І.М.Пістунов

БЕЗПЕКА ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Міністерство освіти і науки України
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«НАЦІОНАЛЬНИЙ ГІРНИЧИЙ УНІВЕРСИТЕТ»

І.М. Пістунов
Є.В. Кочура

БЕЗПЕКА ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Навчальний посібник

Дніпропетровськ
НГУ
2014

УДК 004.738.5:338.46(075)
БКК 32.973.202я73
П34

Рекомендовано вченою радою як навчальний посібник для студентів спеціальності 7, 8.030502 «Економічна кібернетика» (Протокол № 6, від 01.07.2014).

Рецензенти:
Н.К Васильєва, д-р. екон. наук, доц., завідувач кафедри інформаційних систем і технологій Дніпропетровського державного аграрного університету;
Косарєв В.М., канд. техн. наук, проректор з науки Дніпропетровського університету імені Альфреда Нобеля, завідувач кафедри економічної кібернетики.

Пістунов І.М.
П34 Безпека електронної комерції [Електронний ресурс]: навч. посібн. / І.М. Пістунов, Є.В. Кочура ; Нац. гірн. ун–т. – Електрон. текст. дані. – Д. : НГУ, 2014. – 125 с. – Режим доступу: http://pistunovi.narod.ru/6_E_K.pdf (дата звернення: 01.07.2014). – Назва з екрана.

У посібнику подано інформацію про загальні проблеми безпеки діяльності, пов’язаної з електронною комерцією у всіх її аспектах, що може бути корисним для державних підприємств, комерційних структур, банків і приватних осіб.

Матеріал книги включає завдання для самостійної роботи, тому він може слугувати і як посібник для практичних чи лабораторних занять із застосуванням комп’ютерної техніки.

Адресовано студентам вищих навчальних закладів, але може стати в пригоді фінансистам, економістам, плановикам, менеджерам та маркетологам.

Зміст посібника базується на літературних джерелах вітчизняних, зарубіжних авторів, ресурсах Інтернету та на досвіді викладання дисципліни «Безпека електронної комерції» в Державному ВНЗ «НГУ».

УДК 004.738.5:338.46(075)
БКК 32.973.202я73

ЗМІСТ

ВСТУП

Інтернет-комерція, торгівля в Інтернеті це – комерційна діяльність в Інтернеті, коли процес покупки / продажу товарів або послуг (весь цикл комерційної / фінансової транзакції або її частина) здійснюється електронним чином із застосуванням Інтернет-технологій. Електронна комерція (e-commerce): маркетинг, подача пропозицій, продаж, здача в оренду, надання ліцензій, постачання товарів, послуг або інформації з використанням комп'ютерних мереж або Інтернету.

Економічною передумовою електронної комерції є об'єктивна необхідність зниження витрат, що виникають в комерційних циклах. Технічною передумовою електронної комерції стало стрімкий розвиток служб Інтернету.

Для покупця одним з головних переваг електронної комерції є значна економія часу на отримання інформації про товар, його виборі.

Компанії, що займаються електронною комерцією, отримують ряд переваг в порівнянні з підприємствами «реального» бізнесу. Основні з них:

– Розширення ринку збуту з перспективою виходу на зарубіжні ринки;

– Доступність цілодобово;

– Автоматизація збору маркетингової інформації з використанням CRM-систем (CRM, Customer Relationship Management - управління відносинами з клієнтами);

– Зниження витрат на організацію і підтримку інфраструктури, так як в цьому випадку немає необхідності в організації торгових залів, офісів;

– Зниження витрат на рекламу. Реклама в Інтернеті в ряді випадків обходиться дешевше, в порівнянні з засобами масової інформації, до того ж Інтернет надає більше можливостей.

Користувач послуг електронної комерції, в свою чергу, отримує такі переваги:

– Більш зручні можливості вибору: клієнту достатньо відкрити необхідну кількість сайтів;

– Можливість отримання більш повної інформації. Якщо мова йде про покупку товару, то в Мережі, як правило, є повна інформація про нього. При якісному оформленні сайту електронного магазину покупець може скористатися, наприклад, сервісом порівняння товарів, отримати список рекомендованих фірмою-виробником аксесуарів і т. д.

До основних моделей електронної комерції в Інтернеті відносяться наступні [84]:

– B2C (Business-to-Consumer) - «фірма-споживач»;

– B2B (Business-to-Business) - «фірма-фірма»;

– C2B (Consumer-to-Business) - «споживач-фірма»;

– З2С (P2P - Peer-to-Peer, «рівний-рівний») «споживач-спожитвач»;

– B2G або B2A (Business-to-Government, Business-to-Administration) - «фірма-держава»;

- G2B або A2B (Government-to-Business) - «держава-фірма»;

– G2C або A2C (Government-to-Consumer або Administration-to-Consumer) - «держава-споживач»;

– C2G або C2A (Consumer-to-Government) - «споживач-держава»;

– G2G або A2A (Government-to-Government) - «держава-держава»;

– E2E (Exchange-to-Exchange) - «біржа-біржа»;

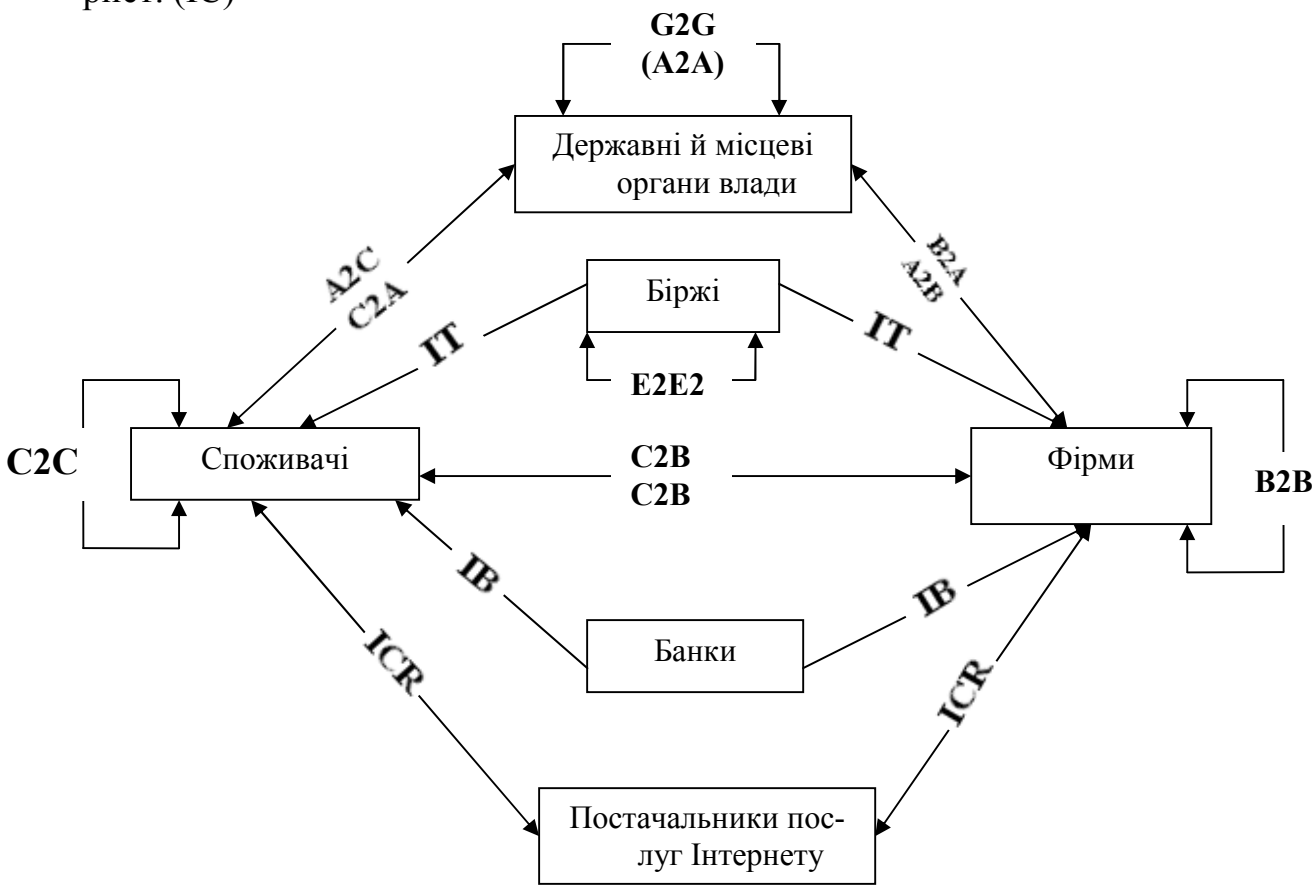
– Інтернет-банкінг; (IB)

– Інтернет-трейдинг; (IT)

– Інтернет послуги: (IS)

– Послуги технологічного ланцюжка електронної комерції: системи електронних платежів, доставка товару;

– Консалтингові послуги; дослідницькі послуги; страхування через Інтернет. (IC)



Всі розрахунки в електронній комерції здійснюються через Інтернет-банкінг – це забезпечення клієнту можливості управління банківським рахунком через Інтернет на основі систем електронних платежів. Окрім цього, управління банківськими рахунками через Інтернет складає основу систем дистанційної роботи на ринку цінних паперів та віддаленого страхування.

Водночас зі зростання кількості послуг зростає й небезпека, оскільки значна кількість чинників можуть викликати втрати, збитки при проведенні електронних операцій.

З урахуванням сформованої практики забезпечення інформаційної безпеки виділяють наступні напрямки захисту інформації:

1. Правовий захист – це спеціальні закони, інші нормативні акти, правила, процедури і заходи, що забезпечують захист інформації на правовій основі;

2. Організаційна захист – це регламентація діяльності і взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнюють неправомірне оволодіння конфіденційною інформацією і про-явище внутрішніх і зовнішніх загроз.

3. Інженерно-технічний захист – це сукупність спеціальних органів, технічних засобів і заходів щодо їх використання в інтересах захисту конфіденційної інформації.

Для реалізації захисту інформації створюється система безпеки.

Під системою безпеки будемо розуміти організаційну сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємств, держави від внутрішніх і зовнішніх загроз. В рамках системи безпеки присутня система захисту інформації. Система захисту інформації (СЗІ) – це організована сукупність спеціальних органів засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

Усю розмаїтість структур і форм суб'єктів безпеки залежно від підпорядкування можна умовно поділити на дві основні групи:

– власні служби безпеки, що входять у структуру господарюючих суб'єктів і повністю утримуються за їх кошти. Структура цих підрозділів базується залежно від рівня становлення фірми, масиву питань, вирішення яких покладає на ці служби керівництво фірми на тому чи іншому етапі її розвитку;

– функціонуючі як самостійні комерційні чи державні організації, що наймає господарюючий суб'єкт для виконання функцій щодо забезпечення окремих або всіх аспектів його безпеки. Такі суб'єкти, як правило, спеціалізуються або на суто режимно-охоронних послугах (охорона будівель, споруд, транспорту, окремих працівників підприємств, установ, членів їх сімей тощо), або — на економічних, правових чи консультаційних послугах. Залежно від безпосередньої участі у забезпеченні безпеки фірми:

– спеціальні суб'єкти, що створені виключно для виконання функцій щодо забезпечення безпеки фірми, як-то її власна служба безпеки, так і залучена на умовах договору;

– напівспеціальні суб'єкти, до безпосередніх функцій яких входять ряд таких, що спрямовані на забезпечення безпеки фірми. Такими суб'єктами є відділ кадрів, фінансово-кредитний відділ, медична частина тощо;

– решта персоналу та структурні підрозділи, участь яких у здійсненні заходів щодо забезпечення безпеки фірми носить винятковий характер.

Залежно від форми власності та підпорядкування:

– державні органи здійснюють повноваження щодо безпеки суб'єктів фінансово-господарської діяльності, у структуру яких вони входять, або ж надають послуги стороннім фірмам на умовах укладених договорів, прикла-

дом чого є діяльність Державної служби охорони МВС України щодо заходів безпеки усіх без виключення комерційних банків в Україні;

– недержавні органи, що представлені охоронними організаціями, аналітичними центрами, інформаційними та консалтинговими службами, які за відповідну плату на умовах договору надають послуги щодо охорони об'єктів, здійснюють захист інформації, комерційної таємниці тощо. До цієї групи суб'єктів належать і власні служби безпеки фірми недержавної форми власності.

Залежно від правової основи функціонування (легітимності) суб'єктів:

– офіційно-функціонуючі органи, в рамках чинного законодавства України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України;

– нелегітимні структури, діяльність яких відбувається поза правовим полем України. Наразі їх функціонування має динаміку до зменшення, що викликано відмовою суб'єктів бізнесу від їх «послуг», однак відкидати їх існування не варто. Зазначені суб'єкти, іншими словами «дах» пропонують свої послуги через погрози, насилля, погроми гарантуючи при цьому захищеність від подібних структур. Зазвичай такі послуги пропонують суб'єктам бізнесу, діяльність яких повністю або ж частково відбувається в тіні, що є підставою до шантажу.

Перелік вищезазначених суб'єктів безпеки фірми, за виключенням останнього успішно формує ринок послуг щодо забезпечення безпеки бізнесових структур. Найчастіше вітчизняні підприємці формують попит на фізичну охорону будівель, інкасацію, комплекс захисних заходів від рекету і прослуховування телефонних каналів зв'язку, приміщень від радіозакладок, комп'ютерів і комп'ютерних мереж від несанкціонованого проникнення і вірусів. Дещо меншим попитом користуються послуги щодо організації захисту документованої інформації, перш за все, тієї, що містить державну і комерційну таємницю. Також недостатньо уваги приділяється роботі з персоналом, що допущений до конфіденційної інформації.

Недостатньо, на нашу думку, з позиції безпеки досліджується проблема зовнішніх контактів фірми. Тут пропонується аналіз репутації співвиконавців, контрагентів, їх кредитоспроможності, фінансової спроможності; вивчення конкурентів, дослідження ринку, тобто забезпечення прикладних аспектів безпеки сучасного маркетингу. Виключення складають лише комерційні банки, для яких вивчення потенційних клієнтів — питання виживання, тісно пов'язане з поверненням кредитів.

З позиції аналізу сучасного світового ринку послуг безпеки близько 60% обсягу укладених угод становлять охоронні послуги; послуги технічного забезпечення та консультування – по 15% відповідно і послуги приватного розшуку – 10%.

У свою чергу, ринок охоронних послуг складається а приблизно рівних частин щодо охорони стаціонарних об'єктів, особистої охорони, охорони масових заходів, супроводження вантажів і цінностей при транспортуванні. При цьому, якщо підприємству не вистачає власних можливостей і можливо-

стей охоронної компанії, найнятої фірмою на постійній основі, то фірма звертається на ринок спеціалізованих послуг, що пов'язані з ринками товарів (технічних засобів безпеки), спеціалістів та інформації.

Варто зауважити, що ринок послуг у сфері безпеки досить складно аналізувати, оскільки він характеризується відсутністю чітких меж. Як правило, фірми, що працюють на цьому ринку, багатопрофільні, а тому виділити компанії , що надають послуги лише у сфері безпеки, можна лише досить умовно [34].

Найбільш поширеними напрямами їх діяльності є такі:

– охорона офісних приміщень;

– підготовка і надання охоронців;

– підготовка професійних охоронців;

– консультації;

– охорона вантажних перевезень;

– охорона автостоянок;

– встановлення технічних засобів безпеки.

Серед інших спеціальних послуг, що надають спеціалізовані компанії (агентства безпеки), переважають такі, як охорона масових заходів, продаж зброї, створення локальних систем криптографічного захисту інформації, спільне з міліцією патрулювання.

До найбільш перспективних видів послуг у сфері безпеки варто віднести збір інформації, в тому числі за кредитоспроможністю бізнес-партнерів і надійності угод, надання комплексних послуг щодо охорони комерційних підприємств, супроводження вантажів і цінностей, а також послуги щодо технічного захисту, підготовки кадрів, захисту інформації. Перспективними їх варто вважати тому, що саме по них обсяг укладених угод постійно зростає.

Інша характерна особливість сучасного ринку охоронних послуг проглядається в розвитку бізнесу у сфері безпеки передусім за рахунок розширення кола клієнтів із залученням більш солідних комерційних структур. І меншою мірою – за рахунок диверсифікації послуг (розширення їх номенклатури або поглиблення спеціалізації). Найбільший попит на послуги охоронних агентств формують комерційні банки і компанії, що займаються фінансовою діяльністю (фінансові і страхові, а також фірми, що працюють на фондовому ринку). Така сфера бізнесу, окрім звичайних охоронних послуг, особливо потребує захисту власної конфіденційної інформації, що забезпечується технічними засобами безпеки. До того ж більшість з них ліквідні, володіють солідною репутацією і можна вважати, що залучення клієнтів саме цієї категорії спровокує основну конкурентну боротьбу в охоронному бізнесі.

В посібнику розглянуто економічну та організаційну складову забезпечення захисту об’єктів і суб’єктів електронної комерції, причому ці заходи розділені згідно існуючої класифікації, по типам суб’єктів: державні, комерційні та користувачі. Кожному типу присвячено окремий розділ.

Після кожного розділу подані індивідуальні завдання, які студенти мають виконати протягом часу на засвоєння предмету «Безпека електронної комерції».

Індивідуальні завдання оформляються як документ, який подається в електронному вигляді, вміщеним на будь-який носій інформації. Формат електронного документу має відповідати електронному процесору Calc Open Office або Excel Microsoft Office.

Титульний лист оформлюється згідно прикладу, поданому нижче.

Міністерство освіти і науки, молоді та спорту України
Державний вищий навчальний заклад
«Національний гірничий університет»
Кафедра економічної кібернетики та інформаційних технологій

ІНДИВІДУАЛЬНА РОБОТА З ДИСЦИПЛІНИ
«БЕЗПЕКА ЕЛЕКТРОННОЇ КОМЕРЦІЇ»

Розроби(ла)в ст. гр. ЕК-09-1 Косач-Квітка Л.П.
Варіант № 5

Прийняв проф., д.т.н. Пістунов І.М.

Дніпропетровськ
2013

Кожне виконане завдання повинно містити опис задачі, початкові значення змінних, які обираються за номером по списку студентської групи, вирішення та висновки щодо отриманих результатів.

РОЗДІЛ 1. ОЦІНКА СТАНУ БЕЗПЕКИ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Вивчивши матеріали розділу, студенти вивчать перелік можливих напрямків завдання шкоди засобам здійснення операцій електронної комерції, навчаться розраховувати міру захищеності інформаційної системи та визначати перші признаки кібератаки.

1.1. Види загроз електронної комерції

Всю множину потенційних загроз комп'ютерної інформації корисно представити згідно природи їх виникнення, розділивши на два класи: природні і штучні, що впливають на роботу інформаційної системи (ІС), яка обслуговує заходи з електронної комерції

Природні загрози – це загрози, викликані впливами на АС і її компонентів фізичних процесів або стихійних природних явищ, незалежних від людини. їх можна розділити на природні і технічні.

Штучні – це загрози, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити [38,42]:

– Ненавмисні, випадкові загрози, викликані помилками людей при проектуванні АС, і її компонентів, а також в процесі їх експлуатації.

– Навмисні загрози, пов'язані з корисливими устремліннями людей (зловмисників).

Джерела загроз по відношенню до АС можуть бути зовнішніми або внутрішніми (компоненти самої ЕОМ – її апаратура, програми, персонал).

Природні загрози.

– Стихійні лиха (урагани, повені, землетруси, цунамі, пожежі, виверження вулканів, снігові лавини, селеві потоки тощо). Загрози цієї групи пов'язані з прямим фізичним впливом на елементи ІС і системи забезпечення (водо-, тепло-, електропостачання) і ведуть до порушення роботи ІС і фізичному знищенню систем забезпечення, персоналу, засобів обробки й пере5дічі даних, носіїв інформації;

Магнітні бурі чинять електромагнітні впливу на магнітні носії інформації, електронні засоби обробки і передачі даних, обслуговуючий персонал та ведуть до відмов апаратури, викривлення або знищення інформації, помилок персоналу;

Радіоактивні випромінювання і опади. Ці загрози аналогічні за наслідками загрозам попередньої підгрупи і, крім того, ведуть до захворювань персоналу.

Технічні загрози. Загрози цієї групи пов'язані з надійністю технічних засобів обробки інформації та систем забезпечення ІС.

Відключення або коливання електроживлення та інших засобів забезпечення ведуть до втрат інформації, виходу з ладу засобів обробки і порушень в управлінні об'єктами в керуючих ІС.

Відмови і збої засобів обробки пов'язані з надійністю роботи апаратно-програмних засобів та ведуть до спотворення і втрат інформації, порушення управління об'єктами.

На рис. 1.1. представлено класифікацію загроз електронної комерції.

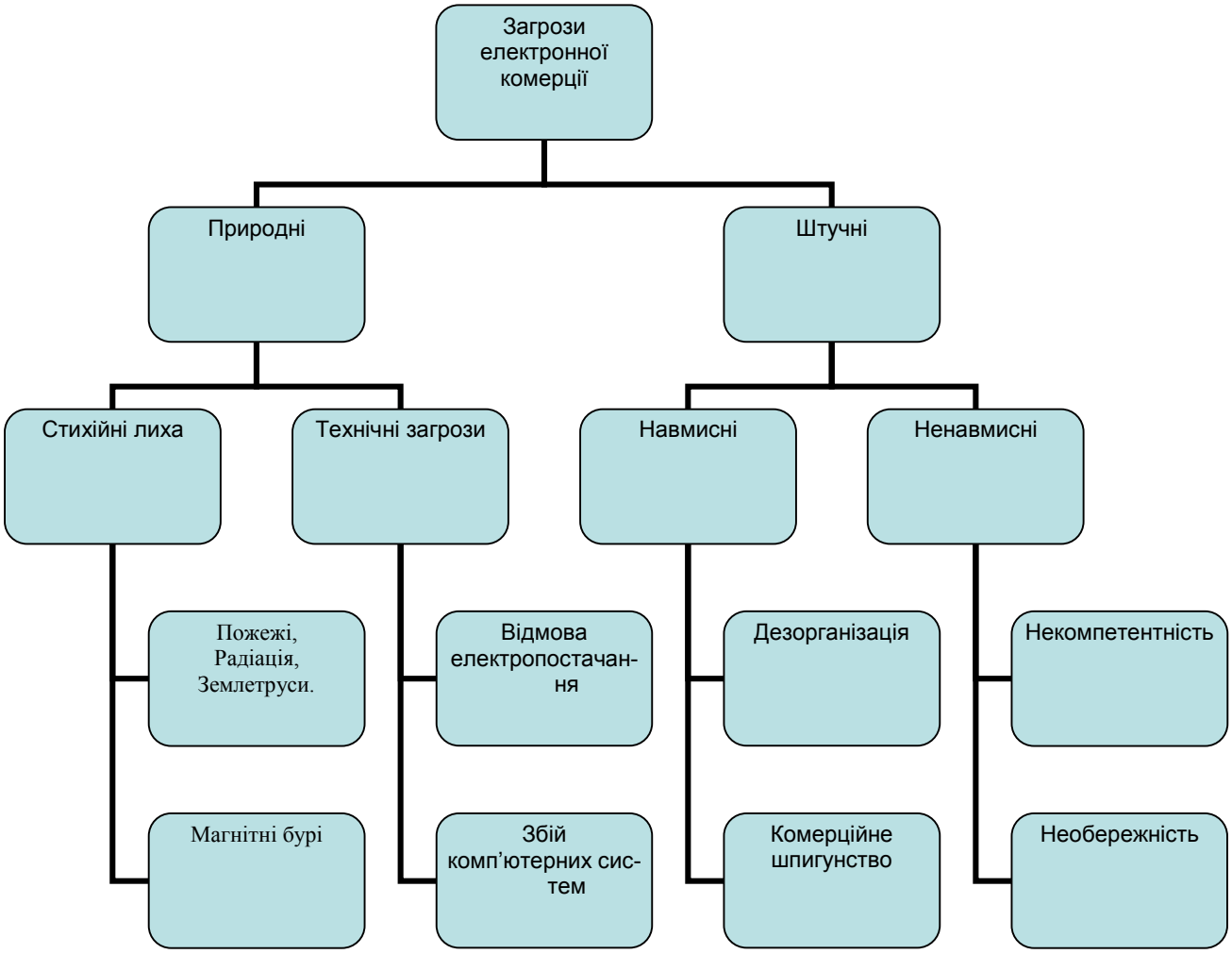


Рис. 1.1. Загальна класифікація загроз електроної комерції.

Ненавмисні загрози пов'язані з діями, які люди вчиняють випадково, через незнання, неуважність або недбалість, з цікавості, але без злого наміру:

– Ненавмисні дії, що призводять до часткового або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи (ненавмисна псування устаткування, видалення, перекручування файлів з важливою інформацією або програм, в тому числі системних і т.п.);

– Неправомірне відключення устаткування або зміна режимів роботи пристроїв та програм;

- Ненавмисне псування носіїв інформації;

– Запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання або зациклення) або здійснюють незворотні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних і т.п.);

– Нелегальне впровадження та використання неврахованих програм (ігрових, навчальних, технологічних та ін які не є необхідними для виконання порушником своїх службових обов'язків) з подальшим необґрунтованим витрачанням ресурсів (завантаження процесора, захоплення оперативної пам'яті і пам'яті на зовнішніх носіях);

– Зараження комп'ютера вірусами;

– Необережні дії, що призводять до розголошення конфіденційної інформації, або роблять її загальнодоступною;

– Розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів, шифрування, ідентифікаційних карток, перепусток і т.п.);

– Проектування архітектури системи, технології обробки даних, розробка прикладних програм, з можливостями, які надають небезпеку для працездатності системи та безпеки інформації;

– Ігнорування організаційних обмежень, при роботі в системі;

– Вхід в систему в обхід засобів захисту (завантаження сторонньої операційної системи з дискети і т.п.);

– Некомпетентне використання, налаштування або неправомірне відключення засобів захисту персоналом служби безпеки;

– Пересилання даних по хибному адресу абонента (пристрою);

– Введення помилкових даних;

– Ненавмисне пошкодження каналів зв'язку.

Навмисні загрози. Це дії людей здійснюються навмисне для дезорганізації роботи системи, виведення системи з ладу, проникнення в систему і несанкціонованого доступу до інформації:

– Фізичне руйнування системи (шляхом вибуху, підпалу тощо) або вивід з ладу всіх або окремих найбільш важливих компонентів АС (пристроїв, носіїв важливої системної інформації, осіб із числа персоналу і т.п.);

– Відключення або вивід з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку тощо);

– Дії по дезорганізації функціонування системи (зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка потужних активних радіоперешкод на частотах роботи пристроїв системи і т.п.);

– Впровадження агентів в число персоналу системи (у тому числі, можливо, і в адміністративну групу, яка відповідала за безпеку);

– Вербовка (шляхом підкупу, шантажу і т.п.) персоналу або окремих користувачів, що мають певні повноваження;

– Застосування пристроїв для підслуховування, дистанційна фото та відеозйомка і т.п.;

– Перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і каналів зв'язку, а також наводок активних випромі-

нювань на допоміжні технічні засоби, безпосередньо не беруть участь в обробці інформації (телефонні лінії, мережі живлення, опалення тощо);

– Перехоплення даних, переданих по каналах зв'язку, і їх аналіз з метою з'ясування протоколів обміну, правил входження в зв'язок і авторизації користувача і подальших спроб їх систематизації для проникнення в систему;

– Розкрадання носіїв інформації (магнітних дисків, стрічок, запам'ятовуючих пристроїв і самих персональних комп'ютерів);

– Несанкціоноване копіювання носіїв інформації;

– Розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації і т.п.);

– Читання залишкової інформації з оперативної пам'яті і з зовнішніх запам'ятовуючих пристроїв;

– Читання інформації з областей оперативної пам'яті, використовуваних операційною системою (в тому числі підсистемою захисту) або іншими користувачами, в асинхронному режимі, використовуючи недоліки мультизадачних операційних систем і систем програмування;

– Незаконне одержання паролів та інших реквізитів доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом підбору, шляхом імітації інтерфейсу системи і т.д.) з наступним маскуванням під зареєстрованого користувача;

– Несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізичну адресу, адресу в системі зв'язку, апаратний блок кодування і т.п.;

– Злам шифрів криптозахисту інформації;

– Впровадження апаратних, програмних "закладок" і "вірусів" ("троянських коней "і" жучків "), тобто таких ділянок програм, які не потрібні для здійснення заявлених функцій, але дозволяють долати систему захисту, потай і незаконно здійснювати доступ до системних ресурсів з метою реєстрації і передачі критичної інформації або дезорганізації функціонування системи;

– Незаконне підключення до ліній зв'язку з метою роботи "між рядків", з використанням пауз в діях законного користувача від його імені з наступним введенням помилкових спілкувань або модифікацією переданих повідомлень;

– Незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його фізичного відключення після входу в систему і успішної аутентифікації з подальшим введенням дезінформації та нав'язуванням хибних повідомлень.

Найчастіше для досягнення поставленої мети зловмисник використовує не один, а деяку сукупність з перерахованих вище шляхів.

Окрім наведених вище загроз, існують загрози, пов'язані з організацією послуг Інтернету, контактів поміж суб'єктами електронної комерції, юридичні аспекти.

Їх перелік подано в табл. 1.1 [19]

Таблиця 1.1.

Проблеми електронної комерції

Проблема	Основні питання в рамках проблеми
1.Регулювання діяльності провайдерів послуг інформаційного суспільства	Порядок визначення місця надання онлайнової послуги. Порядок початку діяльності з надання онлайнових послуг (дозвільний або повідомний). Рамки застосування принципу "свободи установи" (freedom of establishment), закріпленого ст. 52 Договору про створення ЄС
2.Комерційні повідомлення	Визначення поняття "комерційні повідомлення". Правила надання послуг особами так званих регульованих професій (адвокати та ін). Забезпечення добросовісної конкуренції. Забезпечення прозорості умов надання послуг. Виняток практики "нав'язування" послуг
3. Укладення договорів з використанням елект-ронних засобів	Визнання дійсності договорів, що укладаються електронним способом. Юридична сила різних дій сторін, чинених при укладенні договору
4. Відповідальність посередників.	Відповідальність посередників за передачу незаконної інформації Здатність посередників контролювати передану інформацію
5. Вирішення спорів у галузі електронної комерції	Засоби забезпечення таких механізмів правового захисту, які були б найбільш швидкодіючими (з урахуванням географічної віддаленості контрагентів один від одного) і ефективними (з урахуванням того, що даний вид бізнесу має специфічні особливості в якості електронного бізнесу). Ступінь застосування позасудових (третейських) механізмів врегулювання. Поліпшення співробітництва між регулюючими та судовими органами окремих країн
6. Реалізація норм Директиви в законодавстві держав-учасниць	Визначення принципів поширення наглядової юрисдикції того чи іншого учасників держави при транскордонній електронної комерції. Введення уніфікованих правил розкриття інформації про сервіс-провайдерів. Надання однакових гарантій діяльності сервіс-провайдерів

1.2. Розрахунок міри захищеності інформаційної системи електронної комерції

Розрахунок цієї міри ведеться за двома напрямками [56]:

– аналіз наявних видів технічних засобів збереження і захисту інформації;

– експертна оцінка збитків від загроз.

Можна виділити два критерії, що дозволяють оцінити ефективність системи захисту:

– Відношення вартості систем захистів (включаючи поточні витрати на підтримку працездатності цієї системи до збитків, які можуть виникнути при порушенні безпеки;

– Відношення вартості систем захистів до вартості зламу цієї системи з метою порушення безпеки і технічних пристроїв з найбільшими збитками.

В основі аналізу системи захисту інформації можна використовувати економічну модель. В основі цієї моделі лежить теза про те, що всі інформаційні загрози в кінцевому підсумку повинні бути економічно виправдані. Дійсно, реалізація будь-якої інформаційної загрози пов'язана з певними витратами: витрачаються кошти на вивчення обстановки, розробку плану і технології реалізації загрози, придбання обладнання та необхідних спеціальних технічних засобів, існують витрати й на етапі реалізації інформаційної загрози. Джерело загрози сподівається на те, що всі ці витрати окупляться відомостями, які він отримає. Мірою такого зіставлення є величина $\frac{Z}{b}$, де Z – еквівалентна вартість отриманих відомостей, а b – сукупні витрати по організації загрози. Чим більше величина $\frac{Z}{b}$, тим більше вірогідність загрози. Позначимо дане відношення через α – коефіцієнт небезпеки загрози, використовуючи економічну модель загроз, можна зробити наступні висновки:

1. Чим більше інформаційна значимість зони Z, тим більше вірогідність загрози при інших рівних умовах.

2. Чим менше витрати на реалізацію загрози, тим більше вірогідність загрози. Розглянемо як приклад підслуховування ділових розмов в приміщенні. Методику оцінки ефективності системи безпеки в спрощеному вигляді можна представити у вигляді наступної послідовності дій:

1. Скласти повний перелік можливих каналів витоку мовної інформації.

2. Для кожної загрози визначити коефіцієнт небезпеки загрози α, для акустичних загроз

$$\alpha = \overline{Z}\frac{\Delta F * T * Lg_2(1+q)}{b} - \overline{Z}\frac{\Omega}{b}, \qquad (1.1)$$

де Ω – об'єм викраденої інформації, при реалізації загрози; Z – вартість біта інформації (дорівнює 1, оскільки всі загрози порівнюються між собою); ΔF – смуга частот; T – тривалість роботи; q – середня величина динамічного діапазону (можна приймати 2,3 КГц); b – витрати на реалізацію загрози.

3. Визначити необхідні технічні засоби протидії інформаційним загрозам (скласти повний перелік).

4. Для кожного технічного засобу визначити ранговий коефіцієнт

$$\eta_i = \frac{\alpha_i * \Omega_i * \overline{Z}_i}{B_i} \qquad (1.2)$$

Чим більше величина η, тим більше підстав застосувати даний технічний засіб для захисту від відповідної інформаційної загрози.

5. Вибір рішення здійснюється шляхом відбору технічних пристроїв з найбільшими значеннями η.

6. Ефективність системи захисту інформації визначається виразом:

$$Q_i = \frac{\sum_{i=1}^{n} \eta_i B_i \Psi_i}{\sum_{i=1}^{n} \eta_i B_i}, \qquad (1.3)$$

де Ψ_i – ваговий коефіцієнт важливості загрози ($\sum_{i=1}^{n} \Psi_i = 1$).

Оцінку ефективності системи безпеки електронної комерції доцільно здійснювати за допомогою узагальнюючого показника, якого позначимо як θ_{ij}. Він визначає стан захищеності *i*-го суб'єкта при проведенні *j*-ї комерційної операції на ринку електронної комерції.

Мірою захищеності визначимо ймовірність (p) збитку в грошовому еквіваленті U_{ij}, який не перевищить наперед заданий рівень збитку при виконанні *j*-ї комерційної операції на ринку електронної комерції.
(рис. 1.1).

Тоді узагальнений показник θ_{ij} може бути представлений у вигляді

$$\theta_{ij} = P(p \le \widehat{U}_{ij}). \qquad (1.4)$$

Якщо суб'єкт господарської діяльності виконує водночас K видів комерційної діяльності, тоді міра захищеності буде визначатися у припущенні, що ці види діяльності є незалежними подіями

$$\theta^K{}_{ij} = 1 - \prod_{k=1}^{K} (1 - p_{ijk}), \qquad (1.5)$$

де $1 < k < K$ – види комерційної діяльності.

Розрізняють такі рівні захищеності операцій електронної комерції:

$$\left.\begin{array}{ll} \textit{Гарантована,} & \text{якщо} \quad \theta^K{}_{ij} \ge 0.99; \\ \textit{Висока,} & \text{якщо} \quad 0{,}99 > \theta^K{}_{ij} \ge 0{,}8; \\ \textit{Середня,} & \text{якщо} \quad 0{,}8 > \theta^K{}_{ij} \ge 0{,}5; \\ \textit{Низька,.} & \text{якщо} \quad \theta^K{}_{ij} < 0{,}5. \end{array}\right\} \qquad (1.6)$$

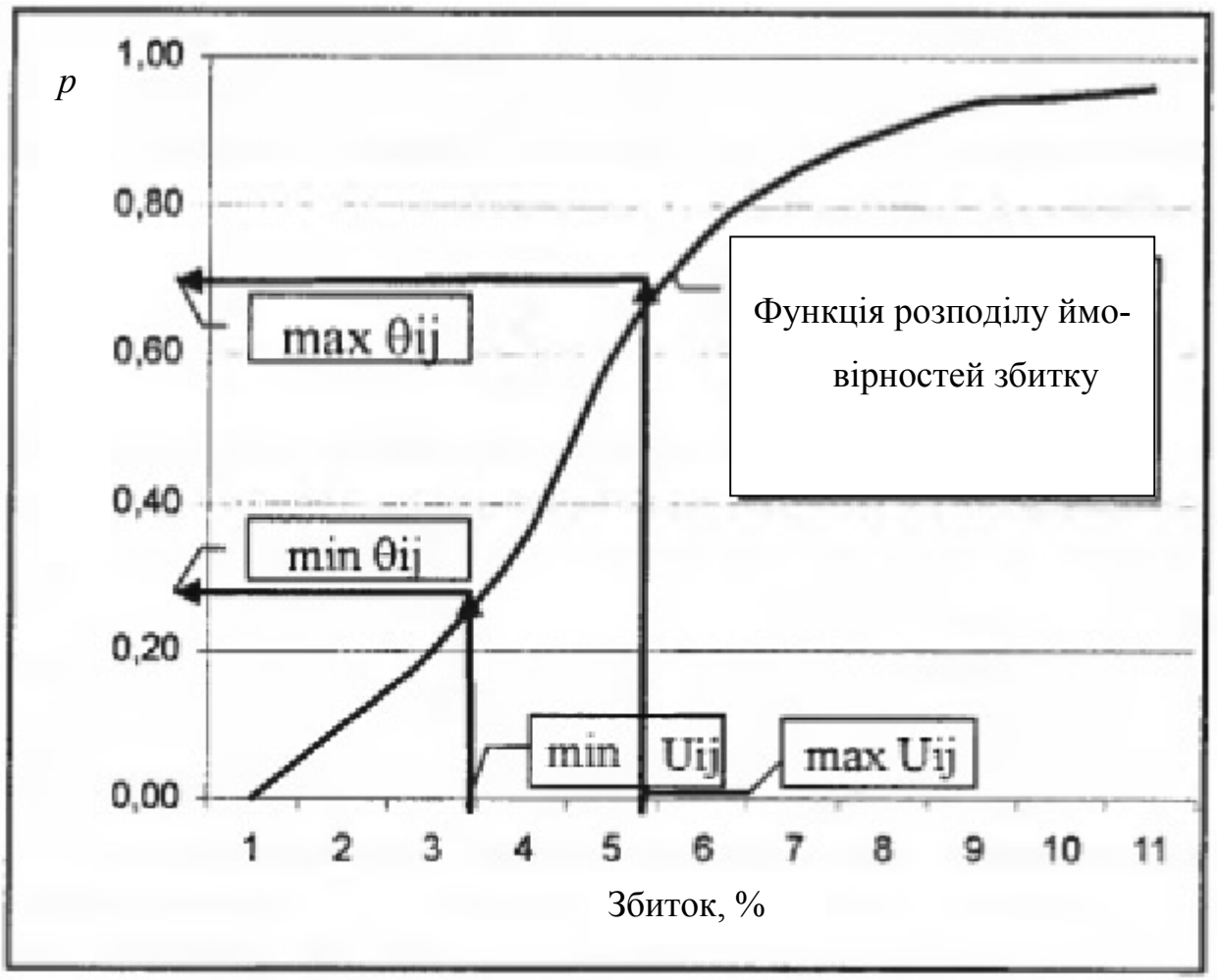


Рис. 1.1. Коридор допустимої ймовірності збитку

Величини можливих збитків, функції їх розподілів, вагові коефіцієнти та інше визначаються за статистичними показниками та методами експертних оцінок.

1.3. Розрахунок початку кібератаки

Кібератакою називається ситуація, коли кількість звернень з Інтернету до інформаційної системи (ІС), що обслуговує запити клієнтів через Інтернет, різко зростає [2]. При цьому, сервер ІС починає працювати все повільніше, намагаючись задовольнити усі запити, доки не припиняє роботу.

Визначити початковий момент кібератаки дуже важливо, оскільки це дозволить зменшити втрати на компенсацію її наслідків.

Знайдемо критерій початку кібератаки за статистичними розрахунками.

Для цього розіб'ємо весь період роботи інформаційної системи, що обслуговує зовнішні запити електронної комерції, на рівні проміжки часу. Ними можуть бути: година, доба, тиждень, але в умовах роботи через Інтернет, краще встановити ці проміжки не більше ΔT = 20-30 хв.

