ISSN 1727-1584

ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

УДК 65.012.8(477)

І.О. ГРОМИКО, *канд. техн. наук, доц.*
Є.Я. ОСПІЩЕВ, *канд. юрид. наук*

Національний університет внутрішніх справ

ПРОБЛЕМНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Досліджується ситуація з відставанням розвитку теорії та практики застосування систем та засобів, що є основою інформаційної безпеки в Україні.

Понад 30 років проблема інформаційної безпеки знаходиться в центрі уваги вчених правознавців, фахівців в галузі інформаційних систем та ін. За період незалежності України була створена державна система захисту інформації, налагоджено виробництво засобів захисту, організована планомірна підготовка і підвищення кваліфікації фахівців відповідного профілю [1]. Функціонування системи захисту інформації було неможливо без нової нормативно-правової бази, на засадах якої було впроваджено організаційно-технічне та страхове забезпечення системи захисту інформації [2]. Як відомо, нормативно-правове забезпечення включає систему законодавчих актів, які встановлюють правовий статус суб'єктів правовідносин, суб'єктів і об'єктів захисту, форм і способів захисту інформації. Організаційно-технічне забезпечення являє собою комплекс координованих організаційних, технічних, програмних і інших заходів, що реалізують усі практичні механізми захисту інформації. Страхове забезпечення призначене для захисту власника інформації або засобів інформації як від традиційних загроз (крадіжок, стихійних лих), так і від таких, що виникають у ході інформатизації суспільства (витік інформації, знищення, модифікація, блокування...).

Проте, не дивлячись на існуюче нормативно-правове та технічне забезпечення, система інформаційної безпеки України не завжди відповідає поставленим перед нею завданням. Чому?

Для того, щоб відповісти на це питання, на думку авторів, по-перш, для коректного аналізу цієї проблеми треба відійти від класичної корпоративної схеми вивчення накопиченого матеріалу та викладення причин із заздалегідь підготовленою підсумковою тезою „про необхідність виділення державних коштів на додаткові дослідження". Виходячи з аналізу вище вказаного необхідно зауважити, що теза про недостатню фінансову допомогу держави вінчає численні виступи спеціалістів з доповідями на наукових конференціях щодо захисту інформації. Але, чи є інформація у цих тезах істиною - ситуація спірна. Такі свіжі приклади, як постійні терористичні прориви глобальної системи інформаційного захисту спецслужб США; знахідка у грудні 2004 року в електричці режимного компакт-диску з планом евакуації жителів Лондона; виявлення каналу несанкціонованого доступу сторонніх осіб до бази даних Державтоінспекції України, та багато інших, ставлять під сумнів винятковість теми „недостатнього фінансування".

По-друге, потрібно відійти від традиційного пошуку найкращого нормативно-правового, організаційно та технічного забезпечення захисту інформації будь-яких країн з метою адаптації цього матеріалу до українських потреб. Практика показує, що всі сучасні системи забезпечення захисту інформації будь-яких країн світу є недосконалими. І США, і Україна, і Англія, і Іспанія, й інші держави „по числу і якості проколів" систем інформаційної безпеки знаходяться на приблизно одному рівні.

Таким чином, для досягнення мети досліджування, автори відійшли від застарілої тези про недостатнє фінансування та пошуку „досконалого" вирішення проблеми за кордоном. Ретроспективний аналіз розвитку підходів до захисту інформації свідчить, що теорія і практика інформаційної безпеки пройшли три етапи [1].

Початковий етап – емпіричний, зміст якого полягав у тому, що на основі аналізу загроз інформації та накопиченого досвіду її захисту, були розроблені і впроваджені необхідні механізми захисту без належного організаційно-правового забезпечення. Перш за все, під захистом розумілося попередження несанкціонованого отримання інформації особами і процесами (програмами), що не мали на це правових підстав та повноважень. Традиційно застосовувалися заходи для забезпечення цілісності інформації. Спроби розробки на цьому етапі строго правового підходу для оцінки загроз виявилися недостатніми. Отримані математичні залежності у зв'язку з відсутністю достатньої вибірки статистичних даних були складні і непрактичні через підвищений вплив на захист інформації випадкових правових чинників.

