новити зміст тексту на папері, який потрапив під дощ). Крім того, змістово-значущі словоформи нерівномірно розподілені у фразах (реченнях). Закономірності розподілу цих словоформ для різних мов також різні. Більш того, самі фрази також мають різну змістову цінність і існують певні закономірності їх розподілу у фрагментах. Так, змістово більш значущі речення, як правило, розміщені на початку абзаців.

При розглянутому підході до побудови комплексної системи захисту цілісності змісту ПМІ її ядром, як випливає з вищевикладеного, є система відновлення змісту частково зруйнованої або перекрученої ПМІ. Вона може бути використана не тільки для вирішення задач відновлення інформації, але і для вирішення задач контролю за витоком ПМІ по технічних каналах, для оцінки ступеня захищеності ПМІ і керування рівнем її захисту.

Захист людини (фахівця-аналітика) від перевантаження інформації полягає в автоматизації перелічених функцій стиснення інформації. В американській настанові FM 100-34 [4] зазначається, що основним призначенням автоматизованої інформаційної системи є звільнення командира від купи зайвої інформації. Суб'єктивність сприймання інформації можна вирішити за рахунок комплексної автоматизації задач ІАД на єдиній методологічній базі.

Висновки: Аналіз факторів інформаційного впливу дозволяє сформулювати вимоги до системи захисту інформаційно-аналітичного забезпечення завдань: власна інформаційна технологія має забезпечувати: випереджувальне володіння ситуацією на основі аналізу всієї доступної інформації у порівнянні з існуючими технологіями; орієнтацію на обробку знань (тобто змісту інформації), а не текстів (тобто форми інформації); орієнтацію на комплексну автоматизацію всіх етапів аналітичного опрацювання інформації; система захисту інформаційного ресурсу має забезпечувати оцінку інформації на достовірність, повноту і об'єктивність. Оцінка інформації на достовірність має включати виявлення суперечливої інформації, в тому числі і дезінформації. Оцінка інформації на повноту спирається на: зовнішню оцінку інформації, яка полягає у перевірці наявності більш ніж одного джерела за певною змістовою інформацією та незалежності цих джерел; прагматичну оцінку інформації на повноту, тобто наявність всіх необхідних даних (фрагментів) знань для вирішення певної прикладної задачі. Об'єктивність інформації має забезпечуватися за рахунок комплексної автоматизації задач інформаційно-аналітичного забезпечення завдань на єдиній методологічній базі; захист людини (фахівця-аналітика) від перевантаження інформацією полягає в автоматизації функцій стиснення інформаційних потоків на основі їх узагальнення з урахуванням вимог щодо її цілісності.

Інструментально-технологічний комплекс автоматизації задач інформаційно-аналітичного забезпечення має забезпечувати реалізацію наступних основних функцій: цілеспрямований пошук потрібної текстової інформації в базі знань; класифікація різномовних текстових документів; інтегрування та узагальнення знань, які містяться в різномовних текстових документах; переклад оригінальних текстів українською мовою; формування рефератів різномовних текстів українською мовою; перевірка знань, які містяться в різномовних текстах та їх сукупності на логічну та семантичну сумісність і суперечливість; виявлення закономірностей і тенденцій в певній предметній області за різномовними текстами; формування аналітичних документів за вимогами користувача щодо їх змісту та обсягу.

1. Воробьев И.Н., Круглов В.В. Основы военной футурологии. – М.: ВАФ, 1998, 175с. 2.Плет В. Стратегическая разведка. Основные принципы. – М.: Издательский Дом "Форум", 1997, – 376 с. 3. Рось А.О., Замаруєва І.В., Петров В.Л. Концептуальні засади моделювання інформаційної боротьби // Наука і оборона. 2000. -№2. -С. 47-53. 4. FM 100-34. Military Department of U.S.A // Field Manual.- June, 1999

Надійшла до редколегії 21.08.09

УДК 681.3

Г.Б. Жиров, канд. техн. наук

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ ПІДПРИЄМСТВ ВІЙСЬКОВО-ПРОМИСЛОВОГО КОМПЛЕКСУ

В статті розглядається питання захисту інформації в корпоративній мережі підприємства й необхідні організаційні міри для захисту технології обробки інформації. Запропонований підхід та алгоритм дій дозволяє зменшити імовірність несанкціонованого витоку інформації в мережі.

Ключові слова: захист інформації, промислове шпигунство, виток інформації.

In the article the question of protection of the information in a corporate network of the enterprise and necessary organizational measures for protection of technology of processing of the information is considered. The approach and algorithm of actions which allows to reduce probability of not authorised source of the information in a network is offered.

