ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ПРОБЛЕМИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ У ДІЯЛЬНОСТІ ОВС, НАВЧАЛЬНОМУ ПРОЦЕСІ, ВЗАЄМОДІЇ З ІНШИМИ СЛУЖБАМИ

Збірник наукових статей за матеріалами доповідей науково-практичної конференції

14 грудня 2012 р.

Львів
2012

ББК 32.973
П 78

Рекомендовано до друку Вченою радою
Навчально-наукового інституту права, психології та економіки
Львівського державного університету внутрішніх справ
(протокол № 2 від 29.10.2012р.)

П 78 Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами. Збірник наукових статей за матеріалами доповідей науково-практичної конференції 14 грудня 2012 року. – Львів: ЛьвДУВС, 2012. – 233 с.

У збірнику вміщено наукові статті за матеріалами доповідей, підготовлених учасниками науково-практичної конференції «Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами», що проводилася 14 грудня 2012 р. у Львівському державному університеті внутрішніх справ.

ББК 32.973

АНАЛІЗ ЗЛОЧИНІВ, СКОЄНИХ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Рудік В. М.
к.ю.н., доцент, м. Київ
Рудий Т. В.,
доцент кафедри інформаційних технологій ЛДУВС
к. т. н. доцент
Фірман В. М.
к.т.н., доцент кафедри промислової безпеки та охорони праці ЛДУБЖД
Семенюк П. В.
старший викладач кафедри промислової безпеки та охорони праці ЛДУ БЖД

В умовах перехідної ринкової економіки інформація, за певних обставин, стає об'єктом дій як конкурентів, так і кримінальних структури. У такому разі активи інформаційних систем (ІС) мають бути достатньо захищеними, з тим щоб виключити можливість несанкціонованого доступу (НСД) до них і незаконного використання.

Слід визнати, що сьогодні кримінальні структури володіють досить потужними системами несанкціонованого збору інформації, високоефективними технічними засобами та найголовніше – якісного, у професійному розумінні, підготованими фахівцями. Злочинність з використанням інформаційних технологій (ІТ) перетворюється у цілу індустрію, яка володіє

перспективними методиками і яка проникає практично в усі сфери економічної діяльності.

Зростання рівня злочинності у сфері ІТ пояснюється, у першу чергу, відносною доступністю сучасних ІТ і телекомунікаційних сервісів, розширенням сфери електронного грошового обігу, недосконалістю чинного законодавства у сфері ІТ [1].

Чинне законодавство України досі не передбачає чіткого трактування складових обігу інформаційних ресурсів, не визначені критерії їх належності до категорій державних і недержавних. Розробники законодавства у сфері інформації та інформаційної політики держави не зовсім компетентні у технічному забезпеченні новітніх ІТ і, як наслідок, – орієнтування на зовнішні запозичення, які, у свою чергу, далекі від досконалості.

Розкриваючи злочини з використанням ІТ, аналізуючи наявну інформацію працівники органів внутрішніх справ (ОВС) зустрілися з проблемою, коли зловмисники, з метою приховування злочинних діянь, захищають свою інформацію абсолютно надійною системою криптографічного захисту інформації (КЗІ). Системи КЗІ, програмні продукти та технічні засоби на їх основі набули широкого поширення та стали легкодоступними не тільки для фахівців у галузі ЗІ (СБУ, МО, МВС), але й широкому загалу зацікавлених користувачів, у тому числі і кримінальним структурам. Використання стандартного математичного підходу до розшифрування такої закритої інформації є неефективним.