Проміжний етап – концептуально-емпіричний. Суть його і зміст полягали в тому, що на основі досвіду захисту інформації, отриманого на етапі емпіричного підходу,

ISSN 1727-1584

вдалося деяким чином підійти до уніфікації організаційно-правового механізму та методико-інструментального базису, що використовується для вирішення задач захисту. Була розроблена схема правових та організаційних заходів захисту інформації, яка в свою чергу стала основою уніфікованої концепції захисту інформації (УКЗІ) [3].

Сучасний етап - теоретико-концептуальний. Його особливість полягає в тому, що на основі досягнень попередніх етапів здійснюються спроби розробити основи цілісної організаційно-правової теорії захисту, і цим самим підвести під реалізацію захисту міцну науково-методологічну базу. Об'єктивною основою формування теорії захисту з'явилася УКЗІ, що була сформульована в попередній період, і яка увібрала в себе весь накопичений до цього часу правовий, організаційний та технічний досвід захисту. Автори навмисно її не приводять, оскільки, на їх думку, структура УКЗІ з початку розробки припускає в основі своїй пасивне (див. рис.) спостереження за уразливістю інформації. Розвиток такої концепції не тільки надав негативного впливу на розвиток теорії захисту інформації. Він з'явився підставою того, що у глухий кут увійшла розробка організаційно-правових та технічних заходів, спрямованих на захист інформації.

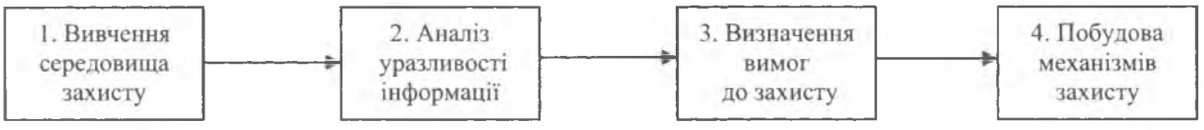

Рисунок - Схема організації захисту інформації

Відповідь на це питання полягає в тому, що в епоху стрімкого розвитку інформаційних технологій вплив авторитетної „пасивної теорії" привів до того, що передові сучасні системи захисту переродилися в системи, що розвиваються під впливом розвитку засобів нападу.

Відсутність нових розробок теорії звело практику боротьби із злочинами у інформаційної сфері до реагування на скоєні злочини. Тобто: „Якщо ми фіксуємо злочин, тоді набираємо статистичні дані (розумій: фіксуємо безкарні „проколи" систем безпеки), досліджуємо нові методи та засоби нападу, розробляємо проект системи захисту, затверджуємо цей проект, проводимо випробування, допрацьовуємо, атестуємо і здаємо в експлуатацію вже морально застарілу систему безпеки".

Негативом такого шляху розвитку систем захисту інформації є:

- факти успішного первинного (а для нас - статистичного) наступу правопорушників до інформації;
- розбазарювання інформаційного потенціалу держави.

Нові засоби нападу за дуже малий інтервал часу проходять шлях від моменту відкриття нових фізичних ефектів до моменту виробництва нових більш проникливих програм. На відміну від них, як було приведено вище, системи і засоби захисту розробляються лише після виявлення цілого ряду проникнення, їхнього аналізу та розробки стратегії і тактики протидії. Крім того, слід зазначити, що витік інформації на етапі розробки засобів захисту "зводить нанівець" усі зусилля фахівців в галузі захисту інформації, які не мають правової наступальної бази. Якщо торкнутися теми наявності каналів витоку інформації в державних установах і на підприємствах, які мають відношення до зберігання конфіденційної інформації, то ми можемо побачити тільки застосування програмного забезпечення, яке реагує на наявні правопорушення і виключає застосування програм попередження злочинів їх профілактики тощо.