Далі потрібно налагодити постійний контроль за кількістю вхідних запитів.

Після визначення кількості запитів у кожному проміжку не менше 40, потрібно розрахувати середню кількість звернень M_x.

Скористаємося гіпотезою, що потік подій частіше за все характеризується експоненційним законом розподілу [3]. Він характеризується функцією розподілу виду $F(x)=\int_0^x \lambda\cdot e^{-\lambda x}dx = 1-e^{-\lambda x}$, при $x\geq 0$, $F(x)=0$, при $x<0$ (1.7)

Математичне сподівання дорівнює

$$M_x=\int_0^\infty \lambda x e^{-\lambda x}dx = \frac{1}{\lambda}\ . \qquad (1.8)$$

Медіана може бути знайдена як

$$M_e=-\mathrm{Ln}0.5/\lambda\approx 0.69/\lambda. \qquad (1.9)$$

Звідкіля,

$$\left.\begin{aligned}\lambda &= \frac{1}{\mathrm{M_x}},\\ \lambda &= -\frac{Ln0.5}{Me}\end{aligned}\right\} \qquad (1.10)$$

Вираз (1.10) дозволяє знайти зв'язок між медіаною і середнім

$$Me=-\frac{M_x}{Ln0.5}. \qquad (1.11)$$

Задамо довірчу ймовірність β, яка визначить допустимий рівень ймовірності попадання кількості вхідних звернень в інтервал [*Me; K*], де *K* – реальне число звернень на проміжку ΔT. Очевидно, що ймовірність попадання на цей інтервал має складати половину довірчої ймовірності

$$\frac{\beta}{2}\geq P(\mathrm{Me}<\mathrm{x}<\mathrm{K}) = \mathrm{EXP}(-\lambda\mathrm{Me}) - \mathrm{EXP}(-\lambda\mathrm{K}). \qquad (1.12)$$

Підставимо значення λ з (1.10) у (1.12)

$$\frac{\beta}{2}\geq \mathrm{EXP}(-\frac{\mathrm{Me}}{\mathrm{M_x}}) - \mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}}), \qquad (1.13)$$

А медіану, в свою чергу виразимо через середнє

$$\frac{\beta}{2}\geq \mathrm{EXP}(\frac{\mathrm{M_x}}{\mathrm{M_x}\,\mathrm{Ln}0.5}) - \mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}}). \qquad (1.14)$$

Приведемо вираз до виду

$$\beta\geq 2\cdot\mathrm{EXP}(\frac{1}{\mathrm{Ln}0.5}) - \mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}}) = 0{,}47258018 - 2\cdot\mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}}). \qquad (1.15)$$

Знайдемо тепер допустиме перевищення кількості вхідних викликів інформаційної системи над середнім їх значенням

$$\frac{\beta-0{,}47258018}{2}\geq -\mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}})$$

звідкіля

$$\mathrm{M_x}\cdot\mathrm{Ln}\left(\frac{\beta-0{,}47258018}{2}\right)\geq \mathrm{K} \qquad (1.16)$$

Отже, якщо кількість звертань до ІС *K* перевищить значення виразу з правої частини (1.16), можна вважати, що кібератака вже почалася.

Розуміючи, що відношення $\frac{K}{M_x}$ є перевищенням середнього у відносних одиницях, зробимо розрахунок відповідності деяких популярних значень довірчої ймовірності до міри перевищення кількості вхідних викликів над середнім. Результати розрахунків представлені у табл. 1.2.

Таблиця 1.2

Розрахунок відповідності значення довірчої ймовірності та міри перевищення кількості вхідних викликів на їх середнім значенням

β	$\frac{K}{M_x}$
0,6	2,753415
0,75	1,975370
0,8	1,809659
0,85	1,667544
0,9	1,543136
0,95	1,432506
0,98	1,371564
0,99	1,352048
0,999	1,334803
0,9999	1,333095

З табл. 1.2 можна зробити висновок, що в разі перевищення кількості запитив до ІС над середньою їх кількістю тільки у півтора рази, можна зі ймовірністю більше 0,9 вважати, що кібератака вже почалася.

1.4. Страхування електронної комерції

При зверненні до страхових компаній бізнесмени, які працюють в галузі електронної комерції, можуть отримати значно завищену пропозицію по тарифним ставкам або навіть відмову. Причиною цього є відсутність надійної статистики щодо можливих втрат при проведенні подібних операцій.

Тому перед укладенням договору страхування бажано провести дослідження щодо кількості випадків (n) втрати бізнесу через кіберзлочинність. Наступними показниками статистики будуть:

N – загальна кількість організацій, які працюють у сфері електронної комерції;

b – середній збиток від кіберзлочинності (ступінь знищення бізнесу);

B – загальна сума договорів, які виконуються цими організхаціями в рамках електронного бізнесу.

Так само, як і в п.1.3, необхідно визначити середнє (M_b) та середнє квадратичне відхилення (σ_b)для збитку від кіберзлочинності за формулами (1.7) та (1.12).

Далі знаходиться коефіцієнт варіації

$$Var_b = \frac{\sigma_b}{M_b}, \tag{1.16}$$

Для розрахунку тарифної нетто ставки необхідно використати довірчу ймовірність (β) та зворотнє значення функції Лапласа ($Л(\beta)$), як в п.1.3.

Тоді тарифна нетто-ставка при страхуванні електронної комерції буде знайдена як

$$T_n = \frac{n}{N}\left(1 + Ë(\beta)\frac{\sigma_b}{M_b}\right). \tag{1.17}$$

Приклад, Визначити розмір нетто-ставки при страхуванні від кіберзлочинності, якщо число негативних випадків n = 13 при загальній кількості організацій, що працюють в галузі електронної комерції становить N = 12456. середнє значення ступеня знищення об'єкта дорівнює $\overline{b}$ = 0,5, $Л(\beta)$ = 1,68, а σ_b = 1235 грн, M_b = 1235478 грн.

Відповідно до формули (1.17), величина тарифної нетто-ставки складе

$$T_n = \frac{13}{12456}\left(1 + 1{,}68\frac{1235}{12345478}\right) = 0{,}0010438$$

Результат розрахунку дозволяє сказати, що при страхуванні бізнесу на суму 1 млн. грн, нетто-ставка складе 1043,8 грн.

Треба враховувати, що страхові компанії до нетто-ставки додають навантаження, яке в декілька разів перевищує саму нетто-ставку. Але в усіх випадках, якщо запропонований страховий тариф буде перевищувати нетто-ставку більше, аніж на порядок, варто відмовитися від таких страхових послуг і пошукати іншого страховика.

1.5. Індивідуальне завдання № 1

Тема роботи: Визначення міри захищеності інформаційної системи, що обслуговує суб'єктів електронної комерції та розрахунок наявності початку кібератаки.

Мета роботи: Вивчити методики розрахунків міри захищеності та початку кібератаки.

Завдання А За даними у табл. 1.2 розрахувати міру захищеності інформаційної системи, що обслуговує суб'єктів електронної комерції, якщо організація має три види захисту, вартістю (B_i) відповідно A, B, C тис. грн, кожен з яких відповідає ранговому коефіцієнту (η_i) D, E, F. Експерти оцінили важливість для перших двох засобів ваговими коефіцієнтами (ψ_i) G та H.

Рекомендація: скористайткеся формулою (1.3) та поняттям вагового коефіцієнту.

Завдання Б: розрахувати імовірність початку кібератаки, якщо середня кількість запитів до інформаційної системи, що обслуговує заходи електронної комерції становить (*a*) K, а в момент ΔT надійшло L запитів.

Рекомендація: скористайтеся формулою (1.16).

Таблиця 1.3

Числові значення згідно індивідуального завдання

№ п/п	A	B	C	D	E	F	G	H	K	L
1	23	102	754	0,1923	0,15789	0,5667	0,6	0,14286	40	625
2	22	36	1102	0,6923	0,55263	0,3	0,5429	0,44643	320	375
3	6	114	1218	0,3077	0,23684	0,5333	0,3143	0,30357	380	425
4	8	54	1160	0,5	0,31579	0,6667	0,0857	0,23214	320	300
5	19	66	1392	0,8077	0,39474	0,6667	0,6	0,05357	400	525
6	6	72	1218	0,8077	0,23684	0,3333	0,4571	0,42857	420	600
7	22	72	290	0,6154	0,10526	0,2667	0,2	0,28571	320	500
8	22	102	290	0,3462	0,65789	0,6667	0,6571	0,05357	320	375
9	5	114	232	0,9231	0,55263	0,4333	0,3429	0,08929	480	100
10	18	132	290	0,7308	0,13158	0,5	0,5714	0,07143	40	500
11	25	66	696	0,9231	0,18421	0,5333	0,6857	0,23214	220	100
12	18	120	1218	0,4615	0,23684	0,2333	0,4	0,14286	480	525
13	17	66	1044	0,1923	0,63158	0,5667	0,1714	0,16071	320	500
14	19	132	870	0,3077	0,5	0,3	0,3429	0,32143	340	200
15	14	24	1334	0,9231	0,60526	0,3333	0,1714	0,05357	160	375
16	18	120	1044	0,7692	0,07895	0,6333	0,3714	0,39286	340	175
17	21	12	522	0,2308	0,55263	0,2	0,5429	0,05357	460	350
18	2	66	1276	0,3846	0,47368	0,4667	0,6857	0,08929	300	600
19	12	108	406	0,5769	0,34211	0,7667	0,3143	0,39286	500	550
20	19	48	1334	0,8462	0,18421	0,4	0,0857	0,03571	480	175
21	9	132	116	0,6538	0,36842	0,1333	0,5429	0,16071	380	450
22	24	48	1218	0,6538	0,39474	0,0667	0,3714	0,08929	480	425
23	23	114	406	0,8462	0,42105	0,1	0,4857	0,17857	300	600
24	13	18	1276	0,4615	0,23684	0,6333	0,1714	0,41071	200	125
25	7	30	928	0,4615	0,57895	0,4667	0,7143	0,41071	440	150
26	20	150	1276	0,5	0,15789	0,8	0,1143	0,26786	260	125
27	20	126	406	0,5385	0,5	0,6333	0,6571	0,08929	80	475
28	15	150	1044	0,5385	0,55263	0,1333	0,0571	0,14286	380	450
29	19	120	1450	0,0769	0,39474	0,6333	0,0857	0,35714	220	125

№ п/п	A	B	C	D	E	F	G	H	K	L
30	16	114	406	0,1154	0,47368	0,2	0,4571	0,19643	220	75

Завдання В: за даними табл. 1.3 розрахувати тарифну нетто-ставку при страхуванні електронного бізнесу якщо ймовірність страхового випадку становить $q = n/N$, при загальній сумі договорів S млн. грн, середньому рівню збитку b, довірчій ймовірності g та середньому квадратичному відхиленні збитку σ_b.

Рекомендація: для визначення $Л(\beta)$ скористайтеся функцією **НОРМСТОБР(*g*)** та формулою (1.17).

Таблиця 1.4

Вихідні дані для розрахунку тарифної нетто-ставки при страхуванні електронного бізнесу

№ вар.	q	S	b	N	g	σ_b
1	0,009	10	0,6	3395	0,92	0,6
2	0,01	11	0,5	4001	0,88	0,6
3	0,007	24	0,8	2428	0,8	0,3
4	0,009	16	0,8	2937	0,95	0,6
5	0,008	25	0,2	4046	0,87	0,5
6	0,005	19	0,4	3445	0,81	0,3
7	0,005	26	0,7	2524	0,96	0,2
8	0,009	11	0,8	3052	0,95	0,3
9	0,008	11	0,9	3120	0,91	0,6
10	0,009	13	0,5	2458	0,99	0,4
11	0,002	21	0,2	2498	0,83	0,4
12	0,01	26	0,5	2551	0,93	0,2
13	0,007	28	0,3	2322	0,96	0,5
14	0,003	29	0,5	3205	0,86	0,2
15	0,004	25	0,7	2611	0,97	0,6
16	0,002	22	0,7	2810	0,94	0,3
17	0,01	25	0,7	3666	0,89	0,4
18	0,01	9	0,7	3164	0,98	0,4
19	0,003	21	0,4	4016	0,99	0,4
20	0,004	24	0,8	3309	0,84	0,4
21	0,002	28	0,8	4165	0,96	0,6
22	0,003	10	0,2	2327	0,84	0,3
23	0,006	22	0,4	4062	0,98	0,5
24	0,008	28	0,2	2942	0,83	0,3
25	0,006	14	0,6	4251	0,95	0,6

№ вар.	q	S	b	N	g	σ_b
26	0,01	11	0,7	3685	0,84	0,4
27	0,006	29	0,3	2711	0,98	0,3
28	0,007	25	0,9	4168	0,95	0,3
29	0,009	13	0,8	2513	0,8	0,4
30	0,006	15	0,4	3688	0,95	0,4

Зробіть висновки з отриманих результатів

Контрольні запитання

1. Що таке „носій інформації”?
2. На які дві основні причини розділяються загрози електронної комерції?
3. До якого типу загроз відносяться магнітні бурі?
4. До якого типу загрози відноситься відключення електроживлення під час роботи інформаційних систем? Дати розгорнуну відповідь.
5. Чи може зараження вірусами комп’ютера вважатися ненавмисною дією?
6. Чи відповідає посередник контракту, укладеного методами електронної комерції, за розголошення інформації, що склаждає комерційну тоємницю сторін?
7. Що таке «еквівалентна вартість отриманих відомостей», які отримані внаслідок порушення правил електронної комерції?
8. Як знайти ранговий коефіцієнт засобу технічного захисту інформаційної системи, що обслуговує заходи з електронної комерції?
9. Наведіть формулу для розрахунку міри захищеннності від K заходів по збереженню інфомрації.
10. Який рівень міри захищеності вважається гарантованим?
11. Що таке кібератака?
12. За якми законом розподілу визначається кількісмть вхідних запитів в інформаційну систему, що обслуговує заходи з електронної комерції?
13. Якими статистичними функціями електронних таблиць Excel необхідно скористатися, щоб розрахувати момент початку кібератаки?
14. Який рівень дові\рчої ймовірності ви вважаєте достатнім?
15. Поясніснть зміст правила для визначення початку кібератаки?

В розділі розглянуто розрахунки міри захищеності інформаційної системи, методи визначення перших ознак кібератаки, а також подано перелік можливих напрямків завдання шкоди засобам здійснення операцій електронної комерції

РОЗДІЛ 2. ЗАХОДИ БЕЗПЕКИ ОРГАНІВ ДЕРЖАВНОГО УПРАВЛІННЯ

Вивчивши матеріали цього розділу, студенти узнають про задачі держави по формуванню безпечнеого середовища країни для електронної комерції, вивчать основні прийоми забезпечення захисту комп'ютерної інформації в державних установах та визначення потенційних порушників безпеки.

В Україні за умов розвитку ринкового середовища дедалі більшого значення набуваються питання безопасности бизнеса, Що є одним з обов'язкових чінніків підтримання усталеності економічного та соціального розвитку країни, підвищенню її обороноздатності, виключення або мінімізації ймовірності виникнення соціальніх, трудових, міжнаціональніх та інших конфліктів, які загрожують безпеці держави.

Проведені в Україні процеси пріватізації засвідчують, що в її економіці значний сектор відведено недержавне господарюючім суб'єктам – комерційнім банкам, акціонернім товариство, спільнім підпріємствам тощо, які пропонують споживачам широкий спектр товарів, робіт і послуг. Будучи порівняно новими структурами у вітчізняній економіці, вони здійснюють вагомий вплив на економіку держави, беруть участь, а зазвічай і продукують розвиток сучасних технологій, створюють робочі місця, збільшують податкові надходження до бюджетів країни тощо

Трансформація економіки під впливим ринкових механізмів видилила як окрему самостійну функцію держави – забезпечення її економічної безпеки з позіції як інтересів особини й колективу, так і складної сукупності національніх інтересів. Зважаючі на це, можна поясниті закономірність зміни підходу до поняття «безпека» в сучасних умовах, адже його зміст з площіні, підпорядкованої раніше здебільшого державним інтересам, переходить у царину реальної економікі, торкаючись рівня суб'єктів підпріємніцтва різніх форм власності та виробничо-господарської спеціалізації. Власне тому становлення й розвиток вітчізняного підпріємніцтва відбувається в умів пошуку нових форм менеджменту та маркетингу, викликаних гострою потребою забезпечення безпеки бизнесу внаслідок загострення конкурентної боротьбі за сировину, ринок збуту товарів, споживачів.

За схемо, наведеною у вступі, відносини бізнес з державою мають індекс G2B B2G. Ця категорія включає в себе взаємодію бізнесу і держави. В принципі, електронний бізнес в цій сфері чимось схожий з B2B, тільки замовником в даному випадку виступає держава. Прикладом можуть служити державні закупівлі, що проводяться за допомогою інтернет, соціологічні та маркетингові дослідження, що проводяться для державних структур, різноманіт-

на соціальна реклама в інтернет, розміщена на замовлення державних органів і спрямована на збереження фізичного та духовного здоров'я нації/

На даний момент, категорія G2B мабуть, найменш розвинений електронний бізнес, одночасно з цим має великі перспективи, оскільки поліпшення взаємовідносин держави з бізнесом в Інтернеті дозволить не лише економити час бізнесу, а й знизити витрати на утримання державного апарату і перенаправити вивільнені кошти на соціальні потреби. Електронний бізнес між державою і бізнесом успішно реалізований у багатьох країнах. Найпоширеніший приклад - це електронна здача звітності контролюючим органам (податкова, статистична звітність). Державні органи здійснюють повноваження щодо безпеки суб'єктів фінансово-господарської діяльності, у структуру яких вони входять, або ж надають послуги стороннім фірмам на умовах укладених договорів, прикладом чого є діяльність Державної служби охорони МВС України щодо заходів безпеки усіх без виключення комерційних банків в Україні.

2.1. Безпека взаємовідносин державних установ з іншими суб'єктами засобами електронної комунікації

(за матеріалами з [35])

Безпека на сьогоднішній день є ключовим питанням при впровадженні та використанні систем електронної комунікації (ЕК). Психологічний чинник, пов'язаний з усвідомленням загрози потенційного шахрайства, залишається основною перешкодою для використання Інтернету в якості засобу проведення операцій, пов'язаних з використатнням можливостей комп'ютерних мереж..

Користувачі та фахівці державних органів управління до цих пір не розглядають Інтернет як безпечне середовище. Опитування показують, що найбільшою потенційною загрозою є несанкціоноване отримання персональних даних при використанні відкритих каналів зв'язку Інтернет. Наприклад, за даними розробників платіжної системи VISA близько 23% транзакцій електронних карток так і не проводиться через острах клієнта ввести власну персональну інформацію при роботі, наприклад, з електронним магазином персональну інформацію про клієнта. Аналогічнап ситуація складається в органах державного управління. Аналіз літературних джерел показує, що для забезпечення необхідно виконати наступні три умови:

– Виключити можливість перехоплення персональної або банківської інформації під час транзакції;

– Виключити можливість вилучення цієї інформації з баз даних;

– Виключити можливість використовувати "вкрадену" інформацію у власних цілях.

Для захисту від перехоплення, для захисту інформації під час транзакції використовують як симетричні, так і асиметричні криптоалгоритми. Ра-

зом з тим використовуються додаткові канали зв'язку відмінні від Інтернет – каналів: факс, телефон, звичайна пошта і т.д.

Враховуючи, що зарубіжне і українське законодавство прирівнює цифровий підпис до рукописного, широкого поширення набула аутентифікація транзакцій на основі концепції цифрового підпису.

При розгляді можливості перехоплення інформації, що цікавить, можна не виключати "людський фактор", тому одночасно з програмно-апаратними засобами необхідно використовувати і організаційні, що забезпечують охорону інформаційних ресурсів, виключення шантажу, контроль за паролями і т.д.

Для захисту інформації від перехоплення використовуються протокол шифрування SSL (Secure Sockets Layer) і SET (Secure Electronic Transaction). Однак в основі SSL лежить схема асиметричного шифрування з відкритим ключем, як шифрувальна схема використовується алгоритм RSA, зважаючи технічних особливостей цей алгоритм вважається менш надійним. SET більш захищений протокол, але технологічно складний і дорогий. Тому його повсюдне впровадження не здійснюється й питання безпеки залишається відкритим.

Оцінювання інформаційних ризиків компанії є одним з найважливіших завдань аудиту інформаційної безпеки корпоративних систем як сегменту мережі Інтернет, оскільки саме ці системи є найбільш поширені в державних установах. Вона вирішується за допомогою ідентифікації ресурсів, оцінювання показників значущості ресурсів, погроз, вразливих місць в системі захисту інформації та засобів забезпечення інформаційної безпеки.

Під загальнодоступною інформацією розуміється інформація збирається, створювана і/або зберігається в процесі комерційної активності в мережі Інтернет та, яка не становить державну чи іншого виду таємницю, визначену законодавством. До інформації обмеженого доступу можна віднести:

Звернення з відомостями, що відносяться до державної таємниці, вимагає особливого режиму, що виключає допуск сторонніх осіб. Права та обов'язки учасників інформаційних процесів при роботі з відомостями, що становлять державну таємницю, регламентуються законом "Про державну таємницю";

Комерційна таємниця – існує цілий ряд відомостей, які не є державними секретами, пов'язаних з виробництвом, технологією, управлінням, фінансами, іншою діяльністю господарюючого суб'єкта, розголошення яких (передача, витік) може завдати шкоди його інтересам. Такі відомості прийнято називати службової і /або комерційною таємницею;

Персональні дані – під персональними даними розуміється будь-яка документована і / або занесена на машинні носії інформація, яка відноситься до конкретної людини і чи що може бути ототожнена з конкретною людиною.

Доступ до загальнодоступної інформації є відкритим і її використання не може завдати шкоди учаснику електронної комерції. Що стосується інформації обмеженого доступу, то доступ до неї повинен бути строго регла-

ментований, тобто має бути чітко встановлено, де, ким, в якому обсязі і на яких умовах може бути здійснене використання даної інформації.

З цього випливає, що інформація обмеженого доступу повинна піддаватися захисту від впливу різних подій, явищ, як внутрішніх так і зовнішніх, здатних в тій чи іншій мірі завдати шкоди даній інформації.

Під об'єктом захисту інформації, розуміється такий структурний компонент системи, в якому перебуває або може перебувати підлягає захисту інформація.

Об'єкти захисту повинні відповідати таким умовам:

– Належність до одного і того ж організаційному компоненту ІС;

– Локалізація (обмеження з точки зору територіального розташування).

До об'єктів захисту в системі забезпечення безпеки електронної комерції можна віднести:

– Робочі станції користувачів;

– Робочі станції адміністраторів;

– Сервери (мережеві, бази даних, додатки);

– Апаратура зв'язку (модеми, маршрутизатори);

– Периферійні пристрої (принтери);

– Приміщення (місця установки устаткування, сховища машинних носіїв інформації і т.д.).

Під елементом захисту мається на увазі що знаходиться в ІС сукупність даних, яка може містити підлягають захисту відомості.

Елементи захисту специфицируются, як правило, для кожного окремого об'єкта захисту. Так, за ознакою локалізації можна виділити наступні основні елементи захисту даних:

– Обробка в ЕОМ;

– На дискеті;

– На локальному жорсткому диску робочої станції;

– На жорсткому диску сервера;

– оброблюваність в апаратурі зв'язку;

– Передання по каналу (лінії) зв'язку;

– Дані, що виводяться з ЕОМ на периферійні пристрої.

Таким чином, в системі забезпечення безпеки електронної комерції повинен здійснювати комплексний підхід до захисту ІС. Комплексний підхід передбачає використання єдиної сукупності законодавчих, організаційних і технічних заходів, спрямованих на виявлення, відображення і ліквідації різних видів загроз інформаційній безпеці.

2.2. Модель потенційного порушника

(за матеріалами з [35])

У моделі порушника визначені чотири класи потенційних порушників, кожен з яких характеризується певним рівнем кваліфікації та ступенем навмисності виконуваних дій. Опишемо таку класифікацію для вірусної загрози.

Порушники, що відносяться до класу "Н-1", являють собою користувачів, в результаті ненавмисних дій яких може відбутися інфікування його автоматизованої системи. Прикладами таких дій є скачування з мережі Інтернет неперевірених файлів і запуск їх на локальному комп'ютері.

Порушники класу "Н-2" виконують навмисні дії, однак для проведення вірусної атаки використовуються відомі екземпляри шкідливого коду, а також опубліковані уразливості програмного забезпечення.

Клас порушників "Н-3" передбачає наявність у зловмисника більш високого рівня кваліфікації, що дає йому можливість використовувати шкідливий код, який може детектувати не всіма антивірусними продуктами.

Порушники класу "Н-4" є найбільш небезпечними і володіють достатньою кваліфікацією для розробки шкідливого коду, який не виявляється антивірусними програмними продуктами.

Необхідно відзначити, що в рамках описаної моделі передбачається, що порушники "Н-2", "Н-3" і "Н-4" є зовнішніми по відношенню до робочої станції, що атакується, володіють мінімумом інформації про автоматизовану систему користувача.

Загальна характеристика описаної моделі порушника для будь-якого виду загроз наведена в табл. 2.1.

Таблиця 2.1.

Модель потенційного порушника антивірусної безпеки

№	Клас порушника	Ступінь навмисності дій порушника	Рівень кваліфікації порушника
1	Клас Н-1	Ненавмисні дії	–
2	Клас Н-2	Умисні дії	Низький
3	Клас Н-3	Умисні дії	Середній
4	Клас Н-4	Умисні дії	Високий

Представлена модель є лише одним із можливих прикладів класифікації порушника.

У хакера, який отримав одного разу доступ до комп'ютерної системи, з'являються можли-ності: спробувати піднятися на більш високий рівень пріоритету, який дозволить красти, змінювати або знищувати інформацію; зробити спробу крадіжки кодів і паролів інших користувачів, що дасть йому ще більші переваги. Деякі з найбільш відомих способів досягнення цих цілей:

1. Шахрайство з даними. Напевно, найпоширеніший метод при здійсненні комп'ютерних злочинів, так як він не вимагає технічних знань і відносно безпечний. Інформація змінюється в процесі її введення в комп'ютер або під час виведення.Наприклад, при введенні документи можуть бути замінені фальшивими, замість робочих дискет підсунуті чужі, і дані можуть бути сфальсифіковані. Цей тип здлочинів здійснюють, як правило співробітники, які мають доступ до бази даних.

2. Сканування. Інший поширений метод отримання інформації, який може призвести до злочину. Службовці, які читають файли інших, можуть виявititам персональну інформацію про своїх колег. Інформація, що дозволяє отримати доступдо комп'ютерних файлів або змінити їх, може бути знайдена після перегляду сміттєвих кошиків. Дискети, залишені на столі, можуть бути прочитані, скопійовані, і вкрадені.Дуже хитрий сканувальник може навіть переглядати залишкову інформацію, що залишилася на комп'ютері або на носії інформації після виконання співробітником завдання і видалення своїх файлів, оскільки в комп’ютерає є можливість поновити стерту інформацію..

3. Троянський кінь. Цей метод передбачає, що користувач не помітив, що комп'ютерна програма була змінена таким чином, що включає в себе додаткові функції. Програма, що виконує корисні функції, пишеться таким чином, що містить додаткові приховані функції, які будуть використовувати особливості механізмів захисту системи (можливості користувача, що запустив програму, з доступу до файлів)

4. Люк. Цей метод заснований на використанні прихованого програмного або апаратного механізму, що дозволяє обійти методи захисту в системі. Цей механізм активується деяким неочевидним чином. Іноді програма пишеться таким чином, що специфічна подія, наприклад, число транзакцій, оброблених в певний день, викличе запуск неавторизованого механізму.

5. Технологія салямі. Названа так через те, що злочин відбувається потороху, невеликими частинами, настільки маленькими, що вони непомітні. Зазвичай ця технологія супроводжується зміною комп'ютерної програми. Наприклад, платежі можуть округлятися до декількох копійок, і різниця між реальною та округленої сумою надходити на спеціально відкритий рахунок зловмисника.

6. Супевідключення. Названа по імені програми, що використовувалася в ряді комп'ютерних центрів, обходить системні заходи захисту і використовувалася при аварійних ситуаціях. Володіння цим "майстер-ключем" дає можливість в будь-який час отримати доступ до комп'ютера й інформації, що знаходиться в ньому.

2.3. Особливості розкриття комп'ютерних злочинів

(за матеріалами з [35, 38, 42, 56])

Для того щоб виявити хакера, потрібно:

• гарне програмне забезпечення поточного контролю;

• регулярна перевірка системних журналів;

• система стеження.

Припустивши, що програмне забезпечення знаходиться в порядку, найбільш очевидні сліди злочину можуть бути розділені на дві категорії: зовнішні і внутрішні.Зовнішніми слідами, пов'язаними зі спробами впровадитися в комунікаційну лініюзв'язку, є:

– Виведені з ладу сигнальні пристрої на кабелях зв'язку;

– Посилення загасання сигналів в оптичній лінії зв'язку;

– Зміни в напрузі, ємності, опорі або частоті.

Внутрішніми слідами, пов'язаними зі спробою отримати доступ через звичайний вхіднийнабір або з дистанційного тракту, є:

– Телефонні дзвінки різної тривалості в кімнату, коли після відповіді можна почути звуки модему, що вказують на атаку, проведену шляхом послідовного автоматичного набору диска;

– Повторювані безуспішно спроби входу в систему;

– Повторювання передача керуючих команд;

– Часте використання підказок;

– Нерозв'язана або незапланована робота;

– Образливі або наклепницькі повідомлення;

– Знищена або зіпсована інформація;

– Переміщені або змінені файли і новостворені довідники;

– Скарги замовників, постачальників і користувачів на виникаючі час від часу помилки і труднощі входу і роботи в системі.

Організація повинна постаратися хоч на один крок випередити хакера. Інформація про особу злочинця може бути зібрана, наприклад, за допомогою:

– Звернення до місцевого провайдера, щоб перевірити наявність облікової інформації про державну структуру в секції зловмисника;

– Підтримання зв'язку з відділом кадрів, які займаються проблемами незадоволених абочимось занепокоєних службовців;

– Використання інших хакерів в якості інформаторів без ознайомлення їх з дета-лями системи даної фірми, наприклад, через третіх осіб.

Щоб виявити потенційну активність промислового шпигуна або професійного хакера, організація повинна освоїти різні методи:

– Виявити спроби крадіжки можна, наприклад, прихованою камерою, спрямованої на мішки з роздруківками, приготованими до вивозу;

– Перевірити добромисність всіх відвідувачів, зокрема фахівців із засобів зв'язку, електриків, водопровідників, а також торгових агентів.

Особливо небезпечними місцями є приміщення, де окрім державних установ, існують орендовані декількома фірмами приміщення, в яких протягом дня можна побачити 10-15 фахівців різного роду, які прагнуть отримати доступ в головний вузол зв'язку. При цьому ідентифікаційні картки, які засвідчують особистість, перевіряються вкрай рідко. Відомо, що, використовуючи коридори та переходи в будівлях, співробітники проводять в приміщення сторонніх осіб. Від них слід вимагати пред'явлення стандартної ідентифікаційної карточки з фотографією і документа, що показує, якого роду роботу виконує дана особа. Завжди слід звіряти по телефону ситуацію, коли заздалегідь підготовлений шифр або код отримав відмову повідомлення. Від службовця необхідно вимагати, щоби він фіксував шифр входу в головний вузол зв'язку, відзначаючи в журналі:

– Дату і час відвідин;

– Прізвище, ім'я;

– Назва організації, для якої виконується робота;

– Факт перевірки ідентифікаційної картки.

Реєстраційний журнал повинен періодично перевірятися. Всі відвідувачі мають бути ідентифіковані. Якщо прийшов відвідувач, він повинен пред'явити посвідчення своєї фірми і номер телефону, по якому бепосередньо можна навести довідки. Штат повинен бути попереджений про те, яких відвідувачів варто остерігатися.

Підозрілими можуть бути:

– Сторонні особи, які стверджують, що вони шукають в даному будинку людини або фірму, якої немає в переліку установ, що орендують дане приміщення;

– Потенційні відвідувачі, охочі в деталях дізнатися про цю установу, але разом з тим, однак, згадавши про мету свого візиту – великі проблеми, – намагаються не вдаватися в деталі щодо їхньої організації.

Штат секретарів зазвичай погано навчений тому, як розпізнати і які вжити дії проти енергійного, наполегливого відвідувача, який не бажає йти без інформації, за якою він прийшов. У подібних випадках секретарю потрібно проявити твердість і випровадитивідвідувача або викликати помічників. Однак частіше в цих випадках інформація видається секретарем раніше, ніж виникає підозра. Щоб запобігти витоку секретної інформації повинна здійснюватися політика «чистих столів»: ніякі документи не повинні залишатисяна столах після закінчення робочого часу, і всі непотрібні папірці повинні бути розірвані перед викиданням їх в корзину.Система реагування повинна бути влаштована таким чином, щоб всі скарги, що надійшли від відвідувачів, прохачів і користувачів, зіставлялися і аналізувалися. В цьому повинні допомогти пакети статистичного аналізу, які контролюють такі незвичайні явища, як, наприклад:

– Кожен вечір в один і той же час системи починають давати збій;

– З'являються помилкові повідомлення; спостерігаються помилки при передачі;

– Спостерігається розбіжність результатів.

Як тільки виникають підозри про можливі розвідувальні дії або злдочини, потрібно розпочати повномасштабне розслідування. Велике число злочинів можна запобігти, якщо слідувати основним правилам:

– Організація не повинна публікувати телефонні номери комутованих портів і зобов’язана мати адресу колишнього директора в системі комутації;

– Після встановлення зв'язку і до моменту входу користувача в систему, останняне повинна видавати ніякої інформації;

– В системі необхідно використовувати паролі, що складаються не менше ніж з семи знаків, і коди користувачів повинні відрізнятися від запропонованих фірмою-виробником;

– Повинна бути реалізована програма динамічних паролів для гарантії їх постійнї зміни при звільненні службовців з даної установи;

– Функції терміналів повинні бути точно визначені, наприклад платіжні відомосі повинні вводитися тільки через певні термінали.

Щоб перешкодити злочинцям, політикам, провідним підривну діяльність, отримати несанкціонований доступ, необхідно технологію захисту пов'язати з технологічними процесами організації. Повинна бути проведена оцінка ризику, з тим щоб витрати на засоби управління і контролю відповідали ступеню ризику. Організація повинна шукати засоби для зниження мотивації злочинів в системі шляхом запровадження:

– Паролів і процедур персональної ідентифікації;
– Засобів контролю за операційною системою;
– Контролю доступу;
– Контролю за базою даних;
− Контролю за мережею.

2.4. Зарубіжній досвід технологій створення захищеного простору суб'єкта підприємніцької діяльності

На механізм забезпечення безопасности фірмі вочевідь вплівають економічні, Соціальні, організаційні и правові чинників. Кожна країна, а відтак кожен її суб'єкт бизнеса має свої особливості у правовому врегулюванні і організаційному забезпеченні особістої безопасности. Враховуючі недостатність нормативно-правового, наукового та навчально-методичного забезпечення у формуванні та забезпеченні безопасности вітчізняного бизнеса, Варто вдатіся до вивчення досвіду розвинутих зарубіжніх країн у даній сфері.

2.4.1. Сполучені Штати Америки

Специфіка соціально-економічних відносін у США пояснюється ринковий розвіненістю та особливим статусом непорушний права пріватної власності. Головна увага діяльності державних правоохоронних органів та громадський и конфіденційність охоронно-детективне агентство спрямована на реалізацію законодавчо закріпленої Програми профілактики й протидії широкому спектру зловживань у сфері бизнесу. Така співпраця органів держави з недержавного інстітуціями має вже трівалий характер та значну результатівність, завдякі чому зміст віщезгаданіх програм щодо протідії злочину проявів у сфері бизнеса виявляється в його стабільності та мінімізації втрат.

Особлівістю законодавчого закріплення діяльності недержавних правоохоронніх організацій США полягає у тому, що ця країна й досі не має єдиного федерального закону про приватну детективну й охоронній діяльність. У сорока з п'ятдесяти штатів для здійснення охоронно-пошукових функцій потрібна ліцензія, яка видається владою даного штату у формі дозволу на офіційне здійснення охоронно-пошукової діяльності в бізнесі. При цьому всі класи ліцензії видає спеціалізована державна комісія, яки оцінює в рамках установи відповідність особістих якостей та професійної підготовки претендента кваліфікаційнім вимогам.

А тому самє цим можна пояснити зростання кількості суб'єктів бізнесу країни, що воліють встановити партнерські угоди з відповіднімі охоронно-детективними агентствами, витрачаючі при цьому значні кошти, що за

підрахункамі спеціалістів, вже перевищують 6 млрд дол. США. Користування охоронними послугами щодо внутрішніх приміщень поступово витісняє укладання договорів зі страховими компаніями, які виплачують компенсацію за збитки від дрібніх крадіжок, що їх вчіняють співробітнікі фірм, особливо у торгівельній сфері. Це пояснюється меншою затратністю і оперативністю діяльності власної або ж найнятої служби безпеки, адже страхова компанія не надає охоронної послуги, а лише компенсує втрати від нанесених збитків. І самє тому 11 млрд дол. США керівники фірм вітрачають саме на охорону внутрішніх приміщень своїх офісів, виробничих, торгівельніх та інших приміщень.

Однак не варто забуваті ї про державні органи правопорядку, аджея в разі легалізації (відмівання) коштів, отриманих злочиннним шляхом, вчинення розбоїв, грабежів, зломів приміщень організації, суб'єкти бизнеса звісно звертають самє до них. У такому разі об'єктом правопорушення виступають публічні суспільні відносини, а відтак самє держава, и притому більшою мірою, має докласті зусіль для відновлення порушених норм права. Водночас, коли йдеться про економічні правопорушення такого характеру, як-то: крадіжкі вантажів, документів; підробка кредитних карток, платіжніх документів; хабарніцтво, фінансові махінації; комп'ютерні злочину; крадіжкі, вчінені співробітнікамі фірм, підпріємці звертають до недержавних інстітуцій в силу незначних обсягів понесених втрата, бюрократічності судових процесів, а також їх довгої тривалості [44, 56].

Причиною відмові керівніків фірм от допомог державних правоохоронніх органів є також їх небажання розголошувати через слідство інформацію про злочин, що може завдаті шкоди бізнесовому іміджу даної фірми. Особливо характерним це є для установ банківської системи, де інформацію про правопорушення, як правило, замовчують, а втрати покривають прибутком організації. Небажаним є також витік інформації про правопорушення до засобів масової інформації, конкурентів, контролюючих державних органів. Усі ці моменти спонукають 70% американського підпріємців звертатись за допомогою до відповідніх охоронно-детективних агентств.

Не менше важливою особливістю американського бизнесу є врахування психологічного моменту, який передбачає зазвічай безконфліктне звільнення працівника-порушніка інтересів фірмі, причому з обов'язковим інформуванням широкого кола підпріємців щодо протиправної поведінки такого горе-працівника, що за умови обов'язкового надання ним рекомендаційного листа від попереднього працедавця новому працедавцю породжує складність при подальшому працевлаштуванні.

До певної мірі співпраця з відповіднімі охоронно-детективними агентствами дає змогу керівнікам фірм самостійно візначаті: рівень такої співпраці; тріваліть та обсяг робіт; об'єкти, що підлягають охороні, способи спостереження за ними; особливі умови виконання домовленостей (конфіденційність, терміновість, обсяг послуг, що надаються та плата за них). тобто керівник фірми самостійно зазвичай, двосторонньо визначає процедури накопичення, зберігання, використання та подальшого знищення комерційної, ділової та

іншої інформації, що може висвітлити чі розголосити фінансове, боргове чи інше становище фірми.

Успішні суб'єкти бизнесу, співпрацюючі з найнятім охоронно-детективними агентством, з метою мінімізації господарських ризіків можуть створювати власні служби безпеки. Більше того, у США характерною при створенні таких служб є частка працівників ФБР та ЦРУ, що дає змогу використовувати власну базу даних, досвід відбору працівників до служби безпеки фірми та сформуваті при них мвої спеціалізовані відділі чі відділення, в якіх, як правило, працюють співробітнікі спеціальніх служб в особі офіцерів безопеки. У такий спосіб держава не втручаючися у виробничо-господарський процес фірми, намагається не допустити, або ж мінімізуваті потенційні втрати суб'єкта бізнесу. Означена ситуація характерна й для банківської системи України, де у штаті служби безпеки комерційного банку перебуває офіцер-оперативник Управління по боротьбі з організованою злочінністю, завдяки чому керівніцтву банку однозначно легше проводити свою кредитну політіку, оскільки потенційного позичальника кредиту перевіряють через систему бази даних спецпідрозділу. Водночас офіцер безопеки спрощує механізм отримання та вивчення банківських документів у разі проведення відповідніх перевірок з боку правоохоронців.