Щодалі частіше оперативні підрозділи ОВС України звертаються за практичною допомогою до провідних фахівців з проблемами доступу до КЗІ. Хоча проблема не є новою, але ефективні методики і тактика поведінки працівників ОВС при роботі з КЗІ відсутні. На відміну від звичайних "хакерів" працівники правоохоронних органів мають право, згідно з чинним законодавством, застосувати оперативно-розшукові методи, які можуть бути єдиним ефективним методом доступу до такої інформації. [2]

Неможливо обійти увагою банківські електронні платіжні системи та електронну комерцію. За статистичними даними, у промислово розвинених країнах середні збитки від одного злочину в сфері ІТ становлять приблизно $ 450 тис., а щорічні

сумарні втрати в США і Західній Європі сягають $ 100 млрд. і $ 35 млрд., відповідно. В останні десятиріччя зберігалася стійка тенденція до зростання збитків, пов'язаних із злочинністю в сфері ІТ.

В усіх аспектах забезпечення захисту інформації основним елементом є аналіз можливих загроз щодо порушення роботи банківських ІС, тобто дій, що підвищують уразливість інформації, яка обробляється в ІС фінансових установ, призводять до її витоку, випадкового або навмисного модифікування, знищення.

За частотою виявлення загрози можна розташувати в такому порядку:

- копіювання і крадіжка програмного забезпечення;
- несанкціоноване модифікування даних;
- зміна або знищення даних на довільних носіях;
- крадіжка інформації;
- несанкціоноване використання ресурсів ІС;
- несанкціоноване використання банківських ІС;
- НСД до інформації високого рівня таємності.

Одним із найважливіших видів інформації у банку є гроші в електронному вигляді, тому основою інформаційної безпеки у банківських ІС є захист електронного грошового обігу. Крім цього, інформація у банківських ІС становить значний інтерес для великої кількості людей та організацій – клієнтів банку. Ця інформація має обмежений доступ і банк несе відповідальність за забезпечення надійного рівня її захисту перед клієнтами та державою.

Одночасно з розширенням мережі користувачів банківських електронних платіжних систем та спрощенням процедури доступу до них збільшується кількість загроз і кількість НСД. Зростання рівня злочинності у банківсько-кредитній сфері пояснюється дуже просто – адже, власне, у даній сфері зосереджені величезні готівкові кошти, які у першу чергу і цікавлять злочинні угрупування.

У даному випадку злочинні угрупування розв'язують діаметрально протилежну задачу – НСД до закритої інформації з метою нанесення власникам систем електронного грошового обігу матеріальних збитків.

Хочемо відзначити, що правоохоронним органам стають відомі далеко не всі випадки викрадення грошей шляхом

використання банківських електронних платіжних систем. Це можна пояснити декількома обставинами. Серед них і небажання вищого керівництва надавати відповідну інформацію через побоювання «компрометації» фінансової установи та можливості виявлення додаткових правопорушень при проведенні слідчих дій.

Переконані, що значний відсоток несанкціонованого доступу до банківських електронних платіжних систем здійснює персонал, який добре ознайомлений з технологією оброблення та захисту інформації. Найчастіше до числа правопорушників потрапляють особи, які, властиво, повинні відповідати за інформаційну безпеку в фінансовій установі.

Наостанок відзначимо, що високий фаховий рівень підготованості особового складу ОВС у галузі ІТ стане запорукою ефективної протидії і розкриття злочинів, скоєних з використанням ІТ.

1. Рудий Т.В. Специфіка протидії злочинам у сфері інформаційних технологій. / Т.В. Рудий, В.М. Слижук, І.М. Ганич, А.В. Нечепуренко. / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали V звітної науково-практичної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 14 квітня 2011 р. – Львів: ЛьвДУВС. 2011, – с. 176-180.
2. Когут В.В. Порядок атестування систем технічного захисту інформації. / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник. / Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 12 березня 2010 р. – Львів: ЛьвДУВС. 2010, – с. 90-97.

АНАЛІЗ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА РЕЗУЛЬТАТАМИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Руда О.І.,
доцент кафедри теоретичної та прикладної економіки ЛьвДУВС, к.е.н.

На поточний момент, коли обсяги інформації, що циркулює, обробляється та накопичується у сучасних ін-