Що стосується технічного забезпечення інформаційної безпеки, то необхідно зазначити, що часто, до моменту випуску діючих зразків апаратури захисту (протидії), виявляється, що вже створена нова апаратура, що атакує, і та яка працює на інших, нових фізичних принципах.

Наступною складною проблемою є оснащення підрозділів системи інформаційної безпеки. И тут справа не тільки в кошторисі. Наріжним каменем цього питання з'явився вельми широкий апаратурний спектр атакуючої техніки, що розширюється усе більше та більше. Системи, що атакують - оптичні, оптико-механічні, оптико-електронні, НВЧ та інші - істотно знизили ефективність протидії систем і засобів захисту.

Прикладом є апаратура, яка може мати настільки вузьку діаграму випромінювання, що виявлення факту атаки може відбутися тільки при влученні прийомної пошукової антени в область вузького радіопроміню шириною в десяток градусів. Цього радіопроміню може взагалі не бути у приміщенні, що атакується, якщо він створений радіозакладкою, розташованою в одній із зовнішніх стін висотного будинку. Імовірність виявлення таких пристроїв за допомогою сканерних приймачів близька до нуля.

Наступним проблемним аспектом з'явився перехід систем, що атакують, у недосяжні раніше діапазони довжин хвиль, наприклад, в область міліметрового діапазону радіохвиль, цілком обеззброїв власників дорогих сканерних приймачів, що не призначені для роботи в діапазоні сотень гігагерц. Ця ситуація показова тим, що створення комплектів, що атакують: "передавач + радіоприймач вузької дільниці міліметрового діапазону хвиль" на кілька порядків дешевше і простіше, ніж створення промислових зразків радіосканерів міліметрового діапазону. При цьому в цих діапазонах процес просторового та частотного сканування і пошуку сигналу, що має частотну смугу в десяток кілогерц та випромінюється у просторовому куті близько двох десятків градусів, виявляється тривалою і марною процедурою.

Надії фахівців на ефективне застосування нелінійних локаторів для пошуку закладених пристроїв також не виправдалися. Правопорушникам достатньо покривати пристрої матеріалами, що поглинають енергію радіохвиль, а також застосовувати імітатори закладних пристроїв. При цьому і пошук, і виявлення пристроїв істотно ускладнюються. Переносні рентгенівські пристрої (навіть без ура-

ISSN 1727-1584

хування їх вартості) також далеко не є панацеєю.

Особливе місце в процесі ускладнення боротьби з апаратурою, що атакує, зайняло застосування нових виробничих технологій і методів. Диктофони, радіозакладки, відеокамери та інші стали зберігати інформацію в мікросхемах пам'яті і передавати її в зашифрованому і стиснутому вигляді по команді ззовні з стрибкоподібною псевдовипадковою зміною значення частоти. Стали активно застосовуватися сигнали носії, що фазоманіпульовані по псевдо-випадковому закону. При цьому спектри сигналів носіїв, у результаті, стали аналогічні спектрам широкосмугових шумоподібних сигналів, і на відстанях, порівнянних із розмірами ближньої зони, стають нижче рівня шумів. Крім того, що ці засоби нападу надзвичайно складно знайти й ідентифікувати, так їх ще оснащують елементами пам'яті з захистом - такі засоби нападу зберігають інформацію "у собі" та самоліквідуються при спробах їх вилучення.

У підсумку, процес захисту оперативної інформації все більш здобуває малоймовірний характер, а виявлення небезпечних каналів витоку інформації й апаратури, що атакує, стає випадковим успіхом працівників спецслужб. Якщо ж користувачі або працівники спецслужб по деяким причинам теж стають загрозою для інформації, то ситуація з безпекою інформації в цілому стає проблематичною і не завжди вирішується.

По-перше, перелічені вище аспекти підводять до наукової доцільності і практично. корисності постановки і вирішення цієї актуальної проблеми шляхом впровадження попереджуючої стратегії захисту [3]. В даній ситуації дуже часто дослідники проблем інформаційної безпеки скочуються до потенційної ями пасивної теорії. Ці дії невірні. Необхідно упередження правопорушень у сфері інформаційних технологій на випереджаючих початкових етапах реалізації злочинних спроб, коли витрати і втрати в результаті протидії атаці виявляються істотно нижче наслідків правопорушення.

