20. Бауэрсокс Д., Класс Д. Логистика. Интегрированная цепь поставок. – М.: ЗАО Олимп-бизнес, 2001.

21. Боброва И. И. Черный PR? Белый GR! Цветной IR:): менеджмент информационной культуры / И. Боброва, В. Зимин. – М.: Вершина, 2006. – 464 с.

22. Гордон Я. Маркетинг партнерских отношений / Пер. с англ. ; [Под ред. О. А. Третьяк. – СПб: Питер, 2001. – 384 с.

23. Дорси В. Анатомия биржевого рынка. Методы оценки уверенности и ожиданий трейдеров и рыночних тенденций. – СПб.: Питер, 2005. – 400 с.

24. Журавлёв А. Л. Психология управленческого взаимодействия (теоретические и прикладные проблемы). – М.: Изд-во “институт психологии РАН”, 2004. – 476 с.

25. Крикавський Є.В. Основи теорії логістичного управління / Матер.VII Міжнар. Науково-практ. Конф. «Теорія і практика управління організацією з погляду тисячоліть» Київ, 24-26 травня 2001р. – К.: Політехніка, 2001. – С.135-137.

26. Хиггинс Р. Отношения с инвесторами: передовой опыт. Пути создания акционерной стоимости / Р. Хиггинс; Пер. с англ. – М.: Альпина Бизнес Букс, 2004. – 219 с.

27. Ястремська О. М. Інвестиційна діяльність промислових підприємств: методологічні та методичні засади: Монографія. – 2-ге вид. – Х.: ВД «ІНЖЕК», 2004. – 488 с.

Статья поступила в редакцию 25.01.2008

М.В. МІНЬКОВСЬКА, ***к.е.н., доцент,***
Донецький національний технічний університет

ОСНОВНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОМИСЛОВОГО ПІДПРИЄМСТВА

Проблеми захисту інформаційних потоків підприємства стає все більш актуальними в умовах розвитку ринкових відносин як в Україні, так і в зовнішньоекономічному середовищі. Цією проблемою займались В.І.Головко, А.В.Мінченко, В.М. Шаманська[1], К.А.Кірсанова, А.В. Малявіна[3] та інші. В даній роботі розглядаються основні задачі, що мають бути вирішені при забезпеченні інформаційної безпеки. Інформаційна підсистема у механізмі управління промислового підприємства відіграє значну роль, тому що впливає на швидкість передачі інформації між внутрішнім та зовнішнім середовищем. Інформаційне забезпечення є складовою частиною функціонально-цільового блоку фінансово-економічного механізму підприємства.

Інформація має велике значення як для внутрішніх користувачів – керівників, управлінського персоналу, менеджерів, працівників підприємства, так і для зовнішніх – засновників підприємства, органів державного контролю, виконавчої влади, інвесторів, банківських та кредитних установ, конкурентів. Тобто інформація передається між суб’єктами як на мікрорівні, так і на макрорівні, тому інформаційна безпека повинна забезпечуватися на кожному з цих рівнів.

Технічний захист інформації представляє собою комплекс заходів, які спрямовуються на запобігання відтоку і блокування інформації, та залежить від фінансових можливостей та кадрової політики підприємства.

Згідно з ст. 7 Закону України № 80/94 від 5 липня 1994 року «Про захист інформації в автоматизованих системах», підприємство на мікрорівні повинно забезпечити захист інформації на базі виконання низки умов:

− дотримання суб'єктами правових відносин норм, вимог та правил організаційного і технічного характеру щодо захисту опрацьованої інформації;

− використання засобів обчислювальної техніки, правил захисту (ПЗ) засобів

зв'язку і автоматизованих систем (АС) у цілому, засобів захисту інформації, які відповідають встановленим вимогам щодо захисту інформації (мають відповідний сертифікат);

− перевірки відповідності ЗОТ, ПЗ, засобів зв'язку і АС у цілому встановленим вимогам щодо захисту інформації (сертифікація ЗОТ, засобів зв'язку і АС);

− здійснення контролю щодо захисту інформації.

Крім цього для забезпечення безпеки інформації на мікрорівні важливими умовами є розподіл відповідальності на різні елементи та сфери діяльності інформаційної системи з певним обмеженням відомостей про її роботу; регулярне тестування працівників підприємства на предмет визначення рівня можливої змови між різними групами переробки та модифікації програмної продукції; створення центральної групи контролю та тестування технічної системи; підвищення корпоративної культури.