Keywords: information protection, industrial espionage, information leakage.

Постановка проблеми. На сьогоднішній день підприємства, корпорації, науково-дослідні установи, конструкторські бюро та інші організації дуже гостро стикаються з загальною проблемою захисту інформації. Це насамперед тому, що відбувається бурхливий розвиток нових технологій, особливо ІТ-технологій з одного боку, а з іншого боку наявності у суспільстві промислового шпигунства. Промислове шпигунство – одна з форм недобросовісної конкуренції, яка використовується на всіх рівнях економіки, починаючи з невеликих підприємств і закінчуючи державами. Основне призначення промислового шпигунства – економія засобів і часу, які потрібно витратити, щоб наздогнати конкурента, що займає лідируюче положення, або не допустити в майбутньому відставання від конкурента, якщо той розробив або розробляє нову перспективну технологію, а також щоб вийти на нові для підприємства ринки. Це справедливо і відносно міждержавної конкуренції, де до питань економічної конкурентоспроможності додаються і питання національної безпеки.

Незважаючи на те, що більшість інформації потрапляють до рук фахівців з офіційних джерел (публікацій, патентів, баз даних), інколи інформація просто викрадається. Промислове шпигунство може торкнутися будь-якого бізнесу, чиєю важливою складовою є інформація. Це і списки клієнтів, підписані угоди, особисті записи, дослідницька документація або плани-макети майбутнього продукту і т.п.

Так, наприклад, уряд Франції був викритий в здійсненні промислового шпигунства за американськими супутниковими і аеродинамічними компаніями. Мав місце і зворотний процес. Схожість Ту-144 і Конкорда також зараховують до найяскравіших прикладів промислового шпигунства XX століття. У червні 1982 року шість працівників японських фірм Hitachi і Mitsubishi було арештовано в Каліфорнії за спробу крадіжки документів і компютерних запчастин з офісу компанії IBM і таких прикладів дуже багато.

В 1993–1994 роках США і Германія розслідували позов концерну General Motors про те, що компанія Volkswagen отримала інформацію що є власністю концерну, завдяки тому, що його колишній заступник президента перейшов на аналогічну посаду в німецьку компанію [1].

Інформація будь-якого підприємства при витоку або крадіжці має унікальну якість видимості її збереженості, а наслідки такої події стають відчутними поступово, проявляючись у зниженні активності клієнтів і партнерів і падінні фінансових результатів. Ще серйозніше наслідки у компаній IT-сфери при втраті інформації: баз даних, результатів аналітичних досліджень, вихідних кодів, програмних продуктів, персональних даних клієнтів, без яких подальше продовження бізнесу стає проблемним, якщо взагалі можливим, а зі знищенням доказів і розслідування стає безперспективним. Визначальний фактор економічної безпеки такого підприємства – інформаційна безпека, а її ключовий аргумент – рівень захисту інформації.

Застосування антивірусних програм зараз розповсюджене дуже широко, що, на жаль, помітно заспокоїло керівників підприємств. Однак, статистика звернень до компаній, що займаються інформаційною безпекою, показує, що інциденти, повязані з роботою інформаційних систем, стають більш серйозними, а причини – менш явними, і, як правило, не завжди можуть бути ліквідовані обслуговуючим персоналом, і це викликає занепокоєність зацікавлених осіб у надійному рішенні проблеми захищеності інформаційних ресурсів [2].

Будь-яка інформація (комерційна, технічна і т.д.) має свою вартість, таким чином, необхідно вирішити як і якими засобами забезпечити її захист. Можна констатувати – для переважної більшості компаній, які знаходяться на територій СНД, завдання захисту інформації може бути безболісно розвязана в осяжні терміни і при незначних фінансових витратах [3].

Визначемо принципові умови. Для досягнення мети, яка полягає в тому, щоб конфіденційна інформація була захищена, необхідно керуватися принципом економічної та політичної доцільності витрат на забезпечення захисту інформації. Такі витрати не повинні перевищувати величину потенційного збитку від її порушення або втрати, як для підприємств так і для держави.

2. Насамперед необхідно уточнити, що необхідно захистити. Інформація не існує сама по собі, вона зберігається на різноманітних носіях: на папері, у базах даних і розрізнених файлах на різноманітних носіях серверів і робочих місць, у головах фахівців і передається по каналах звязку між пристроями й мережами.

Питання захисту інформації на кожному з перерахованих типів носіїв вирішується зовсім різними способами, тому в статті не розглядаються питання фізичного захисту носіїв і способи протидії шпигунству традиційним службам безпеки.

В статті розглядаються пропозиції й необхідні організаційні міри, щодо захисту інформації в корпоративній мережі підприємства, що є досить актуальною науково-технічною задачею.