По-друге, прийнято вважати, що, основні напрями розвитку захисту інформації тісно пов'язані з вирішенням наступних задач.

Перша полягає в розробці нормативно-правової бази, яка б закріплювала створення, діяльність нових організаційних структур та корегування діяльності вже створених (систем захисту інформації СБУ, МВС, податкової міліції та ін.). Друга, це подальший розвиток науково-методологічної бази як основи інтенсифікації процесів захисту, у тому числі формування теорії, орієнтованої не тільки на технічні, але і на правові та соціальні системи. Третя - регулярний збір і обробка статистичних даних про склад і результати функціонування реальних систем захисту. Безсумнівно, що діяльність підрозділів захисту інформації у цьому аспекті повинна знаходитись в межах нормативно-правового поля.

Тобто, на питання як забезпечити безпеку інформації вже у наступний час, можна дати відповідь, скорегувавши приведений матеріал у наступному вигляді:

1. На основі нових організаційно-правових механізмів необхідна активізація науково-дослідницьких лабораторій (центрів), що аналізують не тільки функціонування реальних систем захисту, але й подальший розвиток фізичних наук з метою прогнозування створення нових каналів витоку інформації та апаратної реалізації зразків атакуючої техніки на інформацію.

2. Необхідне формування теорії, що орієнтована на інтегральний підхід до технічних і соціальних систем.

За п.1 теорія однозначно підказує шлях розвитку ефективного захисту інформації в державі - епоха пасивного споглядання закінчилася, давно почалася епоха попереджуючої стратегії захисту. По п.2 першим кроком у цьому напрямі з'явилася "Загальна парадигма захисту інформації", що опублікована у провідних наукових виданнях [3-5] і пройшла апробацію на наукових семінарах та реалізована на різних рівнях учбового процесу. На думку провідного вченого України у системі інформаційної безпеки І.Д. Горбенка, парадигма базується на найбільш структурованої теорії захисту інформації в комп'ютерних (автоматизованих) системах. У цій теорії сформульовано цілу низку аксіом і тверджень (теорем), що розкривають методологію створення й функціонування захищених комп'ютерних систем. Узагальнення цієї теорії, що увібрала світовий досвід боротьби з правопорушеннями в інформаційної сфері, і поширення її на загальну інформаційну сферу дозволило сформулювати парадигму у наступному вигляді: *інформація вважається захищеною, якщо при її переміщенні дотримується режимна адекватність комунікабельних носіїв інформації.*

Аналіз комунікабельності носіїв інформації показує, що цей термін є одним з найважливіших, на підставі яких виникає можливість наукової оцінки та зближення технічних і соціальних систем. Тому "Загальна парадигма захисту інформації в органах внутрішніх справ України", як спеціалізована, відкриває нові горизонти у розвитку теорії захисту. Цей матеріал виходить за межи даної наукової статті та буде розглянутий надалі окремо.

Структуру уніфікованої концепції захисту інформації треба розуміти як комплекс організаційно-правових заходів, де не тільки зазначене місце можливого знаходження підрозділу, що проводить аналіз атакуючих систем, але й це місце виділене окремо, і конкретні люди під державним контролем виконують на цьому місці свої конкретні обов'язки, які діють у правових межах. Наприклад, з метою вироблення рекомендацій для ОВС проводять практично обґрунтований аналіз розвитку систем і засобів нападу та дезактивації систем захисту. Можна припускати, що ця структура працює в державі. Тоді чому, наприклад, не врахований факт масового продажу у державі генераторних діодів Ганна та ЛПД, що з добавкою одного резистора та металізованого об'ємного резонатора перетворюються в злочинний радіопристрій діапазону десятків та сотень гігагерц? Встає питання про монопольне право інформування робітників підрозділів ТЗІ про ти чи інші моменти розвитку практичної науці? Але тут мова ведеться про вельми ймовірне численне застосування зразків злочинних радіопристроїв при практичній відсутності апаратури захисту.

