РОЗДІЛ IV. АКТУАЛЬНІ ПРОБЛЕМИ БОРОТЬБИ З ЕКОНОМІЧНОЮ ЗЛОЧИННІСТЮ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Глава 13. Проблеми забезпечення інформаційної безпеки у віртуальній економіці

Вступ людства в інформаційний етап розвитку супроводжується зсувом центру ваги економічної злочинності зі звичайної у віртуальну економіку. Американці прорахували, що середні збитки від шахрайства проти банків на порядок вищі від звичайних грабежів, але збитки від електронного злочину ще на порядок вищі в порівнянні з шахрайством.

Наприклад, за 2002 рік у США більше 42 тисяч користувачів Інтернету стали жертвами інтернет-шахраїв, а збитки від їх дій склали 54 мільйони доларів. Про це говориться в дослідженні, що було проведено американським Центром боротьби з інтернет-шахрайством (The Internet Fraud Complaint Center), повідомляє Washington Profile.[1]

Інтернет-технології сьогодні все більше розповсюджуються і в Україні: в банківській справі, внутрішній та зовнішній торгівлі, виробництві, наукових дослідженнях тощо. Вже наприкінці 90-х рр. український Інтернет нараховував більше 200 тис. користувачів, було створено понад 3000 Web-сайтів, а швидкісні канали, що обслуговують міжнародній трафік, мали пропускну спроможність більше 10 Мбіт/с[2]. При цьому передує в освоєнні віртуальних технологій в економіці тіньовий і кримінальний бізнес Але, перед тим, як розглянути специфіку проявів загроз і небезпек, засобів захисту від них, необхідно визначитись з сутністю і характерними рисами інтернет-технологій в економіці, тобто віртуальною економікою.

Поняття "віртуальна економіка" є відносно новим в сучасній науковій літературі і, на жаль, має подвійне трактування.

Деякі автори віртуальним вважають сектор економіки (переважно державний, адміністративно-бюрократичний), в якому обер-

[1] Джерело: www.lenta.ru

[2] Див.:Біленчук П.Д., Романюк Б.В. та ін. Комп'ютерна злочинність. – К., Атіка, 2002. - С. 33.

тається фіктивна вартість, тобто знищується реальна вартість, що створена в реальному секторі національного господарства.[3]

Економісти-кібернетики та інформатики вважають, і ми поділяємо цю точку зору, що ***віртуальна економіка – це економіка, в основі якої лежить головний економічній закон організації життя людського суспільства – закон економії часу та інтерактивний бізнес.***

Віртуальна економіка – складова частина реальної економіки, вона функціонує за тими ж принципами і законами. Завдяки їй мінімізуються витрати на трансакції і реалізується можливість проведення інтерактивного бізнесу за допомогою всесвітньої мережі Інтернет (World Wide Web), інтра-, екстра- та інших локальних мереж, мобільного зв'язку. Разом з тим, віртуальна економіка має власні характерні особливості:

- ***вона*** охоплює все світове господарство за допомогою WWW, ***створює*** тим самим ***глобальний ринок***;
- ***ринок віртуальної економіки асиметричний***: в ньому одному з учасників (продавцю або покупцю) відомо про товар більше, ніж іншому тому, що використовується асиметрична інформація;
- ***симетричність віртуального ринку забезпечується*** ринковими сигналами, іміджем продавця або покупця, поручительством, гарантіями.[4]

Основною формою існування віртуальної економіки є Електронна Комерція, під якою розуміється будь-яка форма бізнес-процесу, де взаємодія між суб'єктами здійснюється електронним чином і супроводжується фізичною доставкою матеріальних ресурсів чи продукції. Електронна торгівля є частиною Електронної Комерції і найбільш активно розвивається в мережах Інтернету.

Як відомо, електронна комерція почала розвиватися разом з появою мережної обробки і передачі даних. Цьому значною мірою сприяє відсутність митних рогаток. Не випадково в США електронний business називають «Офшорною зоною Америки».

Ось ще декілька переваг розвитку електронного бізнесу: передусім, прибутковий ринок, висока швидкість обороту капіталу та економічність. Це забезпечується немаловажними моментами організації віртуальної економіки, пов'язаних з:

---

[3] Джерело: Gaddy C., Ickes B. Russia's Virtual Economy // Foreing Affairs. – 1998.- Vol. 77. - № 5; Тимченко Б.П. Вплив тіньової економіки на формування доходів населення в умовах ринкової трансформації. Дисерт. На здобуття наукового ступ. Канд. Екон. наук. – Харків, Харк. нац. ун-т ім. В.Н.Каразіна. – 2003. - С. 57.

[4] Див.: Балабанов И.Т. Электронная коммерция. – СПб.: Питер. 2001. - С. 68-71.

