ІНФОРМАЦІЙНА БЕЗПЕКА

УДК 004.681

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ПО ТЕХНІЧНИХ КАНАЛАХ

Конахович Г.Ф., Назаренко Є.Л., Свириденко В.М.
Національний авіаційний університет
kszi@ukr.net

З розвитком техніки та інформаційних технологій в останні роки відчутно зросли темпи розвитку технічних пристроїв для несанкціонованого оволодіння інформацією. На сьогоднішній день існує безліч засобів перехоплення інформації за допомогою різних приладів: радіомікрофони, пристрої перехоплення телефонних повідомлень та багато інших. Але існує також багато засобів захисту інформації: заглушувачі диктофонів, блокиратори стільникового зв'язку, пристрої захисту електромережі, генератори шуму.

With development of engineering and information technologies, for last years rates of development of technical devices for the non-authorized mastering by the information considerably have increased. For today there is a set of means of interception of the information with the help of different devices: radiomicrophones, device of interception of the telephone messages, and it is a lot of others. But also there are many means of protection of the information: mufflers of dictophones, blockers of cellular connection, devices of protection of the electric system, generators of noise.

Вступ

Із розвитком техніки та інформаційних технологій останніми роками відчутно зросли темпи розвитку технічних пристроїв для несанкціонованого оволодіння інформацією.

Зараз набагато простіше й дешевше здобути інформацію нелегально, ніж намагатись отримати її офіційно. Якщо ж це стосується конфіденційної інформації державного значення, то неможливо отримати таку законним шляхом. Саме тому, існує таке поняття як розвідка, а її технічна забезпеченість у багатьох випадках визначає темпи розвитку деяких галузей, а іноді, й усієї країни в цілому. Саме це й є рушійною силою величезного попиту та вдосконалення шпигунської техніки, тоді як захист далеко не відповідає нинішнім вимогам.

У загальному випадку оволодіння інформацією, щодо якої встановлено обмежений доступ, може здійснюватись шляхом її мимовільної втрати або несанкціонованого доступу до неї.

У сучасній літературі поняття «витік інформації» подається досить неоднозначно або розглядається як мимовільне поширення інформації за рахунок технічних чи експлуатаційних особливостей певного обладнання, втрати, пошкодження, знищення документальних та програмних носіїв інформації в результаті дії стихійного лиха, поширення інформації через потрапляння в інформаційні мережі комп'ютерних вірусів тощо.

Постановка завдання

Розголошення інформації виявляється в умисному або необережному її повідомленні, опублікуванні, переданні, наданні для ознайомлення, пересиланні, втраті особами, яким така інформація була відома у зв'язку з їхньою професійною діяльністю і коли в цьому не було службової необхідності.

Несанкціонований доступ до інформації тут розуміється як доступ до інформації, який здійснюється з порушенням установлених правил розмежування доступу.

Як приклад можна навести спосіб прослуховування телефонної лінії та захисту від цього. При контактному підключенні до телефонної лінії за допомогою стандартної «монтерської трубки» виникає стрибок напруги, який, у свою чергу, легко виявляється за допомогою найпростіших засобів контролю телефонної лінії.

Зменшити ефект знаження напруги так само легко як і його виявити. Для цього потрібно лише підключити трубку через резистор з опором 0,6—1 Ом.

Виявити такий спосіб підключення дуже важко, а то й зовсім неможливо. Однак ми навели лише один спосіб прослуховування телефонної лінії, а їх існує безліч і захиститися повністю не можна.

Аналіз існуючих методів

На сьогодні існує багато засобів перехоплення інформації за допомогою різних приладів: радіомікрофони, «вухо» електронне, пристрої перехоплення телефонних повідомлень, пристрої прийому, запису, управління та багато інших. Дешевизна і простота у використанні робить їх дуже популярними, а маючи мінімальні знання з радіотехніці, такі пристрої легко виготовити самостійно.

Існує багато засобів захисту інформації, про які далі коротко піде мова.