Підводячи підсумок викладеному, зазначимо, що з метою реалізації попереджуючої стратегії захисту інформації в Україні необхідна активізація в системі ОВС аналітичних підрозділів, які повинні виконувати функції:

- вивчення публікацій світових наукових досліджень щодо можливості створення або удосконалення на їх підставі структурних елементів каналів витоку інформації;

ISSN 1727-1584

- моделювання процесів нападу на інформацію та її захисту;
- розробки рекомендацій щодо підвищення ефективності протидії атакуючим системам і засобам, та ін.

Державним стандартом України встановлено [6]: "Заходи захисту інформації повинні бути адекватні загрозам...", а ця мета недосяжна без реалізації попереджуючої стратегії.

ЛІТЕРАТУРА

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие. –М: Горячая линия-Телеком, 2004. –280 с.

2. Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 31.10.2001 р. «Про заходи щодо вдосконалення державної інформаційної політики ті забезпечення інформаційної безпеки України» від 6.12.2001 р., № 1193/2001 // Офіційний вісник України. -2000. -№ 50. -Ст. 2228.

3. Герасименко В.А., Малюк А.А. Сущность и пути перевода процессов защиты информации на интенсивные способы // Безопасность информационных технологий. – 1998. -№ 4.

4. Орлов П.І., Громико І.О., Носов В.В, Логвиненко М.Ф., Громико О.І. Загальна парадигма захисту інформації // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. -2002. -№ 5. -С.84-86.

5. Орлов П.И., Громыко И.А., Носов В.В., Логвиненко Н.Ф., Громыко Е.И. Общая парадигма защиты информации // Защита информации. Конфидент. -2003. -№1. -С.10-14.

6. Орлов П.І. Інформація та інформатизація. Нормативно-правове забезпечення: Наук.-практ. посібник. – Харків: Вид-во Нац. ун-ту внутр. справ, 2003. –724 с.

7. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

Надійшла до редколегії 17.01.2005

ГРОМЫКО И.А., ОСПИЩЕВ Е.Я. ПРОБЛЕМНЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ В УКРАИНЕ
Исследуется ситуация с отставанием развития теории и практики применения систем и средств, что являются основой информационной безопасности в Украине.

***

GROMYKO I.A., OSPISHCHEV E. JA. PROBLEM ASPECTS OF PROTECTION INFORMATION IN UKRAINE
Situation with backlog of development of the theory and practice of application of systems and means that are a basis of information safety in Ukraine is investigated.

А.В. КОФАНОВ
канд. юрид. наук
Національна академія внутрішніх справ України

УДК 343.977

ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ПРОВЕДЕННІ ЗБРОЄЗНАВЧИХ ДОСЛІДЖЕНЬ

Розглянуті теоретичні та практичні аспекти використання комп'ютерних технологій при проведенні зброєзнавчих досліджень.

Сьогодні в Україні зростає кількість злочинів з використанням вогнестрільної зброї. Ці злочини є найбільш тяжкими, направленими проти життя та здоров'я особи – це вбивства та розбійні напади. Слід зауважити, що злочинність в Україні набуває нової структури, підвищується її організованість та технічна оснащеність. Це, у свою чергу, значно збільшило потребу у кількості балістичних досліджень та об'єктах в криміналістичних обліків (зокрема, кулегільзотеках). Робота по перевірці та постановці на облік об'єктів у кулегільзотеку вже потребує не лише застосування традиційних методів, але й вимагає їх удосконалення та розробки нових.

Останні роки ознаменувалися впровадженням у практику розслідування злочинів новітніх технологій, у тому числі комп'ютерних. Цей процес триває і в галузі проведення судово-балістичних експертиз, надзвичайно актуальними стають питання автоматизації балістичних досліджень і обліків, створення автоматизованих інформаційно-пошукових систем ідентифікації вогнестрільної зброї та автоматизованих кулегільзотек.