– наявністю недорогих електронних інструментів для прямої і непрямої реклами;

– дешевизною Інтернету, як способу передачі і публікації рекламної й іншої інформації;

– єдиною інфраструктурою публікації і пошуку даних, обміну повідомленнями;

– високими темпами росту аудиторії Інтернету;

- врешті-решт модою на Інтернет і ажіотажним попитом на інтернет-проекти[5].

Окрім того, сьогодні відбувається інтенсивний процес подолання митних бар'єрів у віртуальній економіці, що несе в собі величезні переваги для суб'єктів економічної діяльності. Спеціалізована комісія ООН ще в 1996 році оприлюднила акт про безмитну електронну торгівлю і міжнародний торговий арбітраж. Безмитну електронну торгівлю з 1 січня 1998 року ведуть країни ЄС і США. Рішення про введення безмитної електронної торгівлі в травні 1998 року прийняла і Всесвітня торгова організація, членом якої готується стати й Україна. Варто додати, що віртуальна економіка функціонує 24 години на добу, без вихідних і відпусток, 365 діб на рік.

З точки зору формування безпечних умов праці в віртуальній економіці мають не абияке значення всі визначені вище її особливості.

Становлення віртуальної економіки супроводжується створенням **глобальної інформаційної інфраструктури,** у якої користувачам надається вільний доступ до величезних масивів економічної інформації в будь-який час і в будь-якому місці. Природно, що для країни інтеграція власної економіки в віртуальну економіку **є показником її розвитку.** Чим вищий рівень розвитку власної інфраструктури віртуальної економіки, тим вищий ефект, який одержується від інтеграції з всесвітньою, глобальною інфраструктурою.

Разом з тим, формування і розвиток віртуальної економіки супроводжується цілою низкою "хвороб" і злочинів, таких як шахрайство, незаконне підприємництво у всіх його формах, авантюризм, дилетантизм і т.д. і т.п. Підвищений інтерес злочинців до віртуальної економіки як джерела одержання доходів протиправними засобами викликається такими її рисами, як висока прибутковість,

---

[5] Березин А.С. Сучасні системи захисту інформації: погляд розроблювача // Информационная безопасность России в условиях глобального информационного общества 2-я Всероссийская конференция 18 июня 2001 года.

асиметричність ринку, широке поле економіки, яке охоплюється інтернет-технологіями. Звичайно, можна ремствувати на діяльність правоохоронних органів, на втрату моральних принципів бізнесменами в період становлення ринку. Але можна викорінити причини й умови, що створюють грунт для виростання даних болячок. Для цього необхідна інформаційна відкритість ринку, можливість інформаційно-аналітичного забезпечення прийняття управлінських рішень у бізнесі та ефективний захист інтернет-технологій. Розв'язання цієї проблеми підвищить і ефективність бізнес-процесів у віртуальній економіці, і рейтинг інвестиційної привабливості України. Крім того, буде реалізоване гарантоване Конституцією право громадян на доступ до інформації.

Потреба в інформації в умовах становлення віртуальної економіки викликала до життя широке коло інформаційних компаній, що добувають цю інформацію і надають її клієнтам. При цьому, відомо, що в такій зразково поліцейській країні як США мінімум необхідної інформації можна одержати з доступних масивів у режимі «on-line» за кілька хвилин і 10–30 доларів.[6] Але в демократичній Україні – за кілька тижнів і кілька сотень доларів. Це відтинає від інформаційного забезпечення малий бізнес через високі ціни, а також великий бізнес при угодах, що мають швидкоплинний характер.

Створення великих масивів інформації, що характеризують віртуальні ринки та їхніх суб'єктів, об'єднання їх у єдину систему на базі сучасних телекомунікаційних технологій для зручності доступу клієнта і взаєморозрахунків із власниками окремих масивів, виявляється рішучою передумовою розвитку віртуальної економіки, забезпечення її безпеки.

Але, **розвиток віртуальної економічної інфраструктури неминуче супроводжується появою нових чи видозміною старих проблем,** нерозв'язаність яких приводить до зниження її ефективності і зростання економічної небезпеки з усіма протиправними наслідками. Інфраструктура віртуальної економіки надає широкі можливості не тільки для розвитку національної економіки та інших прогресивних тенденцій, але також і для розвитку економічної злочинності. Розвиток інтернет-технологій в віртуальній економіці

---

[6] Минаев С.Ю. Рух до інформаційної прозорості ринку, як необхідна умова його інвестиційної привабливості // Информационная безопасность России в условиях глобального информационного общества 2-я Всероссийская конференция 18 июня 2001 года.

супроводжується виникненням так званої **«інформаційної зброї»**[7], спрямованої на економічний потенціал як національного господарства, так і окремих суб'єктів економічної діяльності.