Будемо розглядати підприємства військово-промислового комплексу, т. я. втрата інформації на цих підприємствах може завдати не тільки фінансових збитків, а і підірвати безпеку держави в цілому. Таким чином, вимоги до захисту інформації на таких підприємствах і організаціях повинні бути значно вищими ніж на інших.

Аналіз останніх досліджень. Враховуючи все вищезазначене можно сформулювати основні пропозиції та організаційні заходи щодо захисту інформації в корпоративній мережі:

1. Проводимо інвентаризацію інформаційних ресурсів. Інформацію, яку варто захищати можна класифікувати наступним чином:

- державна таємниця;
- комерційна таємниця;
- інформація бухгалтерії й кадрової служби;
- важлива інформація окремих співробітників;
- технологічна інформація;
- бази даних і знань;
- know-how;
- аналітична інформація;
- результати наукових досліджень;
- і т.д..

Основний обовязок технічного персоналу становить в забезпеченні функціонування корпоративної мережі. За захищеність інформації вони відповідальності не несуть. Ця задача вирішується, у найкращому разі, у межах забезпечення захисту функціонування ресурсів і технологій на прийнятному для них рівні.

2. Проводимо інвентаризацію всіх технічних засобів зберігання, обробки й передачі інформації й інших технологічних елементів і складаємо перелік:

робочі станції, включаючи мобільні;
сервери;
засоби резервного копіювання;
телекомунікаційне устаткування корпоративної мережі;
пристрої вводу/виводу, включаючи персональні;
персональні носії інформації – усілякі накопичувачі, включаючи телефони й фотоапарати;
інші засоби звязку із зовнішнім миром, включаючи мобільні;
самі інформаційні технології, включаючи програмні засоби;
все інше, що упущено вище.

Але породжують інформацію не компютерні системи, вони лише обробляють одні повідомлення й виробляють інші, а інформація у формі відомостей породжується в голові людини, яка потім обробляються і повертається йому у вигляді нових відомостей, що представляють інтерес вже для більше широкого кола споживачів.

3. Виявляємо основні групи користувачів інформацією:

співробітники;
клієнти;
партнери;
обслуговуючий персонал;
особи, які перевіряють;
випадкові люди;
зловмисники й конкуренти.

Із прийнятним ступенем точності класифікуємо інформацію по важливості для наступного вибору засобів захисту й визначення прав доступу.

4. Виявляємо доступність інформації, що підлягає захисту, перерахованим групам користувачів,

при цьому помічаємо, що кожна із груп, і, насамперед, співробітники, не повинні мати повний доступ до всієї інформації. Необхідно визначити їх права по доступу до інформації, побудувавши своєрідну матрицю "інформації-права_доступу" або "інформації-групи_користувачі" і визначити й розмежувати повноваження.

Перераховані раніше дії цілком під силу зацікавленим співробітникам підприємства, які мають відповідні повноваження, але, оскільки вони не є фахівцями в сфері захисту інформації й інформаційної безпеки, залишаються виключення:

настроювання конфігурацій програмно-технічних засобів забезпечує їх функціонування й не відповідають вимогам безпеки;

традиційна (історично сформована) архітектура мережі, як правило, не забезпечує необхідний захист інформаційних ресурсів і технологій їх обробки;

не можна перевіряти самого себе – рішення співробітників можуть містити помилки;

технічний персонал не володіє повною інформацією про ступінь важливості різних даних;

технічний персонал не може оцінювати доцільність прийнятих адміністративних рішень [4].

5.Погоджуємо отримані дані. Необхідно переконаємось, що параметри операційних систем (ОС) робочих станцій, як правило й на жаль, відповідають настройкам постачальника ОС, а всі зміни, якщо й проводилися, були зроблені з єдиною метою забезпечення необхідного функціонування. Те ж саме відноситься й до штатних служб та іншим сервісах, у тому числі й діючих на серверах підприємства, що неприпустимо. Приміром, паролі постачальників устаткування, залишені за умовчанням – часта причина дискредитації систем аутентифікації й авторизації, що надає повний доступ з максимальними правами будь-якому бажаючому в самих захищених системах. Відключення бездіяльних і непотрібних служб, як одного з вимог підвищення захищеності систем, без точних знань їхнього призначення може призвести до непередбачених наслідків, від переустановки операційних систем до втрати даних. Настроювання телекомунікаційного устаткування не менш важливо, тому що неправильно сконфігуровані профілі й функції також можуть призвести до перехоплення керування ресурсами.

