УДК 347.7+334.722

Е. І. НИЗЕНКО
Інститут права ім. князя Володимира Великого МАУП, м. Київ

ЗАГАЛЬНОТЕОРЕТИЧНІ ХАРАКТЕРИСТИКИ ОКРЕМИХ НАПРЯМІВ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ВІД ЗЛОЧИННИХ ПОСЯГАНЬ

Наукові праці МАУП, 2007, вип. 1(15), с. 127–132

Розглянуто актуальні проблеми інформаційної безпеки у підприємництві з урахуванням посилення конкурентної боротьби і розвитку економічного шпигунства. Визначено методи технічного захисту від несанкціонованого доступу до комп'ютерів, автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку, а також технології розвідувальної діяльності, призначеної для перехоплення конфіденційної інформації. Показано значущість механізмів протидії комп'ютерному шпигунству.

Ефективне функціонування підприємства (організації) неможливе без управління ресурсами, що використовується для досягнення мети. Згідно з поширеними сьогодні в управлінській літературі поглядами, поняття "ресурси" охоплює не лише людей, капітал, сировину, а й інформацію.

Зміст цілеспрямованої діяльності підприємства зводиться до винайдення необхідних ресурсів і перетворення їх у корисну продукцію.

Тепер уже не лише з теорії, а й з багаторічної практики відомо, що ресурси у природному середовищі та інформація у суспільстві завжди обмежені. Попит на інформацію набагато вищий, ніж можливості його задовольнити. Справа у тому, що у процесі діяльності підприємства потенційна інформація циклічно актуалізується. Актуалізація потенційної інформації передбачає використання потенційно важливих відомостей саме в той момент, коли необхідно приймати управлінське рішення, наприклад, щодо укладання договору.

Для задоволення інформаційних потреб підприємства необхідно створити оптимальну структуру з обліком вимог, що висуваються для забезпечення інформаційної безпеки.

Принципово важливо, щоб інформаційна структура відповідала розподілу повноважень на підприємстві, щоб інформація, необхідна для вирішення завдань, надавалась у підрозділах не будь-кому, а лише особам, які відповідають за їх вирішення. Інформація всередині інформаційної структури має бути побудована таким чином, щоб вона достатньо відбивала рівні управління підприємством. Можна дійти висновку, що саме такий підхід до побудови інфраструктури підприємства допомагає правильному і оптимальному вирішенню проблеми створення корпоративної мережі підприємства (установи).

Корпоративна мережа підприємства (установи) — спосіб організації зв'язку в інформаційній системі корпорації: через відомчу глобальну мережу, між кількома розміщеними на достатньо великій відстані один від одного, об'єднаними локальною мережею ПК, в яких циркулює інформація.

Розглядаючи особливості, притаманні сфері інформаційної безпеки, необхідно звернути увагу на те, що інформація суттєво відрізняється від інших видів ресурсів підприємства і являє собою дані, що характеризують процеси, які протікають у самому підприємстві та у зовнішній сфері.

У зв'язку з цим не можна не підкреслити, що зміст управління різними видами діяльності підприємства залежить передусім від змісту інформації, що споживається підприємством і засобів

її отримання. Можна з упевненістю заявити, що інформація, яка стосується сировини матеріалів, грошових засобів, технологічних процесів, розглядається в літературі як забезпечувальний фактор управління виробництвом.

Щодо іншого боку інформації, то вона сама є особливим видом ресурсів, а тому для досягнення поставленої мети необхідно за допомогою відповідної сукупності прийомів здійснювати вплив на процеси накопичення, зберігання, поширення і використання даних на рівні підприємства. У цьому випадку інформація виступає об'єктом управління.

Багатоплановий підхід до інформаційних ресурсів зумовлює необхідність вираховування такого суттєвого фактора, як функціонування підприємства в умовах ринкових відносин, для яких характерна боротьба між незалежними суб'єктами господарювання на ринку і гостра конкуренція товаровиробників. По суті, постійна боротьба за економічне виживання — це головний закон ринку.

Забезпечення безпеки підприємства в умовах ринкових відносин вимагає захисту підприємницької інформації. Коли йдеться про підприємницьку інформацію, то у спеціальній літературі вона розглядається як умова, що допомагає або створює перешкоди у досягненні позитивного результату (прибутку) в господарській діяльності [8].