Ця інформаційна зброя використовується в віртуальній економіці з метою досягнення певних політичних і соціально-економічних цілей, отримання матеріальних вигод. Її можуть використати державні і приватні розвідувальні та контррозвідувальні служби, окремі фізичні особи, які працюють, або не працюють за наймом, перебувають на пенсії, в шкільному віці, особи, які не є в повній мірі дієздатними.

Персональні мотиви використання інформаційної зброї в віртуальній економіці пов'язані, більше всього, з отриманням матеріальних вигод, здійсненням персональної помсти, спробами спричинити хаос в суспільному устрою, створити саморекламу.

Злочинність в віртуальній економіці розвивається в двох напрямках:

1. Крадіжки результатів угод між суб´єктами електронної комерції.

За кордоном, де найбільш широко розвивається електронна комерція, вартість угоди звичайно обмежуються середньою вартістю у 300–400 доларів, щоб мінімізувати можливі втрати. Це викликається недостатнім рішенням проблем інформаційної безпеки в мережах інформаційних систем віртуальної економіки. Бурхлива інформатизація, розвиток тенденцій розподіленої обробки даних на базі сучасних засобів обчислювальної техніки супроводжуються виникненням нових чи видозміною старих проблем, що є негативними супутниками технічного прогресу. За оцінкою Комітету ООН з попередження злочинності і боротьби з нею, комп'ютерна злочинність вийшла на рівень однієї з міжнародних проблем. У США цей вид злочинної діяльності по прибутковості займає третє місце після торгівлі зброєю і наркотиками.

2. Кримінальні дії в інформаційній системі з метою отримання конфіденційної інформації для вчинення фінансових та інших злочинів.

---

[7] Див.: Зацаринный А.А. О некоторых проблемах обеспечения информационной безопасности в условиях создания глобальной информационной инфраструктуры // Информационная безопасность России в условиях глобального информационного общества 2-я Всероссийская конференция 18 июня 2001 года.

Наприклад, "Сіті-Бенк" заявив про те, що у 1994 році з території Росії було здійснено більше ста спроб електронних крадіжок, половина з яких була вдалою і спричинила втрати на декілька десятків мільйонів доларів США.[8] Розвиток інформаційної системи віртуальної економіки широко демонструє все більш різноманітні і масштабні прояви небезпек у формі комп'ютерних злочинів.

У травні 2000 року в Інтернеті була розповсюджена Епідемія вірусу ILOVEYOU, яка поширювалась у виді файлу-додатка до електронних листів. У ході її постраждало більше 45 мільйонів комп'ютерів в усьому світі, включаючи комп'ютери Пентагона і парламенту Великобританії.

У серпні 2000 року була зламана комп'ютерна система розвідки Канади, у результаті чого хакери одержали доступ до надсекретних державних документів і тим самим поставили під загрозу національну безпеку країни.

У вересні 2000 року сайт компанії Western Union, що спеціалізується на здійсненні грошових переказів по всьому світові без відкриття банківських рахунків, був також зламаний хакерами. За словами представників WU, зловмисники зняли електронні копії кредитних карт 15700 клієнтів, що переказують гроші через сайт компанії. У тому ж місяці 2000 року США провели перевірку стану комп'ютерної безпеки в урядових закладах. Сім з 24 організацій одержали оцінку «незадовільно», відмінників не знайшлося зовсім, а основна маса державних організацій отримала «трійки» з організації комп'ютерної безпеки. За результатами перевірки всі 24 міністерства і відомства США мають ті чи інші проблеми, що дозволяють неавторизованим користувачам здобути секретну інформацію. Майже всі спроби злому, початі ревізорами, виявилися успішними. «Хакери» одержували можливість читати, змінювати і навіть вилучати дані з комп'ютерів міністерств і відомств.

У січні 2001 року на атомній станції в місті Бредвіле, графства Ессекс (Великобританія) співробітник охорони почав спробу саботажу комп'ютерної системи. Охоронець зламав комп'ютерну мережу станції.

У травні 2001 року відбулась атака на систему енергопостачання штату Каліфорнія, США. Фахівці американської енергетичної компанії California Independent Systems Operator (Cal-ISO), що забезпечує

[8] Див.: 2. - С. 141.

енергопостачання штату Каліфорнія, вияснили, що їхні комп'ютерні системи осаджувалися невідомими хакерами щонайменше 17 днів.[9]

В останньому разі незалежно від мотивів втрати суб'єктів віртуальної економіки можуть досягати величезних розмірів. У зв'язку з цим варто визначитись з поняттям інформаційної безпеки. На наш погляд, ***інформаційна безпека — це стан і здатність інформаційної системи протистояти випадковим чи навмисним впливам на її окремі елементи і зміст відомостей, які виключають неприпустимі ризики їх знищення, перекручування і розкриття, що призводять до матеріальних збитків власника чи користувача інформації.***

Тому формування віртуальної економіки та єдиного інформаційного простору, з точки зору предмета економічної безпеки, вимагає рішення великої кількості проблем. Першою серед них є впорядкованість інформаційної системи. Якщо окремі елементи системи неупорядковані (джерела інформації, кодуючі та декодуючі пристрої, канали обігу інформації, адресати та архіви), то система не буде працювати ефективно, в неї є широке поле для протиправних дій і вона буде небезпечною для клієнтів та учасників.

