22. *Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan*. Power Analysis Attacks of Modular Exponentiation in Smartcards // Cryptographic Hardware and Embedded Systems First International Workshop, CHES'99, Worcester, MA, USA, August 1999, LNCS 1717, pp. 144-157.

УДК 534.87:621.397.7:65.012.8(045) **Кучеренко М.А., Ткаліч О.П.**

КЛАСИФІКАЦІЯ ВИТОКІВ ІНФОРМАЦІЇ

По цій темі написано сотні робіт, проведено десятки конференцій, але багато з них не зрозумілі звичайному читачу. В цій статті розглядається найбільш доступна інформація, яка не потребує від читача поглиблених знань техніки. Аналізуються найбільш прості способи витоку інформації і рекомендації щодо запобігання її втрати.

З найдавніших часів будь-яка діяльність людей ґрунтувалася на отриманні й володінні інформацією, тобто на інформаційному забезпеченні. Саме інформація є одним з найважливіших засобів рішення проблем і завдань, як на державному рівні, так і на рівні комерційних організацій і окремих осіб. Одержання інформації шляхом проведення власних досліджень і створення власних технологій є досить дорогим, тому вигідніше витратити певну суму на придбання вже існуючих відомостей. Таким чином, інформацію можна розглядати як товар. А бурхливий розвиток техніки, технології та інформатики в останні десятиліття викликало ще більш бурхливий розвиток технічних пристроїв і систем розвідки. У створення пристроїв і систем ведення розвідки завжди вкладалися й вкладаються величезні кошти у всіх розвинених країнах. Сотні фірм активно працюють у цій області. Серійно виробляються десятки тисяч моделей «шпигунської» техніки. Тому останнім часом органи влади приділяють питанням захисту інформації більш пильну увагу. Ця галузь бізнесу давно й стійко зайняла своє місце в загальній системі економіки Заходу та має під собою міцну законодавчу базу у відношенні як юридичних, так і фізичних осіб, тобто суворо регламентована й реалізована в чітко налагодженому механізмі виконання. Тематики розробок на ринку промислового шпигунства охоплюють практично всі сторони життя суспільства, безумовно, орієнтуючись на найбільш фінансово-вигідні. Спектр пропонованих послуг широкий: від примітивних радіопередавачів до сучасних апаратно - промислових комплексів ведення розвідки. Звичайно, у нас ще немає великих фірм, які виробляють техніку подібного роду, немає й такої розмаїтності її моделей, як на Заході, але техніка вітчизняних виробників цілком може конкурувати з аналогічно західною, а іноді вона краще й дешевше. Природно, мова йде про порівняння техніки, що є у відкритому продажу. Апаратура ж, використовувана спецслужбами (її кращі зразки), набагато вища за рівнем своїх можливостей, за техніку, використовувану комерційними організаціями. Все це пов'язане з достатнім ризиком цінності різного роду інформації, розголошення якої може привести до серйозних втрат у різних галузях (адміністративної, науково-технічної, комерційної і т.п.). Тому питання захисту інформації (ЗІ) набувають все більш важливого значення.

Метою несанкціонованого збору інформації в цей час є, насамперед - комерційний інтерес. Як правило, інформація різнохарактерна, різноманітна й ступінь її таємності (конфіденційності) залежить від імені або групи осіб, кому вона належить, а також сфери їх діяльності. Діловій людині, наприклад, необхідні дані про конкурентів: їх слабкі й сильні сторони, ринки збуту, умови фінансової діяльності, технологічні таємниці. В політиці або у військовій справі виграш іноді виявляється просто безцінним, тому що політик, адміністратор або просто відома людина є інформантом. Цікаве його повсякденне життя, зв'язок в певних колах, джерела особистих доходів і т.п. А розвиток ділових відносин

визначає сьогодні різке зростання інтересу до питань безпеки саме мовної інформації. Особливістю захисту мовної інформації є те, що вона не матеріальна, тому захищати її просто технічними засобами складніше, ніж секретні документи, файли та інші носії інформації.

Можливі канали витоку інформації

Розглянемо можливі канали витоку інформації та несанкціонованого доступу до ресурсів, які можуть бути використані супротивником, а також можливий захист від них.

Основним напрямком протидії витоку інформації є забезпечення фізичної(технічні засоби, лінії зв'язку, персонал) і логічної (операційна система, прикладні програми та дані) захисту інформаційних ресурсів. При цьому безпека досягається комплексним застосуванням апаратних, програмних і криптографічних методів і засобів захисту, а також організаційних заходів[2, с.27].