Пристрої виявлення підслуховувальних пристроїв: пристрої потрібні для захисту всіх видів телефонних розмов від несанкціонованого отри-

мання інформації, а також для виявлення і знешкодження підслуховувальних пристроїв на телефонній лінії. Це дуже широкий спектр обладнання, що містить в собі різноманітні пристрої для захисту як стаціонарного офісного обладнання, так як і стільникового зв'язку стандарту GSM.

Телефонні апарати передають інформацію про мовний сигнал по телефонній лінії у цифровому вигляді із застосуванням спеціальних алгоритмів стиснення та захисту, що дає змогу будувати корпоративні мережі конфіденційного зв'язку різноманітного рівня захисту.

Стаціонарні пристрої захисту телефонних ліній можуть контролювати всю лінію до АТС від підключення несанкціонованих пристроїв, подаючи при вимкненому телефонному апараті в лінію високовольтні імпульси, що призводить до електричного «випалювання» вхідних каскадів електронних пристроїв перехоплення інформації та блоків їх живлення підключених до лінії.

Фунцією таких пристроїв є: захист усіх видів телефонних розмов (стаціонарні й мобільні телефони) від прослуховування всіма відомими засобами добування акустичної інформації, які включаються в телефонну лінію послідовно чи паралельно, блокування несанкціонованого використання паралельного апарата, сигналізацію про «піратське» підключення, а також розриву й замикання телефонної лінії.

Заглушувачі диктофонів — пристрої створені для захисту від несанкціонованого отримання інформації за допомогою цифрових та кінематичних диктофонів.

Основний принцип їх роботи полягає в створенні високочастотних завад зі спеціальним видом модуляції, які після нав'язування обробляються в колах диктофона разом із корисним сигналом, значно перевищуючи його за рівнем, і відповідно спотворюючи його.

Головними функціями таких пристроїв є:

- захист від несанкціонованого отримання інформації за допомогою цифрових і кінематичних диктофонів;
- запобігання витоку інформації за допомогою провідних мікрофонів, радіомікрофонів, електронних стетоскопів і т. п., портативних відеокамер, малогабаритних передавачів.

Ці пристрої не заважають роботі радіоелектронних приладів, розташованих за зоною заглушування, яка залежно від моделі може сягати від 1,5 до 10 м.

Вони випускаються в стаціонарному, переносному (кейс) і вмонтованому (наприклад, у побутову електроніку) виконанні.

Блокиратори стільникового зв'язку (БСЗ) використовуються як у приміщеннях, так і на відкритому просторі у цілодобовому режимі.

Для захисту території з великою площею використовується метод просторового розміщення необхідної кількості модулів. БСЗ виробляються як у стаціонарному, так і в мобільному варіантах, направленої й ненаправленої дії, різної дальності блокування (від 1м до 80 м) абонентських апа-ратів усіх стандартів стільникового зв'язку.

Функціями таких пристроїв є:

- технічне обмеження використання мобільних телефонів на контрольованих територіях;
- санкціоноване блокування роботи абонентських терміналів;
- захист інформації від витоку з використанням каналів стільникового зв'язку (акустичний і відеоконтроль, визначення місця розташування об'єкта, дистанційне керування різноманітними пристроями й т.п.)

Пристрої захисту електромережі:

- генератори шуму;
- мережеві завадоподавлявальні фільтри.

Генератори шуму, створені для захисту інформації в комп'ютерних мережах від витоку по мережі електроживлення, забезпечують подавлення пристроїв несанкціонованого знімання інформації, використовуючи як канал передавання кола електроживлення через формування та подавання в електричну мережу маскувальних сигналів.

Пристрої не створюють завад для ПК та приладів побутової електроніки, не чуттєвих до перепадів електроструму.

Мережеві завадоподавальні фільтри, створені для захисту радіоелектронних пристроїв та засобів комп'ютерної техніки від витоку інформації за рахунок наведень по колах електроживлення, забезпечують подавлення завад у діапазоні частот 0,1—1000 МГц.

Забезпечують електромагнітну розв'язку по колах електроживлення радіоелектронних пристроїв, засобів комп'ютерної техніки та електромереж промислових та інших генераторів.

Фунціями таких генераторів є:

- захист інформації в комп'ютерних мережах від витоку по мережі електроживлення;
- подавлення пристроїв несанкціонованого зніманні інформації, використовуючи як канал передавання кола електроживлення через формування й передавання в електромережу маскувальих сигналів.