З цією метою необхідно вирішити цілу низку завдань:

- визначити державні і приватні масиви інформації, що можуть бути відкриті для доступу. Для цього треба визначитись законодавчо і досягнути з їх власниками відповідних угод про партнерство в рішенні даної задачі;
- розробити єдині технічні стандарти збереження, обробки і надання інформації;
- визначити необхідні вимоги до клієнтів (юридичних та фізичних осіб), їх ідентифікації з метою забезпечення доступу до тих масивів інформації;
- визначити умови надання інформації клієнтам (юридичним та фізичним особам);
- забезпечити комутацію запитів від споживачів до необхідних баз;
- забезпечити режим захисту інформації від спроб руйнування масивів, несанкціонованого доступу і т.п.;

Якщо виключити природні та антропогенно-природні джерела небезпеки функціонування інформаційної системи віртуальної еко-

---

[9] Джураев Э. Ш., Організаційні аспекти забезпечення моніторингу інформаційної безпеки // Информационная безопасность России в условиях глобального информационного общества 2-я Всероссийская конференция 18 июня 2001 года.

номіки, то головна небезпека надходить від антропогенних джерел. Людина, яка володіє інформаційною зброєю і має злочинні наміри, є головною небезпекою суб'єктів економічної діяльності у віртуальній економіці.

Чим менше впорядкована інформаційна система, тим більш масовий і різноманітній характер мають її правопорушення. Особливістю злочинів в комп'ютерних інформаційних системах є те, що вони, окрім власних, мають ознаки і некомп'ютерних злочинів: крадіжок, розбою, шахрайств, привласнення, розтрат, знищення майна тощо. Щодо власних особливостей злочинів в інформаційних системах віртуальної економіки, то вони поділяються на такі групи:

1. Злочинне вилучення елементів і засобів інформаційної техніки (системних блоків, вінчестерів та інших носіїв інформації, що містять у пам'яті дані про клієнтів, вкладників, кредиторів банку) шляхом розкрадання, розбою, вимагання і самі по собі містять склад злочину звичайних, «некомп'ютерних» злочинів.

2. Незаконне перехоплення (негласне одержання) інформації для отримання визначених відомостей про стан і взаємини суб'єктів діяльності у віртуальній економіці (продавців, покупців, інвесторів, клієнтів, вкладників, кредиторів і позичальників тощо). Воно може здійснюватись з використанням засобів аудио-, відео- й електромагнітного спостереження, отриманих шляхом крадіжок, шахрайств кодами, електронними картами, тощо. Предметами злочинів можуть бути усі елементи інформаційної системи: джерела інформації, пристрої, що її переробляють, трансформують і надсилають у канали обігу, (кодуючі та передавальні пристрої), канали обігу, пристрої прийому та декодування інформації, архіви, службові приміщення для проведення конфіденційних переговорів, паперові і магнітні носії (у тому числі і технологічні відходи).

3. Розпорядження інформацією без згоди власника шляхом несанкціонованого доступу до інформації обмеженого доступу, яка є у власності суб'єкта діяльності віртуальної економіки.

4. Руйнація інформаційної системи шляхом виведення з ладу засобів і програм забезпечення її функціонування з метою нанесення втрат конкуренту, створення сприятливих передумов досягнення власних економічних, соціально-політичних чи аморальних цілей злочинця, або отримання із зруйнованої системи необхідної інформації.

Усі ці злочини здійснюються за допомогою широкого кола методів, найбільш розповсюдженими з яких є:

- фізичне проникнення у виробничі приміщення;
- підключення до ліній зв'язку законних користувачів;
- входженням в обмежену інформаційну систему шляхом декодування і дешифрування систем захисту;
- пошук слабких ланцюжків у програмах і забезпеченні захисту; проникнення в обмежену інформаційну систему, видаючи себе за законного користувача з застосуванням його кодів (паролів) і інших ідентифікуючих шифрів;
- створення дезінформаційних умов, коли законний користувач обмеженої інформаційної системи здійснює зв'язок з нелегальним терміналом, будучи абсолютно упевненим в тому, що він працює з потрібним йому законним абонентом;
- створення аварійної ситуації, в якій за спеціальними програмами одержується необхідна інформація;
- асинхронний напад з різних пунктів і терміналів для проникнення в інформаційну систему через слабкий ланцюжок;
- маніпуляції базами даних інформаційної системи;
- таємне введення до програмного забезпечення команд на власну користь;
- приховування "слідів" шляхом введення комп'ютерних вірусів або "бомб", що руйнують інформаційну систему.

