УДК 004.239:355.404.51:005

М.С.Лисенко, **M.Lysenko,**
аспірант
Національний університет харчових технологій

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ
PARTICULARITIES OF GUARANTEE OF ENTERPRISES' INFORMATION SAFETY

Розглянуто сутність інформаційної безпеки як важливої складової ефективної діяльності підприємств та з'ясовано необхідність її формування. Визначено основні складові забезпечення інформаційної безпеки підприємств, охарактеризовано програмні засоби та методики оцінки стану інформаційної безпеки підприємств.

***Ключові слова**: інформаційна безпека, інформація, конфіденційна інформація, система захисту інформації, ієрархія доступу, людський фактор.*

The essence of information safety as important part of effective activity of enterprises was considered and the necessity of its forming was found out. The basic components forming of enterprises' information safety was defined, software and methods of evaluating the state of enterprises' information safety were characterized.

***Key words:** informational safety, information, confidential information, system of security of informational, human factor.*

Вступ. Основним елементом ведення та розвитку бізнесу виступає інформація, яка є вкрай важливою для ефективного виконання поставлених завдань, отримання прибутку, досягнення конкурентних переваг, протистояння негативним впливам зовнішнього середовища, реалізації потенціалу підприємств, зайняття ним лідируючих позицій.

Інформаційні ресурси містять у собі наукові знання, високі технології, програмні продукти, бази даних, і можуть з'являтися у вигляді окремих документів й окремих масивів документів, а також бути зібранням даних у інформаційних системах – бібліотеках, архівах, фондах, банках даних.

Така інформація, як правило, є об'єктом посиленої уваги конкурентів й потребує захисту. За даними світової статистики втрата тільки 20% інформації веде до руйнування 65% фірм і компаній [3]. Саме тому в системі економічної безпеки кожного підприємства повинна обов'язково існувати система протидії несанкціонованого доступу до конфіденційної інформації, тобто має забезпечуватися інформаційна безпека підприємства.

Проблемі формування і оптимального функціонування системи інформаційної безпеки підприємства приділяється увага в роботах Андрощука Г.О., Безштанька В.М., Дроб'язко В.С., Духова В.Є., Журавльова В.Н., Макогона Ю., Мєдвєдовського І., Нікіморова Г.К., Плаксіна В., Пристайко В, Романюка І.Н., Слєпцова В.І., Ткачука Т., Шликова В.В. та ряду інших науковців.

Постановка завдання. В сучасних високо конкурентних умовах значну увагу необхідно приділяти аспекту забезпечення та формування системи забезпечення інформаційної безпеки підприємств. Оскільки від її злагодженого та ефективного функціонування залежить економічна безпека підприємств, їх фінансово – економічне майбутнє. Оптимальна робота системи захисту дозволить забезпечити технологічний прогрес, конкурентоздатність як на внутрішньому, так і зовнішньому ринках, посилення економічного росту.

Тому, важливим є питання дослідження захисту інформації, що є цінною для підприємств, вироблення шляхів забезпечення інформаційної безпеки підприємства. Сьогодні проблема забезпечення інформаційної безпеки підприємств української економіки у порівнянні з розвинутими державами залишається недостатньо розробленою, а тому потребує подальшого дослідження.

Результати. Забезпечення інформаційної безпеки підприємств можливе шляхом зібрання всіх видів інформації, що має відношення до діяльності того чи іншого суб'єкта господарювання, аналізу одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів і методів, прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів, оцінки рівня економічної безпеки за всіма складовими та в цілому, розробки рекомендацій для підвищення існуючого рівня на конкретному суб'єкті господарювання, інші види діяльності з розробки інформаційної складової економічної безпеки.

Для захисту інформаційного середовища підприємства розробляються та впроваджуються заходи для захисту суб'єктів господарювання від промислового шпіонажу з боку конкурентів або інших юридичних і фізичних осіб, технічного захисту приміщень, транспорту, кореспонденції, переговорів, різної документації від несанкціонованого доступу зацікавлених юридичних і фізичних осіб до закритої інформації, зібрання інформації про потенційних ініціаторів промислового шпіонажу та проведення необхідних запобіжних дій з метою припинення таких спроб.

Власник інформації особисто визначає склад цінної інформації, яка підлягає захисту, засоби й методи її захисту, також розробляє системи матеріального та морального стимулювання співробітників, які дотримуються порядку захисту конфіденційної інформації, і форми відповідальності персоналу за розголошення таємниці фірми.

Система захисту інформації повинна мати чітку ієрархічну структуру, точно визначені можливості доступу конкретних працівників відповідно до посади та необхідності користування, бути конкретизованою і пов’язаною зі специфікою фірми за структурою методів та засобів захисту, що використовуються, відкритою для регулярного оновлення, надійною в звичайних і надзвичайних ситуаціях, а її функціонування має бути злагодженим і не заважати виконанню функціональних обов’язків співробітниками підприємств.