Заслуговує увага досвід американців щодо створення у США широкомасштабної системи колективної безопеки американського бизнесу, що запроваджується з початку 90-х рр. У її рамках Державний департамент і 500 корпорацій США регулярно обмінюються інформацією з найгострішіх питань загрози підприємніцької діяльності з метою захисту американських громадян.

У рамках Програми здійснюється інформаційний обмін через систему «електронного бюлетеня», що містіть інформацію про обстановку, попередження про можліві загрози для життя и власності американців, які працюють в 190 країнах, а також специфічну інформацію. Джерелом інформації при цьому є відомості зарубіжніх представництв, повідомлення ЗМІ, доповіді, довідки й коментарі розкиданіх по всьому світу американських агентств, контор, магазинів, що належать таким багатонаціональнім корпораціям, як American Air Lines, Procter and Gamble, Bank of America, McDonald's, IBM тощо, котрі стали, по суті, «очима й вухами» системи колективної безопеки американського бізнесу.

У 1988 р. створено групу реагування на комп'ютерні події CERT (Computer Emergency Response Team), яка існує на кошти Міністерства оборони США. В даний час CERT – одна з декількох десятків організацій, що стоять на варті мережі. Група збирає інформацію про зломи систем безпеки та пропонує рекомендації щодо запобігання їх у майбутньому. Якщо порушуються закони (наприклад, при розкраданні даних), то дослідники екстрених ситуацій передають отриману ними інформацію в Національний підрозділ по боротьбі з комп'ютерною злочинністю під егідою Федерального бюро розслідування або в Групу боротьби з комп'ютерної злочинністю Інтерполу.

2.4.2. Велика Британія

Беручи До уваги схожість соціальної, правової й економічної систем Великобританії та США, цілком закономірнім є схожість забезпечення безопеки бізнесу в ціх країнах. Так, аби не допустити, розголосу про відповідні правопорушення з боку працівників фірми або ж банку, що може завдаті їм удару по репутації та іміджу, керівництво свідомо йде на їх втаємничення від державних правоохоронців та громадськості. саме тому перелік правопорушен, зазвічай економічних, таких як шахрайство, злочини у комп'ютерній сфері, крадіжка інформації, – розслідують співробітнікі власний служб безопеки й, відповідно, перебувають поза увага правоохоронців та громадськості.

Самє приватні агентства почасти виконують той перелік специфічніх завдань, що їх ставлять суб'єкти, бизнесу за які не беруться правоохоронні органи держави в силу їх досить приватного або ж законом не визначеного характеру. Більшою мірою це стосується конфіденційності розшукових агентств, які обслуговують, окрім суб'єктів підприємніцтва, й осіб щодо їх приватного життя. Кількість таких агентств постійно зростає, позаяк зростає попит на такі послуги з боку як бізнесменів, так і приватних осіб.

Разом із тим у Велікобританії стосовно питання реєстрації конфіденційності детективів взагалі відсутні будь-які нормативні акти, що вимагають обов'язкової реєстрації конфіденційності детективів. Із двох тисяч детективів лише триста зареєстровані як члени Інституту професійніх слідчіх (Institute of Professional Investigators), розташованого у м. Блекберн [261-263].

Упродовж 90-х років уряд неодноразово ставив питання про введення такої реєстрації з обов'язковою спеціальною перевіркою детективів за обліком поліції. Адже ніде не зареєстрованій приватний детектив, без усякої ліцензії може застосовувати на свій розсуд доволі широкий арсенал оперативної техніки, вести спостереження за будь-якою особою, фотографувати об'єкт в усіх громадський місцях. Для нього доступна також криміналістічна лабораторія поліції Лондона. Власне тому Інститутом підготовкі працівніків слідчіх органів Велікобританії разом із парламентом підготовлено законопроект про обов'язкову реєстрацію кваліфікованих детективів. Особам, які у процесі відповідної перевірки й тестових процедур не зможуть пройти державну реєстрацію, буде в майбутньому заборонено працювати та пропонувати свої послуги в ролі приватного детектива. Порушників цього закону очікують штрафні санкції у досить великих розмірах.

Загалом керівники фірм ставлять перед фахівцямі охоронно-детективного агентства доволі складні аавдання, які передбачають приватні розслідування правопорушення, пов'язаних з комп'ютерними системами і шахрайством; забезпечення перевірки безопеки службово пріміщень, автотранспорту, домашнього житла; виявлення підслуховуючої техніки у ціх пріміщеннях; організацію особістої охорони керівніцтва, окремих клієнтів та працівніків фірм.

Значного досвіду набуто у Велікобританії в сфері безопеки вантажних та пасажирських перевезень, завдякі якому транспортні компанії об'єднані ро-

зроблення спільніх заходів протідії щодо нападів на інкасаторів, аварій, а також заходів відстежування на маршрутах перевезення цінностей, тощо. Однією з головних вимог забезпечення безопеки перевезень британці називають дотримання підвищених вимог щодо транспортних засобів: йдеться про куленепробівній, протиударній, пожежостійкій характер транспортних засобів; виготовлення їх із надміцніх матеріалів; обладнання сучасними засобами радіозв'язку, спецсигналами, надійнімі внутрішнімі засувамі, автоматичними замками та іншими засобами, що підвищують безпеку особи та транспорту. Крім того, сучасні спеціальні транспортні засоби обладнані приладами контролю (відеозасобамі) за роботою як самого транспортного засоба, так і обладнання, яким його укомплектовано, що дає змогу потім проаналізуваті дії персоналу та роботу спеціального обладнання.

Досвідом Велікобрітанії, який може бути використаний вітчизняними бізнесменами і державними діячами, є формування системи профілактичних заходів по формуванню та діяльності служб безопеки суб'єктів підприємництва. Вказана система включає в себе як окремі, так и загальні профілактичні заходи. змістом окремого заходу є вплив на конкретних працівніків фірмі з боку фахівців-псіхологів, задля недопущення ними протиправної діяльності або інших дій, що підривають безпеку організації. Таку профілактічну роботу проводять не з усіма працівниками фірми, а ліше з тими, від якіх можна очікувати певних порушень, або з тими, які вже його вчинили, і це може призвести до втрати майна чи завдаті шкоди іміджу фірми. Проведення такої складної профілактічної роботи неможливе без поінформованості керівніцтва фірмі чі її служби безпеки про ймовірність вчинення певних правопорушень. і британці в цьому напрямі пішли досить далеко, адже фірми щороку видиляють значні кошти інформаторам за наданням інформації про вчінені чи про такі, що готуються, правопорушення.

Щодо системи загальної профілактікі, то її основу становляит політичні, економічні, правові та ідеологічні заходь впливим на всіх без вінятку працівніків та клієнтів фірмі. Названа система включає в себе й вищерозглянуті окремі заходи, оскількі виступає макрорівнем загальної системи безопеки фірми.

Система тотального контролю не оминула й найбільші комапанії. У скандал про несплату податків великими компаніями у Великій Британії виявилася замішана компанія Microsoft, яку звинуватили в несплаті податків на прибуток від інтернет-продажів у розмірі 1,7 млрд фунтів стерлінгів.

Компанію підозрюють у тому, що вона уникає підвищених податків, проводячи онлайн-платежі за Windows 8 і скачування іншого програмного забезпечення через Люксембург та Ірландію, де податок на прибуток нижчий, ніж у Великій Британії Це означає, що зареєстрована в Ірландії "дочка" Microsoft – Microsoft Ireland Operations Ltd – отримала 1,7 млрд фунтів стерлінгів прибутку в Британії, на які компанія не виплатила податок.

2.4.3. Німеччіна

Специфіка ментальності німецького народу не могла не позначітіся на особливостях забезпечення безопеки бізнесу в Німеччіні. Приватний охоронно-детективний ринок у Німеччіні представлений широким колом його учасніків, що у змозі надаті бізнесменам якісні послуги у сфері безопасности. Разом із тім, на відміну від інших європейськіх країн, у Німеччіні проглядається висока зацікавленість держави у стабільності вітчізняного бизнеса. Так, уряд Німеччини створив національні спецслужби для контролю за ситуацією на економічно важливих об'єктах країни. Як протідію впливим іноземніх спецслужб, німці створюють на національному рівні контррозвідувальні підрозділі, які у взаємодії з приватними охоронно-детективними агентствами виконують функції безопеки як щодо фірми, так и щодо її керівніцтва, і окремо, щодо працівніків та клієнтів. У зв'язку з цим на приватні агентства інколи покладають обов'язки здійснення окремих заходів оперативно-розшукової діяльності, що в умовах законодавства України категорично заборонено. Головним чином це отримання оперативно-значущої інформації про вчінені чі ті, що плануються, правопорушення як на фірмі, так и на загальнодержавному рівні. причому населення Німеччіні своїм громадянським обов'язком вважає поінформуваті відповідні органи про правопорушення, що стали їм відомі, і отримують за це винагороду, сума якої може перевіщуваті сто тисяч євро.

Особлива увага як детективних агентств, так і державних спецслужб приділяється до створюваних на території країни спільних підприємств, тобто вливання в німецьку економіку іноземного капіталу. Німців, з їх ліберальним господарським законодавством турбує думка, з якою пріїхали до них іноземці, в який спосіб вони здійснюватимуть свій бізнес. особливе занепокоєння викликає в німців інформація про наявність на фірмі співробітніків-агентів спецслужб, що є, зрештою, підставою для їх виселення за межі країни, а також при пинення діяльності або ліквідації такої фірмі.

Власне тому, співробітнікі спецслужб і детективних агентств здійснюють постійний моніторинг ситуації на спільніх підпріємствах і вивчають поведінку іноземніх громадян щодо дотримання ними вимоги закону та інтересів бизнесу. Для цього на спільніх підпріємствах укладають спеціальні домовленості з керівніцтвом та працівнікамі фірмі, яких повинні дотримуватись упродовж усього періоду функціонування фірми. Серйозну допомогу агентствам і спецслужбам надають й інші державні органи – розвідувальні служби ФРН, карної поліції, мітної служби, прикордонних військ та органів місцевого самоврядування земель та округів.

Таке серйозне ставлені держави до системи забезпечення безопасности бизнеса в Німеччіні не могло не позначитися на процедурі державної реєстрації охоронно-детективних агентств. До них ставлять достатності суворі вимоги щодо фінансових, технічних чи професійніх можливостей, критерії якіх закріплені директивами урядових органів окремих земель ФРН. Більше того, отримання дозволу на реєстрацію приватного агентства не позбавляє обов'язку підпріємця отримати дозвіл на укладання контрактів із

замовником, що дає можливість державі контролювати систему оподаткування та недопущення чи зниженя рівня загрози бізнесу [44].

Німецька влада закликала громадян ФРН тимчасово відмовитися від використання Internet Explorer, після того як стало відомо, що він зазнав вірусної атаки Ліків від вірусу поки не існує Є підозри, що він може загрожувати підрядникам Міністерства оборони.

Експерти німецького Агентства із захисту інформації (BSI) вивчили схему поширення вірусної загрози і, як і американські фахівці, прийшли до висновку, що хакери намагаються заманити Інтернет-користувачів на заражений Інтернет-сайт. Вірус здатний поширюватися дуже швидко. З цієї причини громадянам не радять користуватися Internet Explorer, поки Microsoft не випустить оновлення, що усуває дефект у системі захисту браузера.

2.4.4. Україна

Наша держава розуміє важливість створення інформаційного суспільства, прискорення цього процесу. Ще 18 квітня 2002 року на другому засіданні Міжвідомчої комісії з питань інформаційної політики й інформаційної безпеки при Раді національної безпеки й оборони України було запропоновано започаткувати довгострокову програму під умовною назвою «Електронна Україна», у рамках якої передбачено заходи щодо формування завершеної нормативно-правової бази у цій сфері, створення ефективного механізму інформаційної взаємодії органів влади усіх рівнів, впровадження електронного документообігу та забезпечення інформаційної безпеки. Йдеться про утворення в країні такого електронного середовища, у якому наш громадянин зможе ефективно здійснювати усі свої звичайні взаємини з навколишнім світом – працювати, спілкуватися, контактувати з державними органами тощо.

Ще одним важливим аспектом цієї проблеми є надання вичерпної інформації про діяльність органів влади, що, без сумніву, сприятиме зростанню суспільної довіри, без якої неможлива ефективна діяльність держави. Можливість стійкого зворотного зв’язку завдяки Інтернету дозволяє громадянам не тільки одержувати достовірну інформацію про роботу урядових структур, але й надавати їм свою інформацію.

Необхідною умовою створення «Електронної України» є, в першу чергу, формування нормативно#правової бази. У Європі вже розроблено два модельні закони, що рекомендуються для прийняття всіма країнами, які мають намір інтегруватися в електронний простір континенту. Це закон про електронну комерцію і закон про електронний цифровий підпис. Деякі країни імплементують ці закони без змін, інші ж вносять до них певні корективи, продиктовані своїми національними особливостями.

На основі згаданих модельних законів готується і правова база «Електронної України». Уже розроблено законопроекти про електронний документообіг, прийнятий закуно про електронний цифровий підпис, обговорюються пропозиції щодо правил ліцензування діяльності провайдерів, а також правил підключення органів державної влади до Мережі.

Розроблено Web-порталу Кабінету Міністрів, на якому розміщуватиметься інформація про діяльність органів виконавчої влади. Стратегічно Web-портал визначається не як єдина база даних, а як єдина пошукова система державних органів. Знаючи одну Інтернет-адресу, один телефонний номер, громадянин зможе знайти будь-яку інформацію, що його цікавить.

Електронна взаємодія громадян і державних органів забезпечується механізмами спілкування громадян і представників влади у віртуальному просторі в реальному масштабі часу: обговорення пропонованих і прийнятих рішень, з'ясування тих чи інших питань. Наприклад, на сайтах деяких державних органів України вже діють Інтернет-приймальні. Звернувшись до такої приймальні з електронним листом, громадянин має можливість одержати відповіді на свої запитання. Деякі урядовці ведуть мікро-блоги в мережі Twitter.

Електронне обслуговування громадян державними органами здійснюєтьсяустановами, спеціально уповноваженими на це державним органом, у тому числі й на комерційній основі. Наприклад, громадянин може за електронними запитами одержувати ті чи інші документи, що стосуються діяльності державного органу, подавати електронні податкові декларації, вдаватися до електронної реєстрації тих чи інших правових актів (договорів, доручень, прав володіння власністю).

У рамках створення інформаційно-аналітичного забезпечення діяльності органів державної влади розроблено концепції, здійснюються окремі робочі проекти, впроваджуються Закон України «Про Національну систему конфіденційного зв'язку», урядова Постанова «Про порядок формування і виконання галузевої програми (проекту) інформатизації», документи з питань криптографічного захисту інформації. На цей час в інформаційній сфері України застосовується близько 80 нормативно-правових актів.

У Мережі з'являється все більше сайтів державних органів, партійних структур, численних міжнародних неурядових організацій, що містять багату інформацію, яка істотно підвищує політичну поінформованість громадян. Доступними для широкої громадськості, а не лише для «обраних», стають урядові документи. Інтернет стимулює появу нових, ефективніших механізмів політичної мобілізації громадян. Без перебільшення його можна вважати засобом досить оперативної організації і координації дій політичних однодумців, що є прихильниками нетрадиційних соціальних рухів.

«Електронний уряд» є новою, вищою стадією розвитку уряду епохи модерну в умовах інформаційного суспільства. За результатами щорічного огляду „електронних урядів", проведеного компанією Accenture, у ході якого були вивчені державні онлайнові служби 23 країн, перше місце присуджено державному порталу Канади. Критеріями були інформативність, інтерактивность і можливість здійснення трансакцій. До 2004 року громадяни Канади одержать доступ до усіх федеральних служб і програм.

На другому місці виявився Сінгапур, „електронний уряд" якого надає громадянам такі послуги, як реєстрація народження дитини, шлюбу, пошук

житла, відправлення повідомлень у поліцію. До речі, саме в цій країні вперше у світі було реалізовано ідею урядового порталу.

Третє місце одержав „електронний уряд" США. Зі значним відривом від лідерів ідуть Австралія, Данія, Велика Британія, Фінляндія, Гонконг, Німеччина, Ірландія, Нідерланди, Франція і Норвегія [62].

Заходи з комп'ютеризиції державних органів цілком слушні, оскільки вже половина українців постійно користуються Інтернетом. Найбільше Інтернет-користувачів віком від 15 до 29 років.

За наявною статистикою, Близько 19,7 млн, або 50% українців віком від 15 років є регулярними інтернет-користувачами При цьому 13,3 млн людей входять у глобальну мережу щодня Про це свідчать дані опитування, проведеного в жовтні компанією InMind на замовлення Інтернет асоціації України.

За останні два роки кількість постійних користувачів зросла в 1,5 рази – із 33% у третьому кварталі 2010 року до 50% у третьому кварталі 2012 року.

Найбільше Інтернет-користувачів віком від 15 до 29 років - 43%, віком 30-44 років - 35%, і від 45 років і старше - 23%. При цьому інтернетом рівною мірою користуються як чоловіки (51%), так і жінки (49%).

За 2011 рік кількість користувачів глобальної мережі в Україні зросла на 11%. Всього користуються інтернетом 43% опитаних українців.

2.4.5. Цензура в Інтернеті

Зростання кількості злочинів, зчинених із застосуванням всесвітньої мережі, викликає відповідну протидію з боку урядів, які наполягають на цензуруванні інформації, яка доступна з Інтернету в межах своєї країни.

Щорічно до Google звертається влада демократичних держав із проханням цензурувати контент.

У першому півріччі 2011 до Google надійшло більше тисячі вимог від урядів усього світу забрати текстові матеріали або відео образливого змісту 461 вимога надійшла від судової влади, 546 – носили неофіційний характер і надійшли, наприклад, від поліцейських чиновників по телефону. Разом Google задовольнив 54% вимог І ця практика набуває дедалі систематичнішого характеру. "Ми сподівалися, що це виняток із правила, але тепер переконалися, що це не так", – пише в офіційному блозі головний аналітик Google Дорот Чу. Його турбує те, що в практику входять вимоги застосовувати цензуру політичного характеру. Причому деякі такі вимоги, підкреслює Чу, надходять від західних демократичних країн, які не асоціювалися раніше із цензурою.

Щодо Італії, то з цієї країни надійшло 28 вимог, які стосувалися здебільшого відео з колишнім прем'єром Сільвіо Берлусконі: на одному під прицілом виявилися його сексуальні звички (воно не було вилучено), на другому містилися заклики до його усунення (відео піддалося цензурі).

Як зазначає видання, найактивнішими в замовленні "цензури" виявилися Бразилія (128 звернень), Індія, Болівія, Чехія, Україна і Йорданія. Найжорстокішими цензорами визнані Сполучені Штати: число вимог про цензуру за

один рік зросло на 103% У другій половині минулого року уряд США вимагав дані про 6321 абонента Google задовольнив практично кожну другу вимогу.

В цілому у світі ситуація з урядовою цензурою погіршується. Компанія Google опублікувала звіт Google Transparency Report за запитами користувальницької інформації та фільтрації контенту урядовими структурами та правоохоронцями в різних країнах світу.

Згідно з даними звіту, Україна не входить до десятки країн з найвищими показниками за рішеннями від урядових органів і судів забрати контент із сервісів Google. Згідно кількістю запитів в період з липня по грудень 2011 року в Україні було менше 10 запитів на видалення контенту за постановою суду, всі з яких були виконані Водночас не надходило жодного запиту від інших урядових органів.

Найбільше таких запитів компанія отримала в США (117 від суду, 70 від інших органів, на кшталт поліції), Бразилії (128 і 66 відповідно), Німеччини (60 і 43), Аргентини (39) та Індії (менше 10 від суду і 96 від інших урядових органів) Зазначимо, що минулого року даних щодо України у цій категорії у Google взагалі не було. Також Україна не була включена Google в список країн, від урядів яких в період з липня по грудень минулого року надходили запити на передачу даних користувача У Росії таких запитів надійшло 58.

В цілому ж у світі ситуація з урядовою цензурою погіршується, зазначають в компанії Так, в офіційному блозі повідомляється, що політичною цензурою в зазначений період займалися навіть західні демократичні країни, наприклад, Іспанія та Польща. Нагадаємо, в березні Україна вийшла на перше місце серед країн світу за якістю Інтернет-підключення. Згідно з даними рейтингу Netindex, станом на березень 2012 року, середній показник якості доступу до Інтернету в Україні за період з 1 жовтня 2009 року по 13 березня 2012 становив 87,54 пункту, а в Росії, яка посіла друге місце – 87,02.

2.4.6. Міжнародні організації із протидії кіберзлочинам

Жертви кіберзлочинності можуть звернутися в наступні структури:

1. Міжнародну Web-поліцію – International Web Police (www.web-police.org/forms/wp_crimereport.html). Сайт спеціалізується на міжнародних злочинах. У випадку шахрайства зміст заповненої жертвою форми буде передано до відповідних правоохоронних органів країни, громадяни якої беруть участь в афері. Web Police тісно співпрацювати зі спецпідрозділами, які займаються Інтернет-злочинністю.

2. Центр аналізу інтернет-шахрайства - Internet Fraud Complaint Cen-ter (www.ifccfbi.gov / cfl. Asp). Сайт підтримується американським Федеральним бюро розслідувань і відповідно чаші всього займається злочинами, які відбулися в США або якось зачепили інтереси американських громадян. Тим часом співпраця ФБР з правоохоронними органами інших країн дозволяє сподіватися на те, що проблема розслідування злочинів в інших країнах все-таки буде вирішена.

3. Офіційний сайт Центру дослідження проблем комп'ютерної злочинності (http://www.crime-research.org/).

2.5. Індивідуальне завдання №2.

Тема роботи: Вивчення основних державних Інтернет-ресурсів України,

Мета роботи: Визначення небезпек, які можуть спіткати державні портали.

Завдання: За останьою номеру списку в групі згідно табл. 2.2 обрати собі сайт відповідної державної установи.

1. Знайти адресу відповідного сайту.
2. Ознайомитися з його структурою.
3. Визначити, які види комп'ютерної злочинності можуть вплинути на цей сайт.
4. Запропонувати заходи по унеможливленню кіберзлочинності.
5. Написати звіт за виконаною роботою в обсязі до 10 сторінок, кеглем 14, шрифт Times New Roman через 1,5 інтервали. Текс ілюструвати елементами зображень з сайту.

Таблиця 2.2

Числові значення згідно індивідуального завдання

№ п/п	Назва органу державного управління	№ п/п	Назва органу державного управління
1	Президент України	16	Верховна Рада України
2	Конституційний суд України	17	Кабінет міністрів
3	Міністерство фінансів	18	Міністерство енергетики та вугільної промисловості
4	Міністерство юстиції	19	Міністерство оборони
5	Міністерство екології	20	Міністерство економічного розвитку і торгівлі
6	Міністерство регіонального розвитку і будівництва	21	Міністерство культури
7	Міністерство закордонних справ	22	Міністерство соціальної політики
8	Міністерство внутрішніх справ	23	Міністерство аграрної політики та продовольства
9	Міністерство з питань надзвичайних ситуацій	24	Міністерство охорони здоров'я.
10	Державна служба геоології надр	25	Державна служба з питань захисту персональних даних

11	Державне агентство водних ресурсів	26	Державна служба експортного контролю
12	Державне агентство з енергоефективності та енергоконтролю	27	Державна фінансова інспекція
13	Державна служба фінансового моніторінгу	28	Державна податкова служба
14	Державна митна служба	29	Державна казначейська служба
15	Державна авіаційна служба	30	Державне агентство автомобільних доріг

Контрольні запитання

1. Які типи кіберзлочинів найбільш характерні для державних установ?
2. Назвіть методи виявлення кіберзлочинця.
3. Якими правила потрібно користуватися державному слуцжбовцю, щоб забезпечити збереження державвної таємниці?
4. Чи існує можливість звернутися до міжнародних організацій із захисту електронної інформації?
5. Чим викликана поява цензури в Інтернеті?

В розділі подано інформацію про задачі держави по формуванню безпечнеого середовища країни для електронної комерції, вивчать основні прийоми забезпечення захисту комп'ютерної інформації в державних установах та визначення потенційних порушників безпеки. Наведені приклади державного регулювання в різних країнах.

РОЗДІЛ 3. ЗАХОДИ БЕЗПЕКИ ФІНАНСОВИХ УСТАНОВ

В розділі подано перлік можливих загроз та заходів по ї уникнення в роботі платіжних систем.

Розробники приділяють велику увагу безпеці систем Інтернет-банкінгу в силу того, що вся інформація в даних системах від клієнта до банку передається по відкритій мережі Інтернет. Як правило, для підвищення безпеки захист переданої інформації забезпечується на двох рівнях. По-перше, для входу в будь-яку систему від клієнта потрібне введення його ідентифікаційних даних - логіна і пароля. Можливість перехоплення конфіденційної інформації під час її передачі від клієнта в систему запобігається шифруванням даних, що пересилаються.

Другий і найбільш суттєвий момент полягає в тому, що при здійсненні будь-якої транзакції система повинна переконатися, що всі розпорядження здійснюються зареєстрованим клієнтом. Для цього вся передана інформація "підписується" клієнтом електронно-цифровим підписом (ЕЦП). Саме з цієї "підписом" система аутентифікує користувача і дозволяє зробити необхідну операцію. ЕЦП-послідовність байтів, сформована шляхом перетворення електронного документа спеціальним програмним засобом за криптографічним алгоритмом і призначена для перевірки авторства електронного документа. ЕЦП є підтвердженням справжності, цілісності та авторства електронного документа.

3.1. Безпека платіжних систем

(за матеріалами з [23])

При створенні платіжних систем необхідно приділити якомога більше уваги захисту та забезпечення їх безпеки. Зазвичай розрізняється внутрішня і зовнішня безпека. Внутрішня безпека повинна забезпечувати цілісність програм і даних, забезпечення нормальної роботи всієї системи. Зовнішня - повинна захищати від будь-яких загрозливих збоєм в системі проникнень. В даний час існує два підходи до побудови захисту платіжних систем:

* Комплексний підхід –- об'єднує різноманітні методи протидії загрозам;

* Фрагментарний підхід -– протидія певним загрозам (антивірусні засоби і т. п.).

Комплексний підхід застосовується для захисту великих систем (наприклад, міжнародні міжбанківські мережі). У 1985 р. Національним центром комп'ютерної безпеки Міністерства оборони США була опублікована «Помаранчева книга», в якій було наведено звід правил і норм, а також основні поняття захищеності інформаційно-обчислювальних систем. Надалі ця книга

перетворилася на справжнє «керівництво до дії» для фахівців із захисту інформації. У ній визначаються описані нижче поняття.

Політика безпеки, тобто сукупність норм, правил і методик, на основі яких надалі будується діяльність інформаційної системи в галузі поводження, зберігання, розподілу критичною інформації.

Політика безпеки визначає:

1. Цілі, завдання, пріоритети системи безпеки.

2. Гарантований мінімальний рівень захисту.

3. Обов'язки персоналу щодо забезпечення захисту.

4 Санкції за порушення захисту.

5. Області дії окремих підсистем.

Аналіз ризику, що складається з декількох етапів:

1. Опис складу системи (тобто документація, апаратні засоби, дані, персонал і т. д.).

2. Визначення по кожному елементу системи вразливих місць.

3. Оцінка ймовірності реалізації загроз.

4 Оцінка очікуваних розмірів втрат.

5. Аналіз методів і засобів захисту.

6. Оцінка оптимальності пропонованих заходів.

Остаточно аналіз ризику виливається в стратегічний план забезпечення безпеки, важливим при цьому є розбивка інформації на категорії. Найбільш простий метод такого розмежування інформації наступний:

Конфіденційна інформація – доступ до якої суворо обмежений;

– Відкрита інформація – доступ до якої сторонніх не пов'язаний з матеріальними та іншими втратами.

Для комерційної діяльності такої градації цілком достатньо.

Найбільш поширеними погрозами безпеки є:

* Несанкціонований доступ, тобто отримання користувачем доступу до об'єкта без відповідного дозволу;

* Злом системи, тобто умисне проникнення (основне навантаження захисту в цих випадках несе програма входу);

* Маскарад, тобто виконання яких-небудь дій одним користувачем банківської системи від імені іншої;

* Вірусні програми, тобто вплив на систему спеціально створеними програмами, які збивають процес обробки інформації, і т. д.

Проблема забезпечення своєї інформаційної безпеки виходить за рамки однієї країни. Жоден з користувачів мережі не захищений на всі 100%. Виробляються нові програми захисту, але рано чи пізно знаходиться «розумник», який проходить через всі хитромудрі перепони. Одне з найбільших проникнень в банківську мережу за останні роки – спроба зняти більше $ 12 млн із Сітібанку (найбільший банк Америки і найбільший у світі торговець валютою) нашим співвітчизником Левіним в 1994 р. Більше чверті мільйона цієї суми досі не знайдено, і перспектив знайти і повернути гроші їх законному власнику поки немає. Все частіше і частіше засоби масової інформації повідомляють про хакерів, зламували захист у віртуальних магазинах і роблять

покупки по чужих кредитних картках. Йде свого роду змагання між «зломщиками» і «захисниками», і хто кого здолає, поки невідомо.

В залежності від існуючих загроз, розрізняють наступні напрямки захисту електронних систем:

1. Захист апаратури та носіїв інформації від пошкодження, викрадення, знищення.

2. Захист інформаційних ресурсів від несанкціонованого використання.

3. Захист інформаційних ресурсів від несанкціонованого доступу.

4 Захист інформації в каналах зв'язку і вузлах комутації (блкірует загрозу підслуховування),

5. Захист юридичної значимості електронних документів.

6. Захист систем від вірусів.

Існують різні програмно-технічні засоби захисту.

До класу технічних засобів відносяться: засоби фізичного захисту територій, мережі електроживлення, апаратні та апаратно-програмні засоби управління доступом до персональних комп'ютерів, комбіновані пристрої та системи

До класу програмних засобів захисту відносяться: перевірка паролів, програми шифрування (криптографічного перетворення), програми цифрового підпису, засоби антивірусного захисту, програми відновлення і резервного зберігання інформації.

Наприклад, розробники платіжної системи Webmoney Transfer зробили підвищені заходи безпеки для всіх повідомлень в системі за допомогою їх кодування. Використання спеціального алгоритму захисту інформації (схожого на алгоритм RSA, де довжина ключа більше 1024 біт) і використання спеціальних ключів при кожному сеансі передачі інформації дозволяє захистити інформацію про призначення та сумі платежу від чужого цікавості.

Керівні документи в галузі захисту інформації розроблені в Росії Державною технічною комісією (ГТК) при президенті РФ. Для комерційних структур ці документи носять рекомендаційний характер. У державному секторі та за наявності інформації, що відноситься до державної таємниці, вони обов'язкові для виконання. Технологій захисту даних багато, проте постійно з'являються нові. Компанія Intel, процесорами якою оснащені 85% всіх персональних комп'ютерів у світі, оголосила, що скоро почне випускати чіпи, в яких дані будуть захищатися на апаратному рівні, автоматично. США встановили обмеження на експорт потужних шифрувальних технологій, в Росії такими технологіями взагалі не можна користуватися без дозволу ФАПСИ (Федерального агентства урядового зв'язку та інформації при президенті РФ). Ні західних, ні наших сертифікованих програм захисту платежів, проведених через Інтернет, поки немає. Загалом, проблем достатньо, але віртуальна економіка не може не розвиватися. Будь-які платежі і банківські послуги в Інтернеті вигідні для клієнтів, вигідні для банків, вигідні для комерсантів, оскільки собівартість будь-яких електронних транзакцій в кілька разів нижче звичайних. Це шанс для російських банків стати відомими на міжнародному рівні і отримати світове визнання, причому в самі короткі терміни.

Платіжні системи в Інтернет – нові Інтернет-технології. Ідеально лягають на ідеологію мережі.

Розрахунки за допомогою платіжних систем в Інтернет характеризуються можливостями проводити оплату швидко, анонімно, з високим рівнем захисту, з будь-якого ПК підключеного до мережі, в будь-яких розмірах при низькій вартості транзакцій.

В основу цієї ідеї покладено боргові зобов'язання. Сертифікат на зобов'язання являє собою дуже грубо, файл із зобов'язанням виплатити пред'явнику певну суму грошей, підписану цифровим підписом емітента. Далі будь-який клієнт може обміняти в емітента (банку) певну суму грошей на таке зобов'язання і платити їм, передаючи його по Інтернету. Одержувач може пред'явити його до оплати або використовувати далі аналогічним чином. Технологічні проблеми - наприклад, розміну і захисту від копіювання - успішно вирішуються сучасними криптографами.

Переваги: Швидкість, зручність, низька вартість, безпека.

Клієнт-банк - управління банківським рахунком через Інтернет. Звично. Надійно.

У цих системах закладена ідея управління своїм банківським рахунком на відстані.

При цьому і покупець, і продавець мають в системі свої рахунки і процедура оплати зводиться до команди банку передати гроші з першого на другий. Для використання таких систем потрібна спеціальна програма для доступу до рахунку або управління через браузер. При цьому забезпечується захист даних (на комп'ютері користувача) і в процесі передачі, ідентифікація користувачів по секретним і / або симетричним локальним ключам і / або сертифікатами. Рахунки можуть бути прив'язані до реальної особи чи організації або бути анонімними.

Недоліки: модель є внутрішньобанківської, то є можливість проводити оплату, залежить від роботи банку (тільки робочий час); система не забезпечує достатньої приватності навіть при анонімних рахунках.

Схема оплати за картками, розроблена під традиційні продажу, і в принципі повільна і ненадійна. Існує дві схеми оплати за допомогою пластикових карток:

1. Обмін відкритим текстом. По суті це не система, а найпростіший спосіб оплати в Internet - за допомогою кредитної картки (як при замовленні по телефону), з передачею по Internet всієї інформації (номери карт, маючи і адресу власника) без яких-небудь особливих заходів безпеки. Недоліки очевидні: інформація легко може бути перехоплена за допомогою спеціальних фільтрів, і використана на шкоду власникові картки. У продавця буде проблема, пов'язана з відмовами від оплати. Цей спосіб втратив свою практичну цінність.

2. Системи, що використовують шифрування обміну. Кілька більш захищений варіант в порівнянні з попереднім - оплата за допомогою кредитної картки, з передачею по Internet всієї інформації за допомогою безпечних або захищених протоколів сеансу зв'язку (шифрування). Хоча перехопити інфо-

рмацію під час транзакції практично неможливо, така інформація знаходиться під загрозою вилучення на сервері продавця. До того ж існує можливість підробки або підміни identity як продавцем, так і покупцем. Є можливість і у покупця викачати "по кредитній карті" інформацію, а потім відмовитися від оплати - довести, що це саме він користувався своєю карткою, а не "злісний хакер", вельми важко, так як немає підпису.

До недоліків відносяться такі: низький рівень безпеки (1,15% всіх онлайнових покупок є підробленими); високі витрати на проведення транзакції роблять системи непристосованими для мікроплатежів, що є цільовим ринком платіжних систем Internet; відсутність анонімності і, як наслідок, нав'язливий сервіс з боку торгових структур.

Смарт-карти – це нові технічні розробки. Вже є розвинуті системи.

Сучасна смарт-карта – це маленький комп'ютер зі своїм процесором, пам'яттю, програмним забезпеченням і системою введення / виводу інформації. Далеко не всі смарт-карти несуть в собі цифрова готівка. Поки смарт-карта вживається як звичайна дебетова картка, до якої вносяться записи про списання грошей, або просто інформація про клієнта. Готівкові цифрові гроші на базі смарт-карт не тільки можуть забезпечити необхідний рівень конфіденційності та анонімності, але і не вимагають зв'язку з центром для підтвердження оплати, так як на відміну від подібних систем на базі PC.

Переваги: Більш високий рівень захисту, швидкість транзакцій.

Недоліки: Висока вартість, обмежене поширення, вимагає технічного обладнання.

Цифрова готівка – це дуже великі числа або файли, які і відіграють роль купюр і монет.

На відміну від всіх перерахованих вище систем файли і є самі гроші, а не записи про них. Сучасні методи криптографії, зокрема, алгоритми сліпого підпису, не так давно розроблені, забезпечують їх надійну роботу. Витрати на функціонування такої системи значно менше витрат на всі вищеперелічені. Ідеально підходять для проведення мікроплатежів. На думку фахівців, саме мікроплатежі можуть забезпечити основний оборот продажів інформації в Internet.

Крім того, цифрові готівкові можуть забезпечити повну анонімність, так як не несуть ніякої інформації про клієнта їх витратити. Одним з варіантів цифрової готівки може бути цифровий чек.

Переваги: системи підходять для здійснення мікроплатежів; забезпечується необхідна захищеність і анонімність платежів.

Недоліки: порівняно мала поширеність.

3.2. Шифрування, як захист систем «Клієнт-Банк»

(за матеріалами з [65]

Захист інформації дуже важлива для фінансових систем, незалежно від того, засновані вони на фізичних або на електронних трансакціях. У реаль-

ному світі ми приділяємо багато уваги фізичній безпеці, а в світі електронної комерції доводиться піклуватися про засоби захисту даних, комунікацій і транзакцій. Маючи справу з мережевими комп'ютерами, слід пам'ятати про існування декількох ймовірних загроз. Вони перераховані в табл. 3.1, поряд з рішеннями, що дозволяють організувати і значно підвищити захищеність інформації, в тому числі і в ситуаціях, не пов'язаних з електронною комерцією, наприклад, при відправці конфіденційної інформації по електронній пошті.

Таблиця 3.1.

Загрози безпеці та методи їх усунення

Загроза	Рішення	Дія	Технологія
Дані навмисно перехоплюються, читаються або змінюються	Шифрування	Кодування даних, перешкоджає їх прочитанню чи спотворенню	Симетричне або асиметричне шифрування
Користувачі ідентифікують себе неправильно (з шахрайськими намірами)	Аутентифікація	Перевірка справжності відправника і одержувача	Цифрові підписи
Користувач отримує несанкціонований доступ з однієї мережі в іншу	Брандмауер	Фільтрація трафіку, що надходить в мережу або на сервер	Брандмауери, віртуальні приватні мережі

Шифрування використовується для аутентифікації і збереження тайни.

Криптографічні технології забезпечують три основних типи послуг для електронної комерції: аутентифікацію (яка включає неможливість відмови від скоєного (non-repudiation) і збереження таємниці. Ідентифікація (підвид аутентифікації) перевіряє, чи є відправник послання тим, за кого себе видає.

Аутентифікація йде ще далі – перевіряє не тільки особу відправника, але і відсутність змін в посланні.

Реалізація вимоги неможливості відмови не дозволяє кому б то не було заперечувати, що він відправив або отримав певний файл або дані (це схоже з відправкою замовленого листа поштою). І нарешті, збереження таємниці - це захист послань від несанкціонованого перегляду.

Щоб шифрування дало бажаний результат, необхідно, щоб і відправник, і одержувач знали, який набір правил (інакше кажучи, шифр) був використаний для перетворення первісної інформації в закодовану форму (зашифрований текст).

У самому простому випадку шифрування може заміняти кожну букву повідомлення іншої, віддаленої від неї на фіксоване число позицій в алфавіті, наприклад на 13.

Якщо одержувач знає, що відправник зробив з посланням, то він може повторити процес у зворотній послідовності (наприклад, замінити кожну літеру віддаленою від неї на 13 в протилежному напрямку) і отримати початковий текст.

Кількість біт у ключі onределяет число можливих комбінацій, чим їх більше, тим важче їх «розкрити» шифроване повідомлення. Наприклад, підібрати ключ і 8-бітний ключ допускає лише 256 (28} можливих числових комбінацій, кожна з яких також називається ключем. Чим більше можливих ключів, тим важче «розкрити» зашифроване послання. Таким чином, ступінь надійності алгоритму залежить від довжини ключа. комп'ютера не потрібно багато часу, щоб послідовно перебрати кожен з 256 можливих ключів (на це піде менше частки секунди) і, розшифрувавши послання, перевірити, чи має воно сенс.

. Але якщо використовувати 100-бітний ключ (що еквівалентно перебору 2100 ключів), то комп'ютеру може знадобитися кілька століть, щоб відшукати правильний.

Криптографія з відкритим ключем засновано на концепції ключової пари. Кожна половина пари (один ключ) шифрує інформацію таким чином, що її може розшифрувати тільки інша половина (другий ключ). Одна частина ключової пари - особистий ключ, відома тільки її власнику. Інша половина - відкритий ключ, поширюється серед всіх його кореспондентів, але пов'язана тільки з цим власником. Ключові пари володіють унікальною особливістю: дані, зашифровані будь-яким з ключів пари, можуть бути розшифровані тільки іншим ключем з цієї пари. Іншими словами, немає ніякої різниці, особистий або відкритий ключ використовується для шифрування послання; одержувач зможе застосувати для розшифровки другу половину пари.