Захищаючи інформаційну систему, треба враховувати, що розвиток будь-якого злочину від задуму до виконання проходить три етапи.

Перший етап – підготовчий. На ньому йде пошук, купівля, одержання чи розкрадання знарядь злочину у виді комп'ютера, модему й ін. (відшукання засобів і знарядь здійснення злочину); написання спеціальної програми, що дозволяє перебороти захист інформаційних мереж (виготовлення і пристосування засобів здійснення злочину), збір інформації про суб'єктів віртуальної економіки, систем захисту, підбір паролів, подолання системи захисту від несанкціонованого доступу до даних і комп'ютерної інформації (навмисне створення умов для вчинення злочину).

Другим етапом є здійснення злочину. На ньому шляхом маніпуляції даними, що зберігаються в пам'яті інформаційної системи, і її керуючими програмами організується несанкціонований рух коштів на користь зловмисника чи третьої особи, маскуються сліди злочину.

Третім етапом злочину є його закінчення. Він характеризується завершенням всіх несанкціонованих трансакцій, внаслідок чого зловмисник має можливість скористатися плодами свого злочинного діяння.

Особливістю скоєння злочинів в інформаційних системах є те, що суттєво утруднюється можливість їх виявлення і збору доказів. Але існує багато непрямих ознак, серед яких можна визначити такі[10]:

- розкрадання носіїв інформації;
- ненормальний інтерес деяких осіб до змісту сміттєвих ємностей;
- здійснення необґрунтованих маніпуляцій з цінними даними, наприклад, часте переведення коштів з одного рахунка на інший, наявність декількох рахунків у однієї особи, проведення операцій із затримкою підтвердження відповідними паперовими документами і т.д.;
- порушення режиму функціонування комп'ютерних систем;
- втрата значних масивів даних;
- необґрунтоване перебування в приміщеннях сторонніх осіб, включаючи неплановий технічний огляд приміщень, устаткування, різних засобів систем життєзабезпечення представниками обслуговуючих і контролюючих організацій;
- порушення правил ведення журналів і протоколів робочого часу комп'ютерних систем (виправлення в них записів, відсутність деяких записів чи їхня фальсифікація);
- необґрунтовані маніпуляції з даними без серйозних на те причин (перезапис, заміна, зміна, стирання), або дані не обновляються вчасно в міру їхнього надходження (нагромадження);
- поява на ключових документах підроблених підписів або відсутність їх взагалі;
- поява підроблених або фальсифікованих документів чи бланків строгої звітності;
- особливий інтерес деяких співробітників інформаційної системи без наявних на те підстав до робіт надурочно, прояв підвищеного інтересу до відомостей, що не відноситься до їхньої безпосередньої діяльності, або відвідування інших підрозділів і служб інформаційної системи;
- заперечення або висловлення з боку будь-якого співробітника відкритого невдоволення з приводу здійснення контролю за їхньою діяльністю;
- численні скарги клієнтів.

---

[10] Вертузаев М.С., Кондратьев Ю.А., та ін. Способи здійснення злочинів з використанням банківських платіжних карт. – Інформаційні технології та захист інформації. – Запоріжжя, 1999. - С.51.

Упорядкування інформаційних мереж віртуальної економіки потребує чітко поставленого санкціонування доступу до секретної і таємної інформації. Справа у тому, що локальні мережі сьогодні глобалізуються. Зараз рідко зустрінеш зовсім ізольовані мережі, які ні з ким не взаємодіють. Тому, саме поняття локальної мережі стало дуже розпливчастим, оскільки вже в їхньому складі міститься велика кількість підмереж, які об'єднані найрізноманітнішими способами. Таким чином, мережна безпека перетворюється в найбільш актуальне завдання захисту інформації в віртуальній економіці.

Фахівці визначають велику кількість проблем локальних інформаційних мереж з точки зору їх безпеки.[11] У сучасних умовах більш ніж 80% різних атак і спроб отримати інформацію обмеженого доступу здійснюється з середини локальних мереж. Локальна мережа, особливо велика стає головним джерелом різних неприємностей, тому що в ній працюють фахівці різного профілю і, як правило, про заходи безпеки думають в останню чергу. Багато дій з середини локальної мережі слабко контрольовані і керівники організації можуть довго навіть не підозрювати, що в них є проблеми і ці проблеми накопичуються.

При цьому в організації можуть застосовуватись атестовані системи безпеки різних класів, комп'ютери оснащені індивідуальними засобами захисту з використовуванням прикладних криптографічних модулів. Але через наявність досить простих методів підключення до мережі, усе це може виявитися не ефективним.