Ці обставини диктують нові умови продовження роботи, а подальші кроки вимагають залучення фахівців для погодженої роботи із захисту інформації. Необхідно звернутися до спеціалізованих служб та компаній для виконання комплексу робіт, перерахованих вище. Переваги такого підходу в тому, що персонал притягнутої служби або компанії має штат експертів з унікальним обсягом знань і практичним досвідом у суміжних областях IT-сфери:

інформаційна безпека й захист інформації, у т.ч. моделювання процесів, аналіз ризиків і погроз;

архітектура телекомунікаційних мереж;

операційні системи й штатні сервіси;

прикладне програмне забезпечення, додатки;

захисне програмне забезпечення;

технічні та програмні засоби захисту інформації;

інші IT-технології й засоби;

Отже, виняткові обставини переборені, частина специфічних функцій покладена на провайдера інформаційної безпеки, зокрема, пропозиції по застосуванню й вибір технічних засобів захисту інформації при реальній необхідності.

6. Настроюємо програмно-технічні засоби по наданих рекомендаціях та приводимо у відповідність архітектуру корпоративної системи, впроваджуємо політику парольного захисту, розділяємо і/або ізолюємо незалежні інформаційні й бізнес-процеси, впроваджуємо розмежування прав доступу до інформаційних ресурсів. Також необхідно зясувати штатні можливості наявних програмно-технічних засобів – журнали реєстрації системних подій, функції поточного аудита, системи виявлення й попередження вторгнень, захисне ПО, можливості шифрованого зберігання й передачі даних, можливості перерозподілу навантаження, контентній фільтрації, керування внутрішнім і зовнішнім трафіком і багато чого іншого.

Однак, сама людина, як джерело відомостей й їх основний споживач поки залишається осторонь, а "людський" фактор – найбільш часта причина витоку або втрати інформації, тобто безпека підприємства та держави визначається й мірою відповідальності працівника за дії, які він робить, і без впровадження або деталізації формальних відносин поставлена мета залишиться як і раніше не вирішеною.

7. Проводимо розробку й впровадження організаційно-адміністративних мір, що регулюють правила роботи з інформаційними ресурсами й дії персоналу в позаштатних ситуаціях. Масштаб роботи, глибина пророблення й формалізації процесів і кінцева кількість документів визначаються спільною роботою групи відповідального управлінського персоналу підприємства й фахівцями компанії. Необхідно проаналізувати трудові контракти, посадові інструкції й діючі на підприємстві інструкції на предмет визначення зон відповідальності й угод про конфіденційність, визначити перелік необхідних інструкцій і правил роботи із програмними й технічними засобами, регламенти резервного копіювання, визначити методи доступу до інформаційних ресурсів, зокрема, розробити політику парольного захисту, передбачити правила дії співробітників у позаштатних ситуаціях.

Політика парольного захисту – це організаційно-правовий і технічний документ одночасно і при його складанні треба спиратися на принцип розумної достатності. Зрозуміло, що в компанії з єдиним системним адміністратором захоплення розробкою нормативною документацією призведе до невиправданих витрат на розробку документів, а їх педантичного виконання безглуздо поглинатиме час виконавців. Тому, в загальному випадку, цілком достатньо весь комплекс необхідних процедур обмежити мінімальним набором правил і зафіксувати їх в одному документі, наприклад "інструкція по парольному захисту"

Варто передбачити й спосіб доведення розроблених документів до персоналу компанії. Наприклад, постійне подання на внутрішньому корпоративному web-сайті компанії при обовязковому підписанні окремих документів відповідальними працівниками, тоді, навіть ненавмисні, порушення безпеки будуть мати конкретних авторів.

Природно, перелік і склад кожного документа для кожного підприємства унікальні й нерідко відрізняються для різних підрозділів одного підприємства, але при цьому відповідають єдиній політиці інформаційної безпеки, доцільність розробки якої теж визначається на поточному кроці. Щоб уникнути можливих колізій із чинним законодавством зміст доку-

ментів й їх легалізацію варто погодити з юридичною службою.

8. Розробляємо й впроваджуємо метод і засоби аналізу захищеності ресурсів, визначаємо інтервали й призначаємо відповідальних серед штатного персоналу за проведення систематичного контролю створеної системи інформаційної безпеки. Для аналізу програмно-технічних засобів можна застосувати програмні сканери безпеки й впровадити їх у корпоративну систему, а розроблену нормативну документацію приводити у відповідність при змінах характеру й складу бізнес-процесів, змінах архітектури мережі й, з іншого боку, регулярно піддавати створену систему захисту інформації аналізу на відповідність вимогам документації, тобто проводити регулярний внутрішній аудит.