Моделі системи захисту

Існують моделі як для однофазної, так і для трифазної мережі. Випускаються в стаціонарному виконанні.

Широкосмугові генератори, пристрої захисту від витоку по каналах ПЕМВН, створені для захисту інформації від перехоплення засобами радіоелектронного контролю шляхом створення маскувального сигналу в широкому спектрі діапазону, забезпечують маскування побічних електромагнітних випромінювань та наведень технічних засобів і систем, які обробляють конфіденційну інформацію.

Випускаються як стаціонарні, так і переносні моделі генераторів радіошумів, що різняться між собою вихідною потужністю та діапазоном частот.

До функцій таких пристроїв відноситься:

- захист інформації від перехоплення засобами радіоелектронного контролю через створення маскувального сигналу в широкому спектрі діапазону
- маскування ПЕМВН технічних пристроїв і систем, які обробляють конфіденційну інформацію.

Пристрої акустичного та віброакустичного захисту, створені для припинення несанкціонованого зніманя мовної інформації через огороджувальні конструкції та інженерні комунікації виділених приміщень по віброакустичному та акустичному каналах.

Пристрої забезпечують захист від таких технічних засобів: пристрої, що використовують контактні мікрофони, пристрої дистанційного знімання інформації, закладні пристрої, що вмонтовуються в елементи будівельних конструкцій, акустичні мікрофони, диктофони.

Як у випадку з телефонними лініями, методи захисту ділять на два класи:

- захист самої інформації;
- блокування роботи техніки знімання інформації

До першого класу відносять пристрої, які або спотворюють мову, або додають сигнал завад і тим самим дуже сильно знижують розуміння мови. Пристрої, які спотворюють мову, є практично 100-відсотковою гарантією конфіденційності в наших переговорів, але поряд з тим мають один суттєвий недолік — обмежена кількість людей, яка може брати участь у розмові й необхідність використовувати гарнітуру під час розмови, яка складається з навушників і мікрофона.

Пристрої, які додають до мови сигнал завад, називають генераторами акустичного шуму. Основний принцип роботи подібних пристроїв — зашумлення корисного сигналу так званим «білим» акустичним шумом. «Білим» шум називають тому, що спектральний склад шуму однорідний по всьому діапазону випромінюваних частот. Такий сигнал є складним, як і наша мова, і в ньому не можна виділити якихось домінуючих складових.

Справа в у тому, що існуючі на сьогоднішній день методи очищення звукових сигналів з легкістю справляються з простими сигналами завад, які мають у своєму складі одну чи кілька, або обмежену кількіст спектральних складових. «Білий шум» не можна на відфільтрувати сьогоднішній день.

До переваг генераторів акустичного шуму можна віднести їх нешкідливість і достатньо високу ефективність.

До недоліків можна віднести ті, що працюючий генератор додає деякі незручності в ході проведення переговорів.

Принцип пристроїв, які блокують нормальну робот техніки знімання інформації, — це створення електромагнітної завади, що призводить до появи паразитних наведень і, як результат, нестабільної роботи техніки звукозапису.

Основна переваги подібного роду пристроїв — прихована дія, недоліки — низька її ефективність й шкідливість здоров'ю людини.

На підставі викладеного можна зробити висновок, що отримання інформації спецслужбами, конкурентами та зловмисниками здебільшого здійснюється через технічні засоби, які використовуються на фірмах, підприємствах, у банках та через їхніх співробітників. Тобто в основу інформаційної безпеки має бути покладено заходь захисту інформації в засобах і мережах її передання та обробки, а також створення відповідної нормативної бази, яка б регулювала порядок доступу, зберігання й використання інформації фірми, банку, підприємства.

Організаційно-технічні заходи

Заходи захисту інформації в засобах і мережах її передавання та обробки в основному передбачають використання апаратних, програмних та криптографічних засобів захисту.

У свою чергу, апаратні засоби захисту (АЗЗ) застосовуються для вирішення таких завдань:

- перешкодження візуальному спостереженню й дистанційному підслуховуванню;
- нейтралізація паразитних електромагнітних випромінювань і наведень;
- виявлення технічних засобів підслуховування і магнітного запису, несанкціоновано встановлених або принесених до установ фірми, підприємства, банку;
- захист інформації, що передається засобами зв'язку і міститься в системах автоматизованої обробки даних.