Велика кількість прикладних програмних систем, орієнтованих на мережні технології, а також велика кількість прикладних програм захисту, з одного боку, обмежує розвиток інформаційних технологій, а з іншого, внаслідок несистемного підходу, послаблює захист інформації від несанкціонованого доступу. Навіть умонтувавши сертифіковані криптографічні модулі захисту через наявний програмний інтерфейс до додатка, не дають можливості бути упевненим, що використовуваний захист на прикладному рівні є ефективним, що він не «продірявився» за рахунок слабини в інших прикладних системах чи в операційній системі комп'ютера.

Зараз усі бажають працювати в Інтернеті, і будь-які заборони тут дуже погано працюють. Велика кількість організацій правдами

---

[11] Ігнатов В.В. Віртуальні мережі – універсальний метод забезпечення безпеки в локальних і глобальних ір-мережах // Информационная безопасность России в условиях глобального информационного общества 2-я всероссийская конференция 18 июня 2001 года.

і неправдами підключають свої локальні мережі до мережі глобальної. Ті, хто є обережним, фізично відключають кілька комп'ютерів від мережі і підключають їх в Інтернет. Але для великої організації це рішення незручне і тому починають будувати окрему мережу для Інтернет, що поступово перетворюється в основну мережу організації. Багато суб'єктів Інтернету панацеєю від усіх загроз і небезпек вважають установку міжмережного екрану. А те, що через даний комп'ютер можна одержати доступ до інших ресурсів локальної мережі вже забувається, чи те, що якийсь добрий користувач установив на комп'ютер невелику програмку і тим самим створив можливість вийти в Інтернет собі і своїм товаришам, може залишитися непоміченим.

У деяких великих організаціях існують власні інтернет-мережі, і в цьому випадку їх перестає турбувати взагалі будь-яка безпека. Але забувається про те, що така мережа вже має великі можливості неконтрольованих підключень з усіма неприємностями.

Головні недоліки організації інформаційних мереж в віртуальній економіці, з точки зору безпеки, мають наступні прояви:

1. Частіше всього, питання забезпечення інформаційної безпеки зводяться до забезпечення конфіденційності (шифрування і кодування інформації та контролю доступу до неї) і, іноді, автентичності (використання механізмів контролю дійсності). При цьому, недостатня увага приділялася вимогам до надійності й цілісності функціонування інформаційних систем;

2. Важливою проблемою залишається й те, що питання розробки і забезпечення захисту інформації розглядаються окремо. Часто-густо даними питаннями займаються різні підрозділи, які навіть є підрозділами різних організацій (інформаційних технологій, безпеки);

3. Недостатня увага приділяється захисту від загроз, що надходять від внутрішнього порушника, а також від необережних і ненавмисних дій. При цьому система захисту будується без проведення аналізу загроз і оцінки ризиків, зв'язаних з даними загрозами.

Цілісна система захисту інформаційної системи повинна перекривати всі канали можливих загроз її небезпек, виключати слабкі ланцюжки на стиках окремих її компонентів. Вона повинна автоматизовано захищати секретну інформацію, відповідати вимогам і критеріям стандартів інформаційної безпеки.

Формування захисту інформаційної системи повинно починатись з розробки концепції безпеки. Остання визначає систему

поглядів на проблему безпеки інформації. В ній повинно бути визначено:

- систематизована характеристика цілей і задач захисту;
- основні принципи і способи досягнення необхідного рівня безпеки інформації в інформаційній системі;
- визначення функцій і технологій обробки даних;
- характеристика відкритих і закритих інформаційних потоків, що захищаються;
- опис політики безпеки;
- перелік загроз і можливих шляхів їхньої реалізації,
- модель ймовірних порушників;
- рекомендації з реалізації необхідних заходів з захисту інформації.

На підставі концепції захисту розробляються організаційно-розпорядницькі документи, що регламентують режим безпеки інформації. Режим безпеки інформації повинен забезпечувати її захист на декількох рівнях: організаційному; мережному, прикладному і фізичному рівнях.

На організаційному рівні забезпечується захист інформації в процесі документообігу у середині організації і з зовнішніми структурами. Тут визначаються рівні конфіденційності кожного документального потоку і засоби їх захисту в системі загального режиму безпеки.

На мережному рівні вирішуються питання технічного забезпечення захисту в процесі застосування мережної апаратури і настроювань серверів, робочих станцій, міжмережних екранів, іншого комунікаційного і мережного устаткування згідно схем інформаційних потоків з метою виключення потенційних вразливих ланцюгів системи. Система захисту на цьому рівні повинна усунути загрози, що виходять від зловмисників, що знаходяться як у середині, так і поза межами, які захищаються.