Основними причинами витоку інформації є:

• недотримання персоналом норм, вимог, правил експлуатації автоматизованої системи (АС);

• помилки в проектуванні АС і систем захисту АС;

• ведення конфронтуючою стороною технічної й агентурної розвідок.

Недотримання персоналом норм, вимог, правил експлуатації АС може бути як навмисним, так і ненавмисним. Від ведення конфронтуючої стороною агентурної розвідки цей випадок відрізняє те, що в цьому випадку особою, що робить несанкціоновані дії, рухають особисті спонукальні мотиви. Заподій витоку інформації досить тісно зв'язані з видами витоку інформації.

Витік акустичної інформації через підслуховуючі пристрої

Для перехоплення й реєстрації акустичної інформації існує величезний арсенал різноманітних засобів розвідки: мікрофони, електронні стетоскопи, радіомікрофони або так звані "радіозакладки", спрямовані й лазерні мікрофони, апаратура магнітного запису. Система засобів акустичної розвідки, яка використовується для вирішення конкретного завдання, сильно залежить від можливості доступу агента до об'єктів прослуховування. Застосування тих або інших засобів акустичного контролю залежить від умов поставленого завдання, технічних і насамперед фінансових можливостей організаторів підслуховування.

Використання телефонних ліній для дистанційного знімання аудіо-інформації з контрольованих приміщень

Окреме місце займають системи, які призначені не для підслуховування телефонних переговорів, а для використання телефонних ліній при прослуховуванні контрольованих приміщень, де встановлені телефонні апарати або прокладені телефонні лінії.

Прикладом такого пристрою може слугувати "телефонне вухо". Воно являє собою невеликий пристрій, що підключається паралельно до телефонної лінії або електричної мережі в будь-якому зручному місці контрольованого приміщення. Для прослуховування приміщення необхідно набрати номер абонента, у приміщенні якого розташоване "телефонне вухо". Почувши перший гудок АТС необхідно покласти трубку й через 10-15 секунд повторити номер абонента.

Пристрій дає помилкові гудки зайнятий протягом 40-60 секунд, після чого гудки припиняються й включається мікрофон у пристрої "телефонне вухо" - починається прослуховування приміщення. У випадку звичайного дзвінка "телефонне вухо" пропускає всі дзвінки після першого, виконуючи роль звичайної телефонної розетки.

Крім того, можливе використання телефонної лінії для передачі інформації з мікрофона, потай установленого в приміщенні. При цьому використовується несуча частота в діапазоні від десятків до сотень кілогерців з метою не перешкоджати нормальній роботі

телефонного зв'язку. Практика показує, що в реальних умовах дальність дії подібних систем із прийнятною розбірливістю мови істотно залежить від якості лінії, прокладки телефонних проводів, наявності в даній місцевості радіотрансляційної мережі, наявності обчислювальної техніки і т.п.

Із числа, так званих "беззаходових" систем знімання мовної інформації з контрольованих приміщень, коли використовуються телефонні лінії, треба відзначити можливість знімання за рахунок електроакустичного перетворення, виникаючого в телефонних апаратах і за рахунок високочастотного нав'язування. Але ці канали витоку використовуються все рідше. Перший тому, що сучасні телефонні апарати не мають механічних дзвінків і великих металевих деталей, а другий - через свою складність і громіздкість апаратури.

Використання мережі 220 В для передачі акустичної інформації з приміщень

Для цих цілей застосовують так звані мережні "закладки". До цього типу "закладок" найчастіше відносять пристрої, які вбудовуються в прилади, які живляться від мережі 220 В. Передавальний пристрій складається з мікрофона, підсилювача й власне передавача несучої низької частоти. Вона звичайно використовується в діапазоні від 10 до 350 кГц. Передача й прийом здійснюється по одній фазі або, якщо фази різні то їх зв'язують по високій частоті через конденсатор.