Немає системи шифрування, яка б ідеально відповідала потребам для всіх ситуацій. У табл. 3.2 проілюстровані переваги і недоліки кожного типу шифрування.

Таблиця 3.2.

Переваги та недоліки криптографічних систем

Tun шифрування	Переваги	Недоліки
Шифрування з симетричним ключем	– Швидкість; – Легко реалізувати апаратно	– Обидва ключі однакові; – Важко поширювати ключі; – Не підтримує цифрові підписи
Шифрування з відкритим ключем	– Використовує два різних ключі; – Відносно просто поширювати ключі; – Забезпечує цілісність і неможливість відмови від авторства (за рахунок цифрового підпису)	– Працює повільно; – Вимагає великих обчислювальних потужностей

В табл. 3.3 показано, як час на розшифровку ключа методом повного перебору всіх варіантів залежить від довжини самого ключа.

Таблиця 3.3.

Порівняння витрат часу і коштів,
необхідних для «злому» ключів різної довжини

Вартість,	Довжина ключа, біт				
$	40	56	64	80	128
100000	2 секунди	35 годин	1 рік	7000 років	10^{19} років
1000000	0,2 секунди	3, 5 години	37 днів	70000 років	10^{18} років
100000000	2 мілісекунди	2 хвилини	9 годин	70 років	10^{16} років
1000000000	0,2 мілісекунди	13 секунд	1 година	7 років	10^{15} років
100000000000	0,2 мікросекунди	0,1 секунди	32 секунди	24 дня	10^{13} років

Пам'ятайте, що дане співвідношення оцінюється на підставі розрахунків для методу «тотального випробування » Потужність комп'ютерів постійно росте, а їх вартість падає, так що в майбутньому «злом» довгих ключів стане, на жаль, простіше і дешевше. розрахунки зроблені для методу «тотального випробування», тобто перебору всіх можливих ключів. Існують і інші методи «злому» ключів, в залежності від конкретного шифру (ось чому криптоаналитики не залишаються без роботи). Розрахунки для метода «тотального випробування» широко використовуються при оцінюванні стійкості тієї чи іншої системи шифрування.

У шифрах з секретними і відкритими ключами викоють різну довжину ключа, тому таблиця 3.3 не охоплює всіх вимог до безпеки.

У табл.3.4 порівнюються дві системи, однаково стійкі до атак методом повного перебору всіх можливих значень ключів – «Тотального випробування».

Таблиця 3.4.

Довжина таємного та відкритого ключів при однаковому рівні надійності

Довжина секретного ключа, біт	Довжина відкритого ключа, біт
56	384
64	512
80	112
768	1 792
128	2 304

Поширені алгоритми шифрування:

• DES (Data Encryption Standard) - блоковий шифр, створений IBM і затверджений урядом США у 1977 році. Використовує 56-бітний ключ і оперує блоками по 64 біт. Відносно швидкий; застосовується при одноразовому шифруванні великої кількості даних.

• Потрійний DES заснований на DES. Шифрує блок даних три рази трьома різними ключами. Запропоновано як альтернатива DES, оскільки загроза швидкого і легкого «злому» останнього зростає з кожним днем.

• RC2 і RC4 - шифри зі змінною довжиною ключа для дуже швидкого шифрування великих об'ємів інформації, розроблені Роном Райвест. Ці два алгоритми діють трохи швидше DES і здатні підвищувати ступінь захисту за рахунок вибору довшого ключа. RC2 – блоковий шифр, і його можна застосовувати як альтернативу DES. RC4 – це потоковий шифр і працює майже в десять разів швидше за DES.

• IDEA (International Data Encryption Algorithm) створений в 1991 році і призначений для швидкої роботи в програмної реалізації. Дуже стійкий шифр, використовує 128-бітний ключ.

• RSA названий на честь його розробників (Rivest, Shamir і Adelman). Алгоритм з відкритим ключем підтримує змінну довжину ключа, а також змінний розмір блоку тексту що шифрується. Розмір блоку відкритого тексту повинен бути менше довжини ключа, зазвичай складає 512 біт.

• Схема Діффі-Хеллмана (Diffie-Hellman) – сама стара з використовуваних сьогодні криптосистем з відкритим ключем. Не підтримує ні шифрування, ні цифрові підписи. Призначена для того, щоб дві людини могли домовитися про спільний ключ, навіть якщо обмінюються повідомленнями по відкритих лініях.

• DSA (Digital Signature Algorithm) розроблений NIST і заснований на принципі, званому алгоритмом Ель Гамаля. Схема підпису використовує той же тип ключів, що і алгоритм Діффі-Хеллмана, і може створювати підписи швидше RSA. Просувається NIST як стандарт цифрового підпису (Digital Signature Standard, DSS), але поки що далекий від всезагального визнання.

• Для передачі логіна і пароля користувача часто використовуються стандартні засоби забезпечення захисту інформації у відкритих мережах. Найбільш поширеним є протокол SSL (Secure Sockets Layer) - обов'язковий атрибут будь-якого сучасного браузера. Протокол був розроблений компанією Netscape в 1994 році. SSL забезпечує шифрування всієї інформації, що передається від комп'ютера клієнта до сервера банку. Максимальна довжина ключа, використовуваного в даному протоколі, 128 біт, тобто існують 2128 можливих комбінацій "ключів", але лише один з цих ключів дозволяє отримати доступ до інформації.

Одним з найпоширеніших алгоритмів є алгоритм RSA, довжина ключа якого зазвичай 1024 біт. Принцип роботи цього алгоритму досить простий. Кожен учасник криптосистеми генерує два випадкових великих простих числа p і q, вибирає число e, менше pq і яке не має спільного дільника з (p-1) (q-1), і число d, таке, що (ed-1) ділиться на (p-1) (q-1). Потім він обчислює n =

pq, а *p* і *q* знищує. Пара (*n, e*) називається «відкритим ключем», а пара (*n, d*) – «закритим ключем». Відкритий ключ передається всім іншим учасникам криптосистеми (зазвичай це означає, що клієнт повинен прийти в офіс банку для запевнення відкритого ключа), а закритий зберігається в таємниці.

Наприклад, нехай учасники криптосистеми вибрали два простих числа. Перевірку на те, чи є обрані числа простими, легко провести із застосуванням елекутронних таблиць.Для цього достатньо поділити обрані числа послідовно на 2, 3, 5, 7 та 11 і якщо в усіх випадках результат буде не цілим, значить число є простим. Нехай це будуть числа $p = 11$ та $q = 7$. Оскільки прості числа є не парними, то їхній добуток дасть теж непарне число. А от добуток непарних числе мінус одиниця дасть парне число. Насправді, $(p\text{-}1)\ (q\text{-}1) = 60$, $pq = 77$. Отже, для вибору числа e потрібно обирати непарні числа, що у більшості випадків забезпечить дотримання вимоги $e < 77$ і не матиме спільного дільника з 60. Нехай перший учасник криптосистеми обрав $e = 13$. Тепер потрібно обрати число d. Для його знайдення пропонується наступний алгоритм.

Формується цільова функція виду

$ed/(p\text{-}1)\ (q\text{-}1) - \{ed/(p\text{-}1)\ (q\text{-}1), 0\} \rightarrow 0$

з обмеженням, d – ціле число.

Для використання функції Excel «Пошук рішення», потрібно, щоби стартове значення $d \approx 5(p\text{-}1)\ (q\text{-}1)$.

Як видно з рис. 3.1, результатом такого рішення стало число $d = 308$.

З розроахунків виходить, що чисдами «закритого ключа» будуть $e = 13$ та $d = 308$. Саме цими числами будуть кодуватися повідомлення і транзакції учасники криптосистеми, наприклад, два банки.

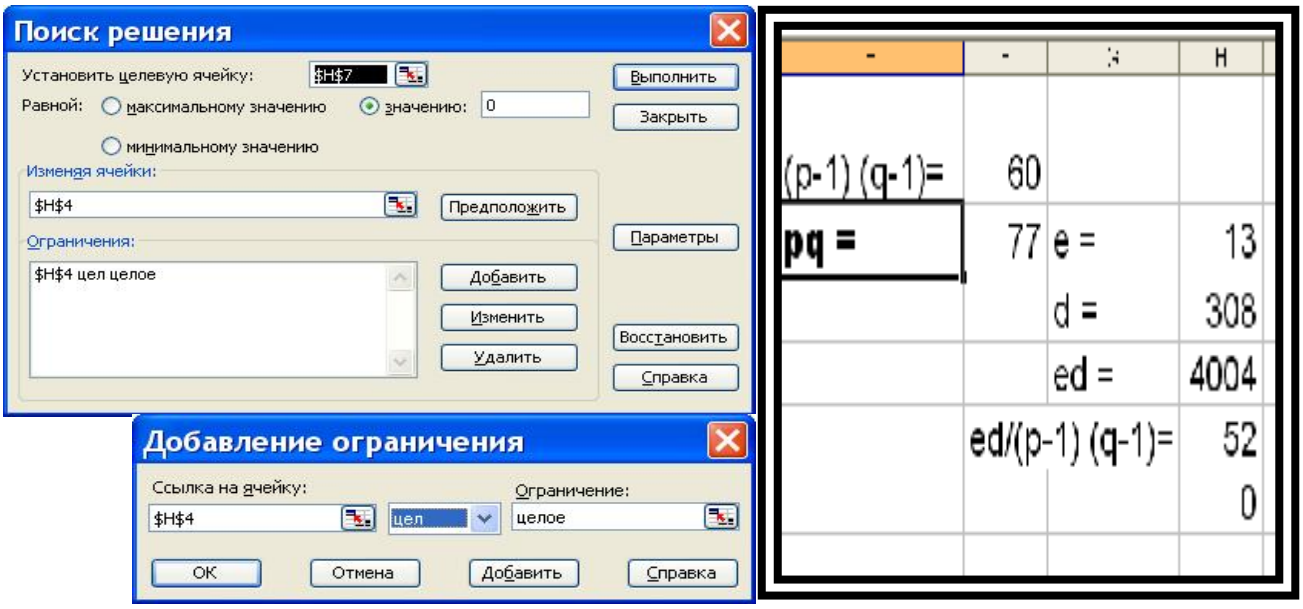


Рис. 3.1. Зображення активних вікон функції «Пошук рішення» елкетронних таблиць Excel та фрагменту результатів розрахунків «закритих ключів»

3.3. Шахрайства з використанням банків

Приховування частини виручки

Клієнти, які продають свої цінні папери через брокера банку, часто не порівнюють процентний дохід, зазначений у звіті про продаж цінних паперів, отриманий від брокера банку, з ринковим котируванням цих паперів на дату продажу. У звіті про продаж цінних паперів реальна ціна може бути занижена, що забезпечує особистий дохід, часто оформляється на третю фірму у вигляді комісійних за посередництво. Цей вид шахрайства зустрічається не тільки при продажі цінних паперів клієнтів, але й при їх придбанні. Тоді у звіті про покупку цінних паперів наводиться ціна вище фактичного біржового курсу.

Заміна знецінених цінних паперів

Сутність прийому полягає у підміні працівником банку своїх цінних паперів, які втратили високу прибутковість, на цінні папери, що належать банку. Звичайно, необхідно внести зміни до реєстру цінних паперів банку, але якщо сам працівник-махінатор його і веде, то проблем з цим не виникає.

В такому випадку не слід дозволяти одному працівнику приймати доручення на купівлю / продаж та доручати проводити організаційні заходи, а також здійснювати контроль за цінними паперами, пов’язаними з цими операціями, якщо звітність по них не перевіряється періодично компетентною особою.

Афери в банках

Останнім часом в Україні, Росії, Білорусі та Прибалтиці значна кількість дрібних банків були збанкрутовані самими засновниками. Схема була стандартна: після реєстрації банку залучалися нові клієнти, які переходили на розрахунково-касове обслуговування в установах банку або клали в банк гроші на депозит, активно залучалися ресурси з міжбанківського кредитування. Після акумуляції в банку достатньої суми засновникам банку видавалися дуже великі кредити, які в сукупності робили банк неплатоспроможним. Після цього засновники вмивали руки, а в збитку виявлялися клієнти банку.

У банківській сфері зловживання з боку персоналу – явище поширене. Особливо, як показує практика, в дрібних банках. Причина цього явища в першу чергу криється у виконанні однією людиною в невеликому банку кількох посад відразу. Це дозволяє зробити розкрадання в якості касира, а потім приховати його в якості бухгалтера.

«Касир помилився»

У цьому випадку працівником вилучається невелика сума грошей, потім доповідається про недостачу, яка виникла нібито через помилки в раніше зроблених розрахунках, і пропонується переробити старі документи. Таким чином, викрадаються невеликі суми, але якщо вміло обманювати вище начальство, яке беззаперечно приймає виправлення, сума може набратися досить велика.

Розкрадання грошей сторонньою особою

Існують також способи обману шахраями недосвідченого касира. У зарубіжній практиці відомі випадки, коли при перевірці каси ревізори знищували свої власні чеки або чеки компаньйона. В результаті у касира виникає нестача на суму чека, а ревізор з компаньйоном отримують дохід.

Списання коштів з рахунків клієнта

Якщо неуважно стежити за рухом грошей на рахунку свого підприємства, то гроші можуть бути списані на іншу фірму. Якщо списання виявляється – шахрай вибачається і повертає гроші. Якщо ніхто нічого не помітив – дохід отриманий.

Підміна справжньої валюти підробленою

Більшість клієнтів до цих пір довіряє банкам та їхнім працівників (хоча можливо, і в якійсь меншій мірі). Ця довірливість допомагає збувати через банк фальшиві грошові знаки. Але все ж основний вид такої афери – «всовування» замість нових купюр старих і пошарпаних, які важко реалізувати за повний номінал.

Присвоєння орендних платежів

Орендні платежі збираються, але в банк не здаються і фігурують у банківській звітності як заборгованість з орендних платежів.

Витягування грошей з пачок

Якщо клієнт отримує достатньо велику суму грошей, то в банку в нього часто немає можливості перерахувати кількість грошей в кожній пачці. Гроші без підрахунку відвезлися з банку і тільки вже в своєму офісі касир клієнта їх перераховує. Але робити це потрібно ще в банку. Тоді у разі помилки перед клієнтом вибачаться і видадуть потрібну суму. Інакше важко буде довести, що це не спроба шахрайства.

Електронне шахрайство

Поширене і так зване «електронне шахрайство» – злочини, які вчиняються за допомогою комп'ютерів. Наприклад, у великі фірми приходять листи з проханням уточнити дані по пластикових картах. При натисканні на посилання в цьому листі клієнт потрапляв на псевдосайт банку, де йому пропонували набрати номер кредитки і пін-код.

Шахрайства в сховищах для власності клієнтів

Деякі банки беруть від своїх клієнтів на безпечне зберігання цінні папери, документи та матеріальні цінності. Найбільш поширене шахрайство, пов'язане з виготовленням дублікатів ключів від сховищ клієнтів. Збитки від несанкціонованого доступу до камер сховища зазвичай виявляються при перевірці клієнтами своїх камер. Довести факт крадіжки з його камери клієнту буває дуже важко. Якщо викрадач не знайдений, то клієнту навряд чи відшкодують збитки.

«Продаж» клієнтів

Поширена практика, коли працівники нижчої та середньої ланки банку надають інформацію про своїх клієнтів банкам-конкурентам. При цьому клієнтам, що бажають покласти значні суми грошей на депозит у першому банку, спеціально повідомляються занижені депозитні ставки. Але тут же

повідомляється, що ставка по депозиту в іншому банку набагато вище. Клієнт дякує і несе гроші до вказаного банку. А цей працівник банку регулярно отримує комісійну винагороду від банку-конкурента.

3.4. Індивідуальне завдання № 3.

Тема роботи: Вивчення фінансових Інтернет-ресурсів України та розрахунок пари кодів за алгоритмом RSA.

Мета роботи: Визначення небезпек, які можуть спіткати портали фінансових установ та набуття уміння розраховувати парні коди за алгоритмом RSA.

Завдання А:

За останьою номеру списку в групі згідно табл. 3.5 обрати собі сайт відповідної фінансової установи, такі як: Банки, Страхові компанії та брокери, Компанії з управління активами, Кредитні спілки, Недержавні пенсійні фонди, Фондові біржі та торгівельні системи, Фінансові компанії.

1. Знайти адресу відповідного сайту.
2. Ознайомитися з його структурою.
3. Визначити, які види комп'ютерної злочинності можуть вплинути на цей сайт.
4. Запропонувати заходи по унеможливленню кіберзлочинності.
5. Написати звіт за виконаною роботою в обсязі до 10 сторінок, кеглем 14, шрифт Times New Roman через 1,5 інтервали. Текс ілюструвати елементами зображень з сайту.

Таблиця 3.5

Числові значення згідно індивідуального завдання

№ п/п	Назва фінансової установи	№ п/п	Назва фінансової установи
1	ПриватБанк	16	Капітал-Страхування
2	ПРАВЕКС-БАНК	17	Класичне страхування
3	ПУМБ	18	Сузір'я
4	ПІВДЕНКОМБАНК	19	ВАТ «Київська міжнародна фондова біржа»
5	Укрексімбанк	20	ТОВ «Dragon Capital»
6	Укрпромбанк	21	ТОВ "КУА "СКМ"
7	УкрСиббанк	22	ТОВ "КУА "Арт Інвест"
8	Укрсоцбанк	23	ТОВ "КУА "ВЛАДІНВЕСТГРУП"

№ п/п	Назва фінансової установи	№ п/п	Назва фінансової установи
9	Надра	24	ТОВ "Компанія з управління активами "Інтерстрой"
10	Мотор-Гарант	25	ТОВ "КУА "ЦЕНТР ФІНАНСОВИХ ТЕХНОЛОГІЙ"
11	Арсенал - Днепр	26	ТОВ "КУА "Український трастовий фонд"
12	Правекс-Страхування	27	ТОВ "КУА "ЮБК ЕССЕТ МЕНЕДЖМЕНТ"
13	Провідна	28	ЗАТ «Українська міжнародна фондова біржа»
14	Українська промислова страхова компанія	29	ЗАТ "Фондова біржа "ІННЕКС"
15	ІНГО Україна ЖИТТЯ	30	ВАТ «Українська біржа»

Завдання Б:

1. Студенти мають розбитися на пари і згенерувати відкриті і закриті кодів за алгоритмом RSA згідно описаної вище схеми.

2. Набір простих чисел у кожної пари має бути різним, але не перевищувати двозначне число.

3. Результати розрахунків представити у вигляді опису порядку розрахунку та зображень активних вікон електронних таблиць Excel.

Контрольні запитання

1. Чому безпека платіжних систем є головним аспектом електронної комерції?
2. Опишіть загальні риси політики безпеки банків.
3. Дапйте перелік найбільш поширених загроз безпеки платіжних систем.
4. Яку частину небезпеки складають віруси? Наведіть власну думку.
5. Чим відрізняються смарт-карти від інших платіжних карт?
6. Дайте перелік захлодів по убепеченню операцій з пластиковими картками.
7. Опишіть порядок створення «закритих ключів» за алгоритмом RSA.
8. Які вида банківських афер ви знаєте?

Ознайомившись з матеіалом цього розділу студент узнав, яким чином може бути порушена банківська таємниця, як шифрувати повідомлення кодом RSA, які існують методи фінансового шахрайства.

Розділ 4. ЗАХОДИ БЕЗПЕКИ КОМЕРЦІЙНИХ ОРГАНІЗАЦІЙ

В розділі ви знайдете опис програмних заходів із захисту мереж, які працюють за IP-протоколом. Подано способи захисту від деяких шихрайств в Інтернеті.

В знайчні мірі заходи безпеки для фірм нагадують такіж заходи, описані в попередньому розділі. Відміну складають заходи з унеможливлення менеджерів компаній попастися на гачок мережевихз аферистів. Окрім того, в цьому розділі будуть описані додаткові програмні заходи по забезпеченню збереження тайни при оформленні договорів, перемовинах щодо майбутніх контрактів, тощо.

4.1. Програмні заходи безпеки. Захист окремих елементів мережевого обміну даними

Web-додатки захищені двома протоколами – Secure HTTP і Secure Sockets Layer, які забезпечують аутентифікацію для серверів та браузерів, а також конфіденційність і цілісність даних для з'єднань між Web-сервером і браузером. S-HTTP, призначений, в першу чергу, для підтримки протоколу передачі гіпертексту (HTTP), забезпечує авторизацію та захист документів. SSL пропонує схожі методи захисту, але для комунікаційного каналу. Він діє в нижній частині стека протоколів між прикладним рівнем і транспортним і мережевими рівнями TCP / IP (рис. 4.1).

SSL можна використовувати не тільки для транзакцій, які проходять в Web, але цей протокол не призначений для забезпечення безпеки на основі аутентифікації, яка відбувається на рівні додатку або документа. Для управління доступом до файлів і документів потрібно використовувати інші методи.

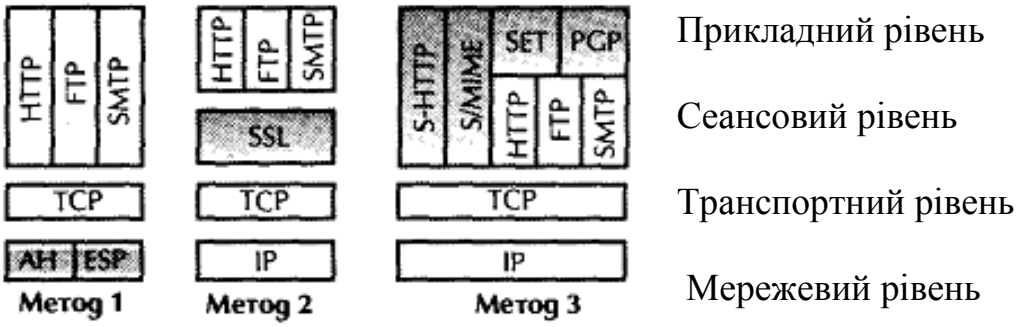


Рис. 4.1. Три способи захисту інформації в мережах

Для захисту електронної пошти в Інтернеті є безліч різних протоколів, але лише один чи два з них використовуються досить широко. PEM (Privacy Enhanced Mail) – це стандарт Інтернету для захисту електронної пошти з використанням відкритих або симетричних ключів. Він застосовується все рідше, оскільки не призначений для обробки нового, підтримуваного MIME, формату електронних послань і, крім того, вимагає жорсткої ієрархії сертифікаційних центрів для видачі ключів. S / MIME – новий стандарт. Він задіює багато криптографічні алгоритми, запатентовані і ліцензовані компанією RSA Data Security Inc. S / MIME використовує цифрові сертифікати, і отже, при забезпеченні аутентифікації покладається на сертифікаційний центр (корпоративний або глобальний).

Ще один популярний додаток, розроблений для захисту електронної пошти захисту послань і файлів – в Інтернеті PGP (Pretty Good Privacy). Ймовірно, це найпоширеніша додаток захисту електронної пошти в Інтернеті, що використовує різні стандарти шифрування (див. табл. 4.1). Додатки шифрування-розшифровки PGP випускаються для всіх основних операційних систем, і послання можна шифрувати до використання програми відправки електронної пошти. Деякі поштові програми, такі як Eudora Pro фірми Qualcomm і OnNet від FTP Software, дозволяють підключати спеціальні PGP-модулі для обробки зашифрованою пошти. PGP побудована на принципі «довіри павутини» (web of trust) і дозволяє користувачам поширювати свої ключі без посередництва сертифікаційних центрів.

Таблиця 4.1.

Деякі стандарти захисту даних для Інтернету [65]

Стандарт	Функція	Застосування
Secure http (S-HTTP)	Захист транзакцій в Web	Браузери, Web-сервери, програми для Інтернету
Secure Sockets Layer (SSL)	Захист пакетів даних на мережевому рівні	Браузери, Web-сервери, програми для Інтернету
Secure MIME (S / MIME)	Захист вкладень в електронні послання на різних платформах	Поштові програми з підтримкою шифрування та цифрового підпису RSA
Secure Wide-Area Networks (S / WAN)	Шифрування одноранго-вих з'єднань між брандмауерами і маршрутизаторами	Віртуальні приватні мережі
Secure Electronic Transaction (SET)	Захист транзакцій з кредитними картами	Смарт-карти, сервери транзакцій, електронна комерція

Коли Ви з'єднуєте ресурси своєї корпоративної мережі з відкритою мережею Інтернет, то піддаєте ризику дані, які містяться в ній, а також і самі комп'ютерні системи. Без брандмауера дані будуть мішенню для зовнішньої атаки. Як і їхні аналоги у повсякденному житті, в електронному світі брандмауери призначені для захисту від пошкоджень, в даному випадку, захисту даних і комп'ютерних систем. Брандмауери здатні забезпечити захист окремих протоколів і додатків і вельми ефективні проти «маскараду». (Ситуація в електронному світі, коли якийсь користувач маскується, видаючи себе за іншу.)

Брандмауери здійснюють контроль доступу на основі вмісту пакетів даних, що передаються між двома сторонами або пристроями по мережі. CryptoAPI u CDSA

В даний час є два основні набору інструментів, покликаних спростити для розробників завдання впровадження криптографічних методів захисту в додатки для персональних комп'ютерів - це CryptoAPI від Microsoft і CDSA (Common Data Security Architecture) від Intel.

Microsoft розробив інтегровану систему безпеки Інтернету – Internet Security Framework – сумісну з Microsoft Windows 95 і Microsoft Windows NT. Важливий компонент цієї інтегрованої системи – CryptoAPI. Цей інтерфейс прикладного програмування (API) діє на рівні операційної системи і надає розробникам в середовищі Windows засоби виклику криптографічних функцій (таких як алгоритми шифрування) через стандартизований інтерфейс. Оскільки CryptoAPI має модульну структуру, він дозволяє розробникам в залежності від їх потреб замінювати один. Криптографічний алгоритм іншим. CryptoAPI також володіє засобами для обробки цифрових сертифікатів.

CDSA від Intel пропонує практично ті ж самі функціональні можливості, що й CryptoAPI, але цей набір інструментів з самого початку призначався для багатоплатформності використання, а не тільки для Windows. Деякі компанії (в тому числі Netscape, Datakey, VASCO Data Security і Verisign) вже включили підтримку CDSA в свої продукти.

Одна з переваг брандмауера в тому, що він дозволяє забезпечити єдину точку контролю за безпекою в мережі. Але ця перевага може обернутися проти Вас: якщо брандмауер виявиться єдиним слабким місцем в системі захисту, то ймовірно, він і приверне до себе підвищену увагу хакерів.

Пам'ятайте, що брандмауери не є універсальним інструментом з перевірки конфіденційності й аутентифікації, він також не здатен захистити мережу від вірусів і не здатен забезпечити цілісність даних. Крім того, брандмауери не аутентифицируют джерело даних і дуже часто не гарантують конфіденційність. Проте в даний час розробляються нові протоколи для забезпечення аутентифікації і конфіденційності пакетів даних в Інтернеті.

Корпоративні мережі часто пов'язують офіси, розкидані по місту, регіону, країні або всьому світу. В даний час ведуться роботи по захисту на мережевому рівні IP-мереж (саме такі мережі формують Інтернет), що дозволить компаніям створювати свої власні віртуальні приватні мережі (virtual private

networks, VPN) і використовувати Інтернет як альтернативу дорогим орендованим лініях.

Провідні постачальники брандмауерів і маршрутизаторів сифікацію і шифрування пакетів виступили з ініціативою: допоможуть досягти сумісності запропонували технологію «ежду маршрутизаторами і S / WAN (Secure Wide Area Net-works). Вони взяли на себе впровадження і тестування протоколів, пропонованих Робочою групою інженерів Інтернету (Internet Engineering Task Force, IETF) для захисту IP-пакетів. Ці протоколи забезпечують аутентифікацію і шифрування пакетів, а також методи обміну і управління ключами для шифрування і аутентифікації. Чим небезпечні сайти-двійники?

допоможуть досягти сумісності між маршрутизаторами і брандмауерами різних виробників, що дозволить географічно роз'єднаним офісам однієї корпорації, а також партнерам, утворюючим віртуальне підприємство, безпечно обмінюватися даними по Інтернету.

Останнім часом, після появи цілого набору стандартів, що охоплюють захист всіх рівнів мережі - від пакета до додатка, складається враження, що питанню захисту інформації в Інтернеті приділяється навіть надмірну увагу. Всупереч думці про Інтернет, як про ненадійного носії інформації (внаслідок його децентралізованості), транзакції можуть бути добре захищені використанням перерахованих у таблиці 4.1 протоколів.

4.1.1. Інструменти безпеки від Google

Міжна родна корпорація Гугл вийшла ни ринок програмних послуг з новими ініціативами, які дозволяють користувачам їхньої продукції мати переваги над іншими в захисті своїх пересилань даних без додаткової оплати. Розглянемо їх.

Дворівнева перевірка

Виходячи з дому, ви почуваєтеся безпечніше, знаючи, що двері замкнено. Але уявіть, наскільки безпечніше ви б почувалися, якби їх ще й охороняли? Те саме стосується й інформації у ваших облікових записах Google. Увімкнувши дворівневу перевірку, ви матимете не один, а два заходи безпеки проти незаконного проникнення.

Створивши пароль для облікового запису Google, можна додати ще один рівень безпеки, увімкнувши дворівневу перевірку. Для дворівневої перевірки під час входу потрібен доступ до телефону, а також ім’я користувача та пароль. Це означає, що якщо хтось викраде чи вгадає ваш пароль, потенційний викрадач не зможе ввійти у ваш обліковий запис, оскільки в нього не буде вашого телефону. Тепер ви можете захистити себе тим, що ви знаєте (ваш пароль) і тим, що ви маєте (ваш телефон).

Шифрування SSL у Gmail

Gmail був першим великим постачальником послуг веб-пошти, який запропонував шифрування SSL за умовчанням для кожного сеансу. Таке шифрування допомагає захистити електронну пошту від проникнення інших користувачів за допомогою інтернет-з'єднання (як у точці доступу WiFi). Протокол SSL також став частиною багатьох служб, таких як веб-пошук, Документи, Picasa тощо.

Безпечний перегляд у Chrome

Одним із найважливіших заходів безпеки в Інтернеті є використання надійного веб-переглядача. Браузер Google Chrome створений для захисту безпеки таконфіденційності в Інтернеті.

Google Chrome містить функції, які захищають кожен ваш комп'ютер від зловмисних веб-сайтів під час перегляду веб-сторінок. Для захисту від фішингу та зловмисного програмного забезпечення Chrome використовує такі технології, як безпечний перегляд, механізм ізольованого програмного середовища й автоматичні оновлення.

API безпечного перегляду

Щоб захистити користувачів від інтернет-шахрайства під час веб-перегляду, Google щодня аналізує мільйони веб-сторінок для виявлення фішингу та зловмисного програмного забезпечення. Щороку виявляється сотні тисяч сторінок, призначених для фішингу та розміщення зловмисного програмного забезпечення. Вони додаються у чорний список, за допомогою якого попереджаються користувачів Firefox, Safari та Chrome через API безпечного перегляду.

Застереження щодо зловмисних завантажень у Chrome

Для захисту від веб-сайтів, які намагаються розповсюджувати зловмисне програмне забезпечення через автоматичні завантаження (тобто віруси, які пошкоджують комп'ютер користувача, коли він просто відвідує вразливий сайт), Google пропонує користувачам API безпечного перегляду. Безпечний перегляд значно допоміг усесвітній мережі, але в Інтернеті все ще багато оманливого та шкідливого вмісту. Можна легко знайти сайти з безкоштовними завантаженнями, які обіцяють одне, а працюють зовсім по-іншому. За допомогою соціальної інженерії вони змушують користувачів завантажувати та запускати зловмисний вміст. Тепер Google Chrome містить функцію, метою якої є захист користувачів від таких завантажень, починаючи зі зловмисних виконуваних файлів Windows. Вона відображатиме застереження, якщо користувач спробує завантажити ймовірно зловмисний виконуваний файл.

Варто знати, що Google пропонує ці інструменти безпеки для підвищення безпеки та захисту в Інтернеті. Читайте наступну тему: Ваші дані в Інтернеті, і як вони допомагають зробити веб-сайти кориснішими

4.2. Електронні злочини в Інтернеті та способи їх уникнення
(за даними з [10])

Найпоширеніші способи шахрайства в Інтернеті

Перший спосіб, а всього їх буде три на сьогодні, полягає в наступному. До Вас на електронну пошту приходить лист від дівчини-негритянки симпатичною зовнішності, з багатої родини, найчастіше з Сенегалу.

Вона Вам англійською, а внизу буде переклад на російську зроблений програмою-перекладачем, буде описувати душе-роздираючу історію, бунт в їхній країні, про те, як її батька генерала чи міністра вбили, а її тримають в ув'язненні.

Розповість, що її батько залишив десятки мільйонів доларів у банку, і що вона готова поділитися 50% цих грошей з Вами, якщо Ви їй трохи допоможете.

Від неї буде йти серія листів. У наступних листах вона Вам дасть номери телефонів банку, щоб Ви переконалися, що внесок дійсно є, і номер свого адвоката. Номери телефонів дійсно реальні, тільки ось люди там липові. Так, забув головне, вона Вам буде визнаватися в любові і пообіцяє заміж вийти, а там така фотка буде …

І фінал, заради чого все це затівалося, їй потрібно всього 100 євро вислати, щоб вона вибралася з полону і ще 100 євро, щоб відкрити рахунок на Ваше ім'я

Другий, найпоширеніший спосіб – фінансові піраміди, кожен день іде сотнями спам-запрошення увійти в чергову лохівський організацію і залишити там гроші!

І, третій популярний спосіб – HYIP-фонди, які обіцяють понад прибуток, якщо порахувати, то вже через рік можна свій перший мільйон доларів зробити Вони збирають наші гроші нібито інвестують їх в рекламу, Forex, цінні папери і т.д. Насправді схема проста, частина грошей з нижче стоячих вони виплачують тимчасово вище стоячим, поки люди стадами йдуть, як тільки ажіотаж пропадає, зникає і сама компанія.

Жадібність і неграмотність штовхає людей на подібні кроки, що дивно багато впевнені у своїх вчинках і бризкаючи слиною доводять, що все це правда, поки компанія не зникне …

Сайти-двійники

За два дні до президентських виборів у Росії зловмисники створили фальшиву веб-сторінку газети «Красная звезда». На цій сторінці вони розмістили «липову» інтерв'ю міністра оборони Сергія Іванова, в якому він позитивно відгукувався про залучення гомосексуалістів до служби в Російській армії. Репутації міністра це, звичайно, особливо не пошкодило, але шуму помилкова інформація наробила багато.

Підробка і провокація були винайдені людиною дуже давно. А технічний прогрес став для шахраїв нескінченним ресурсом нових можливостей

у цій сфері. В Інтернеті з'являється все більше фальшивих сайтів різних організацій. Основна їх мета – фінансова нажива або провокація (так, в період виборів зростає кількість сайтів, які поливають брудом кандидатів-конкурентів). Широке поширення сайти-двійники отримали зовсім недавно. Так що ця галузь шахрайства ще зовсім молода.

Провокаційні сайти-двійники

Провокаційні сайти-двійники – це частина індустрії чорного PR. Раніше вони створювалися заради розваги, а сьогодні це ціла галузь, в якій трудяться сотні людей. Це стало бізнесом, у якого є конкретні замовники і виконавці. Під час недавніх президентських виборів на Тайвані майже кожен кандидат у президенти і кожна велика політична партія або група могли побачити в Інтернеті фальшивий сайт, присвячений їм. Сайти містили забруднюючу і провокаційну інформацію.

Консультація юриста

Творців провокаційних сайтів-двійників можна притягти до кримінальної відповідальності за незаконне використання торговельної марки і шахрайство. Але на сьогоднішній день не відомо жодного судового процесу над творцями провокаційних сайтів-двійників.

«Давайте ваші грошики»

Сучасним інтернет-шахраям важко відмовити у винахідливості. Поряд зі взломами клієнтських баз банків і розоренням рахунків їх клієнтів, хакери промишляють підробкою сайтів відомих компаній. Діючи нібито від їхнього імені, шахраї укладають контракти з замовниками для того, щоб ці компанії перераховували гроші на їхній рахунок.

Найбільший у світі аукціонний Інтернет-портал eBay відомий багатьом, але не всі знають про існування його двійника, організованого шахраями. Фальшивий eBay просив своїх користувачів вводити дані про свою кредитну картку, банківський рахунок, водійські права і номер соціального страхування. Потім цю інформації аферисти використовували для того, щоб знімати гроші з рахунків жертв.

Щоб не стати жертвою шахраїв:

1. уважно вивчіть назву сайту. Якщо, наприклад, поставлена мета скомпрометувати сайт «shoping.ua », то двійник буде носити ім'я типу «shoping.org.ua»;

2. якщо в тексті на серйозному ресурсі трапляються граматичні помилки, логічні невідповідності та інші недоліки – це має змусити вас задуматися над достовірністю сайту. На відміну від фальшивих, над справжніми сайтами працює велика кількість людей, які не допустять будь-яких помилок. До речі, до числа цих недоліків можна віднести і прострочені новини;

3. якщо в якості контактної адреси не вказано поштову скриньку або вона знаходиться на одній з безкоштовних поштових служб, то перед вами, майже напевно, сайт-двійник;

4. відомі веб-сайти серйозних організацій, як правило, мають гостьову книгу і форуми. Причому там ви зможете побачити безліч надісланих повідомлень.

Новий спосіб обдурювання в мережі

В даний час більшість мережних злочинців, як правило, користуються електронною поштою для розсилки спама і вірусів, а також фішингових повідомлень, в яких електронний лист або веб-сайт видаються за лист або сайт банку або іншої установи. Але є і ті, хто використовує більш просунуті технології для пошуку свіжих жертв. Щоб зробити свої уникають більш правдоподібними і переконати людей видати таку цінну інформацію, як номери кредитних карт, реквізити банківських рахунків або особиста інформація, деякі шахраї звернулися до систем інтернет-телефонії.

Новий вид шахрайства вже отримав назву "вішинг", оскільки злочинці, як і у випадку з фішингом, видають себе за представників банків та інших фінансових установ, але технічним засобом обмана є системи Інтернет-телефонії (Voip). Наприклад, в одному з випадків, виявлених нещодавно компанією Websense, користувачам розсилалися електронний лист з проханням зателефонувати 0800 і відкоригувати свої банківські реквізити. Якщо користувач дзвонив по цьому телефону, йому відповів записаний голос, який просив ввести номер рахунку на телефонній клавіатурі.

Подібний вид комбінованого шахрайства за допомогою електронної пошти та телефону, спрямований проти служби інтернет-платежів Paypal, виявила і антивірусна компанія Sophos. Жертвам також пропонувалося зателефонувати за номером телефону і підтвердити реквізити свого рахунку.

Компанія Secure Computing зіткнулася з більш витонченим способом обману, коли електронна пошта взагалі не використовується. Замість цього злочинці програмують комп'ютер так, щоб він набирав номери з довгого списку телефонних номерів і проігривал записане повідомлення будь-кому, хто відповів би. У записаному повідомленні людини попереджають, що інформація про його кредитній карті потрапила до шахраїв, і просять ввести номер кредитної картки.

Новий вид шахрайства може виглядати досить правдоподібно, так як технологія інтернет-телефонії дозволяє фальсифікувати номер абонента. Пол Генрі (Paul Henry), представник Secure Computing, вважає, що у нового виду обману є шанси на успіх, оскільки дуже мало людей недовірливо ставляться до телефонному дзвінку сообщающему про проблему з кредитною картою. «Здоровий глузд – перша лінія захисту, – говорить пан Генрі. – Будь-хто, кому телефонують з банку, повинен вжити відповідних заходів для захисту своєї особистої інформації і свого банківського рахунку». Він зазначив, що банк або компанія-оператор кредитних карт повинні знати деяку особисту інформацію про клієнта, якому вони дзвонять. Тому люди повинні насторожено ставитися до всіх дзвінків, коли телефонує представник банку або фінансової установи не знає навіть базової особистої інформації – наприклад,

імені та прізвища клієнта. Про всіх таких випадках слід негайно повідомити в банк.

Алан Нунн, старший специалист по технологій у компанії Newport Networks, що займається продажами технологій Voip, говорить, що в перший час свого існування фішинг був успішним завдяки тому, що люди не мали уявлення про його небезпеки. «Ми частково вирішили цю проблему шляхом освіти користувачів», – говорить він, додавши, що цей же метод необхідний для боротьби з новим видом шахрайства. Крім того, на його думку, компанії, що займаються інтернет-телефонією, поступово повинні будуть зробити ряд технічних заходів для вирішення нових проблем.