Забезпечення комплексного підходу системи захисту інформації досягається шляхом поєднання в ній важливих елементів – правових, організаційних, технічних та програмно – математичних. Їх співвідношення та зміст забезпечують індивідуальність системи захисту інформації компанії і гарантують її неповторність та стійкість. Забезпечення захисту інформації в залежності від ступеня її цінності потребує відповідного поєднання елементів системи.

Як правило, в установчих та організаційних документах підприємств, в контрактах, що укладаються їх співробітниками, в посадових інструкціях наявні положення та зобов'язання щодо захисту відомостей, що складають конфіденційні дані компанії та її партнерів. Окрім того здійснюється формулювання і доведення до відома всіх співробітників компанії порядку правової відповідальності за розголошення конфіденційних відомостей, реалізується страхування цінної інформації. Таким чином функціонує правовий елемент системи захисту інформації.

При розробці методів організаційного захисту інформації головним стає питання формування обмежувальних (дозвільних) систем і доступу персоналу до конфіденційних відомостей, документів і баз даних. Дана система доступу забезпечує співробітників усіма необхідними для роботи документами й інформацією, обмежує коло осіб, які допускаються до конфіденційних документів, виключає несанкціоноване ознайомлення з документом[2].

Ієрархія доступу реалізується у відповідності з ієрархією цінності конфіденційних даних: чим вища цінність інформації, тим менше коло осіб може мати до неї доступ. Відповідно до цього визначається необхідний ступінь посилення заходів захисту, структура рубежів (ешелонів) захисту інформації. Доступ персоналу до захищеної інформації, який є дозволеним та здійснюється у відповідності з дозвільною системою, називається санкціонованим. Дозвіл на доступ до цих відомостей завжди видається працівникові персонально і в письмовому вигляді. Як правило, це наказ, що затверджує схему посадового чи іменного доступу до інформації.

Проте злагоджене функціонування елементів системи неможливе без врахування людського фактору. Створюють, отримують, опрацьовують, зберігають інформацію, забезпечують її конфіденційність, цілісність і доступність для виконавця – співробітники тих же таки підприємств. Вони є одночасно вкрай необхідним елементом і потенційним джерелом загроз. Людський фактор, у ряді випадків, стає причиною та рушійною силою порушень чи навіть злочинів з боку всіх категорій користувачів інформаційної системи[4].

Кожне підприємство формуючи соціально - психологічний клімат в колективі, ставить собі за мету не лише створення умов для підвищення ефективності виробничої діяльності, але й усунення причин для виникнення конфліктів у підрозділах, що становлять загрозу для цієї діяльності. Міжособистісні відносини особливо у колі користувачів і розпорядчиків системних інформаційних ресурсів, що визначають можливість виникнення конфліктів, безумовно, здійснюють безпосередній вплив на стан системи інформаційної безпеки. Тому таким важливим є уміння правильно керувати персоналом, підбирати кваліфіковані кадри, враховуючи психологічні портрети працівників і їх попередній досвід роботи з конфіденційної інформації.

Особливої уваги потребує робота з попередження витоку інформації при роботі персоналу з документами. Схематично можливі шляхи збереження конфіденційної інформації представлені на рис.1.

Стрімкий розвиток комп’ютерної техніки спричинив активне використання сучасних інформаційних технологій у діяльності практично кожного підприємства. Проте разом із ростом ефективності роботи від впровадження техніки, підприємства зіткнулися із загрозою втрати захищеності цінної інформації. Джерелами загроз інформаційним ресурсам організацій, що використовуються злочинцями стали комп’ютерні віруси, хакерські атаки, атаки направлені на «відмову в обслуговуванні». Глобалізація й об’єднання приватних мереж ускладнюють можливість забезпечення контролю за доступом до них. Тому для побудови комплексної системи захисту інформації

організації потрібно здійснити аналіз ризиків за допомогою існуючих методик і обрати оптимальний по ефективності варіант захисту.

Рис.1. Шляхи збереження конфіденційності інформації при роботі з документами.

Спеціалістами різних країн в області інформаційної безпеки були розроблені програмні комплекси аналізу та контролю інформаційних ризиків: британський «GRAMM» (компанія Insight Consulting), американський «RiskWatch» (компанія Risk Watch), російський «ГРИФ» (компанія Digital Security)[1].

Програма «GRAMM», the UK Government Risk Analysis and Management Method, використовується з 1985 року, є універсальною і підходить як для різних за розміром підприємств. Застосування даної методики дає можливість здійснення економічного обґрунтування витрат організації на забезпечення

інформаційних безпеки і безперервності ведення бізнесу. У основі «GRAMM» лежить комплексний підхід до оцінки ризиків, що поєднує в собі кількісні та якісні характеристики.