На прикладному рівні забезпечується захист в операційних системах, серверах додатків, клієнтських додатків, за допомогою яких відбувається обробка, передача і збереження конфіденційної інформації. Тут важливе усунення загроз, зв'язаних з некоректними (випадковими, помилковими і т.д.) діями персоналу чи навмисними діями нелояльних співробітників компанії чи третіх осіб (розмежування доступу до інформаційних ресурсів, захист від несанкціонованого доступу, аутентифікация користувачів, включаючи вилучених і мобільних співробітників компанії і т.д.).

На **фізичному рівні забезпечується** охорона приміщень, у яких обробляється чи зберігається конфіденційна інформація, контролюється доступ співробітників у дані приміщення, зберігаються копії резервних (архівних) конфіденційних інформаційних ресурсів, забезпечується енергетична і пожежна безпека всієї інформаційної системи.

Немаловажне значення, з точки зору здійснення безпеки інформаційної системи, має тип засобів захисту інформації (ЗЗІ). Серед них можна виділити:

- **однокомпонентні ЗЗІ,** що будуються на базі одного, як правило, вузько спеціалізованого продукту захисту інформації (у більшості випадків таким продуктом буває антивірусний пакет);

– **багатокомпонентні ЗЗІ,** що будуються вже на базі декількох продуктів, кожний з який вирішує свою конкретну задачу. При цьому продукти і технології, які використовуються в багатокомпонентних ЗЗІ для захисту інформації ніяк не пов'язані між собою ні на технічному, ні на організаційному рівнях;

– **комплексні ЗЗІ** – подальший розвиток багатокомпонентних ЗЗІ, у яких продукти, технології і рішення поєднуються в єдину систему на організаційному рівні для того, щоб забезпечити максимальний ступінь захищеності системи. Очевидно, що при цьому стійкість усієї ЗЗІ еквівалентна стійкості «найслабшої» її ланки;

– **інтегровані ЗЗІ,** у яких всі елементи комплексних ЗЗІ поєднуються не тільки на організаційному, але й на мережному і прикладному рівнях. У такій інтегрованій системі компрометація одного з елементів захисту повинна надійно компенсуватися протидією інших її елементів.

Інтегровані засоби захисту інформації дають можливість використання явища синергизма в масштабах усієї інформаційної системи. Побудова багатокомпонентних, а тим більше однокомпонентних систем захисту інформації в більшості випадків уже не є сучасним рішенням проблеми інформаційної безпеки, особливо для великих мереж.

На мережному рівні для захисту складних систем необхідне застосування вже досить дорогих технологій, таких як міжмережне екранування, VPN, засоби виявлення вторгнень і т.д. До тепер багато хто визначає поняття віртуальних мереж — як з'єднання локальних мереж через відриту IP-мережу з використанням на виходах цих мереж спеціальних пристроїв, що здійснюють шифрування

минаючого через них трафіка і тунелювання його між двома такими пристроями.

Варто говорити про дійсно захищену віртуальну мережу тільки в тому випадку, коли в такій мережі присутні, як рівноправні об'єкти захисту, і окремі комп'ютери, не важливо, де вони знаходяться, і захищені організаційними заходами виділені фрагменти локальної мережі, наприклад, групи серверів.

Агенти VPN, що перехоплюють весь мережний трафік, установлюються на кожний комп'ютер, що вимагає захисту при його інформаційній взаємодії з навколишнім середовищем. Чи навпаки, комп'ютер, що працює з локальної мережі з відкритими ресурсами, може бути за допомогою технології VPN ізольований від локальної мережі. Агенти VPN, що перехоплюють мережний трафік незалежно від додатка що його створює, шляхом криптографічних перетворень кожного IP-пакета індивідуалізують його і роблять недоступним для будь-яких інших комп'ютерів, крім пари комп'ютерів, що обмінюються між собою інформацією. Якщо йде обмін з якимсь сервером, то стає недоступною парольна інформація і можна вже не дуже турбуватися про ступінь захищеності прикладної системи. Можна не задумуватися, яка технологія використовується — Oracle це чи Informix, Microsoft SQL чи просто файловий сервер. Зовсім просто для VPN-агентів, виходячи з логіки необхідних інформаційних зв'язків, незалежно від додатків, мережної операційної системи, без будь-яких настроювань мережного устаткування, без участі мережних адміністраторів створювати замкнуті чи пересічні групи користувачів. При цьому не важливо, де знаходяться такі користувачі — в одній чи різних локальних мережах безпосередньо, чи в глобальній мережі, що підключилися до Інтернет через провайдера.

Ефективно сформована система захисту інформаційної системи реалізується завдяки удосконаленому моніторингу небезпек і загроз.