Необхідно підкреслити, що підприємницька інформація, яка створює суб'єкту вигідні умови для прийняття оперативних рішень і досягнення ефективного результату, вважається корисною.

Враховуючи важливість і цінність підприємницької інформації, з метою захисту її від сторонніх осіб, як правило, використовують комплекс методів технічного та організаційного характеру.

Підприємницька інформація, яка циркулює у ринково-конкурентній сфері діяльності, поділяється на організаційну, технічну, комерційну, фінансову, рекламну. Вона охоплює дані про попит і пропозицію, про конкурентів, про кримінальний стан, у тому числі відомості про способи і засоби забезпечення безпеки інформації в корпоративній мережі підприємства, про діюче законодавство та ін.

Інформація про діяльність підприємства зберігається у різноманітних формах: в пам'яті людини, у картотеках, книгах обліку або у пам'яті ЕОМ.

Необхідно звернути увагу на деякі питання, пов'язані з практичним використанням технічних засобів зберігання, видачі, обробки і пошуку інформації.

Інформаційна структура має відбивати організаційну структуру управління підприємством, але необов'язково її ототожнювати. Слід відзначити, що вирішення завдань управління скероване на об'єднання всіх видів ресурсів і потоків інформації в єдиний процес досягнення мети.

У технології управління вагоме місце посідає інформаційне поле підприємства, під яким розуміють носіїв потенційної інформації, необхідної для успішного виконання підприємством своїх завдань і функцій.

Існують взаємопов'язані технології функціонування (виробничі технології), але вони вирізняються своїми характеристиками.

Управлінська технологія забезпечує процес управління підприємством (установою). Для глибшого осмислення управлінської технології важливо виокремити її елементи: це інформація, операція і методи здійснення управлінських технологій, персонал, обладнання, структура.

Необхідно пам'ятати, що підрозділи у складі інфраструктури підприємства пов'язані завдяки своїм властивостям і вирішуваним завданням. У цілому наявність тієї чи іншої структури з її елементами у складі підприємства зумовлена необхідністю їх об'єднання в технологічний процес. На наш погляд, з'ясування цих обставин важливо з точки зору визначення значення безпеки інформації в корпоративній мережі установи, оскільки велика кількість підприємств є доступ до мережі Інтернет. Він беззаперечно надає явні переваги підприємствам у здобутті інформації, але водночас надає доступ до внутрішньої мережі всім країнам світу.

Найбільш сучасним обладнанням в управлінській технології є персональні комп'ютери, а також стаціонарні й рухомі засоби зв'язку. Перелічимо це обладнання:

- технічні засоби і методи обробки інформації та захисту каналів її циркулювання (фіксування, передавання, пошук, обробка інформації);
- носії інформації — матеріальні предмети, за допомогою яких передається інформація.

Наближеним до поняття "інформаційне поле" є поняття "комунікаційний простір підприємства". Останнім часом було достатньо публікацій і різноманітних досліджень у цьому напрямку.

Комунікаційним простором підприємства називають ту частину середовища його функціонування, в якій він має змогу за допомогою наявних у нього ресурсів і засобів управляти інформаційними процесами, зокрема процесом актуалізації потенційної інформації. Водночас комуні-

каційний простір підприємства можна суттєво збільшити шляхом об'єднання зусиль з іншими інформаційними системами (наприклад, з Інтернетом).

Не можна не зазначити, що на сьогодні відсутні управлінські інформаційні технології, які можуть бути реальною альтернативою магнітному збереженню інформації.

В інформаційних системах, базовим елементом яких є комп'ютер, основна інформація зберігається на жорстких магнітних дисках. Саме у накопичувачу на жорстких магнітних дисках інформація зберігається, потім вона завантажується в оперативну пам'ять комп'ютера, обробляється у процесі використання, а вже непотрібна інформація знищується.

Один з найважливіших показників — енергетична незалежність робить накопичувач на жорстких магнітних дисках (НЖМД) практично незамінним для оперативного і довготривалого зберігання великих масивів інформації.