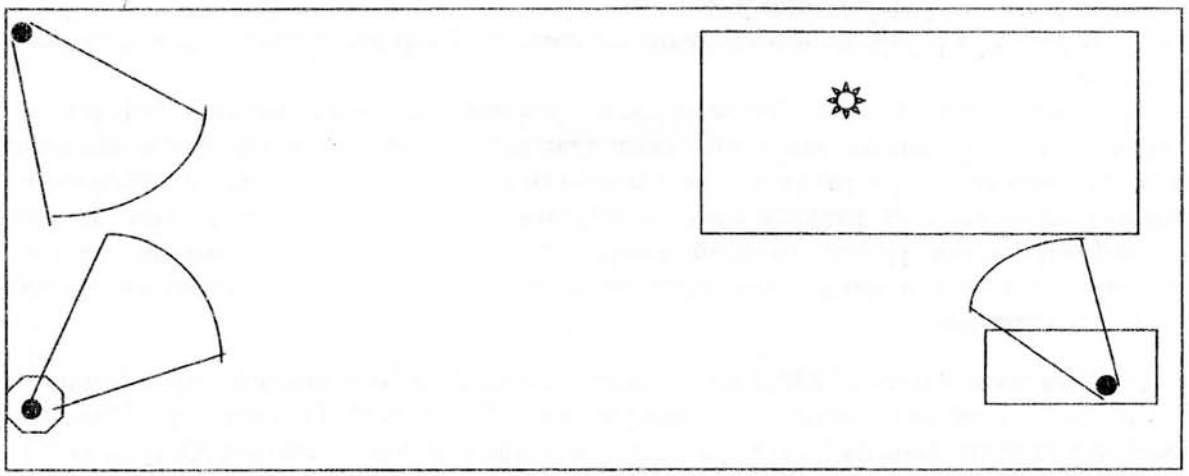
Витік інформації за рахунок прихованого й дистанційного відеоспостереження

Із засобів даного типу найбільше широко застосовуються приховано встановлювані фото-, кіно-, і відеокамери з вихідним отвором об'єктива кілька міліметрів. Використовуються також мініатюрні відеосистеми, які складаються з мікровідеокамери з високою чутливістю й мікрофоном. Встановлюються на двері або в стіні. Для конспіративного спостереження використовуються також мікровідеокамери в настінних годинниках, у датчиках пожежної сигналізації, невеликих радіомагнітолах, а також у краватці або брючному ремені. Відеозображення може записуватися на малогабаритний відеомагнітофон або передаватися за допомогою малогабаритного передавача по радіоканалу в інше приміщення або автомашину на спеціальний або стандартний телеприймач. Відстань передачі, залежно від потужності передачі досягає від 200 метрів до 1 км. При використанні репітерів сигналу відстань передачі може бути значно збільшено.
На цьому рисунку показано приклад розташування мікровідеокамер(●) та мікрофону (✿). Відеокамери розміщені на стіні, настінному годиннику та у телевізорі. Мікрофон, який вмонтовано у телефон, розміщенно на столі.

Привертає увагу автомобільна система схованого відеоспостереження. Відеокамера, що забезпечує круговий огляд, закамуфльована під зовнішню антену стільникового телефону. Плоский екран встановлюється або на сонцезахисному козирку, або в "бардачку", пульт керування - або в попільничці, або в кишені на дверях. Відеосигнал, залежно від комплектації набору для спостереження, може записуватися прямо на відеомагнітофон або передаватися по радіолінії на відстань до 400 м. Відеокамера комплектується змінними об'єктивами з різними кутами огляду.

Лазерне знімання мовної інформації

Для дистанційного перехоплення інформації (мови) із приміщень іноді використовують лазерні пристрої. З пункту спостереження в напрямку джерела звуку посилає зондуючий промінь. Зондуючий промінь звичайно направляється на скло вікон, дзеркала, інші предмети.Всі ці предмети під дією мовних сигналів коливаються у приміщенні й своїми коливаннями модулюють лазерний промінь, прийнявши який у пункті спостереження, можна шляхом нескладних перетворень відновити всі мовні сигнали, що циркулюють у контрольованому приміщенні. На сьогоднішній день створене ціле сімейство лазерних засобів акустичної розвідки.



Такі пристрої складаються із джерела випромінювання (гелій-неоновий лазер), приймача цього випромінювання із блоком фільтрації шумів, двох пар головних телефонів, акумулятора живлення й штатива. Наведення лазерного випромінювання на шибку потрібного приміщення здійснюється за допомогою телескопічного візира. Знімання мовної інформації з віконних рам з подвійними стеклами з гарною якістю забезпечується з відстані до 250 метрів. Такою можливістю, зокрема, володіє система SIPE LASER 3-DA SUPER виробництва США.

Однак на якість прийнятої інформації, крім параметрів системи впливають наступні фактори:

- параметри атмосфери (розсіювання, поглинання, турбулентність, рівень скла);
- якість обробки зондуючої поверхні (шорсткості й нерівності, обумовлені як технологічними причинами, так і впливом середовища - бруд, подряпини та ін.);
- рівень фонових акустичних шумів;
- рівень перехопленого мовного сигналу.