Як відомо, багато провайдерів Інтернету мають чорні списки адрес, з яких надсилається спам. Повинні бути складені аподаткичные списки абонентів, які займаються вишингом, щоб будь-який вихідний від них дзвінок блокувався до того, як він дійде до абонента. Тим не менш, р-н Нунн визнав, що, швидше за все, між компаніями, які намагаються зупинити поширення нового виду шахрайства, і злочинцями, які шукають нових жертв, розгорнеться «гонка озброєнь»: «Підозрюю, що зловмисники поки знаходяться на стадії експериментування. Але я також думаю, що одночасно з цим відбувається і реальне шахрайство».

Спамери вигадують нові способи шахрайства в інтернеті

За даними «Лабораторії Касперського», в Рунеті зростає кількість шахрайства в інтернеті, а саме шахрайських повідомлень спаму. За 2011 рік частка спаму тематики «комп'ютерне шахрайство» і «шахрайство в Інтернеті» зросла з 11% до 18,2%.

Шахраї також винаходять нові способи обмана та виманювання грошей у довірливих інтернетчиків. Так, з'явився новий вид листів, в яких спамери провокують одержувачів нібито безкоштовно відправити sms (що містить заданий кодове слово і/або номер) на номер платного сервісу. Прийменники бувають найрізноманітніші, але спамери переслідую єдину мету – поповнити свої особисті рахунки за рахунок користувачів.

В одному з таких листів шахрай посилається на новий закон «Про рекламу» і пропонує інтернетчикам відписатися від спам-розсилок. Для цього їм необхідно відправити Sms певного змісту на короткий номер 1045, отримати у відповідь посилання на сайт, де нібито опубліковані спамерські бази адрес, і видалити свою адресу з цієї бази. Називаючи себе «законослухняним громадянином», спамер стверджує, що SMS є повністю безкоштовним, всі закони дотримані.

Насправді ж, відписатися від спаму за допомогою SMS неможливо. Крім того, відправлення повідомлення на номер 1045 є платною. Причому обходиться SMS набагато дорожче, ніж звичайне повідомлення. Якщо користувач повірив і вирішив відмовитися від спаму таким чином, він отримає sms-повідомлення у такого змісту: «спасибі за розуміння».

Щоб уникнути проблем і не дати поживитися шахраям за свій рахунок, аналітики "Лабораторії Касперського" рекомендують користувачам не

довіряти повідомленням від невідомих адресатів, не попадатися на вудку «доброзичливців», що пропонують легкі і швидкі способи збагатитись, і не вірити добрим намірам спамерів.

Кардинг – неэлектронный і електронний фішинг

В «традиційному» фішингу користувачам інтернету розсилаються електронні листи із запрошенням відвідати веб-сайти, схожі на сайти електронної комерції різних фірм і банків, але створені і контрольовані шахраями з метою виманити номери кредитних карток і паролі доступу до банківських рахунків. У схемах неелектронного фішингу створюються реальні торгово-сервісні підприємства або використовуються вже існуючі.

Як стверджує Сургутнефтегазбанк, вперше такий вид шахрайства був зафіксований російськими банками в 2006 році в Туреччині, куди в розпал туристичного сезону направляється безліч туристів з Росії. У багатьох з них є банківські карти, і періодично виникає необхідність зняти готівку. Але кількість банкоматів в туреччині не завжди може задовольнити потреби туристів.

Найчастіше їх просто немає поруч з готелем, іноді вони не працюють або видають кошти в режимі, який не влаштовує власника. У зв'язку з цим в Туреччині з'явилася нова послуга – отримання готівкових грошових коштів на підприємствах торгівлі. Часто вони називаються post-office (поштове відділення). Для держателя карти процедура дуже схожа з одержанням коштів в пунктах видачі готівки банків, до якої він звик. Але насправді ця процедура не відповідає правилами міжнародних платіжних систем і відрізняється від обслуговування клієнта в таких пунктах. Для банку, що випустив карту, такі операції виглядають як звичайна купівля в магазині, що вже передбачає обман з боку підприємства торгівлі.

При цьому при отриманні грошових коштів держателя просять ввести свій Пін-код, правильність введення якого повинен перевірити банк-емітент. Але ПІН не направляється емітенту, а записується шахраями за допомогою пристрою, що імітує ПІН-ПАТ (додатковий модуль торгового терміналу, спеціально призначений для введення пін-кодів і забезпечення їх конфіденційність). Клієнт банку, повернувшись з туреччини, через якийсь час може виявити у виписці по рахунку своєї банківської картки операції зняття коштів у банкоматах, що він не здійснював. /Crime-Research.ru, 28 травня /

Бізнес-піраміди в інтернеті

В інтернеті знайшли відображення фактично всі види людської діяльності. Звичайно, в першу чергу, це стосується бізнеса. Одним з його типів mlm, мережний маркетинг так звані "піраміди". Тут у нього своя ніша, свої шанувальники й інструменти просування.

П'ятий клік фальшивий

Серйозна проблема для розвитку контекстної і пошукової реклами - шахрайські кліки. Цей спосіб шахрайства базується на тому, що деякі рекла-

модавці виплачують певну суму за кожне звертання на їхню рекламну сторінку тим особам чи фірмам, які забезпечують це звертанн. Відомо, наскільки серйозна – за оцінкою компанії Click Forensics в першому кварталі 2007 рівень "click fraud" в середньому становить 14,8%. Для більш дорогих сайтів цей рівень вище – більше 20%. Дані ґрунтуються на моніторингу кампаній трьох з половиною тисяч рекламодавців, які беруть участь у системі Click Fraud Network.

Шахрайські кліки бувають двох типів. По-перше, «клікуванням», як це явище називають, займаються конкуренти фірм-рекламодавців. Вони тим самим спалюють даремно бюджет конкурентів (адже кожен клік оплачується). По-друге, "накручувати" лічильник кліків може непорядний власник рекламної площадки, коли Google Adwords, "Яндекс.директ" або "Бігун" розміщують оголошення на його сторінках і деляются грошима, отриманих за кліки з рекламодавців. І коли клікають конкуренти, і коли клацає власник майданчика, рекламодавець не отримує реальних відвідувачів, тобто витрачає гроші марно. Зрозуміло, торгові майданчики усвідомлюють проблему.

Тим більше, що ображені рекламодавці судяться з ними – в одному з таких випадків Google довелося заплатити 90 мільйонів доларів, щоб залагодити проблему. Власники рекламних систем застосовують різні заходи, щоб зняти цю проблему Google випустив докладний документ, що стосується моніторингу фальшивих кліків сторонніми спостерігачами, правильних методик і дій рекламодавців (у форматі pdf). Крім того, Google дає рекламодавцям можливість блокувати показ оголошень комп'ютерів з певних адрес – тоді вони зможуть заблокувати офіси конкурентів, і тим буде складніше "клікати". Крім цього, є і програмне визначення частини кліків як фальшивих – системи не зараховують такі кліки, причому не розкривають алгоритмів, як вони ділять спрвжніх потенційних клієнтів і шахраїв. Керівник відділу рекламних технологія "Яндекса" Євген Ломідзе назвав на конференції etarget частку кліків, які "Яндекс.директ" відкидає як підозрілі: 17,7% на пошуку Яндекса, 22,35% – у мережі (тобто на сайтах партнерів).

Як дізнатися IP і інші дані і при цьому залишитися анонімним?

Завдяки масовому розповсюдженню Інтернет, шахрайством можуть займатися некваліфіковані користувачі. Для цього вже з'явилися сайти, що пропонують послуги з визначення, наприклад даних певної людини, IP-адресу його комп'ютера, його місцезнаходження, яким броузером він користується, операційну систему і навіть Інтернет-провайдера і звичайно, при цьому, Ви захочете залишитися непоміченим.

Для цього такому користувачеві потрібно зареєструватися в системі «2IP Шпигун», ввести свій E-mail і інвайт-запрошення. Запрошення (інвайт) можна отримати підписавшись на розсилку і дочекавшись необхідного уроку. Зареєструвавшись Ви отримаєте докладні інструкції і на додачу купу корисних сервісів.

Очевидно, що такми способом, професійнеі кіберзлочинці відшукують нові об'єкти для хакерських атак. Тому ж, хто спокуситься на цю пропозицію

варто чекати на візит правоохоронців, оскільки при вдалому пограбуванні клієнтського рахунку, всі реквізити кіберграбіжника будуть визначатися саме такого горе-злодія.

Для захисту комп'ютерів фірми від подібних явищ, рекомендується обмежити для співробітників доступ в Інтернет тільки сайтами, потрібними для виконання своїх службових обов'язків.

4.3. Програма кодування текстових повідомлень PortablePGP

Цю програму можна отримати з сайту за адресою http://sourceforge.net/projects/ppgp/?source=dlp. Зручність програми полягає у тому, що її можна інсталювати на вашій флеш-карті і постійно носити з собою, кодуючи свої повідомлення на будь-якому комп'ютері, де є Інтернет.

Програма створена за відкритим кодом, розробленими Філіпом Ціммерманном (його сайт http://www.philzimmermann.com/UA/keys/index.html), який він розповсюдив безкоштовно в Інтернеті.

У своїй заяві до Підкомісії з Науки, Технології, і Космосу Американської Сенатської Комісії з Торгівлі, Науки, і Транспортування від 26 червня 1996 він сказав:

«Я створив PGP, скомпілювавши інформацію із загальнодоступних книжок у зручному пакеті, який можна використовувати на декстопі та палмтопі. Потім я віддавав її безкоштовно заради демократії. Це могло статися будь-де і розповсюдитися. Інші люди могли зробити це і вони зробили б. Вони роблять це зараз. Знову і знову. На всій планеті. Ця технологія належить кожному…

У 1991 вийшов Сенатський Законопроект 266, ні до чого не зобов'язуюча резолюція, котра, якби стала законом, примусила б кожного виробника устаткування для комунікації додавати до їхньої продукції спеціальні пристрої ("trap doors"), щоб уряд міг прочитати кожний зашифрований лист. Для того, щоб ця міра була попереджена, я опублікував PGP. Я зробив це тому, що хотів, щоб американські люди мали доступ до криптографії ще до того, як вона стане незаконною. Я віддавав її безкоштовно, щоб вона могла поширитися. Це було своєрідне щеплення для країни.» Ініціатива Ціммермана насправді стала щепленням для всього світу, бо ця методика шифрування є найпопулярнішою.

Такми чином, тепер кожному доступна безкоштовна система кодування, яка дозволяє шифрувати текстові повідомлення з високим рівнем захисту.

Після запуску програми інсталяції у першому вікні потрібно визначити, чи вперше ви налаштовуєте PGP-кодування. Якщо впеше (на рис. 4.2 верхня кнопка ліворуч), з'являється таблиця запиту на генерацію нового ключа (на рис. 4.2 праворуч). В цю таблицю потрібно ввести свої дані: Ім'я та прізвище, адресу електронної пошти, розмір ключа та фразу, якою буде закодований текст. Останню потрібно записати, оскільки при її повторному веденні має значення навіть регістр, а не тільки мова. Краще всього всі ці дані вводити

латинницею. Далі необхідно натиснути кнопку «Generate» і після закінчення процедури з'явиться вікно зі згенерованим ключем. Весь цей текст потрібно скопіювати і вставити до файлу у будь-якому текстовому форматі.

Якщо користувач вже має потрібний ключ (на рис. 4.2 нижня кнопка праворуч), то система завершить інсталяцію і запропонує почати роботу з налаштування пар ключів із різними адресатами (рис. 4.3) – режим «Keyring».

У вікні «Private keys» будуть розташовані ключі користувача програми, а в «Public keys» –користувача та його адресатів. Користувач має можливість згенерувати скільки завгодно власних ключів у цьому режимі. Головне, для кожного ключа потрібно мати іншу кодувальну фразу.

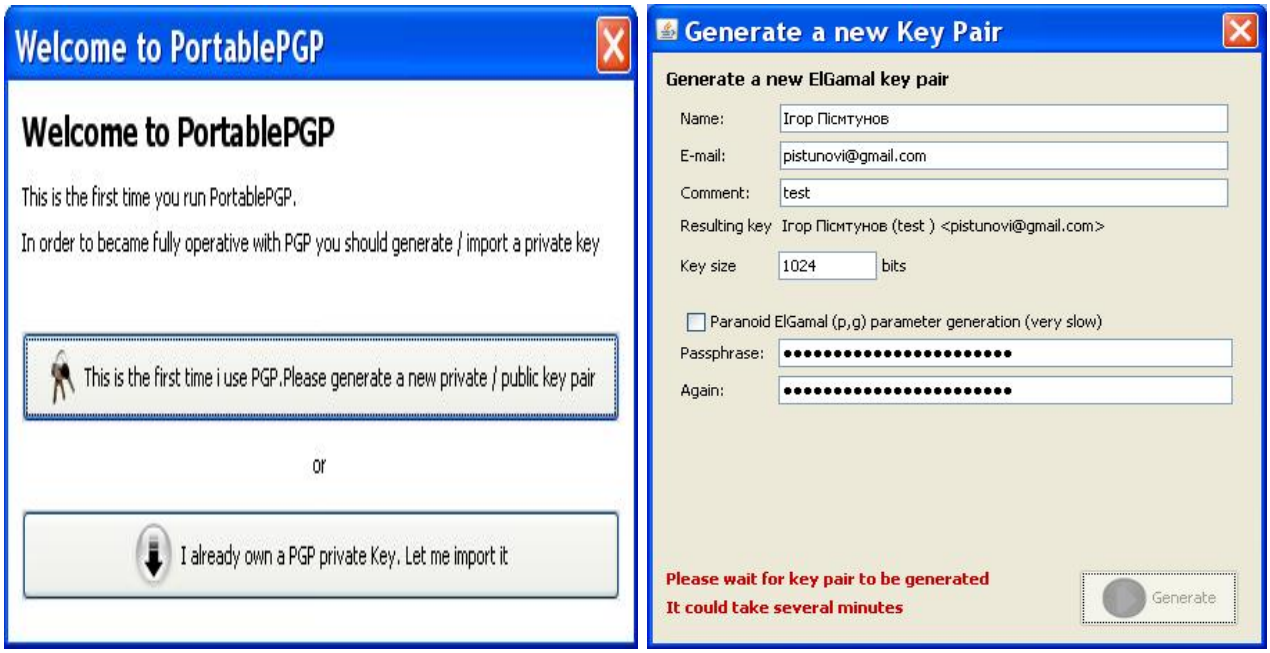


Рис. 4.2. Інсталяційний діалог програми PortablePGP

Кожен ключ має вигляд, представлений на рис. 4.4. При його копіюванні потрібно захоплювати і рядок зі словом «BEGIN» на початку ключа та зі словом « END» наприкінці ключа.

Пересилання кодованих повідомлень починається для кожної пари адресатів з пересилання своїх ключів іншому. Тобто, потрібно надіслати прикріплений файл з цим ключем або вставити ключ прямо у текст листа, як на рис. 4.5.

Отримавши такого листа, кожен із адресатів повинен зберегти цей ключ у вигляді файлу, краще всього прямо в теці PortablePGP, яка буде строрена на флеш-пам'яті при інсталяції програми. Далі, потрібно ввести цей ключ у свою програму PortablePGP, натиснувши кнопку «Keyring». Потім, у вікні «Public keys» треба натиснути кнопку з стрілкою вниз. Вдкриється файл-менеджер, в якому потрібно вказати на файл з приватним ключем адресата. Якщо все зроблено вірно, у вікні «Public keys» з'явиться нове ім'я адресата

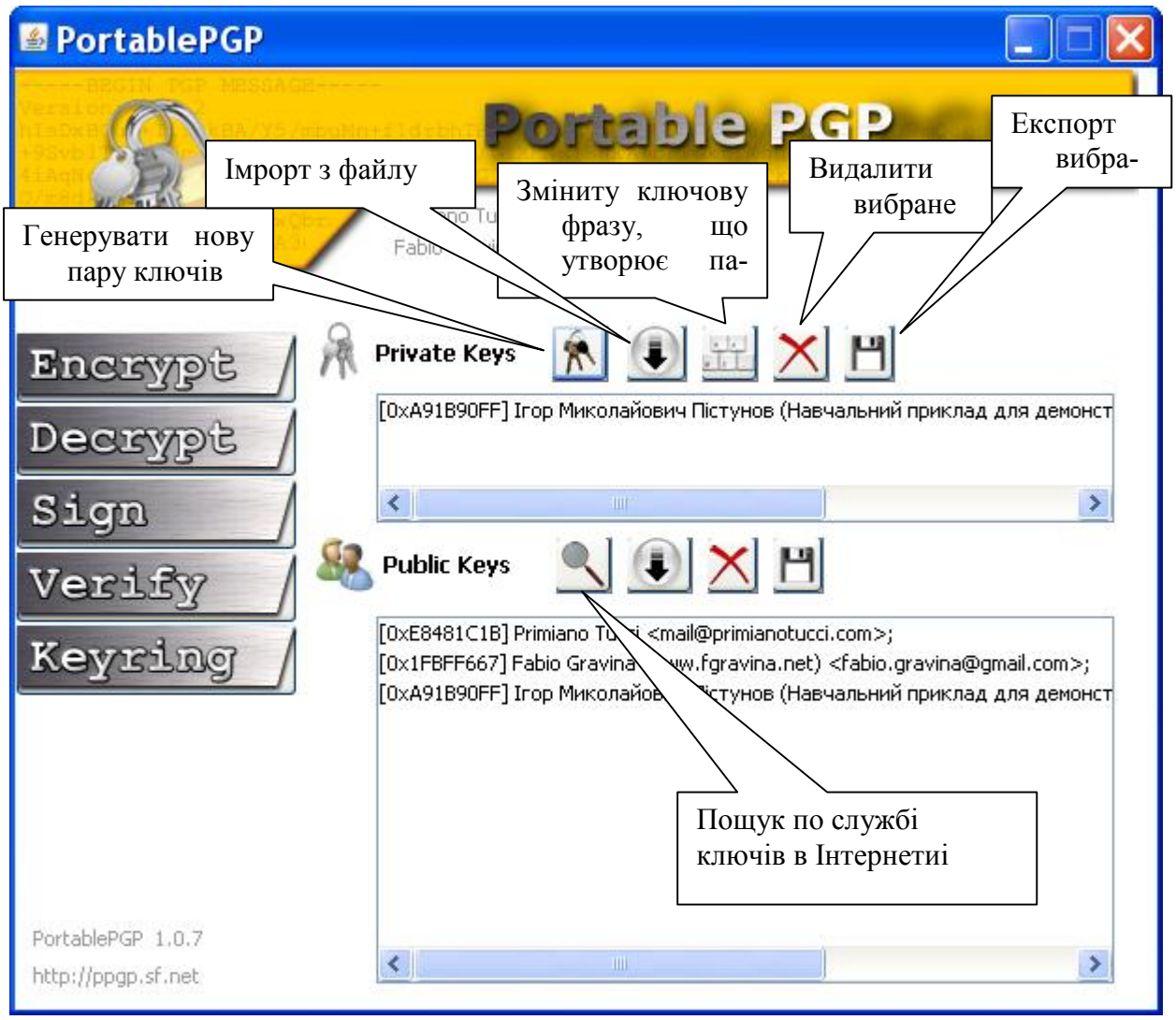


Рис. 4.3. Основні кнопки вікна «Keyring»

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: BCPG v1.47

lQHpBFDYeakRBADHC9skDKMyJIWLpAvTdvylOT45Mt+rQEk+WqIvw/
Aq10eRrYPF
 . . . . . .