Зазначимо, що сьогодні великі об'єми інформації зберігаються, обробляються і передаються електронними засобами, при цьому відповідно супроводжуються електромагнітним випромінюванням. Тому існує реальна можливість несанкціонованого доступу до цієї інформації за допомогою радіоперехоплення або контактного підключення до комунікацій [6, *89*].

Комп'ютер у режимі автономної роботи сьогодні практично не застосовується. На автономних комп'ютерах здійснюється обробка і зберігання інформації, а при окремому підключенні або при підключенні до Інтернету відбувається передавання інформації (обмін інформацією). У локальній мережі здійснюються всі процеси з інформацією: її зберігання, обробка і передавання.

Персональний комп'ютер є центральною ланкою в системі автоматизованої обробки інформації, а тому перебуває в зоні особливої уваги конкурентів, правопорушників і розвідувальних служб [10]. Для отримання цінної інформації вони використовують усі доступні засоби і методи, у тому числі різноманітні типи аналізаторів, що підключаються до ліній електроживлення. Тому найбільш жорсткі вимоги щодо захисту інформації мають встановлюватися для комп'ютерів, що працюють у складі локальної обчислювальної мережі. У такій мережі всі елементи пов'язані між собою кабельною системою (як правило, екранована або неекранована плетена пара). Локальну комп'ютерну мережу сьогодні вже недоцільно використовувати автономно, без взаємодії з іншими мережами.

Розвиток комп'ютерних технологій і наступне їх використання у багатьох сферах економіки є сьогодні одним з головних факторів її ефективності. При цьому треба пам'ятати, що прогрес в інформаційно-технічній сфері створив потенційні загрози у вигляді розробки нових і вдосконалення вже відомих методів наукового шпіонажу, які дають змогу швидко знаходити необхідні відомості, що зберігаються в пам'яті комп'ютера.

Збирання інформації про розробки високих технологій завжди було і залишається одним з пріоритетів у діяльності розвідок світу, тому сьогодні все активніше застосовують перевірені на практиці методи отримання відомостей в учасників науково-практичних конференцій, організаторів виставок і обслуговування персоналу.

Перехоплення секретної інформації, що обробляється з використанням засобів обчислювальної техніки і передається лініями зв'язку абонентів, здійснюється за допомогою портативних розвідувальних радіоприймачів, що забезпечують багатоканальний прийом сигналів з різних напрямків і на різних частотах. Цей технічний спосіб радіорозвідки найбільш поширений серед інших методів розвідувальної діяльності [5, *63*].

Зазначимо, що арсенал спеціальних технічних засобів і методів, що використовуються для викрадення секретних відомостей з інформаційних систем підприємств, установ, корпорацій, досить широкий. Конкуруючі комерційні фірми можуть здобути цінну інформацію шляхом введення в комп'ютерну систему (зокрема, у графічні і звукові файли) спеціальної програми — закладки для таємного передавання даних, що містяться у знайдених нею файлах. Водночас програма дає змогу не лише надійно приховати факт передавання повідомлення, а й зашифрувати його за допомогою криптоалгоритма. Деякий інтерес разом з методами перехоплення випромінювальних електромагнітних хвиль у процесі обробки інформації в комп'ютері, викликають засоби таємного стеження за екраном монітора.

Якщо відеомонітор, як правило, недосяжний для огляду випадковим особам, оскільки його встановлюють таким чином, щоб не можна було бачити інформацію на екрані, то в оптичному діапазоні отримати інформацію все-таки можна, але через світове випромінення монітора.

Зображення на відеомоніторі після багаторазових відображень від різноманітних поверхонь (стін, стелі, меблів та інших предметів) може бути

перехоплено за допомогою спеціальної техніки, яка надає можливість перетворити цей світловий потік в іншу відеоінформацію. Під час прихованого візуального спостереження за екраном відеомонітора відбувається перехоплення композитного сигналу, при цьому будь-які перешкоди у вигляді мерехтіння на поверхні дисплея відсутні, а тому у оператора не виникає підозри в тому, що за його електронним засобом ведеться оптико-електронне спостереження.