Моніторинг інформаційної безпеки являє собою комплекс заходів (організаційних, технічних і правових), спрямованих на проведення спостережень, оцінки і прогнозу змін в інформаційних і телекомунікаційних системах, а також компонентах даних систем. Необхідність використання моніторингу визначається тим, що стандартні засоби і механізми захисту інформації недостатні тому, що звичайно забезпечують тільки базові функції, не дозволяючи контролювати їхнє виконання і працездатність інформаційної системи в цілому. Так практично в усіх інформаційних системах, як мінімум,

необхідно відслідковувати та реєструвати в системі спроби-помилки, спроби несанкціонованого доступу, спроби втручання в програмне забезпечення, факти доступу до ресурсів, позаштатні ситуації, зниження рівня захищеності і багато чого іншого.

Моніторинг призначено для виконання функцій контролю функціонування інформаційних систем, систем передачі даних, засобів і механізмів захисту. Ефективність моніторингу залежить від правильної його організації. Попереднє вивчення, оперативний контроль, аналіз і забезпечення механізмів реагування дозволяє не тільки виявити факт інформаційної атаки чи порушення працездатності, але і сформувати комплекс заходів щодо попередження, локалізації й усунення наслідків.

Моніторинг небезпеки в інформаційних мережах спирається на наступні базові принципи:

- спостереження за факторами впливу і станом інформаційних систем;
- оцінку фактичного стану інформаційної системи;
- прогноз стану інформаційної системи на визначений термін.

Система моніторингу містить у собі цілий комплекс заходів, що пов'язані з вибором технічних засобів і методів аналізу; розробкою методів збору, реєстрації і протоколювання небезпечних подій; аналіз. Для забезпечення моніторингу використовуються як технічні (технологічні) методи (аналіз захищеності, виявлення несанкціонованої активності, контроль інформаційних потоків, протоколювання і реєстрація), так організаційні і правові.

Якщо йдеться про організаційні заходи щодо забезпечення моніторингу безпеки, то вони включають:

– створення й експлуатацію системи забезпечення реагування і відновлення елементів інформаційної системи, що обмежує масштаби втрат в інформаційній інфраструктурі на об'єктах підвищеного ризику;

– створення й експлуатацію системи обміну інформацією про факти і методи комп'ютерних нападів і несанкціонованих вторгнень в інформаційно-телекомунікаційні системи об'єктів підвищеного ризику;

– розробку вимог з безпеки інформації, що враховують особливості функціонування інформаційних систем на об'єктах підвищеного ризику.

Моніторинг небезпек в інформаційній системі – це найважливіша передумова здійснення безпеки. Ми не будемо торкатись технічного боку цього питання. Але дуже важливе значення для забезпечення

безпеки інформаційних систем у віртуальній економіці має нормативно-правова база. Ми згодні, що три статті XVI розділу КК України не охоплюють усі злочини ані в комп'ютерних,[12] ані в інформаційних мережах в цілому. Кримінальна відповідальність повинна розповсюджуватись на руйнацію інформаційних систем за допомогою спеціальних програм, на розробку спеціальних програм, що руйнують інформаційні системи в цілому та їх окремі елементи.

Щодо охорони комерційної таємниці, яка обертається в інформаційних мережах віртуальної економіки, то враховуючи місце і роль приватної власності в сучасній економіці, вона заслуговує на спеціальний Закон про захист комерційної таємниці (а не ст.ст. 231 та 232 КК України), аналогічно тому, як охорона державної таємниці регулюється спеціальним законом.

Елементарною економічною істиною є те, що гроші – це платіжні засоби, але платіжні засоби – не тільки гроші. Перший-ліпший студент економічного відділення вищої школи може розповісти, що нарівні з грішми платіжну функцію виконують безготівкові гроші, "електронні гроші", чеки, сертифікати інші цінні папери. Але відповідальність за підробку різних платіжних засобів не однакова (див. ст.ст. 199-200 КК України).

Таким чином, захист інформаційних систем в віртуальній економіці сьогодні стає однією з головних проблем забезпечення її безпеки за допомогою різноманітних засобів: технічних, технологічних, організаційних, економічних, фінансових, правових тощо.

Глава 14. Особливості розслідування економічних злочинів, вчинених з використанням комп'ютерних технологій

Вчинення злочинів з використанням комп'ютерної техніки давно відомі в західних країнах. В криміналістичній літературі відзначаються труднощі у виявленні і розслідуванні цих злочинів. Зокрема підкреслюється, що в окремих випадках власники компаній, дізнавшись про подібні операції своїх підлеглих з комп'ютерною технікою, не тільки не повідомляли про це в поліцію, а й допомагали приховувати їх з метою подальшого використання злочинної

[12] Дутов М.М. Відповідальність за комп'ютерні злочини, передбачена новою редакцією КК України - fecha@skif.net