QJMyH7uPckdKZ3KyiQCfYxW3uqMnSRkQVgLfAUnDvUD4Mrs=
=YMpa
-----END PGP PRIVATE KEY BLOCK-----
```

Рис. 4.4. Початок і закінчення відкритого ключа

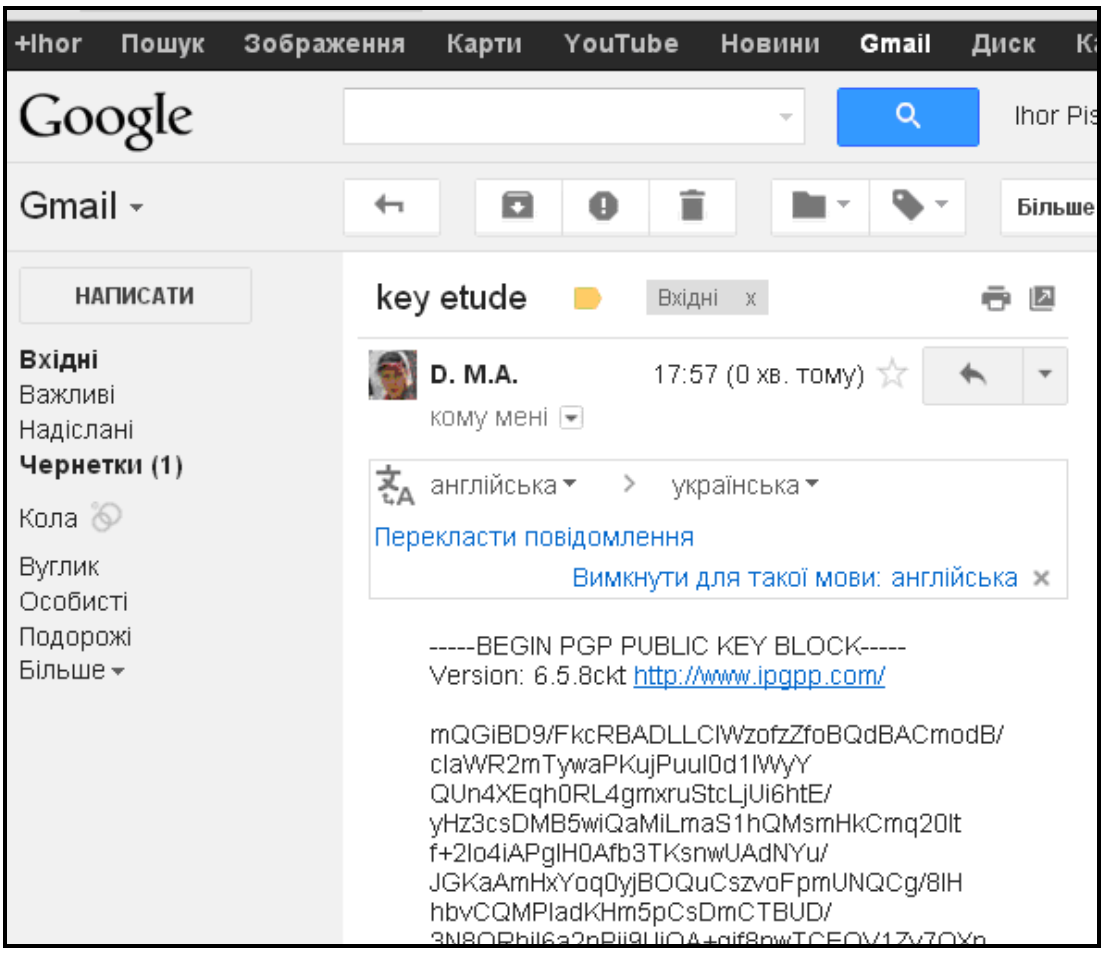


Рис. 4.5. Фрагмент електронного листа з ключем у тексті

.

Програма готова до роботи.

Якщо необхідно відправити закодоване повідомлення, користувач вмикає режим «Encript», натиснувши відповідну велику кнопку ліворуч. Текст, який необхідно попередньо набрати, можна вмістити прмо у нижнє вікно і натиснути кнопку «Encript», розташовану внизу (рис. 4.6). З'явиться маленьке віконечко з написом «Enter passphrase», в яке необхідно ввести кодову фразу для того ключа, який був надісланий конкретному адресату. Через деякий час в окремому вікні буде вже закодоване повідомлення. В описаній програмі з вікна «Encript text» коректно кодується текст набраний литинницею. При небхідності закодувати текст з кирилицею, потрібно скористатися пукнтом «Encript a file», в якому необхідно вказати місце знаходження файлу, призначеному для кодування. Рекомендується ставити свій підпис. Для цього, в пункті «Sign» треба вибрати своє ім'я.

Після закінчення кодування відкриється новіе вікно з кодом повідомлення (рис. 4.7). Отриманий закодований текст необхідно скопіювати і вставити, або у файл, або прямо в текст листа (рис. 4.8).

Рис. 4.6. Вікно програми в режимі «Encript»

Рис. 4.7. Вікно із закодованим текстом

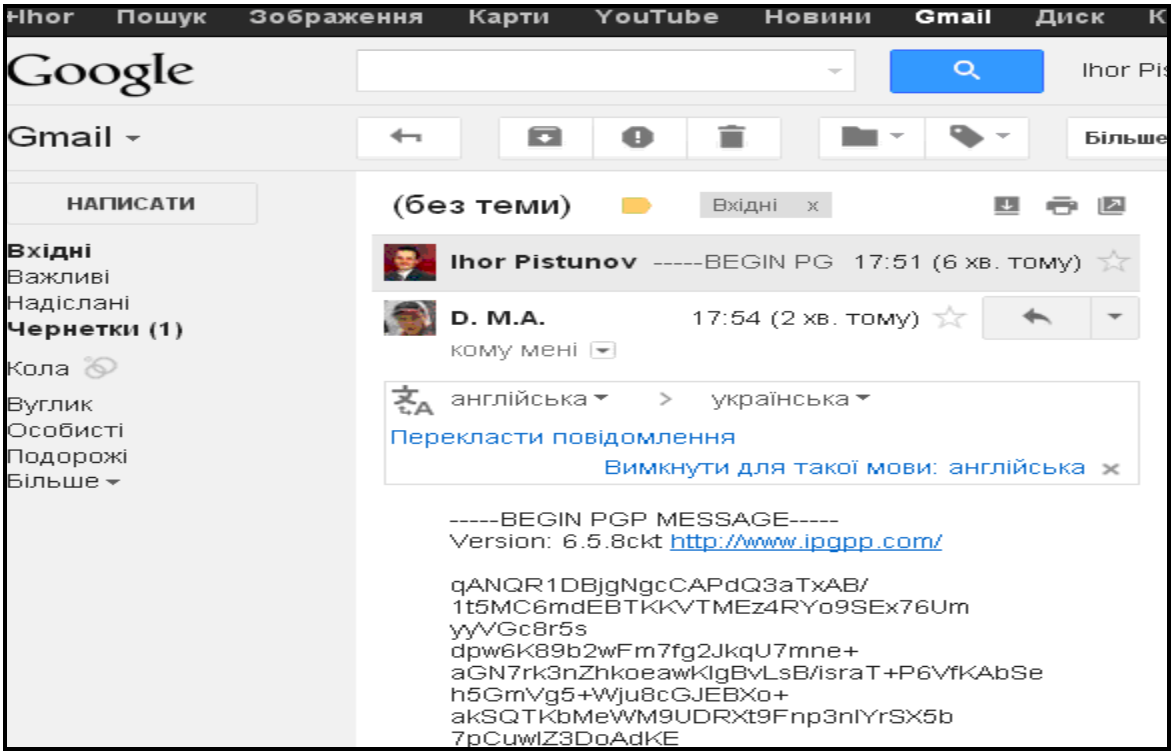


Рис. 4.8. Лист електронної пошти із закодованим файлом.

Рис. 4.9. Розкодування тексту в режимі «Decript»

Якщо отримано листа із закодованим повідомленням, вмикається режим «Decript» (рис. 4.9). Код тексту можна вставити прямо у нижнє вікно, або зберегти все послання у вигляді файлу і вказати на нього у вікні «Decript a

file». Розкодований текст, після введення passphrase з'явиться у вікні «Text editor».

Описаний порядок роботи здається складним тільки на перший погляд. Постійне використання програми PortablePGP дозволить виконувати всі процедури механічно, не помиляючись.

4.4. Індивідуальне завдання № 4

Тема роботи: Визначення можливих небезпек на підприємстві, яке пряцює в режисммі електронної комерції та вивчення роботи програми PortablePGP.

Мета роботи: Навчитися розпізнавати можливі небезпеки на підприємстві, яке пряцює в режисммі електронної комерції та вивчення роботи програми PortablePGP.

Завдання А: За останньою цифрою номера залікової книжки вибрати завдання і написати коротке ессе на вибрану тему.

0. Опишіть можливі небезпеки щодо онлайнового бюро подорожей, наприклад, www.expedia.com. Які рекомендації ви могли б дати для збільшення небезпеки?

1. Ознайомтеся з Web-сайтом Hobbes Internet Timeline (www.zakon.org / robert / internet / timeline). Які небезпеки ви можете знайти в його діяльності?

2. Уявіть, що Jeff Bezos, засновник amazon.com, найняв вас для розвитку нової галузі бізнесу для amazon.com. Які, в першу чергу вимоги з безпеки ви б висунули і чому?

3. Використайте наступні Web-сайти для збору інформації: CompUSA, Office Depot, і Staples. Напишіть короткий реферат про можливі способи шахрайства з використанням сайтів-двійників і методи їх запобігання.

4. Ви є консультантом фірми, яка хоче організувати систему електронної комерції для продажу відеопродукції. Визначте основні напрямки захисту такої фірми від можливих небезпек. Вкажіть на них.

5. Дослідіть Web-сайти таких компаній, як Amazon.com, Barnes and Noble, Books-A-Million, Borders, і Internet Bookshop. Ідентифікуйте можливі способи шахрайства із застосуванням цих сайтів і методи їх унеможливлення.

6. Уявіть себе на посаді консультанта з менеджменту однієї з консалтингових фірм, що спеціалізуються на розвитку і стратегіях електронної комерції. Одна з недавно створених компаній найняла вас з метою отримання рекомендацій щодо стратегії захисту своєї інформації при входження в онлайновий ринок юридичних послуг. Компанія планує надання рутинних юридичних послуг, таких як: не спірні розводи, патенти, заповіти і опікунство. У 350 (або більше) словах дайте рекомендації компанії, щодо заходів безпеки.

7. Виберіть бренд-якої компанії, за своїм розсудом. Зробіть пошук в Інтернеті, щоб визначити, чи використовувався цей бренд для створення сайту-двійника.

8. Визначіть п'ять Web-сайтів, асоційованих з бізнесом, які вам знайомі. Для кожного з сайтів визначте, який із методів захисту буде найбільш доцільним для кожної компанії

9. Опишіть дві можливих онлайнових Web-пропозиції, що базуються на моделі типу «плата за послугу». Доведіть можливість шахрайства.

Завдання Б:

1. Студенти розбиваються на пари і, використовуючи власні пристрої флеш-пам’яті, інсталюють гна них програму PortablePGP.

2. Генеруютьт відкриті ключі.

3. Через власні аккаунти електронної пошти обмінюються ними попарно.

4. Надсилають закодовані повідомлення і розкодовують їх.

5. Весь процес потрібно описати, ілюструючи його елементавми активних вікон у файлі тестових редакторів Word або Writer.

Контрольні запитання

1. Які рівні захисту інформації існують в Інтернеті?
2. Які заходи по збільшенню безпеки розробила фірма Microsoft?
3. Які заходи по збільшенню безпеки розробила фірма Google?
4. Для чого призначені протоколи S/WAN?
5. Які види шахрайства і Інтернеті є найпоширенішими?
6. Чим небезпечні сайти-двійники?
7. Перелічіть види захисту від сайтів-двійників?
8. Чим шкідливі «шахрайські кліки»?
9. Як розпізнати бізнес-піраміду?
10. Поясніть відміну кардингу від фішингу.
11. Як спамери обдурюють клієнтів?

Вивчивши матеріали цього розділу студенти унають про основні протоколи захисту інформації в Інтернеті, узнали про прийоми шахрайтсва і засоби його уникнення, вивчили порядок кодування текстових повідломленб методом PGP.

Розділ 5. ЗАХОДИ БЕЗПЕКИ ПРИВАТНИХ КОРИСТУВАЧІВ

В розділі описані прийоми шахрайства, спрямовані на довірливих людей, подано методи розпізнавання зловмисних дій та прийоми їх уникнення.

У будь-яку сферу, що приносить прибуток, рано чи пізно обов'язково проникають шахраї. Одні грають всерйоз, створюючи фінансові піраміди й інші схеми масового вилучення грошей у населення. Інші, слідом за офісними працівниками, геймерами, програмістами, блогерами й студентами, перемістилися у сферу Інтернету, де успішно пожинають плоди чужої довірливості.

Як видно з попередніх розділів, найбільшу шкоду приносять непродумані або зловмисні дії, тому цей розділ буде корисним не тільки приватним особам, але й керівниками служби комп'ютерної безпеки фірм та компаній. Описані тут методи шахрайства у чомусь перекликаються з методами, описаними вище, але тут подано такі види обману, якеі спрямовані в першу чергу на довірливих людей. А офісні працівники, користуючись службовим доступом до Інтернету можуть нашкодити не тільки собі, але й організації, де вони працюють.

В цілому, всі ті ж старі схеми махінацій, що переслідували споживачів і інвесторів протягом багатьох років до створення Інтернету, зараз з'являються у віртуальному просторі (іноді їм властива певна тонкість, викликана інтернет-технологіями). При стрімкому зростанні Інтернету, особливо електронної комерції, віртуальні злочинці прагнуть представити свої злочинні схеми так, щоб вони були якомога більш схожі на товари і послуги, пропоновані більшістю добросовісних електронних торговців. При цьому вони не тільки завдають збитку споживачам і інвесторам, але і підривають довір'я споживача до законної електронної комерції і Інтернету.

5.1. Шахрайство у фінансовій сфері

(за даними з [10])

Банківська афера, або фішинг

Якщо ви отримали електронного листа від свого банку, в якому сказано, що хтось намагався скористатись вашим рахунком, і для розблокування рахунку вам необхідно передати банку інформацію, що підтверджує особу, у жодному разі не слід цього робити. Банки ніколи не запитують таку інформацію через е-мейли. Аферисти (фішери), отримавши вашу особисту інфор-

мацію, скористаються нею для одержання доступу до вашого ж банківського рахунку.

Фішинг є найбільш розповсюдженою аферою. Шахраї вдаються до різних прийомів, аби витягти цю інформацію від довірливої людини.

«Інтернет-транзакції є операціями з найвищим рівнем небезпеки серед операцій з використанням платіжних карток, – Оксана Задорожня, начальник управління моніторинга клієнтських операцій ПАТ «Укрсоцбанк». – Шахраї можуть перехопити інформацію під час її передачі до необхідного сайту (якщо система захисту сайту є недосконалою). Окрім цього, навмисно створюють Інтернет-фішинг-сайти, які клонують web-ресурси, при цьому назва такого сайту дуже схожа на назву оригінального, але відрізняється на декілька букв, цифр, крапок, підкреслень".

Варто пам’ятати, що навіть одна невірно вказана літера може свідчити про те, що сайт є шахрайським. Слід звернути увагу, чи коректно вказано протокол передачі даних, що використовується в комп’ютерних мережах. Якщо перед назвою сайту замість "http" зазначено "https", клієнт може бути впевненим, що сайт є безпечним та обмінюється з ним інформацією по захищеному каналу. Також варто перевірити, чи усі меню на сайті є робочими та зателефонувати до служби підтримки сайту, щоб пересвідчитись, що телефон вказано вірно.

За словами експертів, зібрати інформацію про картки можна лише завдяки безпечності і неуважності громадян. «Смс-повідомлення на мобільний телефон, листи на робочу і домашню електронну адресу, дзвінки від імені банку з вимогою під слушним приводом підтвердити номер картки та пін-код, її термін дії і кодове слово повинні насторожити власників карт. Особи, що намагаються отримати обманним шляхом особисті ідентифікаційні дані власника картки, або так звані «фішери», також вставляють в повідомлення посилання на підставні сайти банків, компаній, що надають послуги оплати картками в мережі. Щоб ваші кошти на картці не потрапили до рук шахраїв, здійснювати переходи за такими посиланнями не варто",- додає Юлія Морозова.

Для того, щоб зробити розрахунки в мережі безпечними, рекомендується здійснювати покупки на сайтах, в надійності яких ви абсолютно впевнені. Також варто віддавати перевагу тим, що підключені до програм Verified by Visa (Перевірено Visa) або Secure Code (Безпечний Код); не використовуйте картки на сайтах без додаткового захисту даних, що передаються (адреса сайту має починатися з «https», а не з «http»). Також бажано віддавати перевагу сайтам, на яких номер картки при введенні замінюється на "*" ("зірочку") або інший символ заміни.

Ні в якому разі не використовуйте PIN-код при проведенні Інтернет-транзакцій (у тому числі в якості пароля) і не тримайте залишок на карткових рахунках, що значно перевищує суму угод (для того, щоб потенційні шахраї не мали можливості проводити подальші операції).

Для оплати покупок через Інтернет-сайти українські банки пропонують спеціальні картки, призначені виключно для цих операцій. Краще використо-

вувати окрему дебетову карту Visa Virtual (назва картки може відрізнятися, залежно від банківської установи), яка буде використовуватися тільки для покупок у мережі. Кошти на неї рекомендується переводити безпосередньо перед наміром здійснити покупку в обсязі, трохи більшому запланованих витрат.

Власникам платіжних карток фахівці радять купувати речі тільки в перевірених Інтернет-магазинах і платіжних сервісах, а угоди на аукціонах і за приватними оголошеннями оплачувати лише після перевірки інформації про продавця (рейтинг на аукціоні, відгуки покупців). Користувачам інтернету також треба бути обережними при використанні комп'ютерів загального доступу, які розташовані в інтернет-клубах і кафе. Практично у всіх програмах, які забезпечують доступ до Інтернет-банкінгу, передбачена кнопка виходу з системи управління вашими банківськими рахунками, натискання якої забезпечує завершення зв'язку (сесії) вашого браузера і віддаленого банківського серверу. Слід також знати, що всі браузери схильні запам'ятовувати дані відвідуваних сторінок, в тому числі імена і паролі. На всякий випадок необхідно завжди проводити чищення пам'яті браузера, видаливши тимчасові файли Інтернет-сесії.

Крім того, убезпечити свою платіжну картку можна за допомогою встановлення індивідуальних авторизаційних лімітів. Це один із найбезпечніших і найдешевших способів захисту. Таким чином корегується максимальна сума для операцій з використанням платіжної картки.

Окрім цього, якщо вам обіцяють виплатити виграш або винагороду на картковий рахунок і при цьому просять надати дані вашої картки (номер картки, термін дії, три останні цифри на смузі для підпису, нанесені способом індент-друку (CVV2/CVC2), або ПІН-код) – це шахрайство. Для перерахування грошових коштів на ваш картковий рахунок потрібні інші реквізити: назва, МФО, ЄДРПОУ та адреса банку, номер рахунку (ці дані вказані в Договорі про відкриття та обслуговування карткового рахунку), а також ваші персональні дані (ПІБ та ідентифікаційний код).

Інвестування

Такі якості Інтернету як анонімність, можливість охоплення великої аудиторії, висока швидкість передачі інформації і набагато більш низька вартість її розповсюдження, в порівнянні з традиційними засобами, роблять Інтернет дуже зручним і доступним інструментом для шахрайських дій. Інвесторів, які оцінили простоту роботи в мережі, з'являється щорічно мільйони. А інвестиційна діяльність завжди була улюбленою середовищем для діяльності будь-якого роду шахраїв. Те, що за допомогою Інтернету відбувається масове вкладення грошей в різноманітні проекти, визначило народження різного роду гарячих пропозицій для бажаючих заробити на онлайні.

Комплекс шахрайських прийомів у сфері інвестицій грунтується на звичайній людській жадібності. Люди вкладають гроші через Інтернет в надії на легкий прибуток. Як правило, ця пропозиція неіснуючих, але дуже популярних проектів, як, наприклад, вкладення в «високоліквідні» цінні папери

банків і телекомунікаційних компаній. Неодмінна умова таких пропозицій – гарантії повернення вкладеного капіталу разом з високими прибутками.

Наприклад, один заповзятливий підліток 18-ти років на ім'я Коул Бартіромо, житель штату Каліфорнія, розмістив на своєму сайті і декількох форумах повідомлення, в якому він обіцяв потенційним інвесторам прибуток до 2500% від короткострокових інвестицій. За один місяць він уклав 268 віртуальних угод і отримав на спеціальний рахунок у коста-ріканському банку понад 100 тисяч доларів. Природно, ніяких відсотків від своїх вкладень довірливі люди не отримали.

Таких масштабних злодійських «справ» в історії Інтернету, на щастя, не так багато. Одні тільки афери з кредитними картами в Мережі обходяться інтернет-бізнесу більш ніж в 10 мільярдів доларів щорічно. Кібершахрайство вже перетворилося на справжній злочинний бізнес, який існує в World Wide Web разом з бізнесом легальним і завдає останньому відчутний фінансовий та моральні збитки.

Часто у всіляких засобах масової інформації можна побачити рекламу різних семінарів. Їх організатори пропонують навчити учасників секретів того, як швидко розбагатіти. Гроші заробляють в цих випадках на зборі з довірливих учасників грошей за вхід і на продаж ним же книг і аудіокасет

Піраміда

Добре відомий принцип побудови фінансової піраміди: доходи перших інвесторів підприємства забезпечуються внесками нових учасників. Можливості Інтернету роблять його дуже зручним інструментом для організаторів подібних схем. Всім інвесторам обіцяється високий дохід, але шанс отримати його є тільки у перших учасників піраміди. Величезний куш отримують самі організатори, вміло імітують діяльність з вигідного вкладення залучених коштів. Насправді вони виплачують старим вкладникам гроші нових інвесторів. Засновники електронної версії піраміди поширюють через Інтернет листи та повідомлення, що обіцяють познайомити вас з тим, як просто сидячи за домашнім комп'ютером, всього за три тижні можна перетворити 5 доларів на 50000.

Оксана Павлюченко, випускниця одного з московських вузів, влітку 1998 року зареєструвала компанію SG Ltd, створила сайт в Інтернеті і заявила всьому світу про відкриття Stock Generation – першої ігрової фондової біржі. На сайті чесно згадувалося про те, що це всього лише гра. Суть її полягала в наступному: на сайті продавалися акції одинадцяти неіснуючих компаній. Курс восьми з цих компаній визначався за підсумками торгів самих гравців, акції дев'ятого стабільно зростали на 10% на місяць, десята компанія забезпечувала до 50% щомісячних, а одинадцятого компанія давала всі 100% прибутку на місяць. Мінімальний внесок, з якого можна було починати торги – $ 50. Але завдяки привабливій системі бонусів, гравці починали з більш великих сум і залучали в гру своїх друзів.

До середини 1999 року гра закінчила своє існування, e-mail перестав відповідати, автовідповідач компанії весь час просив передзвонити пізніше.

У цю глобальну аферу, за оцінками фахівців, було залучено понад 250 тисяч чоловік, що проживають на території США, Канади, Європи та Австралії.

Суть більшості пірамід:

1. Організатор піраміди оголошує про створення фонду, вступ у який буде приносити прибуток.

2. Розмір прибутку є наживкою і може варіюватися на розсуд організатора.

3. Щоб вступити до фонду, відвідувач повинен сплатити внесок, розмір якого коливається від $ 10 до десятків тисяч.

4. Щоб отримувати прибуток клієнт повинен залучати нових учасників до вступу до фонду.

5. З кожного залученого клієнта нараховується прибуток та виплачується того, хто залучив.

Ці виплати провокують ще більш активний пошук новачків, розповіді про фонд підкріплені реальними фактами виплат і т.д.

Піраміда зростає зверху вниз. Нагорі завжди знаходиться організатор, що привласнює левову частину грошей.

Відсотки клієнтам сплачуються виключно з вступних внесків інших клієнтів, які залучені пізніше. З кожним вдень існування піраміди наближається її падіння.

Врешті-решт вона розвалюється, а організатор домагається своєї мети, забирає гроші, припиняє діяльність і безслідно зникає. Природно, інші учасники фонду втрачають свої гроші

Афери з цінними паперами

Серед способів шахрайства з цінними паперами, спрямованих на заволодіння грошовими коштами, найбільш поширеною стала реалізація справжніх цінних паперів, що не належать злочинцям. Різними способами шахраї отримують у своє розпорядження цінні папери, втрачені законним власником чи викрадені в нього. Потім злочинці виготовляють підроблені документи, що засвідчують особу і права на цінні папери і знаходять потенційного покупця. Після чого, представляючись законними власниками цінних паперів, злочинці реалізують їх, а отримані гроші привласнюють.

Один шахрай, представляючись директором ТОВ «Стек ЗКМ», уклав з Комітетом з фізичної культури і спорту адміністрації району міста угоду про проведення робіт з реконструкції лижної бази.Фінансування таких робіт повинно було здійснюватися підприємствами та організаціями через проведення взаємозаліків по податках до міського та обласного бюджетів. Для цього, Комітет з фізичної культури і спорту адміністрації району в рахунок погашення заборгованості перед бюджетом передав псевдо-директору векселі для здійснення фінансування запланованих робіт. Після чого шахрай спокійно реалізував векселі і з виручениими коштами зник.

В даний час ринок цінних паперів – один з інтенсивно розвиваються секторів економіки України, і сюди спрямовуються великі фінансові потоки. Це не могло не привернути в дану галузь кримінальні структури.

До способів шахрайства, спрямованих на заволодіння цінними паперами можна віднести:

- укладання фіктивних угод на виконання робіт. Роботи ж виконувати ніхто в цьому випадку не планує, а ця ілюзія необхідна для отримання оплати за передбачувані роботи у формі цінних паперів та подальшого їх присвоєння;
- розкрадання бездокументарних цінних паперів;
- розкрадання цінних паперів з депозитарію;
- шахрайське придбання цінних паперів у емітента шляхом надання фіктивних документів про оплату.

Доля привласнених цінних паперів може бути різною. Наприклад, отримані злочинним шляхом цінні папери можна реалізувати, а отримані грошові кошти привласнити. В інших випадках, придбані шляхом шахрайства цінні папери можуть бути використані для встановлення контролю над підприємствами (пакети акцій).

Використовується і схема з переказом коштів на рахунок нового власника. Злочинці надають підроблене передавальне розпорядження, завірене печаткою та підписом зареєстрованого власника цінних паперів. Розпорядження містить вказівку про переведення бездокументарних акцій на особовий рахунок спеціально створеної для цього організації (частіше одноденки). Реєстратор виконує вимоги передавального розпорядження, і цінні папери переводяться на особовий рахунок нового власника. Після цього шахраї збувають отримані злочинним шляхом акції та ліквідовують юридичну особу, що виступала в якості «нового власника» цінних паперів.

Для здійснення шахрайського розкрадання цінних паперів з депозитарію злочинці заздалегідь укладають будь-яку угоду. Знаючи реквізити організації, що помістила цінні папери в депозитарій та реквізити самих цінних паперів, вони готують підроблену довіреність на їх отримання з депозитарію. Пред'явивши підроблені паспорт та довіреність, шахраї отримують цінні папери і надалі реалізують їх.

Дії Комісії по цінних паперах і біржах по забезпеченню дотримання законів, а також кримінальні процеси показують, що злочинці використовують два основні методи маніпулювання ринками цінних паперів для отримання особистої вигоди. По-перше, в так званих проектах "pump-and-dump" («зростання і падіння») вони звичайно поширюють помилкову і таку що вводить в оману інформацію, прагнучи викликати різке підвищення цін на акції, що не користуються попитом, або на акції компаній, що не мають істотних активів і тих що не ведучих операцій ("pump"). Зразу ж вслід за цим вони продають акції таких компаній ("dump"), що належать їм, щоб витягнути значний прибуток до того, як ціна акцій опуститься до свого нормального низького рівня. Вся решта покупців таких акцій, не обізнаних про шахрайський характер інформації, стає жертвами такої схеми, як тільки ціна падає.

Наприклад, в одному федеральному розслідуванні в Лос-Анджелесі відповідачі, як затверджується, придбали на суму 130 000 доларів, напряму або через посередника, акції компанії-банкрота, NEI Webworld, Inc., активи якої були ліквідовані за декілька місяців до того. Потім відповідачі, як затверджу-

ється, направили недостовірні електронні повідомлення в сотні біржових бюлетенів в Інтернеті з обманним твердженням про нібито плановане поглинанні NEI Webworld компанією бездротового електрозв'язку. В той час, коли відповідачі, як затверджується, придбавали акції NEI Webworld, ціна акцій складала від 9 до 13 центів за штуку. Проте одного прекрасного дня ціна акції NEI Webworld виросла за 45 хвилин з 8 доларів США за акцію до 15,5-16 доларів, а потім, за півгодини, впала до 25 центів за акцію. Відповідачі, як затверджується, одержали прибуток у розмірі 362 625 доларів США.

В іншій федеральній справі в Лос-Анджелесі людина, що працювала в каліфорнійській компанії PairGain Technologies, створила фальшивий вебсайт новин Блумберга, де містилося помилкове твердження про нібито підготовлюваному придбанні PairGain Technologies однією ізраїльською компанією, і розіслав такі, що вводять в оману електронні повідомлення з посиланнями на підроблений сайт новин Блумберга в бюлетені фінансових новин. В день публікації твердження в Інтернеті акції PairGain Technologies виросли приблизно на 30% до того, як компанія випустила власний прес-реліз із спростуванням.

По-друге, в схемах продажу без покриття, або "scalping" (спекуляціях з невеликим прибутком), використовується аналогічний підхід - розповсюдження помилкової або сфабрикованої інформації в спробі викликати зниження цін на акції певної компанії.

Наприклад, в одному недавньому федеральному розслідуванні людина, що називала себе «одноденним трейдером», як стверджується, випустив (більше 20 разів) помилковий прес-реліз, де стверджувалося, що найбільша телекомунікаційна і інтернет-компанія Lucent Technologies, Inc. не зможе вийти на планові квартальні показники прибутковості. Одноденний трейдер провів операції приблизно з 6000 акцій Lucent в день публікації їх прес-релізу. Фальшиві публікації, згідно наявним даним, привели до зниження ціни на акції на 3,6% і понизили ринкову вартість Lucent більш ніж на 7 мільярдів.

Обмін валют

1. Вам пропонують обмінювати електронні гроші спочатку за одним курсом, а потім здійснювати зворотний обмін вже за іншим курсом на іншому сервісі.

2. Обіцяються гарні прибутки від обміну.

3. Гроші зникають при спробі зворотного переказування грошей.

У цьому суть обману, на який клюють довірливі новачки кожен день і приносять шахраям прибуток. Потрібно розуміти, що курси електронних валют встановлюються за такими ж правилами, що і курси паперових.

Чарівні гаманці WebMoney

Суть методу полягає в тому, що в Інтернеті пропонуються номери гаманців WebMoney або інших систем, перераховуючи гроші, на які Ви отримаєте суму, що у два-три рази перевищує вкладену через певний час.

Це звичайно ж обман, оскільки такі гаманці в платіжних системах ніколи не існували і не будуть існувати. Ці електронні гаманці належать авторам шахрайсьуої оборудки.

Було придумано і продовження історії про те, як покарати чарівний гаманець. Говорилося, що на цей гаманець потрібно посилати гроші, не перевищують певної суми. І знову грошики потекли на гаманці шахраїв!

Якщо пошукати на офіційному сайті платіжної системи таку форму благодійності, Ви нічого не знайдете.

5.2. Інші види шахрайства

Нігерійські листи [34] – вид шахрайства поширеного в Інтернеті Суть афери полягала в тому, що організовані групи зловмисників із Західної Африкирозсилали спам із пропозицією оплатити невелику суму в обмін на майбутні солідні відсотки від фінансових операцій. Зазвичай людині приходить лист в якій шахрай граючи роль багатого, але недосвідченого іноземця, переважно корумпованого африканського чиновника, просить допомогти йому в незаконних оборудках — вивезенні грошей за кордон, приховуванні великих сум тощо, або ж пропонує інвестиції. Але перед переказом мільйонної суми треба під якимось приводом заплатити якусь суму грошей — на технічні витрати, в якості гарантії тощо. Звісно ніяких переказів не буде, а шахраї лише видурюють гроші з людей, які купилися на можливість легкої наживи.

Першими цей метод шахрайства освоїли жителі Нігерії, звідки й назва. З'явився він ще в другій половині 90-х років XX століття, але й досі популярний і в наш час людям приходять подібні листи з багатьох африканських країн (Нігерії, Беніну, Того, ПАР). «Нігерійське шахрайство» становить сьогодні більш 8% від усіх афер в Інтернеті.

Існують підвиди цього шахрайства:

1. «привабливий варіант» – нібито планується інвестувати у бізнес уливанням грошей безпосередньо на рахунки. А для цього необхідно «усього лише» повідомити повні банківські реквізити фірми з зразками підписів і відбитком печатки.
2. «розрахунок на довірливих» – нігерійські бізнесмени бажають інвестувати у фірму суму в розмірі 200-300 тисяч доларів. Ці гроші передбачається зарахувати на спеціальний трастовий рахунок. Від жертви вимагається «лише» 4-5 тисяч доларів, необхідних для погашення «операційних витрат».
3. «небезпечний» – автори листа заманюють жертву на свою територію де за допомогою насильства, шантажу й залякування «вибивають» з неї гроші.

В цілому цей вид шахрайства не новий, але нігерійці навчилися вигадувати «наживки» і поставили справу «на потік».

Викрадення особистої інформації

Ось типове повідомлення з Інтернету: «У компанії, в якій я працюю, зарплата перераховується на пластикову картку. Якось я отримав електронного листа:

“Здравствуйте! До вас звертається менеджер Вашого банку. Ми проводимо звірку даних клієнтів і просимо повідомити нам номер Вашої кредитної картки та термін її дії”. Я, не замислюючись, відправив ці дані і незабаром не виявив залишку грошей на картці. Пізніше з’ясувалося, що аналогічний лист отримали понад 1500 користувачів пластикових карт, і третину з них надіслали запитані дані, які шахраї й використовували у своїх цілях».

Щонайменше, сім мільйонів американців стали жертвами крадіжки особистих даних у 2005 році. Більше за всіх від крадіжки особистої інформації постраждали ті, хто необачно зберігав в Інтернеті, наприклад, номер своєї картки соціального страхування (у США він відповідає номеру посвідчення особи), дані водійських прав або банківські реквізити. Володіючи тим же номером соцстрахування, зловмисники можуть відкривати банківські рахунки з можливістю надання кредиту. Обов’язок ж погашення боргів припадає справжньому власникові рахунку.

Такі злочини полягають в незаконному привласненні особистої інформації без відома її власника з метою здійснення шахрайства або крадіжки.

Подібні злочини відбуваються приблизно так:

1. використовуючи вкрадені дані (ім’я, дату народження, номер соціального страхування), злочинці відкривають рахунок і оформляють нову кредитну карту. Всі несплачені рахунки шахраїв погашає його жертва;

2. шахраї телефонують емітенту кредитної карти жертви і, прикриваючись її ім’ям, змінюють поштову адресу рахунку. Потім зловмисники починають активно витрачати гроші. Але відразу виявити проблему неможливо, так як рахунки надсилаються на нову адресу.

Колективний обман

Для того, щоб завоювати довіру своїх майбутніх жертв, багато злочинців використовують їх етнічну, релігійну, вікову, професійну або іншу приналежність. Аферисти знають про характерну особливість людської природи довіряти тому, хто на тебе схожий. Часто організатори шахрайства самі є членами громади або ж декларують свою приналежність до неї, посилаючись на її авторитетних і шанованих членів. За словами представників американських контрольних органів, колективні обмани особливо складно виявити. Це пояснюється закритістю більшості груп і природним небажанням з їх боку виносити сміття з хати. Жертви подібних афер часто вважають за краще самостійно розбиратися з проблемою всередині громади або групи.

Зокрема, шахраї почали використовувати у своїх аферах так званий «чорний ящик» (black box), що запам’ятовує номери кредитних карток відвідувачів міських ресторанів і магазинів. Дані скриньки використовуються зловмисниками для виготовлення фальшивих кредитних карток.

Інтернет і телефон

За кількістю Інтернет-сайтів з аферами лідируючі позиції займають ті, на яких жертвам пропонується купити програму для мобільного телефону, що нібито дозволяє користуватися стільниковим зв’язком безкоштовно. Отримати уявлення про масштаби цієї афери можна, якщо набрати в будь-якому пошуковому сервісі, наприклад, в «Яндексі» слова free GSM – і ви отримаєте 8

млн. посилань на відповідні сайти. Текст на всіх цих сайтах один і той же. Його просто копіюють з першого такого сайту, що з'явився в мережі близько семи років тому.

Цьому виду афер важко відмовити у грамотній організації. Його відрізняє наукоподібна побудова тексту, список операторів мобільного зв'язку, з якими працює програма, перелік мобільних телефонів і т.д. Після переказу жертвою грошей на рахунок такого аферіста, вона або нічого не отримує у відповідь, або їй приходить абсолютно непрацездатна програма, яка не тільки не виконує обіцяних функцій, але ще й вбиває програмну начинку мобільного телефону.

Проекти Free GSM далеко не єдині варіанти шахрайства, пов'язані з мобільним зв'язком. Також в Інтернеті можна зіткнутися з проектом «GSM-пират». Тут вам запропонують модернізувати телефон так, щоб ви могли розмовляти за рахунок інших абонентів. На інших сайтах вам можуть запропонувати купити програму, яка генерує пін-код для поповнення рахунку. У цьому випадку після оплати покупки, ви отримаєте звичайний генератор випадкових чисел, який був створений за кілька хвилин. Всі ваші спроби «згенерувати код» не принесуть ніяких результатів, до того ж після тривалих спроб оператор просто заблокує вашу sim-карту. Шансів підібрати пін-код – 1 до 300 тисяч. Не вірте, коли шахраї заявляють, що працюють у того чи іншого оператора і мають доступ до бази. Це чиста брехня.

Одією з останніх подій у сфері інтернет-афер – sms-революція. На сайті ви дізнаєтеся про «унікальної можливості», що дозволяє отримати необмежений доступ до відправки SMS-повідомлень з телефону. Ця можливість з'явилася завдяки тому, що автори сайту створили свій центр для надсилання SMS. Не вірте таким обіцянкам і пропозиціям. Це обман!

В інколи зустрічаються оголошення про продаж спеціальних програм – прошивок для стільникових телефонів, встановлення яких робить всі розмови безкоштовними. І багато купують ці прошивки, встановлюють на телефон і з подивом продовжують поповнювати рахунок свого телефону з колишньою періодичністю.

Безкоштовний Інтернет

Безкоштовний доступ в Інтернет – ще один варіант афери. Здійснити це можливо, за заявою одного з сайтів, за допомогою гостьового входу. Його надають деякі великі провайдери своїм користувачам. Під гостьовим входом мається на увазі можливість безкоштовно походити по сайту самого провайдера. Вартість програми $8. Це, само собою, обман, тому що не можна користуватися Інтернетом через гостьовий вхід. Можуть вас надути і на $20, запропонувавши послуги провайдера «нового покоління». За цю суму ви за допомогою зазначеного провайдера зможете нібито необмежено користуватися Інтернетом. Це також чудовий спосіб подарувати дуже винахідливому аферистові свої гроші.

Ви повинні знати, що платежі в Інтернет найчастіше здійснюються за допомогою системи WebMoney. А це означає, що можливість вийти на реального отримувача коштів виключається.

Звичайно, будь-яких працюючих програм, які зводять нанівець весь бізнес операторів стільникового зв'язку або провайдерів доступу в Інтернет, не існує. У будь-якому випадку, навіть найпростіша програма, яку можна законно використовувати, повинна бути написана більш-менш відомою компанією і мати відповідну ліцензію.

«Фішингові» електронні листи

«Фішингові» листи - найпоширеніша тактика шахраїв. Більшість крадіжок записів відбувається якраз через такі листи. Мова йде про повідомлення і посиланнях на сайти, замаскованні під офіційні листи і сайти RIA.ua. У такому повідомленні Вам пропонується - природно, добровільно - відповісти на лист, вказавши своє ім'я користувача (email) та пароль, або ввести їх на сайті. Після чого, зрозуміло, вони потрапляють до рук злодіїв.

Набір або переклад тексту вдома

Людей, готових до набору або перекладу текстів вдома завжди вистачає. Це і студенти і молоді мами і просто бажаючі.

Суть методу в тому, що Ви надсилаєте запит роботодавцю за електронній пошті і в якості застави перераховуєте певну суму грошей для отримання пробної партії роботи.

Зазвичай ви не знайдете ні телефону, ні офіційного сайту роботодавця. Як тільки Ви перерахуйте суму застави, інтерс до Вас пропаде.

Дана схема працює і в інших лохотронах. Головна її відмінність – передоплата для отримання чого-небудь.

Фальшиві товари на аукціонах

На онлайн-аукціонах типу eBay досить часто попадаються фальшиві товари. І незважаючи на те, що в того ж eBay є комісія для відстеження шахраїв, однаково ймовірність купити підробку існує, навіть якщо надані сертифікати, котрі підтверджують справжність.

Ще на інтернет-аукціонах бувають випадки накручування ціни за допомогою спільників. Продавець з іншого акаунту або його друзі підвищують ставку, щоб ви заплатили більше. Тому якщо якийсь користувач часто трапляється у списку тих, що зробили ставки в одного продавця, можливо, він просто накручує ціну. І ще одне: ніколи не переказуєте гроші за товар напряму. Якщо вам нічого не надішлють, повернути гроші в такому випадку буде практично неможливо.

Афера «Ви виграли безкоштовний Xbox!»

Щоразу, коли вам в Інтернеті безкоштовно пропонують те, за що зазвичай треба платити, варто бути вкрай обережним. Виробники товарів, які ви «виграли, отримавши е-мейл» – комерційні організації, і в їхні плани не входить роздавати тисячі Xbox'ів, Ipod'ів чи інших гаджетів безкоштовно. У таких аферах звичайно просять оплатити тільки доставку, якої, природно, не буде.

Благодійна афера

Як тільки трапляється трагедія, що вимагає доброчинності, активізуються не тільки благодійні фонди, але й аферисти. Якщо вам приходить е-мейл із проханням про внесок, не варто зразу пересилати гроші. Впевніться на 100%,

що ці кошти підуть куди треба. А взагалі в таких випадках краще довіряти великим благодійним організаціям, таким як Червоний Хрест або Міжнародна амністія.

Шантаж

Іноді трапляється, що «жертві» приходить лист із погрозами викрадення кого-небудь із близьких і вимогами перерахувати енну сумі грошей на рахунок відправника листа. Звичайно ж, це афера. Навіть якщо ви відчуваєте, що хтось справді може викрасти ваших родичів або має у розпорядженні компромат, найкраще звернутися в правоохоронні органи.

Буває й зворотна ситуація: вам приходить лист від сищиків, які знайшли ваші контакти в затриманого злочинця, і просять допомогти в розслідуванні. Насправді аферисти просто виманюють у вас особисту інформацію.

Штучний ажіотаж

Нерідко шахраї, видаючи себе за незалежних аналітиків або просто обізнаних осіб, поширюють завідомо неправдиву інформацію про компанію для формування агресивного попиту на її акції. Автори подібних заяв посилаються на володіння закритою інформацією про важливу корпоративному подію або використання надійної системи відбору вигідних акцій, що грунтується на фундаментальному та технічному аналізі. Але автори замовчують про те, що вони заздалегідь купили ці акції за низькою ціною, щоб потім вигідно продати їх на хвилі штучно підігрітого інтересу.

У результаті створеного таким чином штучного ажіотажу навколо акцій, ціна на них зростає. Злочинець заробляє на продажі своїх акцій за завищеною ціною. Після чого все повертається на круги своя, в тому числі і ціна акцій, яка повертається на вихідний рівень. Це найбільш популярний останнім часом і дуже простий в організації вид ринкової маніпуляції.

Найчастіше подібні афери провертаються з рідко торгованими акціями маловідомих і невеликих компаній. При цьому маніпуляцію з такими акціями крім низької ціни полегшує відсутність доступу до достовірної інформації про компанію.

Файлове шахрайство в Інтернеті

Суть такого виду обману полягає у наступному:

Шахраї заманюють жертву нібито безкоштовним, швидким завантаженням потрібних Вам файлів.

Насправді вся представлена інформація на лже-сайтах є помилковою. Після переходу за посиланням – користувач потрапляє на сайт шахраїв, де користувачеві пропонується завантажити потрібний йому файл. Користувач завантажує програму – при запуску якої, з'являється вимога відправити SMS повідомлення на один з коротких номерів.

Шахраї замасковують свій сайт під популярний файловий обмінник RapidShare, щоб ввести користувача в оману.

Оновивши сторінку на тому ж сайті, з'являється інший дизайн, на цей раз маскування під файлобмінник DepositFiles.

Оновивши ще один раз сторінку, з'являється третій варіант шахрайського сайту, на цей раз любителі легких грошей замаскувалися під соціальну мережу «Вконтакте».

Після кількох оновлень сторінки, так само були знайдені маскування під Google, і торрент – Rutracker.

Ось типовий лист ін Інтернету: «Довго не думаючи, я вирішив завантажити файл, в даному випадку фільм: "Сурогати / Surrogates (2009) BDRip 1080p".

Я нажав зберегти як завжди і тут мене насторожило наступне.

Що це? Насправді викачується не фільм, розмір якого 8 ГБ, а файл розміром 16,5 мб. Мені стало цікаво, що відбудеться далі.

Файл зберігся і треба було розархівувати архів і відбулося найцікавіше. При розархівуванні з’явилося вікно із запитом дати пароль. А для цього що би ви думали треба зробити? Правильно – відправити смс-ку.

Якщо ви це зробити, тим самим себе самі обдурите»

На рис. 5.1 показано вікно такого запиту.

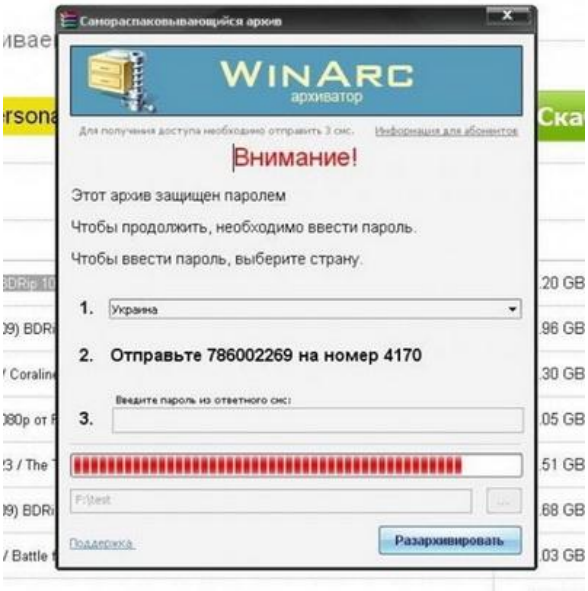


Рис. 5.1. Приклад шахрайського повідомлення, що для розпоковки файлу потрібно відправити SMS

Транспортна компанія і фіктивне підтвердження від адміністрації AUTO.ria.ua

Шахраї розміщують на сайті оголошення з автомобілями за ціною в 3-4 рази меншою середньоринкової. При цьому, в ролі "продавця" зазвичай виступає іноземець з однієї з країн Європи.

За номером телефону, вказаним в оголошенні, часто не можна додзвонитися або на телефоні відповідає диспатчер, який просить писати на e-mail. Зв'язок відбувається через електронну пошту.

Після відправки e-mail на таке оголошення, покупець отримує лист з описом мотивів продажу і пропозицією перерахувати повну або часткову вартість автомобіля грошовим переказом. Зверніть увагу, в листі не вказується ні модель, ні марка продаваного автомобіля.

Автомобіль знаходиться з-за кордоном, і його відправку повинна здійснити міжнародна транспортна компанія. В ході переговорів потенційний покупець автомобіля отримує підтверджені від транспортної компанії, що автомобіль вже знаходиться у них і всі витрати з доставки оплачені "продавцем".