Процес перехоплення таємної інформації шляхом прийому композитного сигналу відеомонітора потребує чимало часу, оскільки в усіх випадках таємного спостереження необхідно чекати, поки користувач виведе на відеомонітор необхідну інформацію. Інколи такі очікування вимірюються тижнями. Спеціалісти науково-дослідних установ, які займаються проектуванням і створенням нової техніки, не випадково припускали можливість і необхідність "примусити" комп'ютер передавати інформацію тоді, коли це необхідно особі, яка приступила до ведення таємної форми спостереження за відеомонітором [4]. Зміст ідеї вчених зводиться до "зараження" потрібного комп'ютера спеціальною програмою — закладкою ("троянський кінь") будь-яким з відомих способів у технології вірусів: можливо, через дискету з драйверами, а якщо персональний комп'ютер знаходиться в системі локальної обчислювальної мережі, то через мережу.

В інформаційних мережах, базовим елементом яких є комп'ютер, основні об'єми інформації зберігаються на жорстких магнітних дисках. Саме тому програма-закладка шукає необхідну інформацію на цьому носії (диску), при цьому звертаючись до різноманітних електричних пристроїв, викликає негативні опромінення електромагнітних коливань у просторі. За допомогою зазначеної програми можна вмонтувати у композитний сигнал відеомонітора повідомлення, що містить розвідану інформацію. При цьому користувач ПК, наприклад, граючи з комп'ютером у карти, візуально не може визначити, що зображення різноманітних гральних карт містить у собі ще якусь інформацію — у вигляді секретних текстових повідомлень [9, *22*].

Для забезпечення перехоплення паразитного опромінення монітора і виділення необхідного корисного сигналу необхідно мати розвідувальний приймач (у найпростішому вигляді це звичайний доопрацьований телевізор).

Експериментальні дослідження, виконані у різних країнах, підтверджують можливість отримання таємної інформації шляхом прийому паразитного випромінення композитного сигналу відеомонітора. Результатом усіх цих досліджень стала технологія SOFT TEMPEST — технологія таємного передавання даних каналом негативного електромагнітного опромінення за допомогою програмних засобів.

Згадаємо основні передумови історії виникнення TEMPEST як технології розвідувальної діяльності, призначеної для перехоплення інформації, опрацьованої (що передається чи переказується) в локальних обчислювальних мережах і захисту інформації від витоку каналами негативних опромінень і наведень. Серед спеціалістів, які працюють у цьому напрямку, утвердився подвійний підхід до розглянутої технології: сьогодні вони виділяють як засоби TEMPEST-нападу (розвідки), так і засоби TEMPEST-захисту.

У 1918 р. Герберт Ярдли и Black Chamber дійшли принципового висновку, що різноманітні електронні пристрої для обробки секретної інформації мають паразитичні випромінення, які можна використовувати для відновлення і перехоплення зашифрованих повідомлень. У 1946 р. була заснована Канадська Організація із захисту зв'язку (CSE), основною метою якої була комунікаційна безпека (COMSEC).

В Україні теж здійснюються дослідження щодо захисту інформації від витоку каналами непрямого випромінення. Цей канал витоку інформації називається у нас ПЕВН (побічне електромагнітне випромінення і наведення). В Європі та Канаді застосовується термін "компрометуюче опромінення", а у США термін "TEMPEST" визначає таємну програму Міністерства оборони США з розробки методів попередження витоку інформації через демаскуюче і паразитичне випромінення електронного обладнання.

З метою концентрації зусиль у сфері захисту інформації Указом Президента України на базі Головного управління урядового зв'язку СБ України у 1999 р. було створено Департамент спеціальних телекомунікаційних систем і захисту інформації СБ України. Це головна структура у державі, яка займається питаннями криптографічного і технічного захисту інформації.

Зосередження значних об'ємів конфіденційної та іншої інформації на жорстких магнітних накопичувачах, що є одним з основних вузлів комп'ютера, використання в управлінській технології електронного документообігу — все це зумовлює можливість несанкціонованого доступу до комунікацій.

Витік інформації з обмеженим доступом, що має реальну цінність для її власника, напряму залежить від очікуваної ефективності у разі її отримання. Іноді перехоплення такої інформації може завдати значної шкоди інтересам власника інформації [2].