Впровадження розроблених мір займе деякий час, як і підготовка персоналу, перш, ніж захист інформації буде забезпечений на належному рівні. Але є ще кілька питань, від вирішення яких залежить досягнутий рівень захисту інформації.

По-перше, розвиток технологій, у тому числі і тих, які використовують зловмисники, це постійний процес, вимагає й удосконалювання засобів захисту.

По-друге, ніхто не гарантує, що при впровадженні навіть незначних змін і наступної експлуатації корпоративної інформаційної системи в ній не зявляться нові вразливості. На жаль, але, на відміну від розвинених країн, у нашій країні практика страхування інформаційних ризиків поки ще відсутня.

По-третє, неможливо якісно перевірити самого себе.

Висновоки. Єдине рішення – в проведенні періодичного зовнішнього аудиту для підтвердження й підтримки заданого рівня захищеності. Поява "слабкої" ланки в побудованій системі призведе до послаблення системи в цілому. Регламент і регулярність проведення зовнішнього аудита можуть бути визначені в процесі розробки організаційних мір і закріплені у відповідних розпорядницьких документах.

Запропонована послідовність дій визначена виходячи з досвіду провідних компаній, які займаються інформаційною безпекою підприємств із різними формами власності, різних сфер діяльності й різної величини – від декількох робочих місць в одному приміщенні до територіально розподіленої структури з багатотисячним колективом.

Безумовно, даний підхід має деякі недоліки з погляду побудови комплексної системи керування інформаційною безпекою, але це вже інше завдання,

Перевагами запропонованого підходу є:

досягнуто поставлену мету – конфіденційна інформація захищена;

значна частина робіт виконана штатним зацікавленим персоналом;

документовано поточний стан інформаційної системи підприємства;

запропонований підхід дозволив уникнути невиправданої бюрократичної тяганини з розподілом обовязків при виконанні робіт;

гранично знижені витрати на досягнення мети;

створена логічно повязана система захисту інформації;

створено базу для побудови системи інформаційної безпеки;

істотно підвищений рівень безпеки підприємства та держави.

Таким чином, запропонований підхід є раціональним, щодо захисту конфіденційної інформації на підприємствах при застосуванні принципу доцільності витрат на забезпечення даного захисту.

1. Даллес А. Великие шпионы / А. Далес; [пер. с англ. Б.Г. Любарцева]. – Ростов н/Д: Феникс, 1998. – 511 с. 2. Ленков С.В. Методы и средства защиты информации / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008. – Том I. Несанкционированное получение информации. – 464 с. 3. Петраков А. Информационная безопасность и защита информации / Петраков А., Мельников В, Клейменов С. – М.: Academia, 2008. – 336 с. 4. Курбатов В. Руководство по защите от внутренних угроз информационной безопасности / Курбатов В., Скиба В. – С.Петербург.: Питер, 2008. – 320 с.

Надійшла до редколегії 21.08.09р

УДК 519.676:681.51

С.В. Ленков, д-р техн. наук, проф.,
О.В. Рыбальский, д-р техн. наук, проф.,
В.А. Хорошко, д-р техн. наук, проф.,
Л.П. Крючкова, канд. техн. наук, доц.

ПРИНЦИПЫ БЛОКИРОВАНИЯ СЪЕМА ИНФОРМАЦИИ СПОСОБАМИ ВЧ-НАВЯЗЫВАНИЯ

Запропонована нова концепція захосту акустичної інформації від збору із застосуванням ВЧ-навязування, основана на зміні якостей зондуючого сигналу.

Ключові слова: защита информации, зондирующий сигнал, блокирование.

The new concept of protection of the acoustic information from gathering with application high frequency-imposing based on change of qualities of probing signal is offered.

Keywords: the information protection, probing signal, blocking.

Вступ. Большинству специалистов в области защиты информации известно, что способ снятия акустической информации, получивший название "ВЧ-навязывание", был изобретен в 1945 г. и впервые реализован в "подарке" советских пионеров послу США в СССР А. Гарриману. "Бесценный дар" был выполнен в виде гипсового герба США, принят с благодарностью растроганным послом и размещен на стене его кабинета, где благополучно провисел до 1950 г., поставляя оперативную и стратегическую информацию советскому руководству [1].

С тех пор прошло много лет и способ, изобретенный выдающимся ученым Л.С. Терменом, получил дальнейшее развитие. Были разработаны методы его применения в токопроводящей среде с использованием в качестве пассивной закладки отдельных электрорадиоэлементов (ЭРЭ) электронной техники. В настоящее время такие методы съема акустической информации являются одними из самых перспективных беззаходовых способов ее добывания и имеют тенденцию к дальнейшему развитию.