Покупець отримує фіктивний лист, в якому адміністрація AUTO.ria.ua нібито поддтверждается реєстрацію даного автомобіля в Україну, а також надійність транспортної компанії. При цьому, в лист можуть бути вставлені логотипи сайту, а підписи до нього може бути вказано ім'я одного зі співробітників Служби підтримки сайту.

Після цього, "продавець" просить перерахувати гроші на його рахунок, а на доказ своєї чесності надсилає скановані копії свого паспорта і посвідчення водія.

Будьте уважні – так діють шахраї! Пам'ятайте, AUTO.ria.ua не співпрацює з яким-небудь транспортними компаніями , нібито займаються ввезенням автомобілів з-за кордону. Якщо Ви отримали лист подібного змісту, відразу ж припиняйте будь-які контакти з даними "продавцем" і ні в якому разі не переводите гроші на його рахунок.

Ось, наприклад такий лист від Авто.ріа:

«Здравствуйте!

Нещодавно ми писали по одному з наших партнерів – Ria Avtobazar Speditions Europa – про покупку автомобіля - 2000 Volkswagen Passat - Продавець - г-н Paul Ian Williamson.

Ми можемо підтвердити, що автомобіль зареєстрований в Україну, всі документи в порядку, машина не потребує митне оформпення – ви можете зареєструвати безпосередньо на своє ім'я.

Ця угода контролюється Auto.Ria.ua, ми гарантуємо, що транспортна компанія повністю надійним, і що вони будуть віддавати вас в автомобі виражений період часу – не біпьше 3 днів – починаючи з дня після підтвердження вашої оплати»

У підтримку цього листа подається дист про співпрацю з транспортною компанією:

«Dear Customer.

This message was sent to you at the request of the sender to notify you that the car is in our custody. The car has actually been placed with our company for shipment. To verify the actual transit status. click HERE and verify your tracking number M4403731840. The shipping fees have been paid by the Seller.»

Далі бажаючому придбати дешевий апвтомобіль приходить лист від фізичної особи (шахрая):

«Hello, I've just returned from the transportation company and I am glad to announce you that the transaction has started. The tracking number for the car is M4403731840. You can check it on their website.

The delivery company should contact you with the invoice and all the payment instructions. Since I have asked for your personal details, I believe it is

fair that you have mine also, so I have scanned and attached you a copy of my passport + a copy of my driving license in this email.

Thank you, please let me know if the delivery company has contacted you.

Dr. Paul Ian Williamson»

Ось інший варіант шахрайства, який пропонує придбати атвомобіль, що знаходиться в Україні або може бути туди привезений:

«В даному листі я опишу умови продажу мого автомобіля.

Якщо ці умови будуть для Вас прийнятні, то зв'язатися зі мною Ви зможете ось по цій пошті: (e-mail приховано)

Розмитнений.

Ні юридичних, ні інших проблем не має.

В ідеальному стані і насправді не вимагає ні яких вкладень.

У зв'язку з тим, що я отримав новий, більш вигідний робочий контракт в USA, я поміняв місце роботи і відповідно місце проживання. Живу на дві країни: Ізраїль-США.

У Вашій країні у мене залишився автомобіль, який на даний момент попроменя мені не потрібен і тільки дешевшає, простоюючи в орендованому мною гаражі на території НДІ, де я раніше працював. Я працюю в нафтовому бізнесі.

У зв'язку з чим, я вирішив продати автомобіль швидко і не дорого, але тільки так, як зручно мені. Саме в зв'язку з описаними нестандартними умовами продажу і обумовлена настільки низька вартість автомобіля.

Умови продажу:

1. Необхідно зробити грошовий переказ на суму що дорівнює вартості автомобіля на зазначені мною дані через систему швидких грошових переказів Western Union.

2. Після здійснення платежу, Ви висилаєте мені на e-mail в електронному вигляді копію квитанції про оплату.

3. Я дзвоню в банк і, якщо мені підтверджують, що переклад існує, то в плині двох-трьох днів я вилітаю до Вас для переоформлення автомобіля.

4. А контрольний номер з десяти цифр, який Вам видасть операцій-ність банку при відправленні переказу і який в свою чергу необхідний для отримання цього перекладу, Ви вкажіть мені тільки тоді, коли ми переоформимо авто на Вас і Ви отримаєте його в своє користування.

Те, що даний спосіб прозорий і безпечний для Вас, можна переконатися, поговоривши з банківським працівником будь-якого банку, де є Western Union.

Тобто ризику з Вашої сторони втратити свої гроші немає ніякого.

Якщо Вас все таки не влаштовують мої умови продажу мого автомобіля, то прошу Вас не писати мені взагалі, так як по іншому продавати я просто не буду»

А ось іще один варіант:

«Я разом з машиною перебуваю в Палермо, Італія. Автомобіль у відмінному стані, ніяких пригод, ніяких проблем. Розмитнений. Я хочу про-дати

його швидко. Загальною вартістю 2900 $, якщо я наводжу вам автомобіль в Україні. Автомобіль має український номерний знак, можу зняти з обліку.»

А ось іще:

«Я можу привести машину в Україну наступного тижня. Я буду знімати його з обліку. Але мені потрібна гарантія, що ви реальний покупець, все таки Па-лерми від України велика відстань. Я продаю цей автомобіль, тому що у мене немає більше роботи тут в Італії, я знайшла роботу в Англії там знаходиться моя сестра, там мені нічого робити з цією машиною, так як там всі машини праворульні. Моя пропозиція така: ви перещлете з вартість за автомобілі 1500 $ через Western union наприклад на ім'я своєї матері або (чоловікка, дружини, брата .....) Ви відправляєте гроші в Англію наприклад на ім'я ваше мами. Ви, напевно, не маєте родичів у Англії, але це не має значення. Ви йдете у Western union і ви кажете, що ви хочете відправити $ 1500 вашої матері яка зараз перебуває в Англії (і відправляєте копію на мою електоную пошту).

Я перевірю якщо передача є реальною і приїду з машиною в Україну. Там ви можете перевірити всі документи автомобіля, двигун, все що ви хочете ..... а потім ми разом поїдемо в банк і ви поміняєте прізвище вашої мами на моеі сестри, і вона знімить гроші з Western union в Англії, а решту дасте готівкою.

Я буду чекати вашої відповіді!»

Ще раз розглянемо основну схему шахрайства:

– вартість автомобіля в 3-4 рази дешевше ринкової ціни;

– "Продавець" розповідає історію про те, що купив авто в Україні і вимушений виїхати назад додому, при цьому розмитнювати авто дуже дорого (історія може мінятися);

– "Продавець" веде переговори тільки за допомогою листування;

– "Продавець" пропонує доставити авто за допомогою транспортної компанії і навіть пересилає Товаро-транспортну накладну для заповнення;

– в ході листування продавець пропонує перерахувати йому 50% заявленої вартості, через те, що на машину з'явився ще один покупець.

– в ході переписки покупця, з так званим "продавцем" можуть з'являтися нові обставини, кінцева мета яких – виманити ще більше грошей з довірливої жертви. Так, якщо шахраям вдалося роздобути 1 переказ за бажаний і настільки дешеві автомобіль, в гру вступає "транспортна компанія":

– "транспортна компанія" надсилає лист і повідомляє, що виникли труднощі на митниці і пропонує покупцеві доплатити, щоб швидше вирішити ці труднощі;

– якщо продавець вимагає повернути йому гроші, "транспортна компанія" пропонує відшкодувати в цьому випадку транспортні витрати, після чого гроші за автомобіль повернуть.

– зрештою, якщо шахраям вдалося виманити у настільки довірливого покупця не тільки передоплату за автомобіль, рішення митних проблем та відшкодування транспортних витрат, шахраї припиняють контакти з покупцем.

– іноді шахраї не зупиняються, і через деякий час з жертвою зв'язується якийсь "поліцейський", який веде слідство і хоче розкрити шахраїв, ніж вселяє в довірливу жертву надію на повернення грошей. Через деякий час, "поліцейський" повідомляє, що зазнав фіаско і справа, на жаль, закрито, але за деякий скромну винагороду він виступить уже в ролі приватного детектива і допоможе знайти шахраїв. Винагороду, як заведено, слід оплатити за допомогою грошового переказу.

5.3. Методи захисту від шахрайства в Інтернеті

5.3.1. Організаційні заходи безпеки

Вашу особисту інформацію можуть намагатися отримати різними способами. На деяких інвестиційних сайтах вашу особисту фінансову інформацію можуть запитувати для визначення відповідності вашого статусу акредитованого інвестора. Іноді використовується пояснення такого роду: зазначена інформація необхідна для складання пріоритетного списку (lead list) потенційних інвесторів.

Щоб не стати жертвою обману, ретельно перевіряйте будь-яку отриману інформацію. Особливо будьте уважні при отриманні електронною поштою листи від якогось Інтернет-провайдера або постачальника інформації з проханням оновити або знову ввести дані про свою кредитну картку для подальшої оплати послуг. Необхідно виявляти максимальну обережність, вирішивши повідомити кому б то не було особисті відомості.

Інтернет-хакери намагаються знайти "дірки"у програмному забезпеченні, які вони можуть використовувати для отримання доступу до приватних комп'ютерів. Щоб перешкодити їм робити це, завантажте останні патчі (доповнення до програми, які оновлюють і забезпечують захист).

Ви можете знайти патчі для Windows на www.windowsupdate.com.

Для оновлення інших операціних систем спосіб оновлення зможете знайти в документації дистрибутива.

Перевірте, чи не була змінена без вашого відома персональна інформація: це вірна ознака, що хто-то дійсно незаконно користувався Вашої записом.

Якщо Ви ще можете авторизуватися в своєму записі – негайно змініть пароль.

Не варто довіряти ніяким заходам, за допомогою яких вас обіцяють познайомити з різними способами швидкого і легкого збагачення.

Ось деякі правила, що зберігають час і гроші:

1. Не потрібно купувати суперприбуткові бізнес-пакети за символічну плату. Якби такі пакети існували, вигідніше було б заробляти за їх методикою, а не пробувати їх продати.

2. При пошуку роботи потрібно шукати офіційний сайт роботодавця, його контактний телефон, e-mail і т.д. Якщо контактних даних немає, то відразу виникає сумнів у його чесності.

3. Перед придбанням товару або послуги бажано почитати відгуки на форумах, познайомитися з готовими роботами або послугами на сайті.

4. Потрібно стежити за новими схемами шахрайства в Інтернеті, щоб бути готовими до будь-якого обману.

5. Не потрібно погоджуватися на передоплату при пошуку роботи вдома. Передоплата – це ознака шахрайства.

Користуючись цими простими правилами можна в більшості випадків розпізнати шахрайство в мережі і зберегти свої гроші.

Якщо в додатковій інформації оголошення, просять відправити SMS нібито для зв'язку з власником (або з якоїсь іншої причини) – це шахрайство, в таких оголошеннях авто чи нерухомість не продаються! Найчастіше за зв'язок з цим номером з балансу буде списана значна сума грошей, тому настійно не рекомендується відправляти SMS на подібні номери .

Якщо вас просять зателефонувати на номер з комерційної серії, що починається, наприклад з "8-900-ххххххх" або "8-703-ххххххх", не робіть цього. Такі серії спеціально створюються для надання платних послуг, слід уважно ставитися до дзвінків на такі номери.

Уникнути крадіжки імені користувача та пароля просто: нікому і ніколи не повідомляйте свій email користувача і пароль! Якщо Ви їх комусь передали і підозрюєте, що ваш запис зламали, негайно змініть пароль. Бажано не входити на сайт з чужого комп'ютера, а якщо ви це зробили, ні в якому разі не ставте галочку навпроти тексту «Запам'ятати мене». Хоча Ваш домашній комп'ютер добре захищений, але якщо ви авторизуєтеся з іншого, на якому повно вірусів і програм-шпигунів, дані з вашого рахунку моджуть потраприти до нечесних рук.

Клієнту необхідно контролювати рух своїх грошових коштів – регулярно отримувати виписки у банку і підключити послугу СМС-повідомлення про кожну транзакцію. У разі виявлення несанкціонованої операції необхідно відразу ж зателефонувати до Контакт-центр банку, заблокувати свою картку, звернутися з письмовою заявою до фінустанови і до органів МВС.

Сім порад, як вберегти свої кошти від інтернет-шахраїв:

1. Не використовуйте ПІН-код під час замовлення товарів або послуг через мережу Інтернет, а також за телефоном/факсом.

2. Не повідомляйте інформацію про платіжну картку або картковий рахунок через мережу Інтернет, наприклад ПІН-код, паролі доступу до рахунків, термін дії платіжної картки, кредитні ліміти, персональні дані тощо.

3. Для оплати товарів (послуг) через мережу Інтернет використовуйте окрему платіжну картку (так звана "віртуальна картка") з граничним лімітом, яка передбачена тільки для цього та не дає змоги здійснювати з її використанням операції в торговельній мережі та зняття готівки.

4. Необхідно використовувати сторінки в мережі Інтернет (сайти/портали) тільки відомих і перевірених інтернет-магазинів.

5. Обов"язково переконайтесь у правильності зазначення адреси сторінок у мережі Інтернет (сайтів/порталів), до яких підключаєтесь і через які збираєтеся здійснювати оплату товарів (послуг), оскільки схожі адреси мо-

жуть використовуватися для здійснення незаконних дій або сумнівних операцій з використанням персональних даних платіжної картки.

6. Здійснювати оплату товарів (послуг), придбаних через мережу Інтернет, тільки зі свого комп"ютера з метою збереження конфіденційності персональних даних та/або інформації про картковий рахунок. Якщо оплата товару (послуги) здійснюється через чужий комп"ютер, після завершення всіх розрахунків переконайтеся, що персональні дані та інша інформація не збереглися (знову відкривши сторінку продавця, на якій здійснювалась оплата товару).

7. Слід встановити на свій комп’ютер антивірусне програмне забезпечення і регулярно здійснювати його оновлення та оновлення інших програмних продуктів (операційної системи, прикладних програм). Це захистить вас від проникнення неліцензійного програмного забезпечення (вірусів).

Адміністрація сайту AUTO.ria.ua настійно рекомендує:

– не відповідати на електронні листи від підозрілих продавців

– не проводити повну або часткову передоплату за допомогою грошового переказу (Western Union, Webmoney, MoneyGram, ...);

Якщо оголошення на здається Вам підозрілим, звертайтеся до служби підтримки за тел.: (0432) 555-200.

Як розпізнати «фішинг»? Ось кілька ознак:

1. У «фішинговому» листі Вас просять вказати пароль і ім'я користувача (email). У справжніх листах від RIA.ua Вас НІКОЛИ не попросять повідомити пароль.

2. У «фішинговому» листі Вас лякають терміновою необхідністю: стосовно Вашого облікового запису, нібито порушено розслідування з приводу шахрайства або злому, і від Вас потрібно негайно повідомити свої ім'я користувача та пароль - інакше, мовляв, підуть санкції.

3. «Фішингові» листи і сайти можуть заманювати приємними пропозиціями: спеціальні пропозиції, знижки, безкоштовні послуги, достроковий доступ до бета-тестування нових функцій і т.д.

4. У «фішингових» листах, як правило, багато орфографічних і пунктуаційних помилок. Якщо лист рясніє помилками, швидше за все, це обман.

5. У деяких «фішингових» листах вказати пароль прямо не просять, але пропонують клацнути по посиланню на підроблений сайт, замаскований під один з проектів RIA.ua. У даному випадку бажано включити в браузері «фішинговий»фільтр!

6. У деяких «фішингових» листах адресу відправника замаскований або дуже схожий на справжній, щоб одержувач листа думав, що повідомлення було відправлено компанією RIA.ua. Перевіряйте відомості про лист, щоб переконатися в достовірності адреси відправника.

Щоб не стати жертвою «фішинга», краща порада – ставитися якомога обережніше до будь-яких повідомлень, що надходять нібито від RIA.ua. Якщо в листі вас просять повідомити свій пароль, загрожують терміновими заходами, обіцяють що-небудь неймовірно привабливе або дають посилання на «підрозділ управління обліковим записом», яка веде не на офіційний сайт

RIA.ua, – перед вами «фішинг». Додайте адресу відправника до «чорного списку», перешліть лист на адресу support@ria.ua, а потім видаліть його. Якщо Ви піддалися «фішингу», негайно змініть пароль.

У справжніх листах від RIA.ua Вас ніколи не попросять повідомити пароль.

Захист від фішингових схем та інших форм шахрайства в Інтернеті

Фішинг – це спосіб шахрайства в Інтернеті, яким користуються злочинці, щоб обманним шляхом примусити вас розкрити свої особисті відомості та надалі використовувати їх для:

- отримання грошей із вашого банківського рахунку та сплачування витрат за допомогою вашої кредитної картки;
- отримання кредитів на ваше ім’я;
- зняття грошей із ваших рахунків;
- використання копії вашої платіжної картки для зняття грошей у будь-якій частині світу.
- Попереджувальні ознаки
- Імовірно, відбувається спроба здійснити шахрайство, якщо вам пропонують:
- надати особисту інформацію невідомому джерелу;
- підтвердити ваші облікові дані, погрожуючи призупинити дію вашого рахунку;
- продати щось за ціною, яка значно перевищує вартість цього предмету;
- здійснити прямі грошові внески.
- Під час здійснення покупок в Інтернеті рекомендовано використовувати кредитні картки.

На жаль, фішингові атаки стають дедалі складніші, тому звичайному користувачу нелегко визначити шахрайські повідомлення електронної пошти або веб-сайти. Це пояснює успішність і популярність фішингових схем серед злочинців. Наприклад, багато шахрайських повідомлень електронної пошти та веб-сайтів мають посилання на логотипи реальних відомих компаній і тому виглядають як справжні. Нижче наведено кілька порад щодо захисту від зловмисників.

- Запити особистих даних у повідомленнях електронної пошти. Більшість серйозних компаній не надсилають запит на надання особистих відомостей електронною поштою. Такі повідомлення мають викликати підозру, навіть якщо здається, що вони справжні.
- Терміновість. Фішингові повідомлення електронної пошти зазвичай написані у ввічливому та люб’язному тоні. Вони здебільшого спонукають відповісти на повідомлення або перейти за посиланням, яке міститься в повідомленні. Щоб збільшити кількість відповідей, автори повідомлення намагаються створити відчуття терміновості, щоб користувач відповів, не думаючи. Підроблені повідомлення електронної пошти зазвичай неперсоналізовані, на відміну від справжніх повідомлень від банків або компаній, що займаються електронною комерцією, які зазвичай персоналізовані.

- Вкладення. За багатьма фішинговими схемами вам пропонується відкрити вкладення, яке може містити вірус або шпигунське програмне забезпечення. Якщо шпигунське програмне забезпечення завантажено на комп'ютер, воно може записувати натискання клавіш, яке ви використовуєте для входу до своїх особистих облікових записів в Інтернеті. Перш ніж відкрити будь-яке вкладення, яке потрібно переглянути, його слід зберегти, а потім перевірити за допомогою оновленої антивірусної програми. Для захисту вашого комп'ютера програма Outlook автоматично блокує певні типи файлів вкладень, які можуть розповсюджувати віруси. Якщо програма Outlook виявляє підозрілі повідомлення, вкладення будь-якого типу файлу в цьому повідомленні блокуються.
- Підроблені або підозрілі посилання. Автори фішингових повідомлень занадто майстерні у створенні підроблених посилань, щоб звичайні користувачі могли відрізнити їх від справжніх. Завжди краще ввести у вікні браузера правильну веб-адресу, яку ви знаєте. Ви також можете зберегти правильну веб-адресу в папці браузера Уподобання. Не копіюйте та не вставляйте веб-адреси з повідомлень у вікно браузера.

Нижче перелічено ситуації, у яких з'являється оповіщення системи безпеки.

1. Користувач вибирає у відкритому документі посилання на веб-сайт, адреса якого потенційно містить підроблене ім'я домену.
2. Користувач відкриває файл із веб-сайту з адресою, яка потенційно містить підроблене ім'я домену. З'являється повідомлення системи безпеки. Прочитайте повідомлення та зробіть потрібний вибір.
3. Користувач може вибрати, чи продовжувати відвідувати цей веб-сайт надалі. У цій ситуації рекомендовано натиснути в повідомленні системи безпеки кнопку Ні. Ця функція допомагає захиститися від атак із використанням омографів.
4. Якщо фільтр небажаної пошти не вважає повідомлення спамом, але вважає фішинговим, воно залишається в папці "Вхідні", але всі посилання в ньому вимикаються, а функції Відповісти таВідповісти всім не працюють.
5. Якщо фільтр небажаної пошти вважає повідомлення і фішинговим, і спамом, воно автоматично переміщується до папки "Небажана пошта". Кожне повідомлення в папці "Небажана пошта" перетворюється на звичайний текстовий формат, і всі посилання вимикаються. Крім того, деактивуються функції Відповісти й Відповісти всім. Оповіщення про ці функціональні зміни відображається на інформаційній панелі.
6. Маскування посилання. Хоча посилання може містити справжнє ім'я компанії або його частину, воно може бути "замасковане". Це означає, що за відображуваним посиланням буде виконано перехід не до вказаної адреси, а до іншої, зазвичай до підробленого веб-сайту. Після наведення вказівника на посилання в повідомленні Outlook може відображатись інша числова адреса в Інтернеті. Це має викликати підозру. Пам'ятайте, що навіть посилання в полі з жовтим тлом можна підробити.

7. Омографи. Омографи – це слова з однаковим написанням, але з різними значеннями. У комп'ютерній термінології атака з використанням омографів – це веб-адреса, яка виглядає як відома веб-адреса, але насправді її змінено. Мета використання підроблених веб-адрес у фішингових схемах – обманним шляхом примусити користувача перейти за посиланням.
8. Відстежуйте свої транзакції. Перевіряйте свої підтвердження замовлень і баланс кредитної картки й банківських рахунків.
9. Використовуйте кредитні картки для транзакцій в Інтернеті. У більшості регіонів платіжні зобов'язання за кредитними картками значно обмежено.

Іноді хакери зловживають не наївністю, а винахідливістю і талантом користувачів. Віруси та шахрайські програми – в першу чергу, «шпигуни» – вбудовуються в цілком законні і добропорядні модифікації інтерфейсу («Аддони»), які створюються користувачами. У кращому випадку, вони просто знесуть вам сайт. У гіршому – завдадуть непоправної шкоди комп'ютера, фінансового благополуччя (якщо «зламають» вашу кредитну картку) або навіть гірше (якщо дістануться до поштової адреси).

Будьте гранично пильні і обережні, якщо завантажуєте аматорські модифікації інтерфейсу й інші програми. Якщо при завантаженні файл веде себе як виконуваний, негайно припиніть завантаження і видаліть файл з жорсткого диска і з кошика. Якщо ви побоюєтеся, що нещодавно завантажили таку програму, то як можна швидше запустіть антивірус, перевірте весь комп'ютер, потім змініть пароль.

Існують сайти, які автоматично виявляють вразливі місця вашого браузера, щоб встановити на ваш комп'ютер шкідливі програми. Кінцевий результат приблизно той же, що і при установці хакерських «аддонів». Іноді з першого погляду очевидно, що сайт – «липа», але іноді такі сайти замасковані, і непогано, під сайти RIA.ua. Єдиний спосіб визначити, офіційний сайт перед вами чи ні, – подивитися на URL (адресну рядок). Якщо це не адреса RIA.ua, але на сайті стверджується, що це офіційний ресурс, то, швидше за все, це шахраї.

Щоб не стати жертвою підробленого сайту, головне – регулярно оновлювати антивірусну програму і користуватися новітньою версією браузера. Уважно читайте посилання, навіть якщо вам їх прислав знайомий. Якщо ви думаєте, що останнім часом потрапили на такий шахрайський сайт, то як можна швидше запустіть антивірус, перевірте весь комп'ютер, потім змініть пароль.

Використовуйте лише новітню версію антивіруса і браузера.

Останнім часом все частіше почав зустрічати в Інтернеті інформацію про можливості безкоштовної відправки SMS і навіть безкоштовних розмов по мобільному телефону. Якщо ви знайшли сайт з *. exe-файлом, який можна скачати, заплативши всього $20, і потім безкоштовно відправляти короткі текстові повідомлення. Якщо заплатити гроші через платіжну систему і отримати пароль для завантаження програми, то після її встановилення, ніякого зменшення платежу не відбудеться. Рахунок за sms-повідомлення все одно прийде.

Запам’ятайте – існування безкоштовного мобільного зв’язку це міф. Але людей, які розуміють це, не так багато. Тому ще недавно на аферах в цій області шахраї отримували величезні прибутки.

Нагадаємо деякі правила захитсу від цього виду шахрайства:

1. Перш за все, слід встановити на свій комп'ютер необхідний захист, а саме антивірусне програмне забезпечення відомого виробника. Його необхідно регулярно оновлювати, про що забувати не слід.

2. Дуже важливо намагатися не розміщувати в мережі особисту інформацію, таку як ваше ім'я, адреса, телефони тощо.

3. Ніколи не відповідайте на спам.

6. Важливо не зберігати свої паролі на комп'ютері. Краще використовуйте для цього зовнішні носії, тобто ту ж звичайний папір або блокнот, або ж зберігайте їх у спеціальних програмах, захищених від злому.

7. Не виконуйте жодних дій, що вимагаються в повідомленнях, отримані від невідомих користувачів на вашу електронну пошту. В іншому випадку нічого хорошого не чекайте.

4. Не відкривайте і не запускайте файли або програми, які прислали вам невідомі люди. У них може міститися що завгодно і в більшості випадків ці віруси.

5. Якщо навіть від ваших знайомих приходять підозрілі повідомлення, не відповідайте і не відкривайте їх, оскільки їх сторінки можуть бути зламані і використані шахраями. Це дуже поширене явище.

6. Не проводьте операцій зі своїми банківськими рахунками через Інтернет у громадських місцях та Інтернет-кафе. Це дуже небезпечно.

Ще поради:

1. Уважно ставтеся до всіх електронних листів, які містять посилання на інші ресурси. Далеко не завжди зазначена посилання веде туди, куди вказано в описі.

2. Не надсилати особисту та конфіденційну інформацію з мережі, якщо вона не зашифрована.

3. Уважно ставтеся до адрес сайту, які схожі на сайти великих компаній або відомих брендів. Створенням подібних ресурсів займаються шахраї, єдиною метою яких є обман клієнтів та збір особистої інформації.

4. Використовуйте тільки надійні пін-коди та паролі для доступу до різних ресурсів, соціальним мережам, електронній пошті і т.п. Не використовуйте однаковий, нехай навіть складний, пароль для кількох сайтів.

Працюючи або розважаючись в Інтернеті, ми реєструємося на масі сайтів. Щоб ваш логін і пароль не потрапили в чужі руки, а ваша особиста переписка не стала надбанням громадськості, дуже важливо дотримуватися безпеку в Інтернеті.

Запорука безпеки в Інтернеті – надійний пароль. Часто користувач не може придумати пароль і використовує прості поєднання букв або цифр по типу "qwerty" або "123456". Але такий пароль дуже легко підібрати, і при спробі злому хакери перевіряють такі комбінації в першу чергу. Тому дійсно безпечний пароль повинен відповідати певним критеріям.

Пароль не повинен складатися з простого слова, небажано використовувати в якості пароля своє ім'я, прізвище, дату народження, імена близьких людей і т.п. Краще використовувати не слово, а безглузду комбінацію букв. Якщо вам важко її придумати, наберіть українське слово в англійській розкладці, наприклад, слово "захист" перетворюється в "pf[bcn". Але, знову ж таки, українське слово не повинно бути занадто простим, до того ж, більшість зломщиків пароля з цією хитрістю знайомі.

Кращий пароль – це комбінація великих і малих літер, цифр і спецсимволів у довільному порядку. Чим важливіше для вас пароль від аккаунта на тому чи іншому сайті, тим складнішим він повинен бути. Багато сайтів визначають ступінь безпеки вашого пароля при реєстрації і не дають можливості використовувати занадто простий пароль.

Ті ж вимоги відносяться і до секретного питання, службовцю для відновлення забутого пароля. Занадто просте питання з очевидною відповіддю, відомим не тільки вам, анітрохи не убезпечить ваш аккаунт електронної пошти. Краще замість стандартного секретного питання придумати власний, відповідь на який буде відомий тільки вам. Це підвищить вашу безпеку в Інтернеті. Якщо сайт, на якому ви реєструєтесь, пропонує здійснити прив'язку вашого аккаунта до номера мобільного телефону – скористайтеся цією можливістю, тоді при втраті пароля він прийде не на електронну пошту, а у вигляді SMS. Погодьтеся, зловмисникові важче отримати фізичний доступ до вашого телефону, ніж до електронної поштової скриньки.

Для забезпечення безпеки в Інтернеті дуже важливо правильно зберігати ваш пароль. Найкраще запам'ятати його напам'ять і ніде не записувати – тоді ймовірність того, що він потрапить у чужі руки, мінімальна. Якщо ви не можете обійтися без підказки, придумайте кодову фразу, в якій буде зашифрований ваш пароль. Існують також програми для збереження паролів, які зберігають всі ваші паролі в базі даних. Але для доступу до бази теж використовується пароль, так що занадто довіряти програмам не варто.

Багато браузерів пропонують зберігати ваші паролі. Але якщо ви дорожите безпекою в Інтернеті, зберігайте паролі в браузері тільки на вашому особистому комп'ютері, до якого маєте доступ тільки ви. На роботі, в університеті або в інтернет-кафе запам'ятовувати пароль в браузері не варто. При роботі з чужого комп'ютера при вході на сайт, що вимагає авторизації, ставте галочку біля фрази "чужий комп'ютер" або "не запам'ятовувати пароль", якщо така функція присутня. Закінчуючи роботу з сайтом, обов'язково натисніть на кнопку "вихід", інакше наступний користувач, який сяде за комп'ютер, отримає доступ до вашого аккаунту.

Намагайтеся на різних сайтах використовувати різні паролі. Наприклад, пароль вашої електронної пошти не повинен співпадати з паролем в соціальній мережі. Щоб підвищити рівень безпеки в Інтернеті, використовуйте різні електронні поштові скриньки для особистого листування і для реєстрації на сайтах. З електронною кореспонденцією краще працювати не безпосередньо в браузері, а в спеціальній програмі - поштовому клієнті.

Ваш пароль можуть перехопити і за допомогою спеціальних скриптів. Наприклад, в соціальних мережах популярні скрипти, що дозволяють відзначити відразу всіх друзів на фотографії. Вам пропонується просто скопіювати код та вставити його в адресний рядок браузера. Можливо, цей код і правда безпечний – але якщо ви не розбираєтеся в скриптах і не впевнені на 100%, як працює код, ризикувати не варто, якщо ви не хочете втратити свого аккаунта. З тих же міркувань безпеки в Інтернеті постарайтеся не використовувати програми, що пропонують скачати з соціальних мереж музику і відео, якщо вони пропонують вам ввести свій логін і пароль.

Для перехоплення паролів використовуються трояни – шкідливі програми, які маскуються під нешкідливі файли. Щоб убезпечити свої особисті дані, не завантажуйте файли з недовірених джерел і не запускайте незнайомі програми. Обов'язково встановіть на свій комп'ютер антивірусне програмне забезпечення – існує безліч антивірусів, і багато безкоштовних антивірусів не поступаються по надійності і функціональності комерційним. Наприклад, антивірус avast. Також підозрілі файли і посилання можна перевірити онлайн, щоб упевнитися в їх безпеці.

5.3.2. Заходи безпеки при налаштуванні браузера

Якщо ви є користувачем брапузера Google Chrom, то описані нижче заходи в цій програмі діють автоматично. Отже нічого більше робити не потрібно. Але значна кількість людей користується продуктами фірми Micrjsjft.

В системі Office виявлення підозрілих посилань на веб-сайти ввімкнено за замовчанням. Виявлення можна вимкнути, і, в такому разі, оповіщення системи безпеки не з’являтимуться. Але робити це не рекомендовано.

1. У будь-якій програмі системи Office перейдіть на вкладку Файл.
2. Виберіть пункт Параметри.
3. Виберіть категорію Центр безпеки та конфіденційності та натисніть кнопку Настройки центру безпеки та конфіденційності.
4. Виберіть пункт Параметри захисту конфіденційної інформації.
5. У розділі Параметри захисту конфіденційної інформації встановіть або зніміть прапорецьПеревіряти документи Microsoft Office, отримані з підозрілих веб-сайтів, або які містять посилання на такі веб-сайти.
6. Натисніть кнопку ОК.

Наведене нижче зображення – приклад області Параметри захисту конфіденційної інформації Центру безпеки та конфіденційності.

Дізнатися, що посилання на веб-сайт підозріле, важко. Проте функції системи безпеки в Office можуть попередити проблеми, викликані переходом за посиланням на веб-сайт, що має зловмисні наміри.

На рис. 5.3. показано приклад попередження програми-мейлера Outlook Express у разі переходу за підозрілим посиланням.

Параметри Центру безпеки та конфіденційності можуть допомогти захистити вас від зловмисних намірів, наприклад омографів, тобто веб-адрес, що

використовують літери з різних мов. Веб-адреса виглядає легітимною, але може відкрити сайт зі зловмисними намірами.

Наприклад, наведена веб-адреса виглядає легітимною, але користувачу не видно, що літера і в адресі microsoft.com – кириличний символ з українського алфавіту: www.microsoft.com.

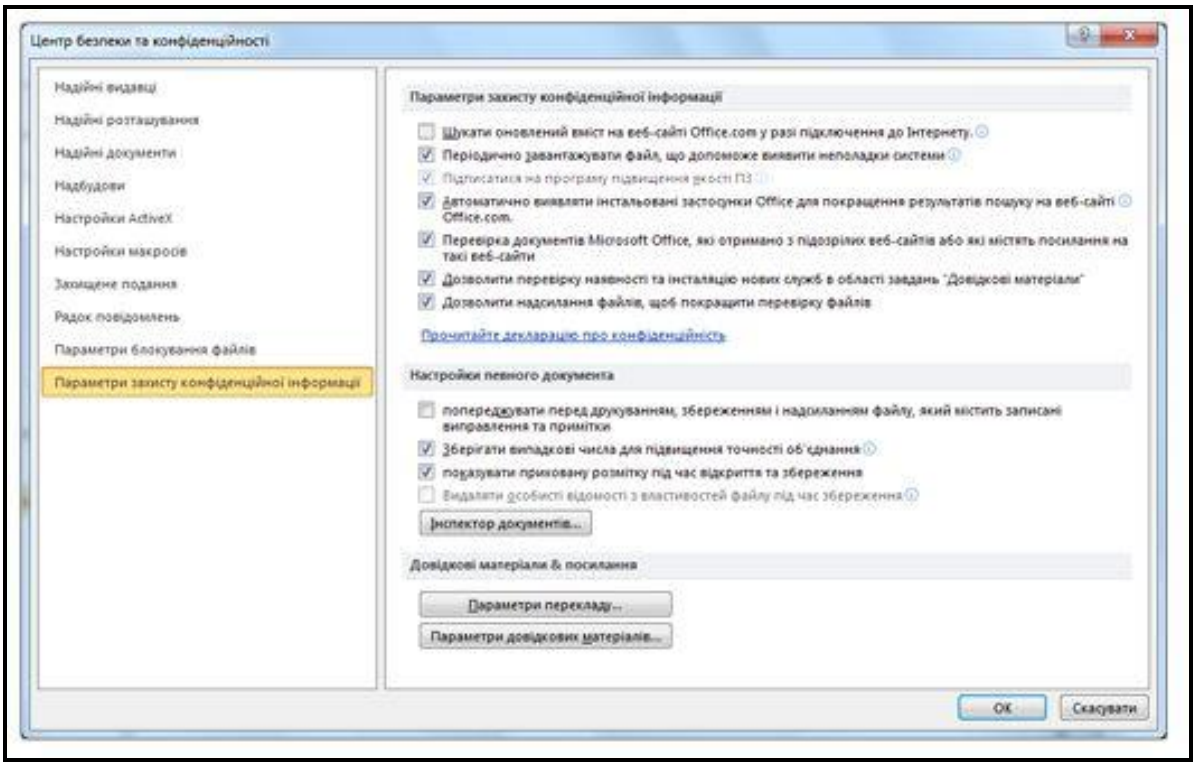


Рис. 5.2. Область «Параметри захисту» браузера Internet Explorer

.

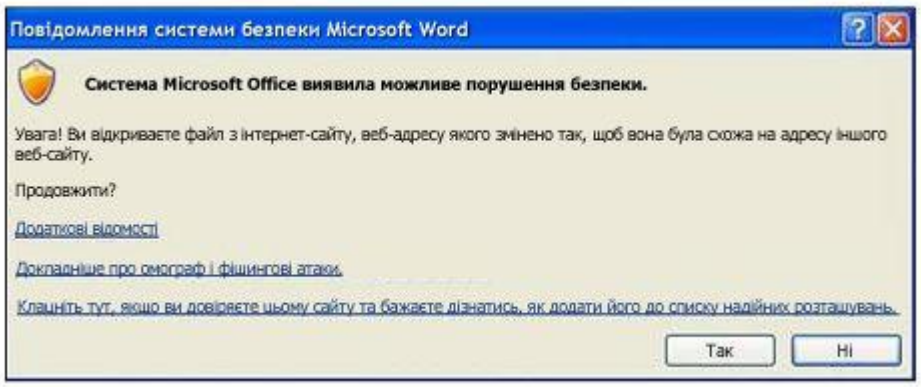


Рис. 5.3. Приклад повідомлення мейлера Outlook Express
про перехід за підозрілими посиланнями

Як реагувати на оповіщення

Оповіщення відображається в разі вибору посилання на веб-сайт, що використовує потенційно підроблене ім’я домену. Можна вирішити відвідати цей сайт або натиснути кнопку Ні у вікні оповіщення (рекомендовано).

Докладніші відомості про заходи безпеки та шахрайство в Інтернеті

Докладніше про шахрайство в Інтернеті можна дізнатися в розділі Захист від фішинг-махінацій та інших форм шахрайства в Інтернеті.

Зведіть ризик кібер-хуліганства до мінімуму, допоможіть дітям безпечніше користуватися сайтами соціальних мереж і використовуйте елементи керування батьківським наглядом у продуктах компанії Майкрософт, щоб покращити безпеку своєї сім'ї в Інтернеті: Центр безпеки в Інтернеті компанії Майкрософт.

Якщо вам відомо, що певний веб-сайт надійний, можна вимкнути відображення оповіщень, додавши цей сайт до зони надійних сайтів у браузері Internet Explorer. До надійних сайтів може належати інтрамережа вашої установи або сайти, про які ви довідалися з надійних джерел.

1. У браузері Internet Explorer версій 5, 6, 7, 8 або 9 у меню «Знаряддя» виберіть пункт «Властивості браузера». Щоб дізнатися версію програми, у програмі Internet Explorer виберіть команду «Довідка». Потім виберіть пункт «Про програму.» Відобразиться номер версії.
2. На вкладці «Безпека» виберіть елемент «Надійні сайти» та натисніть кнопку «Сайти».
3. У полі «Додати веб-сайт» до зони введіть або виберіть адресу веб-сайту та натисніть кнопку «Додати».
4. Якщо потрібно, щоб у браузері Internet Explorer виконувалася перевірка надійності сервера для кожного веб-сайту в цій зоні перед підключенням, установіть прапорець «Потрібна перевірка сервера» (https:) для всіх сайтів у цій зоні.
5. Натисніть кнопку ОК.

Якщо отримане повідомлення електронної пошти здається вам шахрайським, можна надіслати звіт і вкласти до нього підозріле повідомлення. Надсилання звітів про підозрілі повідомлення допомагає боротися з викраденням особистих даних.

APWG – Анти-фішингова робоча група http://www.antiphishing.org/?lc=uk-UA

FTC – Федеральна комісія з торгівлі https://www.ftccomplaintassistant.gov/?lc=uk-UA

BBB – Бюро з покращення ділової практики http://www.bbb.org/?lc=uk-UA

Повідомлення стосовно проблем, до яких має відношення корпорація Майкрософт, можна надіслати за адресами:

- abuse@msn.com
- abuse@microsoft.com

5.3.3. Програма Password Safe

Зберігання списків паролів на клаптиках паперу, або в текстових документах на робочому столі небезпечно і легко доступне для сторонніх очей. Використовувати один і той же пароль знову і знову в широкому спектрі систем та веб-сайтів, створює кошмарну можливість ситуації, коли

варто комусь узнати цей пароль, як можна отримати доступ до будь-якого іншого сайту: електронної пошти, роздрібної торгівлі, фінансових операцій, роботи.

Отже, для кожного сайту, яким ви користуєтеся, потрібно мати власний логін та пароль. Щоб не завантажувати голову переліком цих даних, які мають властивість постійно зростати, розроблена програма Password Safe, яка дозволяє безпечно і легко створити захищене і зашифроване ім'я користувача та пароль зі списку, будь якого розміру.

Програма розміщена за одресою http://passwordsafe.sourceforge.net/, причому автор розробки розповсюджує її безоплатно.

Password Safe дозволяє Вам управляти вашими старими паролями, легко і швидко створювати, зберігати, організовувати, шукати та використовувати нові складні паролі, використовуючи парольну політику, під вашим контролем. Після збереження, ваші імена користувачів і паролі стануть доступними всього лише за кілька кліків мишкою.

Разом із Password Safe ви можете організувати ваші паролі, використовуючи ваші власні настроювання посилання, наприклад, ідентифікатор користувача, категорія, веб-сайт, або місце розташування. Ви можете зберігати всі ваші паролі в одному зашифрованому списку (зашифрованій базі паролів), або використовувати декілька баз даних для подальшої організації ваших паролів на роботі і вдома.

При першому запуску інсталяційного пакету pwsafe-3.30.exe потрібно погодитися з ліцензійною політикою та вибрати портативний режим (рис. 5.4)

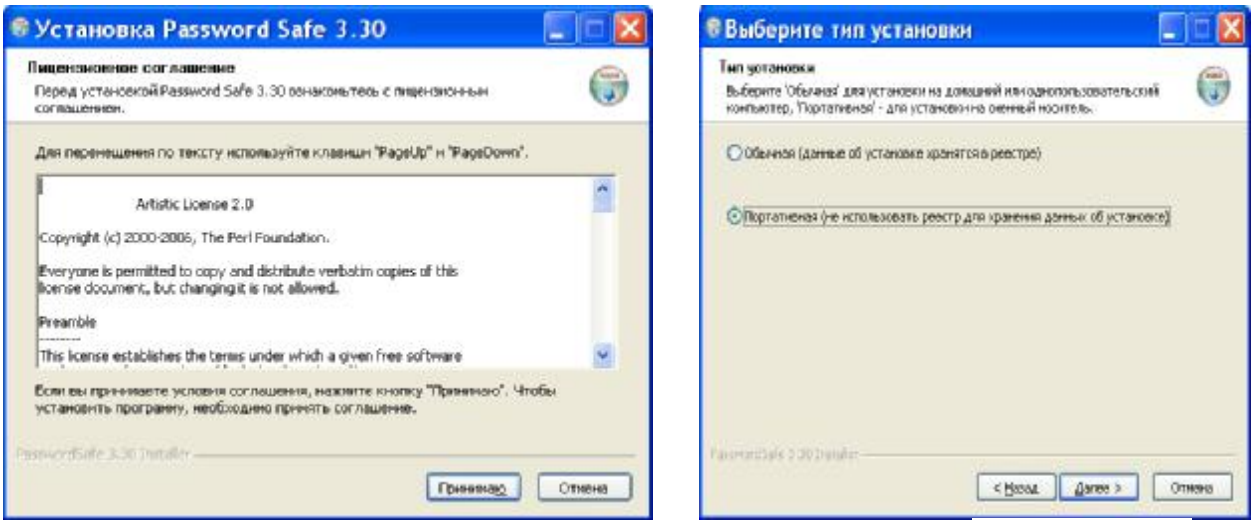


Рис. 5.4. Інтерфейс запуску процесу інсталяції програми Password Safe

Після вибору мови інтерфейсу та місця на компютері, куди буде встановлено програму (рис. 5.5), починається створення бази паролів.

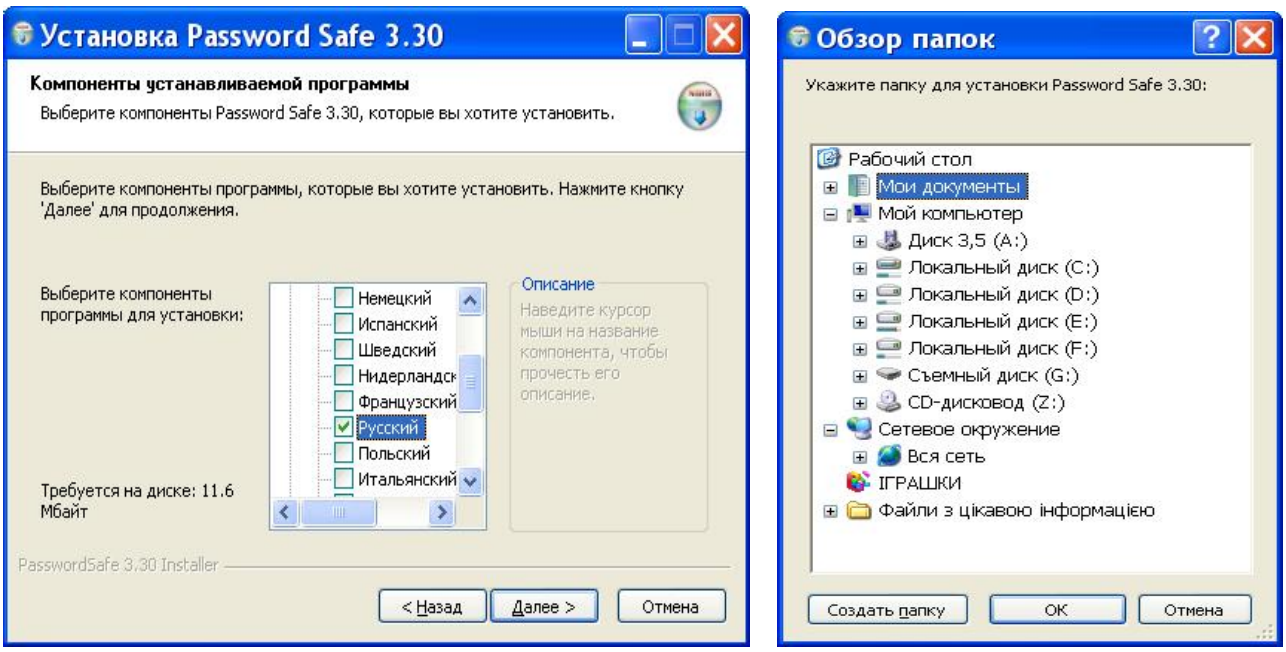


Рис. 5.5. Вибір мови інтерфейсу та місця розташування в комп’ютері користувача програми Password Safe

Password Safe дозволяє користувачам зберігати всі паролі в одному "безпечному" паролі бази даних. Можливо також створення декількох баз даних для різних цілей (наприклад, один для роботи, один для особистого користування). Кожна база даних є незалежною, її можна переміщати і використовувати на різних комп’ютерах. Для кожної бази потрібно знати всій пароль. Цей пароль не зберігаються в базі даних в будь-якій формі, що підвищує рівень запхисту ваших ключових слів та логінів.

При першому запуску потрібно натиснути кнопку New Database (рис. 5.6). Вам буде запропоновано вибрати ім'я й розташування пароль бази даних (за умовчанням ім’я цієї бази буде pwsafe.psafe3). Після цього вам буде запропоновано ввести майстер-пароль, який використовується для шифрування і блокування вмісту вашого нового безпечного.

Є два способи створення нової бази паролів:

1. Натиснувши кнопку «Створити базу даних» при запуску програми .

2. З меню File-New Database, коли програма Password Safe вже відкрита

Використання будь-якого з цих методів призводить до того, що з'явиться. діалогове вікно Add Enry (рис. 5.7.)

За замовчуванням Password Safe покаже останню базу даних. Якщо ви використовуєте кілька баз даних, ви можете вибрати між ними за допомогою випадаючого списку. Крім того, ви можете ввести шлях до бази даних, щоб відкрити, або вибрати його із діалогового вікна файлу, натиснувши на три крапки, розташовані на кнопці ("..."). Так само можна змінити базу даних.

У вікні Add Entry найбільш важливим є заповнення першого (Group), третього (Username), четвертого (Password) і п’ятого (Conform Password) вікон. Заповнення інших не обов’язкове.

Перше вікно містить довільно обрану назву того пароля, який ви будете зберігати. Саме за цією назвою потім ви його знайдете. У третє вікно потрібно вписати логін, з яким використовується той чи інший пароль. Четверте і п'яте вікно повинно містити один і той же пароль, який необхідно запам'ятати в програмі.

Кнопка Show дозволяє переглядати сам пароль. Якщо вона не натиснута, замість пароля будуть видні тільки жирні крапки або зірочки. Кнопка Generate дозволяє згенерувати новаий і безпечний, з точки зору криптографії, пароль.

Рис. 5.6. Створення нової бази паролів в програмі Password Safe

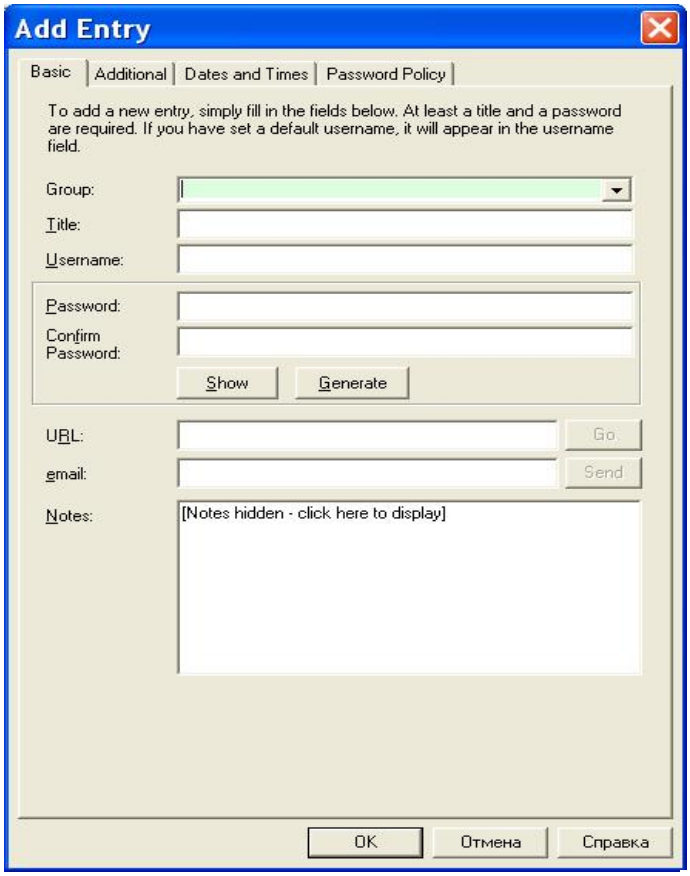


Рис. 5.7. Створення нового логіна та пароля в програмі Password Safe

Після закінчення процесу інсталяції, програма створює теку Password Safe, в якій для запуску програми потрібно знайти файл pwsafe.exe.

Password Safe надає декілька механізмів для використання збережених імен (логінів) і паролів. Більшість способів вимагають копіюванні імені користувача або пароля в буфер обміну, а потім вставлення цих даних у відповідні поля введення на тобі сатй на який ви бажаєте зайти. Password Safe забезпечує функцію, Auto Type, який автоматизує введення імені користувача і пароля у веб-форми.

Розберемо детально ці способи (рис. 5.8).

Ім'я користувача:

Виберіть значок ім'я користувача з панелі інструментів

або

Кклацніть правою кнопкою миші по назві обраного сайту і виберіть **Копіювати ім'я користувача в буфер обміну.**

або

• За допомогою **Ctrl + U**

і потім переходите до обраного сайту, сативте курсор клавіатури у вікно логіну і вставляєте ім'я користувача в потрібне поле кнопками **Ctrl+V**.