Розглянемо питання несанкціонованого зняття інформації, що зберігається на НЖМД. Користувачам відомо, що у процесі експлуатації комп'ютера інколи з ладу виходять різноманітні електронні пристрої, у тому числі накопичувач на жорстких магнітних дисках. Відповідно до чинного законодавства, що регулює відносини між споживачами товарів і виробниками, продавцями і виконавцями в умовах різноманітних форм власності, виробник забезпечує нормальну роботу товару, у тому числі комплектуючих деталей, впродовж гарантійного строку, встановленого законодавством, а у разі його відсутності — за договором. Гарантійними зобов'язаннями, що зазначені у договорі, передбачена заміна НЖМД, але лише за умови збереження пломб і дотримання правил експлуатації комп'ютера.

Деякі користувачі ПК, віддаючи у сервісний центр, що забезпечує поставку комп'ютерної техніки, несправний НЖМД, досить часто не знищують інформацію, що зберігається на ньому. Тобто постачальнику комп'ютерної техніки разом з несправним накопичувачем добровільно передається інформація, у тому числі конфіденційна.

Зазначимо, що вітчизняні постачальники комп'ютерної техніки закуповують комплектуючі деталі у зарубіжних виробників через їх представників. Після обміну на аналогічний НЖМД належної якості несправний накопичувач відправляють зарубіжному представнику.

Нестандартну поведінку користувача ПК у разі виходу з ладу НЖМД можна зрозуміти. Адже техніка псується, образно кажучи, у дуже непідходящий момент.

Порушення звичної діяльності користувача ПК, достатній тиск з боку керівництва, яке вимагає негайного усунення недоліків — усе це помітно впливає на поведінку людини, його настрій, мислення і досить часто перешкоджає виконанню службових обов'язків. У такій ситуації, не маючи змоги критично оцінити її, користувач, не знищуючи інформацію, передає НЖМД на заміну. Але може скластися також інша ситуація, коли настає час знищити непотрібну інформацію. Для цього застосовують стандартну для операційної системи операцію — знищення. Тут засоби візуалізації комп'ютера інформують користувача про знищення файлу, що створює ілюзію повного його знищення. Насправді інформація, як і раніше, зберігається на НЖМД і може бути поновлена. Отже, проблема тут полягає у належному знищенні інформаційних відходів [1, *38*].

Цікаво, до речі, розглянути технології розподілу інформації в базі даних ЕОМ. Відомості, що зберігаються там, на жорстких або гнучких дисках, мають здатність виводитись на паперову роздруківку (лістинг).

Накопичувач на жорстких магнітних дисках називають вінчестером. На ньому зберігають і з нього завантажують в оперативну пам'ять комп'ютера його операційну систему. В основі фунціонування вінчестера лежить принцип магнітного запису, тобто зчитування сигналів на обертаючому диску, який покритий магніточутливим робочим шаром. При зчитуванні ділянки диску з різною намагніченістю рухаються під магнітною головкою та індукують в ній електромагнітні сигнали, які перетворюються у цифрові дані. Сучасний накопичувач на жорстких дисках складається з блока (пакета), дисків, шпиндельного двигуна — приводу обертання дисків, блока головок запису/зчитування, посилювача — комутатора головок і контролера, який являє собою друковану плату з електронними схемами управління.

У разі передавання диска в іншу організацію або комп'ютера в ремонт у повному комплекті вся інформація на жорсткому диску має бути знищена. Гарантоване знищення інформації при виведенні накопичувача з експлуатації, на думку спеціалістів, зокрема компанії "ЕПОС", яка є ліцензіатом Департаменту спеціальних телекомунікаційних систем і захисту інформації СБ України, досягається шляхом запису на те місце, де розміщено знищений файл, іншої інформації з наступним знищенням її засобами операційної системи. Для цього існують спеціальні програми. Нова інформація записується безпосередньо замість старої, знищуючи її. Багатократний запис на місці знищуваної інформації пошкоджує магнітну структуру лише тих ділянок доріжок, на яких зберігались дані, що підлягають знищенню. Перезапис — це процес запису нетаємних даних у пам'ять комп'ютера, де раніше зберігались таємні дані. Під час перезапису інформаційна працездатність накопичувача на жорсткому магнітному диску зберігається, якщо він був цілком справним. На несправному НЖМД виконати надійне знищення інформації неможливо.

