думка, 1999.- 268с.

5. Законодавчі та нормативні документи України у сфері інформації, видавничої та бібліотечної справи: Тематична добірка: У 2-х ч. Ч. 1. Правове регулювання у сфері інформації/ Укл. Т.Ю.Жигун.- 2-ге вид., доп.- К.: Книжкова палата України, 2002.- 124с.- 13.00

6. Кулик, Анатолій Ярославович Адаптивні алгоритми передавання інформації: Монографія.- Вінниця: Універсум, 2003.- 214с.- 18.00

Андрій Володимирович Погребняк,
спеціаліст системотехнік, магістрант
інформаційних технологій

ТЕХНОЛОГІЇ КОМП'ЮТЕРНОЇ БЕЗПЕКИ

КНИГА 3

ІН 11М

Комп'ютерний набір, верстка і макетування та дизайн в редакторі Microsoft®Office® Word 2003
А.В.Погребняк. Науковий керівник Р. М. Літнарович, доцент, кандидат технічних наук

Міжнародний Економіко-Гуманітарний Університет ім. акад. Степана Дем'янчука

Кафедра математичного моделювання
33027,м.Рівне,Україна
Вул.акад. С.Дем'янчука,4, корпус 1
Телефон:(+00380) 362 23-73-09
Факс:(+00380) 362 23-01-86
E-mail:mail@regi.rovno.ua
E-mail: angel1990_07@mail.ru