Дослідження щодо захищеності інформації підприємств за методикою «GRAMM» починається із визначення меж дослідження, ідентифікації та оцінки активів, що складають інформаційну систему підприємств. Для цього шляхом опитування збирають інформацію про відповідальність за фізичні та програмні ресурси, про особи користувачів інформаційної системи, характер даних в інформаційній системі, які використовують окремі групи користувачів, відомості про конфігурацію інформаційної системи. Респондентами можуть виступати фінансисти, системні адміністратори, спеціалісти служби інформаційної безпеки, начальники основних відділів, а також інші особи здатні оцінити вартість інформації різного характеру.

Наступним етапом роботи є оцінка залежності сервісів користувачів від визначених груп ресурсів та існуючих загроз і слабких сторін. Спочатку ресурси групуються по типам, потім програмне забезпечення для кожної створеної групи ресурсів генерує варіанти рівня загроз та слабких сторін. Далі підприємство аналізує й обирає достатній для неї рівень ризику.

Третій етап – вибір контрзаходів та рекомендацій – порівнюються рівні ризиків визначених на попередньому етапі з вибраними організацією та при потребі пропонує заходи для підвищення рівня, проводиться порівняльний аналіз ефективності різних варіантів захисту.

На відміну від розглянутої «GRAMM», американська методика «RiskWatch» передбачає проведення дослідження в чотири етапи:

визначення предмету дослідження;

введення даних, що описують конкретні характеристики системи;

оцінка ризиків;

генерації звітів.

Перший етап здійснюється через опис типу організації, складу інформаційної системи, що підлягає дослідженню та базових вимог до безпеки.

Введення даних, що характеризують систему – другий крок у проведенні дослідження за методикою «RiskWatch». Тут детально описуються та співставляються втрати та ресурси, визначаються інциденти, потім знову ж таки за допомогою опитування виявляються можливі загрози та задається частота виникнення загроз, ступінь вразливості і цінності ресурсів. Здійснюючи аналіз ризиків на третій фазі, виявляються ефект та доцільність впровадження захисних заходів.

Останній етап – генерація звітів у формі коротких підсумків, повних і коротких звітів про елементи на початкових стадіях проведення дослідження, звітів про вартість ресурсів, що захищаються, і можливих втрат від реалізації загроз, звітів про існуючі загрози та заходи протидії.

«ГРИФ» являє собою комплексну систему аналізу та управління ризиками інформаційної системи організацій. Вона визначає цінні ресурси та ступінь їх захищеності на підприємстві, оцінює можливий збиток, який понесе організація в результаті реалізації загроз інформаційній безпеці, дозволяє ефективно управляти ризиками за допомогою вибору контрзаходів, найбільш оптимальних по співвідношенню ціна-якість. Для аналізу ризиків інформаційної системи використовуються моделі інформаційних потоків та моделі загроз і слабких сторін залежно від початкових та бажаних кінцевих результатів. Забезпечити створення моделі інформаційних потоків та роботу з нею шляхом внесення до системи «ГРИФ» повної інформації про всі наявні ресурси, засоби захисту кожного ресурсу, мережеві взаємозв’язки, а також характеристики політики безпеки організації. Потім алгоритм системи аналізує побудовану модель і створює звіт про значення ризику кожного ресурсу, про всі причини визначеного рівня ризику, найбільш оптимальні контрзаходи, які дозволять встановити необхідний рівень ризику з найменшими затратами.

Кожна з охарактеризованих методик має свої переваги та недоліки, а тому потребує удосконалення, а, можливо, й розробки нового продукту на базі існуючих, що матиме найбільш оптимальні характеристики для забезпечення інформаційної безпеки підприємств.

Висновки. До сьогоднішнього дня питанню захисту інформаційної безпеки на підприємствах не приділялося належної уваги. В той же час ефективність діяльності підприємств безпосередньо залежить від стану їх інформаційної безпеки. В умовах жорсткої конкуренції все частіше зустрічаються ситуації з витоку важливої для діяльності підприємств інформації. Саме тому виникає необхідність у розробці та впровадженні комплексної системи захисту інформації кожного підприємств. Для цього слід застосовувати методики аналізу ризиків, які дозволяють обрати оптимальний по ефективності варіант захисту.

Література.

1. *Безштанько В*. Аналіз існуючих програмних засобів та методик оцінки стану інформаційної безпеки організації // Бизнес и безопасность. – 2007. - №1. – с.32 – 35.

2. *Пристайко В.* Поняття та ознаки комерційної таємниці // Бизнес и безопасность. – 2007. - №1.- с.23 - 25.

3. Ткачук Т. Забезпечення безпеки діяльності торгового підприємства в Україні: сучасний стан та перспективи // Бизнес и безопасность. – 2007. - №6. – с.30 – 33.

4. *Мазур И. И., Шапиро В.Д., Ольдероги Н.Г.* Эффективный менеджмент. – М.: Высшая школа, 2003. – 555с.

Стаття рекомендована до друку
д-ром економ. наук, проф. Т.Л. Мостенською
Національний університет харчових технологій