Крім того, застосування подібних засобів вимагає більших витрат не тільки на саму систему, але й на встаткування по обробці отриманої інформації. Застосування такої складної системи вимагає високої кваліфікації й серйозної підготовки операторів.

Із усього цього можна зробити вивід, що застосування лазерного знімання мовної інформації дороге задоволення й досить складне, тому треба оцінити необхідність захисту інформації від цього виду розвідки.

Висновки

1. Основними причинами витоку інформації є: недотримання персоналом норм, вимог, правил експлуатації автоматизованої системи; помилки в проектуванні автоматизованої системи і систем захисту автоматизованої системи; ведення конфронтуючою стороною технічної й агентурної розвідок.
2. Виділяють наступні технічні канали витоку інформації: електромагнітний, акустичний, візуальний інформаційний.
3. Для перехоплення й реєстрації акустичної інформації існує величезний арсенал різноманітних засобів розвідки: мікрофони, електронні стетоскопи, радіомикрофони або так звані "радіозакладки", спрямовані й лазерні мікрофони, апаратура магнітного запису.

Список літератури

1. *Богуш В.М.* Розвідка в інформаційному суспільстві. - К.: МОУ, 2000 750. с.
2. *Богуш В.М., Юдін О.К.* Основи інформаційної безпеки держави. - Харків: "Консум" П, 2004. 510 с.
3. *Богуш В.М., Кривуца В.Г., Кудін А.М.* Інформаційна безпека: термінологічний навчальний довідник. Київ:"Д.В.К.". 2004. 508 с.
4. *Мухачов В.А., Хорошко В.А.* Методи практичної криптографії. Київ 2004. 124 с.
5. Вступ до комп'ютерної інженерії: Методичні рекомендації до самостійної роботи студентів / Уклад. В.М.Богуш, В.В.Богданов - К.: ДУІКТ, 2004 - 40 с.
6. Інформаційна культура: Методичні рекомендації до самостійної роботи студентів / Уклад. В.М. Богуш - К.: ДУІКТ, 2004 - 40 с.
7. Теорія інформації та кодування: Методичні вказівки до самостійної роботи студентів / Уклад. В.М. Астапеня - К.: ДУІКТ, 2003 - 36 с.
8. *Г.А.Максименко, В.А. Хорошко.* Методи виявлення, обробки й ідентифікації сигналів радіозакладних пристроїв. - К.: ТОВ "Поліграфконсалтинг" , 2004. - с.317, іл.
9. Термінологічний словник з питань технічного захисту інформації (Хорошко В.О., Огаркова Й.М., Чирков Д.В. та інші, за ред. проф. В.О. Хорошка.) - 3-є вид., доп. І перераб. - К.: Поліграфконсалтінг, 2003. 286 с. - Бібліогр.: с. 269-270

УДК 004.681

Зыбин С.В.

МОДЕЛЬ ОБЪЕКТА ЗАЩИТЫ ИНФОРМАЦИИ И МОДЕЛИ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Использование методов моделирования в области обеспечения безопасности привело к разработке большого количества формальных моделей безопасности. Формальные модели используются достаточно широко, потому что только с их помощью можно доказать безопасность системы опираясь при этом на объективные и неопровержимые постулаты математической теории. Основная цель создания политики безопасности информационной системы и описания ее в виде формальной модели – это определение условий, которым должно подчиняться поведение автоматизированной системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию.

Наиболее общей моделью формального описания систем защиты является модель системы безопасности с полным перекрытием, в которой определяется полный перечень объектов защиты и угроз информации. В модель вводится набор объектов $O=\{o_j\}$, которые нуждаются в защитных мерах, и набор угроз $T=\{\delta_j\}$, каждая из которых направлена на один или несколько защищаемых объектов. Множество отношений угроза-объект образует двухдольный граф, в котором ребро $<\delta,o>$ существует тогда и только тогда, когда угроза δ является способом получения доступа к объекту o. Следует отметить, что угроза δ может быть направлена на несколько объектов и один объект может подвергаться нескольким угрозам. Цель моделируемой системы защиты АС УВД в том чтобы перекрыть все возможные ребра в графе $\{<T,O>\}$, т.е. добиться того, чтобы к каждому объекту не было ни одного не перекрытого пути ни от одной угрозы. Это достигается введением третьего набора $M=\{m_k\}$, который включает способы обеспечения безопасности. В идеальной системе каждый способ m_k, должен устранять, по крайней мере, одно ребро $<\delta,o>$ графа $\{<T,O>\}$. Введение набора M способов обеспечения безопасности преобразует