Пароль:

Виберіть значок пароля на панелі інструментів

або

Про клацніть правою кнопкою миші по назві обраного сайту і виберіть **Копіювати пароль в буфер обміну**

або

Ø використання **Ctrl + C**

і потім вставте пароль в потрібне поле кнопками **Ctrl+V**.

В усіх випадках ця процедура простіша, аніж пригадування пароля для конкретного виду вашої діяльності.

5.4. Індивідуальне завдання № 5

Тема роботи: використання програми Password Safe для роботи з Демобанком системи PayCash.

Мета роботи: вивчити основні прийоми викоистання програми Password Safe

Завдання: виконати наступні операції:

1. Вставити свій пристій флеш-пам’яті в компютер.
2. Інсталювати на ньому програму Password Safe.
3. Відкрити браузер та набрати адресу сайту "Демобанк"**:** https://www.demobank.ru/download/chrome.php.
4. Перед введенням паролів на сайт, створити новий обліковий запис, відкривши вікно Add Entry .
5. Встановити плагін
6. Згенерувати ключ за допомогою програми Password Safe.

7. Вставити цей ключ у вікно сайту PayCash
8. Ознайомитись з основними можливостями системи електронних розрахунків PayCash.
9. Зробити огляд Інтернет–магазинів, натиснувши клавішу Магазини з пункту меню Деньги–товар.
10. Вибрати один із них для детального огляду послуг згідно номера свого комп'ютера в локальній мережі. Зайшовши на домашню сторінку, переглянути послуги, скопіювати їх з допомогою команди Копировать з меню Правка, а потім помістити у звіт, використавши команду Вставить.

Рис. 5.8. Основне вікно програми Password Safe

11. Ознайомитись з вимогами, які необхідні, щоб стати користувачем системи PayCash та занотувати їх у звіт.
12. Оформити звіт, описавши всі пункти виконання.
13. Виконати огляд регіонального сайту www.vin.com.ua.
14. Проаналізувати розвиток електронної комерції в нашому регіоні та відобразити результати аналізу в звіті у вигляді таблиць та діаграм.

Коротка довідка про систему еклектронних платежів PayCash:

Демобанк призначений для іспитів і демонстрації можливостей платіжної системи PayCash. Він оперує тільки "іграшковими" грошима. На даний час у системі використовуються наступні валюти: рублики, доларики, йенки, лірики і гривеньки.

Набір валют, а також розцінки на послуги Демобанку умовні і не можуть тлумачитися як обов'язкові чи обмежуючі для банків, що оперують реальними цінностями в рамках системи PayCash.

Будь–хто з бажаючих може стати клієнтом Демобанку, завантаживши параметри Демобанку в Кошелек і відкривши в ньому за допомогою Кошелька рахунок (у повнофункціональному Кошельку можна відкрити кілька рахунків).

Кошелек – електронне меню, з допомогою якого здійснюються всі операції в системі PayCash.

Демобанк обслуговує "іграшкові" гроші: рублики, доларики, йенки і лірики. Номер свого рахунку можна дізнатись, вибравши пункт "Рахунки" зведеного меню Кошелька. Там же зазначена сума, що знаходиться на рахунку. Зараховувати миттєво невеликі суми на рахунки в Демобанку можна за допомогою Демобанкомата. Зараховувати на рахунок можна тільки рублики, доларики і лірики. Витратити демогроші можна в Демомагазині.

Контрольні запитання

1 . Назвіть перші ознаки фішінгу?
2. Дайте перелік простих прихомів захисту від фішінгу.
3. Що таке «шахрайство при інвестуванні»?
4. Дайте ознаку фінансової піраміди?
5 . Що таке «нігерійські листи»?.
6 . Чи буває Інтернет бехкоштовним?
7 . Як розпізнати штучний ажіотаж?
8. В чому полягає сутність файлового шахрайства в Інтернеті?
9. Які небезпеки чатують на покупця автомобіля через Інтернет?
10. Чим відрізняються організаційні заходи безпеки від програмних?
11. Яким браузером краще користуватися для збільшення рівня захисту вашої інформації?
12. Куди можна надіслати звіт про можливі шахрайські дії в Інтернеті?
13. Для чого розроблена програма Password Safe?
14. Як правильно вибирати пароль?
15. Скільки символів повинен мати пароль?

Вивчивши матеріали цього розділу, студенти опанують методи захисту від різноманітного електронного шахрайства та отримають у власне користування програму, яка полегшує запам'ятовування різноманітних логінів та паролів на сатах в Інтернеті.

ПІДСУМКИ

Захист інформації при виконанні операцій електронної комерції розпадається на два великих напрямки:

– захист від кримінальних дій злочинців, які намагаються проникнути в систему електронної комерції і зашколдити її діями;

– захист від неправомірних дій людей, які через власну довірливість попадаються на шахрайських оборудках.

Якщо брати перший тип небезпекеи, то тут в пригоді стають прогамні засоби захисту, такі як:

– антивірусні програми;

– брандмауер;

– система аутентифікації інформації;

– складні паролі доступу до інформації.

Для другого типу найбільш прагматичним є навчання персоналу прийомам захисту від кіберзлочинців:

– методи розпізнавання фішингу, як головного методу виткрадення особистої інформації;

– прийомам пересилання захищених повідомлень;

– частій зміні паролів;

– постійному контролю за операціями на своїх сторінках з конфіденційною інформацією, тощо.

Всі описані вище методи захисту доступні в сучасних умовах для будь-якого некваліфікованого користувача. Задачею керівництва організації, яка проводить операції з електронної комерції, вимагати від співробітників жорсткого дотримання правил безпеки, а зі свого боку – забезпечення апаратно-прогрманого захисту.

В цьому на пригоді стане описана в посібнику методика визначення найбільш економічно обгрунтованих заходів безпеки, способи розрахунку ймовірності зламу інформаційної системи, методи визначення тарифної нетто-ставки при страхуванні свого бізнесу.

В посмібнику описано більше двадцяти основних методів елеуктронного шахрайства та наведені прийоми захисту від нього.

Програми Password Safe та PortablePGP дозволять окремим користувачам збільшити рівень захисту при персилання текстових повідомлень та при користуванні кодовими ключами в своїй роботі.

Кожен з розділів присвячегний небезпекам у фінансах, в бізнесових операціях та при приватному користуванні можливостями електронної комерції, описує схожі небезпеки, але кожному виду діяльності притаманні свої особливості.

Виконання індивідуальних завдань дозволить студентам не тільки закрінити вивчений матеріал, але й дозволить отримати зручні програми для власної діяльності в сфері електронної комерції.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 5 шагов к B2B. Учебный курс //http:// www .oborot.ru/order/17.
2. Bradford De Long J., Michael Froomkin A. The Next Economy. 1997. April, http:// www. law, mi ami.edu/~froomkin/articles/ newecon.htm.
3. Cohen B.J. Electronic Money: New Day or False Dawn? // International Studies Association Working Papers. 2000. March, //http:// www.polsci.ucsb.edu/faculty/cohen/working/ emoney.html,
4. CyberPlat [Электронный ресурс]. - Российская Интернет-система сетевых денег «КиберПлат» (CyberPlat). – Режим доступа: http://www.ipname.ru/article/pla/
5. DKWLabs [Электронный ресурс]. – Ввод/вывод денежных средств с использованием электронных платежных систем. – Режим доступа: http://www.dkws.org.ua/index.php?page=show&file=a/eps/e4
6. Encyclopedia of the New Economy, WIRED. 1998. May. //http://www.hotwired.com/ special/ene/.
7. European Telcwork Online. Сайт Европейской организации по телеработе //http:// www.eto.org.uk/.
8. Faucheux C. How virtual organizing is transforming management science. //Association for Computing Machinciy. Communications of the ACM; New York; 1997. Sep.
9. Friedman B.M, The Future of Monetary Policy: the Central Bank as an Army With Only a Signal Corps? // International Finance. 1999. November. Vol.2. Issue 3. //http;//papers-nber9.org/pape rs/w7 420.
10. Опис електронного шахрайства // history.lohotron.in.ua
11. Hsing 0. New Technologies in Payments— A Challenge to Monetary Policy. European Central Bank. Press Division. 2000. http: //www. ec b. int.
12. Massachusetts Telecommuting Initiative. //http://www.magnet.state.ma.us/doer/ programs/trans/telecomm.htm.
13. Schneider G.P. Electronic commerce. Third annual edition
14. The Commerce Business Daily (CBD)) //http://cbdnet.gpo.gov/.
15. WWW.CREDCARD [Электронный ресурс]. - CyberPlat: CyberPOS + CyberCheck. – Режим доступа: http://www.credcard.ru/russys.html
16. АбдрахимовД. Программное обеспечение конкурсных закупок продукции для государственных нужд // Бюллетень "Конкурсные торги". 2000. Январь-февраль. С. 7-11.
17. Авдошин С.М., Савельева А.А., Сердюк В.А., Технологии и продукты Microsoft в обеспечении информационной безопасности – электронный ресурс http://www.intuit.ru/department/security/mssec/
18. Алексунин, В.А. Электронная коммерция и маркетинг в Интернете / В.А. Алексунин, В.В. Родигина. – М. : Издательский Дом «Дашков и К», 2006.
19. Ананько А. Заключение договоров путем электронного обмена данными //http:/ /www. ra ssi a n la w. net/la w/do c/a 12 3. htm.
20. Афонина С. В. Электронные деньги. – СПб: Питер, 2001. – 128 с

21. Интернет-бизнес и электронная коммерция [Текст]: учебное пособие / А. Э. Калинина. – Волгоград: ВолГу, 2004. – 148с.
22. Ашманов И. Анализ спроса и повышение видимости в поисковых машинах // http://www.ashmanov.ru/pap/searchopt.phtm!.
23. Балабанов И.Т. Электронная коммерция. – Спб: Питер, 2006. – 122с.
24. Борботько Т.В. Лекции по курсу: Защита информации в банковских технологиях для специальностей: 45 01 03 —Сети телекоммуникаций 98 01 02 –Защита информации в телекоммуникациях.
25. Безопасность электронной коммерции – электронный ресурс http://www.klerk.ru/soft/articles/6795/
26. Библиотека I2R. Электронная коммерция //http://www.i2r.ru/static/210/.
27. Бокарев Т. Количественный и качественный состав аудиторий Интернета, тенденции развития и их значение для рекламодателя // Материалы конференции "1п1егпе1-маркетинг-98", http://www,citfo-rum.ru/marketing/im98/,
28. Бокарев Т. Энциклопедия интернет-рекламы // http://book.promo.ru/book/.
29. Бурдинский А. "Домашний банк" – система удаленного управления банковскими счетами через Интернет и ее использование в электронной коммерции //http:// www.avtobank. ru.
30. Вакка Д. Секреты безопасности в Internet. Киев: Диалектика,
31. Варналій З. Основи підприємництва: Навчальний посібник/ Захарій Варналій,. - 3-тє вид., виправл. і доп.. - К.: Знання-Прес, 2006. - 350 с.
32. Введение в криптографию / Под общей ред. В. В. Ященко. – СПб.: Питер, 2001. – 288
33. ВейсмааДжон. 10 ключевых событий в электронной коммерции. Пер. Анны Артамоновой //http://creatu res.pochtamt.ni/in to/ bibl/24.htm, http://creatures. pochtamt.ru/info/ bib!/23.iitm,
34. Википедия. Свободная энциклопедия [Электронный ресурс]. - CyberPlat. – Режим доступа: http://ru.wikipedia.org/wiki/CyberPlat
35. Виноградська А. Основи підприємництва: Навч. посіб./ Алла Виноградська,. - 2-е вид., перероб. і доп.. - К.: Кондор, 2005. - 540 с.
36. Войтович А.И. Электронная торговля: Курс лекций / Войтович А.И. – Академия управления при Президенте Республики Беларусь, 2005. – 117с
37. Волков С.В. Платежные системы для коммерции в Интернете // Мир карточек. 2000. № 1-2,
38. Волокитина А.В. Электорнная коммерция Под ред. Реймана Л.Д. – М.: НТЦ "ФИОРД-ИНФО", 2002.
39. Волчков С.А,, Бшюхопоеа И,В. Безопасность платежей в Интернете. Ч. 2.5. "Решение проблем безопасности в электронной коммерции" //http://www.oborot.ru/ article/199/ 16/prim.
40. Гаврилов, Л.П. Электронная коммерция : учеб. пособие по выполнению практических работ / Л.П. Гаврилов. – М. : Солон-Пресс, 2006.
41. Гетьман О. Економіка підприємства: Навчальний посібник/ Оксана Гетьман, Валентина Шаповал,; Мін-во освіти і науки України, Дніпропетровський ун-т економіки і права. - К.: Центр навчальної літератури, 2006. - 487 с.
42. Глоссарий по информационному обществу //http://www.ijs.ru/glossary.

43. Голдовский И, Безопасность платежей в Интернете. СПб.: Питер, 2001.
44. Грачева М. Центральные банки в эпоху электронных денег: потеря былого могущества? // Сервер издательства "Открытые системы", http://www.osp.ru/ecom/2000/10/ Q40.htm.
45. Донець Л. Основи підприємництва: Навч. посіб./ Любов Донець, Надія Романенко,; М-во освіти і науки України, ДонДУЕТ ім. М. Туган-Барановського. - К.: Центр навчальної літератури, 2006. - 315 с.
46. Достов В, Электронные наличные в новом веке // Инфо-Бизиес, № 2(147). http:/ /www.ibusiLiess.ru/offline/2001/147/6800/.
47. Дратвер Б. Основи підприємницької діяльності: Навчальний посібник/ Борис Дратвер, М-во освіти і науки України, Кіровоградський держ. пед. ун-т ім. В.Винниченка. - Кіровоград, 2003. - 186 с.
48. Економіка підприємства: Навчальний посібник/ П. В. Круш, В. І. Подвігіна, Б. М. Сердюк та ін.. - К.: Ельга-Н: КНТ, 2007. - 777 с.
49. Електронна комерція: Навчальний посібник, А.М. Береза, І.А. Козак та ін., - К.: КНЕУ, 2002.
50. Енциклопедія шахрайств та лохотронів – history.lohotron.in.ua
51. Ермаков А., Хухдаев Е. Электронная цифровая подпись в системе госзакупок // Сервер издательства "Открытые системы", http://www.osp.ru/os/2002/07-0!i/062_l.h1m.
52. Землянова Л. М. Зарубежная коммуникативистика в преддверии информационного общества. – М., 1999. – С. 56.
53. Интерактивный маркетинг и электронная коммерция: Электронный учебно-методический комплекс для студентов специальности I -26 02 03 Маркетинг. / Сост. Е.В.Бесчастная. – Мн.: БГУИР, 2007. – 303 с.
54. Интернет-Банк – новая реальность (цикл статей) //http://www.bankir,ra/ a nalytics/i -banking/3/226.
55. Интернет. Энциклопедия /Под ред. Л. Мелиховой. - СПб: Питер, 2001.
56. Интернет-маркетинг: учебник [Электронный ресурс]: И. В. Успенский. / Режим доступа http://www.aup.ru/books/m80/
57. Информационная безопасность и защита информации: Учебное пособие. – Ростов-на-Дону, 2004. – 82 с.
58. Информационное обеспечение государственного управления / Под ред. Ю.В, Гуляева. М.: Славянский диалог, 2000.
59. Информационный бюллетень Microsoft для государственных служб. Выпуски 5-14. http://www.microsoft.com/rus/ government/.
60. Информационный ресурс "Платежные системы Интернет", Организация расчетов через Internet //http://www.emoney.ru/ bibl/org.asp/.
61. Как мошенники обманывают владельцев платежных карт//http://dit.perm.ru/ a rt icles/ manage me nt/data/0 20104. ht m.
62. Катаев А. В. Виртуальные предприятия – новая ступень в организации НИОКР // Стратегические аспекты управления НИОКР н условиях глобальной конкуренции: Отчет по НИР № 01.2.00100692. Таганрог: ТРТУ, 2001.
63. КиберПлат [Электронный ресурс]. – Платежная система CyberPlat. - Режим доступа: http://www.cyberplat.ru/

64. Кисилев Ю.Н. Электронная коммерция: Практическое руководство - СПб: Питер. 2001.
65. Кобелев О. А. Электронная коммерция: Учебное пособие/Под ред. С.В. Пирогова.- 3-е изд.,- М.: Издательско-торговая корпорация "Дашков и Ко", 2008.
66. Козье Д. Электронная коммерция: Пер. с англ. — Москва: Издательско-торговый дом «Русская Редакция». 1999. — 288 с: ил
67. Колесников А.Н., Веденеев Г,М. Применение современных информационных технологий при проведении конкурсных торгов (тендеров) // 29,11,2000 http://www.bitpro.aha.
68. Компьютерная преступность и информационная безопасность / Под общ. ред. А.П. Леонова, Минск: АРИЛ, 2000,
69. Крылов В.В. Информационные компьютерные преступления: Учебное и практическое пособие. – М.: Инфра-М – Норма, 1997. – 285 с.
70. Крылов В.В. Информационные компьютерные преступления: Учебное и практическое пособие. – М.: Инфра-М – Норма, 1997. – 285 с.
71. Курушин В.Д., Минаев В.В. Компьютеніье преступления и информационная безопасность. – М.: Новіьй юрист, 1998. – 256 с.
72. Лебедев А. Как подписать электронный документ? Современные методы цифровой подписи //httpr//users,g.corn.ua/ -batmanb/box/12/38 .shtml.
73. Лебедев А. Современные методы цифровой подписи //http://old.Iogoart.ru/ ?text=Iinks017.
74. Луквицкий. А.В. Системы обнаружения атак// Банковские технологии. 1999. № 2.
75. Макарова М.В. Електронна комерція посібник, Київ, видавничій центр „Академія” 2002.
76. Меджибовська Н.С. Електронна комерція: Навчальний посібник, - К. 2004.
77. Мочерний С. Основи підприємницької діяльності: Посібник/ Степан Мочерний, Олександр Устенко, Сергій Чеботар. - К.: Академія, 2001. - 279 с.
78. Мошенники в Сети. Руководство по безопасности //http://www.batman.ru/ rogue, him.
79. Мэйволд Э. Электронная коммерция: требования к безопасности http://www.intuit.ru/department/security/netsec/Электронный бизнес и безопасность / В.А.Быков.-М.:Радио и связь, 2000.
80. Опорний конспект лекцій з дисципліни «Електронна комерція» для всіх спеціальностей/ Укладач: Нестеренко С.Д., Сімферополь – 2011, Кримський Економічний Інститут Двнз “Київський Національний Економічний Університет Ім. Вадима Гетьмана”. – 16 с
81. Основи підприємницької діяльності: Навчальний посібник/ Борис Дратвер, Наталія Пасічник, Дмитро Закатнов та ін.; М-во освіти і науки України, АПН України, Ін-т проблем виховання. - Кіровоград, 2004. - 223 с.
82. Основы электронной коммерции: уч. пособие / под ред. С.Ю. Глазьева. – М: Изд. МГУК, 2001.
83. Основы электронной коммерции: уч. пособие / под ред. С.Ю. Глазьева. – М: Изд. МГУК, 2001.

84. Пістунов І.М. Теорія ймовірності та математична статистика для економістів. З елементами електронних таблиць: Навч. Посібник/ І.М.Пістунов, Н.В.Лобова – Дніпропетровськ: Національний гірничий університет, 2005.– 110 с
85. Пістунов І.М. Актуарні розрахунки: Навчальний посібник. - Дніпропетровськ, РВК НГУ,. 2004. - 164 с
86. Повышение качества предприятия с помощью информационных систем класса ERP (на примере MFG/PRO) //http:// www. ci tforum. ru/c fm/m rp/e rp_is. shtml.
87. Пономаренко Л.А., Філатов В.О. Електронна комерція: Підручник. За ред. А.А. Мазаракі.- К.: Київ.нац.торг.-екон.ун-т, 2002.
88. Попов, В. М. Глобальный бизнес и информационные технологии. Современная практика и рекомендации [Текст]: Учебное пособие / В. М. Попов, Р. А. Маршавин, С. И. Ляпунов; под ред. В. М. Попова. - М: Финансы и статистика, 2001. – 320с.
89. Рейнольдс М.Л. Электронная коммерция. – М.: Лори, 2006. – 560с.
90. Сіленко А. Електронна Україна// Політичний менеджмент, – №3, 2003. – С.71-81.
91. Сервер "MAG'a RU – электронная коммерция сегодня, создание" //http:// www.egovernment.ru/.
92. Сервер "E-Government". Технологии и решения для "электронного правительства" //http://www.egoveniment.ru/.
93. Сибирская, Е.В. Электронная коммерция: учеб. пособие / Е.В. Сибирская, О.А. Старцева. - М.: ИНФРА-М, 2008. – 288с.
94. Соколова Л.Н., Геращенко Н.И. Электронная коммерция: мировой и российский опыт. М.: "Открытые системы", 2000.
95. Специальная техника и информационная безопасность том 1, / Под ред. В.И. Кирина – М.:2000. – 783 с.
96. Телеработа и теледоступ: Общие понятия и определения //ETO, 1997, http:// ieie.nsc.ru/~eto/faq/faq02-r.htm.
97. Усоскин В. М. Банковские пластиковые карточки. М.: ИПЦ «Ва-
98. Царев, В.В. Электронная коммерция [Текст]: учебное пособие / В.В. Царев, А.А. Кантарович. - СПб: Питер 2006. - 320 с.
99. Центр исследования проблем компьютер ной преступности //http ://www. c ri me -research.ore/.
100. Цигилик І. І. Основи підприємництва: Навч. посіб./ І. І. Цигилик, Т. М. Паневник, З. М. Криховецька; Мін-во освіти і науки України, Ін-т менеджменту та економіки "Галицька академія". - К.: Центр навчальної літератури, 2005. – 239 с.
101. Шалева О. І. Електронна комерція. Навч. посіб. – К.: Центр учбової літератури, 2011. – 216 с.
102. Шваб Л. Основи підприємництва: Навч. посібник/ Людмила Іллівна Шваб,. – К.: Каравела, 2006. - 343 с.
103. Шипицына, И.В. Технологии электронной коммерции: Учеб. пособие / И.В. Шипицина. – Омск: Максимум, 2006. – 188с.

104. Электронная коммерция : метод. указания / сост. : Н.В. Молоткова, М.А. Блюм. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2008. – 16 с.
105. Электронная коммерция: уч. пособие / под ред. проф. Брагина – М.: Экономист, 2005.
106. Электронная коммерция: уч. пособие / под ред. проф. Брагина – М.: Экономист, 2005.
107. Электронная коммерция: Учебное пособие / В.В. Ежунинов– ДУЭП, 2005. – 104 с.
108. Электронная коммерция: Учебное пособие/О.А.Кобелев; под ред. проф. С.В. Пирогова. – 3-е изд., перераб. и доп. – М.: Издательско-торговая корпорация «Дашков и К°», 2012. – 684с.
109. Электронные банковские услуги: особенности управления рисками (ч. 1—2) // http://www.ifin.ru/publications/read/298.stm, http://www.ifln.ru/ publications/read/299.stm.
110. Электронные платежные системы [Электронный ресурс]. – Платежная система CyberPlat. – Режим доступа: http://www.paysystems.org.ua/ cyberplat.html
111. Юрасов А.В. Електронная коммерция: Учеб. Пособие. – М.: Дело, 2003. – 480 с.
112. Язев А. Электронный документооборот: основные понятия // Мир электронной коммерции. 2001. № 01, http://www.osp.ru/ ecom/2001/Ol/.
113. Яковлев, А.А. Раскрутка и продвижение сайтов. Основы, секреты, трюки / А.А. Яковлев. – СПб. : БХВ-Петербург, 2007.
114. Ярочкин В. И. Информационная безопасность. Учебное пособие для студентов непрофильных вузов. – М.: Междунар. отношения, 2000. – 400 с.
115. E-Commerce 2012/ Eihth Edition/ Kennet C. Laudon, Carol Guercio Traver/ – Pearson Education Limated: Esseccs, 2012/ – 908 p.
116. Keizer J. A Basic Guide to Internatonal Business Law/ J. Keizer, H.Wevers/ – Wolters-Noirdhoff Gronengen: Houten, 2005. – 184 p.

ПРЕДМЕТНИЙ ПОКАЖЧИК

ДОДАТОК. Словник спеціальних термінів

ADSL – це технологія передачі даних, що дозволяє одночасно використовувати звичайну телефонну лінію одночасно для телефону і для швидкісного Інтернету. Телефонний та ADSL-канал не впливають один на одного. Можна одночасно завантажувати сторінки, отримувати пошту і розмовляти по телефону.

Bluetooth (англ. *Bluetooth*) – це технологія бездротового зв'язку, створена у 1998 році групою компаній:Ericsson, IBM, Intel, Nokia, Toshiba.

Chargeback – повернення платежу.

Спайдер – програма? що індексує веб-сторінки в якійсь пошуковій системі. Кожна система індексує сторінки своїм особливим способом і пріоритети при пошуку за індексами теж різні, тому запит за одними і тими ж ключовими словами в кожній з пошукових систем породжує різні результати.

DoS-атака (від англ. Denial of Service - відмова від обслуговування) – здійснюється за допомогою відсилання великої кількості пакетів інформації на сервер, що атакується.

IP-адреса (адреса інтернет-протоколу) – це номер, присвоєний пристрою, під'єднаному до Інтернету. Веб-сайти використовують її, щоб надсилати потрібну вам інформацію на ваш комп'ютер, а не на інший комп'ютер десь поблизу чи на іншому кінці світу. Оскільки ці номери присвоюються на підставі географічного розташування, IP-адресу часто можна використати для визначення країни, області й міста, з яких комп'ютер під'єднується до Інтернету. Однак на відміну від домашньої адреси, IP-адреси більшості користувачів присвоюються динамічно, тобто вони постійно змінюються.

Pump & Dump ("збільшити і скинути") – метод заснований на "вкиданні" в електронні ЗМІ (можливо, за допомогою "злому" новинних сайтів) завідомо неправдивої інформації, наприклад новини про підготовлюваний поглинанні невеликої компанії транснаціональним гігантом. Шахрай заздалегідь купує великий пакет акцій компанії, що поглинається. Ажіотажний попит, викликаний цією новиною, спричинить завищення ціни на папери компанії, і шахрай продасть їх на піку попиту.

Авторизація – керування рівнями та засобами доступу до певного захищеного ресурсу, як в фізичному розумінні (доступ до кімнати готелю за карткою), так і в галузі цифрових технологій (наприклад, автоматизована система контролю доступу) та ресурсів системи залежно від ідентифікатора іпароля користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних)

Безпека – це стан, при якому отсутвие можливість причини-ня шкоди потребам і інтересам суб'єктів відносин.

Веб-переглядач – програма у вашому комп'ютері, за допомогою якої ви відвідуєте веб-сайти. Популярними веб-переглядачами є Windows Internet Explorer, Mozilla Firefox, Google Chrome, Safari та Opera. www.whatbrowser.org

Використання вірусів – метод шахрайство і пошкодження комп'ютерних систем доступно в даний час не тільки професійним програмістам, але і людям, що володіють лише поверхневими знаннями в цій сфері. Багато в чому це обумовлено доступністю самих шкідливих програм і наявністю простої технології їх створення.

Вірус – комп'ютерна програма, здатна копіювати сама себе та заражати комп'ютер

Довідкові служби (Directory Services) – Інтернет-служби, що забезпечують отримання відомостей про потенційних партнерів, а також цікавлять товарах і послугах.

Допоміжні служби (Third-Party Services) – покликані сприяти розвитку стратегії електронної торгівлі, її впровадженню в повсякденне фінансово-економічну інфраструктуру країни і регіонів.

Доставка товарів – метод шахрайства. Починається з пропозиції з тих чи інших причин отримати товар за когось і переслати його потім поштою або передати з оказією за пристойну винагороду. Домовившись про суму винагороди, виконавши умови жертва шахрайства дізнається, що товар, куплений на її ім'я в електронному магазині, був придбаний за допомогою краденої пластикової карти. Тому магазин вимагає повернення купленого продукту або відшкодування його повної вартості, а в іншому випадку загрожує порушити кримінальну справу.

Електронний гаманець – це будь-яка платіжна карта або функція карти, що містить реальну цінність у формі електронних грошей, які власник карти заплатив авансом.

Електронні гроші – електронний аналог готівкових грошей. Цифрові гроші можуть бути куплені, вони зберігаються в електронному вигляді в спеціальних пристроях і знаходиться в розпорядженні покупця.

Електро́нні гро́ші (також відомі як **e-money**, **е-гроші**, **електронна готівка**, **електроні обміни**, **цифрові гроші**, **цифрова готівка** чи **цифрові обміни**) – означення грошей чи фінансових зобов'язань, обмін та взаєморозрахунки з яких проводяться за допомогою інформаційних технологій.

Електронні платіжні системи – це системи розрахунків між Інтернет-користувачами в мережі Інтернет. Ці системи являють собою електронні версії традиційних платіжних систем та за схемою оплати поділяються на: Дебетові (працюють з електронними чеками і цифровою готівкою); Кредитні (працюючі з кредитними картками).

Журнал – під час вашої взаємодії з веб-сайтом комп'ютер, на якому розміщено веб-сайт, може зберігати записи цієї взаємодії, подібно до виписки. Ці записи називаються журналом.

Загроза – намір нанести зло (збиток).

Захист – огорожа суб'єкта отошеній від загроз.

Зловмисне програмне забезпечення – це програмне забезпечення, розроблене з метою проникнення в комп'ютерну систему без згоди власника чи її пошкодження. Це загальний термін, який використовується фахівцями з комп'ютерних технологій для позначення багатьох форм ворожого, агресивного чи нав'язливого програмного забезпечення, зокрема переліченого нижче.

Ігор – метод шахрайства типу «Доставка товарів»: жертві пропонують допомогти перевести гроші, тобто гроші повинні пройти транзитом через її рахунок. Після здійснення транзиту жертва шахрайства дізнається, що гроші переведений з краденою пластикової карти.

Кіберсквоттінг (від англ, cybersquatting) – вид шахрайства, пов'язаний з викупом та реєстрацією, як правило, масової, доменних імен для їх подальшого перепродажу за значно завищеними цінами. Перепродажа доменних імен веб-сайтів приймає промислові масштаби.

Комерційна таємниця – існує цілий ряд відомостей, які не є державними секретами, пов'язаних з виробництвом, технологією, управлінням, фінансами, іншою діяльністю господарюючого суб'єкта, розголошення яких (передача, витік) може завдати шкоди його інтересам.

Кошик – це умовна назва того місця, де зберігається інформація про вибраних користувачем товарах. Названо так за аналогією з кошиком / візком в супермаркетах. Також як і в супермаркеті, користувач може не тільки класти товари в кошик, але і викладати їх звідти. Додавання товару в кошик не означає автоматичного оформлення замовлення на нього.

Люк – див Пошук пролому.

Маскарад – ситуація, коли користувач, видає себе за іншого.

МММ – один з варіантів пірамід Понці.

Мультиме́діа (лат. *Multum* + *Medium*) – комбінування різних форм представлення інформації на одному носієві, наприклад текстової, звукової і графічної, або, останнім часом все частіше – анімації і відео. Характерна, якщо не визначальна, особливість мультимедійних веб-вузлів і компакт-дисків – гіперпосилання. Поняття, що означає сполучення звукових, текстових і цифрових сигналів, а також нерухомих і рухомих образів. Так, мультимедійна база даних буде вміщувати текстову і образну інформацію, відеокліпи і таблиці, і все це має однаково легкий доступ. Мультимедійна телекомунікаційна послуга дозволяє користувачеві посилати і одержувати будь-яку форму інформації, взаємозамінну за бажанням.

Накрутка – некоректні дії сайтів, спрямовані на збільшення показників лічильників. Це можуть бути лічильники відвідувань, банеропоказів, що зареєструвалися користувачів, які підписалися на розсилку або прочитали рекламні листи, і т. п.

Обдурювання з даними – найпоширеніший метод при здійсненні комп'ютерних злочинів. Інформація змінюється в процесі її введення в комп'ютер або під час виведення. Наприклад, при введенні документи можуть бути

замінені фальшивими, замість робочих дискет підсунуті чужі, і дані можуть бути сфальсифіковані.

Особиста інформація – інформація, за допомогою якої можна визначити чиюсь особу, наприклад, ім’я, електронну адресу, платіжну інформацію чи інші дані, які можна пов’язати з такою інформацією.

Партнерські програми – метод побудований на використанні недоліків платіжних систем на основі пластикових карт. Зазвичай шахраї просять жертву, що живе за кордоном, погодитися приймати на своє ім'я чеки від сервісних партнерських організацій. Якщо людина, до якої звернулися шахраї, погодилася їм допомогти, то на її адресу починають приходити чеки. Прийнявши на себе відповідальність зняти готівку з чеку і розписуючись на ньому, людина, таким чином, заявляє в банку, що ці гроші належать саме йому. Через якийсь час Інтернет-магазин виявляє багато опротестованих платежів, і стає ясно, що деякі покупки вироблялися з використанням крадених реквізитів пластикових карт.

Піраміди і листи по ланцюжку – такий лист містить список призхвищ і адрес, за якими одержувачу пропонується надіслати незначну суму грошей (технологія електронних грошей ідеально підходить для таких "підприємств"). Далі, потрібно замінити прізвище одного з одержувачів на свою і розіслати листи далі. Одержувачі у свою чергу мають внести своє прізвище у список.

Піраміди Понці – від схеми пірамід полягає в тому, що в цьому випадку рекламується нібито вигідну ділову пропозицію, часто пов'язану з торгівлею. Фактично при цьому акумульовані кошти шахрай не інвестує, а просто використовує вклади більш пізніх інвесторів, щоб заплатити більш раннім, таким чином, створюючи видимість прибутковості та залучаючи нові жертви.

Повітряний змій – метод, в якому потрібно відкрити в двох банках рахунки з можливістю кредитування. Далі гроші переводяться з одного банку в інший і назад з поступово підвищуються сумами. Хитрість полягає в тому, щоб до того, як у банку виявиться, що доручення про переведення грошей з рахунку не забезпечено необхідною сумою, приходило б повідомлення про переведення коштів у цей банк, так щоб загальна сума коштів на рахунку покривала вимога про перший перекладі.

Пошук пролому – метод заснований на використанні помилки в логіці побудови програми, що працює на чужому комп'ютері. Виявлені проломи можуть експлуатуватися неодноразово. У знайденому «проломі» програма «розривається» і туди уставляється необхідне число команд.

Протокол безпроводової передачі даних, *(WAP, Wireless Application Protocol)* – технологія, що використовується для запуску Інтернет-застосувань на мобільних терміналах. Інтернет-застосування, призначені для такого використання повинні бути підготовлені в спеціальному форматі і придатні для відпрацювання на мобільних терміналах з використанням низькошвидкісних каналів передачі даних існуючих мереж стільникового зв'язку.

Псевдомагазін – Інтернет-магазин, що відкривається для крадіжки грошей, що знаходяться на пов'язаних з картами цього магазину реквізитів платіжних карт. Після того як в руках кримінальних структур з'являються реквізити карт ошуканих покупців, ними можна скористатися. Поширена технологія роботи псевдомагазінов: здійснення трансакцій на невеликі суми (не більше 10 дол). Насправді, такий Інтернет-магазин нічим не торгує, але він регулярно спрямовує авторизаційні запити, що використовують реквізити карток, отримані шахрайським шляхом, в обслуговуючі карткові системи банки, а, отже, магазин може отримувати від банків відшкодування за зроблені в ньому "покупки". Так продовжується до тих пір, поки рівень таких запитиів не насторожить банк і той відмовиться від обслуговування. Тоді такий магазин зникає.

Рекламні програми – будь-який пакет програмного забезпечення, яке автоматично відтворює чи відображає рекламу або завантажує її на комп'ютер

Релева́нтність (англ. *relevance*) – міра відповідності отримуваного результату бажаному. В термінах пошуку — це міра відповідності результатів пошуку завданню поставленому в пошуковому запиті. Визначає, наскільки повно той або інший документ відповідає критеріям, вказаним в запиті користувача.

Розкрадання інформації – можуть приймати різні форми залежно від характеру системи, відносно якої здійснюється несанкціонований доступ. Інформація, що є об'єктом злочинного посягання, може бути віднесена до одного з чотирьох типів: персональні дані; корпоративна інформація, що становить комерційну таємницю; об'єкти інтелектуальної власності та матеріали, захищені авторським правом; інформація, що має значення для розвитку галузей промисловості, економіки окремих регіонів і держав.

Ро́умінг (англ. *roaming* «бродити, мандрувати») – процедура надання послуг зв'язку (мобільний зв'язок, Wi-Fi) абоненту поза зоною покриття «домашньої» мережі (або базової станції) шляхом використання ресурсів базової станції іншого оператора мобільного зв'язку.

Персональні дані – будь-яка документована і / або занесена на машинні носії інформація, яка відноситься до конкретної людини і чи що може бути ототожнена з конкретною людиною.

Cookie (технічною мовою, файл HTTP cookie) – це невеликий файл, який зберігається веб-переглядачем. Він має вигляд рядка з цифр, літер і символів. Файл cookie реєструє вподобання користувача. Наприклад, пошукова система Google використовує їх, щоб запам'ятовувати, якою мовою користувач хоче бачити свої результати пошуку, англійською чи французькою, або чи хоче він використовувати фільтр Безпечного пошуку.

Салямі – злочин вчиняється потроху, невеликими частинами, настільки маленькими, що вони непомітні. Зазвичай ця технологія супроводжується зміною комп'ютерної програми. Наприклад, платежі можуть округляти

до декількох центів, і різниця між реальною та округленої сумою вступати на спеціально відкритий рахунок зловмисника.

Сканування – поширений метод незаконного отримання інформації. При якому службовці, які читають файли інших, можуть виявити там персональну інформацію про своїх колег. Інформація, що дозволяє отримати доступ до комп'ютерних файлів або змінити їх, може бути знайдена після перегляду сміттєвих кошиків. Дискети, залишені на столі, можуть бути прочитані, скопійовані, і вкрадені. Дуже хитрий скануючий може навіть переглядати залишкову інформацію, що залишилася на комп'ютері або на носії інформації після виконання співробітником завдання і видалення своїх файлів.

Служби безпеки (Security Services) – Інтернет-служби, що сприяють забезпеченню конфіденційності при підготовці та укладанні комерційних угод через Інтернет, надають кошти для закриття інформації при підтримці зв'язку, здійснюють контроль за їх використанням.

Служби розрахунків (Payment Services) – Інтернет-служби, що забезпечують надійність і безпеку проходження фінансових коштів через канали електронної торгівлі. В даний час працюють наступні системи електронних переказів.

Сулжбова таємниця – див. Комерційна таємниця

Спам – Зловживання системами обміну електронними повідомленнями з метою безладного масового надсилання небажаних повідомлень.

Створення ажіотажу споживачів – метод використовується при торгівлі на Інтернет-аукціонах і є одним з найбільш поширених способів сконцентрувати навколо виставленого на торги товару увагу покупців. Чим більше покупців збирається навколо виставленого лота, тим психологічно безпечніше почувають себе інші учасники, що примикають до групи тих, хто торгується. Таким чином, щоб створити активний попит на товар, до участі в торгах залучаються "підставні" покупці, що беруть участь в торгах до того моменту, поки реальний покупець не оголосить досить високу ціну за предмет торгу.

Супервідключення – названа по імені програми, що використовувалася в ряді комп'ютерних центрів, обходиться системні заходи захисту і використовувалася при аварійних ситуаціях. Володіння цим "майстер-ключем" дає можливість в будь-який час отримати доступ до комп'ютера та інформації, що знаходиться в ньому.

Транзакція (трансакція) – це здійснення закінчених дій стосовно визначеного об'єкта, що переводить цей об'єкт з одного постійного стану в інший. В різних областях використання цього поняття існують певні відмінності у тлумаченні слова: в *економіці*, транзакція означає зміну права розпорядження матеріальними благами або послугами, в якій бере участь більш ніж один суб'єкт; в *інформатиці*, транзакція відіграє важливу роль в базах даних, є логічною одиницею і зобов'язана відповідати принципам ACID (від англ.*Atomicity*, *Consistency*, *Isolation*, та *Durability*). Гарантує збереження цілісності бази даних; Банківська

операція, яка полягає в переведенні коштів з одного рахунку на інший; Операція, угода, що супроводжується взаємними поступками.

Трафік – відвідуваність сайту

Троянський кінь – метод полягає в таємному введенні в чужу програму таких команд, які дозволяють здійснювати інші, не планувалися власником програми функції, але одночасно зберігати і колишню працездатність.

Троянський кінь – руйнівна програма, яка видає себе за звичайну програму; спочатку вона ніби виконує потрібну користувачеві функцію, але потім краде інформацію чи пошкоджує систему

Уівінг – одне з найбільш поширених злочинів цього виду пов'язано з крадіжкою послуг і відбувається з використанням схеми "заплутування слідів". Зловмисник проходить через численні системи і численні телекомунікаційні мережі Інтернет, системи стільникового і звичайного телефонного зв'язку, щоб сховати справжнє ім'я та місцезнаходження.

Фішинг – це вид шахрайства в Інтернеті, коли хтось намагається обманом змусити жертву надати інформацію делікатного характеру, як-от ім’я користувача, пароль або дані кредитної картки, видаючи себе за надійного учасника електронного спілкування.

Фішинг – це спосіб шахрайства в Інтернеті, яким користуються злочинці, щоб обманним шляхом примусити вас розкрити свої особисті відомості та надалі використовувати їх для обкрадення ваших електронних рахунків.

Фоун-фрейкінг – використання комп'ютера для проникнення в комутаційну телефонну систему для незаконного користування послугами з надання міжміського телефонного зв'язку.

Ха́кер (від англ. *to hack* — рубати) — особливий тип комп'ютерних спеціалістів. Нині так часто помилково називають комп'ютерних хуліганів, тобто тих, хто здійснює неправомірний доступ до комп'ютерів та інформації. Інколи цей термін використовують для позначення спеціалістів взагалі – у тому контексті, що вони мають дуже детальні знання в якихось питаннях, або мають достатньо нестандартне і конструктивне мислення.

Хробак – зловмисне комп’ютерне програмне забезпечення, яке самовідтворюється та використовує комп’ютерну мережу, щоб надсилати свої копії на інші комп’ютери

Цифрові гроші – див. Електронні гроші.

Чарджбек – відмова від платежів за картками банком, котрий запідозрив шахрайство.

Шахрайство з передоплатою – користувачеві пропонується придбати товари, які не володіють в насправді тими властивостями, про які повідомляється. Часто пропозиції товарів є засобом шахрайського привласнення грошей потенційного покупця.

Шифрування – процес приховування інформації для того, щоб доступ до неї мали лише авторизовані користувачі.

Шпигунські програми – зловмисне програмне забезпечення, яке збирає невеликі фрагменти інформації про користувачів без їхнього відома

Навчальне видання

Пістунов Ігор Миколайович
Кочура Євген Віталійович

БЕЗПЕКА ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Навчальний посібник

Видано за редакцією авторів

Підписано до видання 10.01.2014.
Електронний ресурс. Авт. арк. 7,04.

Підготовлено й видано
в Державному вищому навчальному закладі
«Національний гірничий університет».
Свідоцтво про внесення до Державного реєстру ДК № 1842, від 11.06.2004 р.
49600, м. Дніпропетровськ, просп. К. Маркса, 19.