За своїм призначенням АЗЗ поділяються на засоби виявлення і засоби захисту від несанкціонованого доступу.

Слід зазначити, що універсального засобу, який би давав змогу виконувати всі функції, немає, тому для виконання кожної функції відповідно до виду засобів несанкціонованого доступу існують свої засоби пошуку й захисту. За таких умів заходи щодо протидії незаконному вилученню інформації за допомогою АЗЗ досить трудомісткі та дорогі й потребують спеціальної підготовки фахівців безпеки.

На практиці всі заходи щодо використання АЗЗ діляють на три групи: організаційні, організаційно-технічні, технічні.

Організаційні заходи апаратного захисту — це заходи обмежувального характеру, які передбачають регламентацію доступу і використання

технічних засобів передавання та обробки інформації.

Організаційно-технічні заходи забезпечують блокування можливих каналів витоку інформації через технічні засоби забезпечення виробничої і трудової діяльності за допомогою спеціальних технічних засобів, які встановлюються на елементи конструкцій споруд і будівель, приміщень і технічних засобів, потенційно створюючи канали витоку інформації.

Технічні заходи — це заходи, які забезпечують використання в процесі виробничої діяль-ності спеціальних, захищених від побічних випромінювань технічних засобів передавання та обробки конфіденційної інформації.

Під програмними засобами захисту розуміють систему спеціальних програм, включених до складу програмного забезпечення комп'ютерів та інформаційних систем, які реалізують функції захисту конфіденційної інформації від неправомірних дій і програми їх обробки.

Програмні засоби забезпечують захист інформації від несанкціонованого доступу до неї, копіювання її або руйнування.

Висновки. Під час захисту від несанкціонованого доступу (НСД) за допомогою програмних засобів здійснюється:

- ідентифікація об'єктів і суб'єктів;
- розмежування доступу до інформаційних ресурсів;
- контроль і реєстрація дій з інформацією та програмами.

Захист інформації від копіювання забезпечується виконанням таких функцій:

- ідентифікація середовища, з якого запускатиметься програма;
- аутентифікація середовища, з якого запущена програма;
- реакція на запуск із несанкціонованого середовища;
- реєстрація санкціонованого копіювання;
- протидія вивченню алгоритмів роботи системи.

Заходи захисту від руйнування інформації, враховуючи велику різноманітність причин руйнування (несанкціоновані дії, помилки програм і обладнання, комп'ютерні віруси та ін.), передбачають обов'язкові страхувальні дії, спрямовані на попередження і профілактику можливих причин руйнування інформації.

Програмні засоби захисту у таких випадках бувають як спеціалізованими, так і універсальними.

Під криптографічними заходами розуміють використання спеціальних пристроїв, програм, виконання відповідних дій, які роблять сигнал, що передається, абсолютно незрозумілим для сторонніх осіб.

Тобто криптографічні заходи забезпечують такий захист інформації, за якого у разі перехоплення її та обробки будь-якими способами вона може бути дешифрована тільки протягом часу, який потрібен їй для втрати своєї цінності. Для цього використовуються різноманітні спеціальні засоби шифрування документів, мови, телеграфних повідомлень.

ЛІТЕРАТУРА

1. *Адріанов В.И., Бородін В.А., Соколов А.В.* «Шпигунські штучки» і прибудую для захисту об'єктів й інформації / В.І. Адріанов, В.А. Бородін, А.В. Соколов. — СПб.: Лань, 1996. — 272 с.

2. *Хорошко В.А., Чекатков А.А.* Методи й засоби захисту інформації / В.А. Хорошко, А.А. Чекатков. — К. : ЮНІОР, 2003. — 501 с.

3. *Безпека* зв'язку в каналах телекомунікацій. — М.: 1992. — 124 с.

4. *Полмар Н., Аллен Т.Б.* Енциклопедія шпигунства : пер. з англ. В. Смирнова. — М.: КРОНА-ПРЕСС, 1999. — 816 с.