Засоби знищення інформації на НЖМД поділяються на кілька груп: безпрограмні, механічні,

фізичні. За впливом на пристрій НЖДМ: а) без знищення конструктивної структури і поверхні НЖМД; б) зі знищенням НЖМД.

Механічні методи знищення інформації на НЖМД за способом впливу на носій поділяються на такі: механічний, термічний, піротехнічний, металотермічний, хімічний, радіаційний.

Інформацію, що зберігається на НЖМД, можна знищити шляхом впливу на диски міцним постійним або тимчасовим магнітним полем, при якому знищується магнітна структура робочих поверхонь.

Проблема гарантованого знищення інформації з магнітного носія постає сьогодні перед багатьма користувачами [7, *14*]. Під гарантованим знищенням інформації з магнітного носія розуміють такі зміни його магнітної структури, при яких неможливе зчитування інформації стандартними засобами накопичувача, а поновлення за допомогою спеціальних методів втрачених даних, що зберігаються на жорстких дисках, економічно недоцільно.

Література

1. *Болдырев А. И., Сталенков С. Е.* Надежное стирание информации — миф или реальность? // Защита информации. Конфидент. — 2001. — № 2. — С. 38.

2. *Вертузаєв М. С., Голубєв В. О., Котляревский О. І., Юрченко О. М.* Безпека комп'ютерних систем. Комп'ютерна злочинність та її попередження / За ред. О. П. Снігерьова. — Запоріжжя: ПВКФ "Павел", 1998. — 316 с.

3. *Вертузаєв М. С., Хрипко С. Л.* Шифрування як засіб захисту інформації // Інформаційні технології та захист інформації: Зб. наук. пр. — Запоріжжя: Юрид. ін-т МВС України, 1998. — Вип. 2. — С. 24–32.

4. *Генне О. В.* Основные положения стеганографии // Защита информации. Конфидент. — 2000. — № 3. — С. 48–54.

5. *Гуцалюк М.* Захист інформаційних ресурсів України // Правова інформатика. — 2003. — № 1. — С. 63–67.

6. *Гуцалюк М., Гордус М.* Захист інформації у підприємницькій діяльності: Зб. наук. пр. // Приватне право і підприємництво. — 2003. — Вип. 3. — С. 88–91.

7. *Коженевский С., Солдатенко Г.* Жесткие диски и побочные излучения компьютера // Информационная безопасность офиса: Науч.-практ. сб. — Вып. 1: Технические средства защиты информации. — К.: ООО "ТИД", "ДС", 2003. — С. 47–50.

8. *Недержавна* система безпеки підприємництва як суб'єкт національної безпеки України: Матеріали наук.-практ. конф., Київ, 16–17 трав. 2001 р. — К.: Вид-во Європ. ун-ту, 2003.

9. *Провозін А. П., Солдатенко Г. Т.* Деякі аспекти створення персонального комп'ютера для оборони інформації з обмеженим доступом // Бізнес і безпека. — 1998. — № 6. — С. 22.

10. *Чеховский С.* Концепция построения компьютеров, защищенных от утечки информации по каналам электромагнитного излучения // Безопасность информации в информационно-телекоммуникационных системах: Тез. докл. Междунар. науч.-практ. конф. — К.: Інтерлінк, 2002. — С. 80.

Важливість реалізації адекватних заходів щодо протидії комп'ютерній злочинності знаходить все більше порозуміння з боку відповідних посадових осіб органів державної влади та управління і користується підтримкою керівництва підприємницьких структур. Можна припустити, що ця обставина потребує консолідації зусиль усіх зацікавлених державних органів і суб'єктів недержавної системи безпеки підприємництва — від правоохоронних структур до науково-дослідних і навчальних закладів та фахівців, які організують та забезпечують інформаційну безпеку підприємства.

*Importance of realization of the adequate measures concerning counteraction of computer criminality finds escalating understating on the part of correspondent officials of bodies of the government and management and uses support managements {*manuals*} of enterprise structures. Therefore we can assume, that the named circumstance demands consolidation of efforts of all the state bodies and subject of the private system of safety of business, starting {*beginning*} from law-enforcement structures up to research and educational institutions, expert who organize and provide information safely of the enterprise.*

Надійшла 12 березня 2007 р.