На макрорівні захист інформації в АС визначаються документами ВР України. Управління захистом інформації здійснює уповноважений Президентом України орган, який контролює виконання таких задач:

− проведення єдиної технічної політики щодо захисту інформації;

− розроблення концепції, вимог, нормативно-технічних документів і науково-методичних рекомендацій щодо захисту інформації в АС;

− затвердження порядку організації, функціонування та контролю за виконанням заходів, спрямованих на захист опрацьованої в АС інформації, яка є власністю держави, а також рекомендацій щодо захисту інформації − власності юридичних та фізичних осіб;

− організації випробувань і сертифікації засобів захисту інформації в АС, в якій здійснюється опрацювання інформації, яка є власністю держави;

− створення відповідних структур для захисту інформації в АС; проведення атестації сертифікаційних (випробувальних) органів, центрів і лабораторій, видачі ліцензії на право проведення сервісних робіт у сфері захисту інформації в АС;

− здійснення контролю захищеності опрацьованої в АС інформації, яка є власністю держави;

− визначення порядку доступу осіб і організацій іноземних держав до інформації в АС, яка є власністю держави, або до інформації — власності фізичних та юридичних осіб, щодо поширення і використання якої державою встановлено обмеження [1, с.300-335].

Підприємство при співпраці з банківською системою виступає як клієнт банку та довіряє банку свої фінансові перекази, які є підприємницькою таємницею. Тому банки повинні відповідати за таємницю фінансової політики підприємства і бути гарантами її захисту.

Міністерства, відомства та інші центральні органи державної виконавчої влади забезпечують вирішення питань щодо захисту інформації в АС у межах своїх повноважень. Згідно зі ст. 7 Закону України № 679-XIУ від 20 травня 1999 року «Про Національний банк України», НБУ визначає напрями розвитку сучасних електронних банківських технологій, створює, координує та контролює впровадження електронних платіжних засобів, платіжних систем, автоматизації банківської діяльності та засобів захисту банківської інформації. Крім того, згідно зі ст. 40 цього Закону, НБУ встановлює правила, форми і стандарти розрахунків банків та інших юридичних і фізичних осіб в економічному обігу України із застосуванням як паперових, так і електронних документів, а також платіжних інструментів та готівки, координує організацію розрахунків. Згідно зі ст. 46, 66 Закону України № 2121 -III від 7 грудня 2000 року «Про банки та банківську діяльність», НБУ виконує контрольно-наглядові функції щодо діяльності комерційних банків, котрі співпрацюють з суб'єктами господарської діяльності та з фізичними особами. З цією метою створено службу банківського контролю, яка через відповідні структурні підрозділи у регіональних управліннях НБУ здійснює нагляд за дотриманням суб'єктами банківської діяльно-

сті чинного законодавства, економічних нормативів та нормативних актів НБУ. Завданням служби банківського нагляду є забезпечення фінансової стабільності та безпеки банківської системи, захист інтересів вкладників і кредиторів, регулювання банківської діяльності з метою приведення її у відповідність до встановлених норм і законодавчих вимог. Взаємодія під час проведення перевірок служби банківського нагляду та правоохоронних органів (МВС, СБУ, Генеральної прокуратури) дозволяє виявляти шахрайства з фінансовими ресурсами та попереджувати «відмивання» грошей через банківську систему на національному та міжнародному рівнях. У свою чергу, така взаємодія уможливлює виявлення злочинів на стадії підготовки та притягнення винних до кримінальної відповідальності, а також забезпечення захисту інтересів вкладників та кредиторів [1, с. 350] .

Закон України № 2346 − III від 5 квітня 2001 року «Про платіжні системи та переказ грошей в Україні» визначає загальні засади функціонування платіжних систем в Україні. Згідно зі ст. 1 цього Закону, електронний цифровий підпис (ЦЕП) − сукупність даних, отриманих за допомогою криптографічного перетворення змісту електронного документа, який дає можливість підтвердити його цілісність та ідентифікувати особу, яка його підписала. Електронний цифровий підпис на електронному документі має однакову юридичну силу з підписом на паперовому документі.

Платіжна картка − спеціальний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для ініціювання переказу грошей з рахунка платника або з відповідного рахунка банку з метою оплати вартості товарів і послуг, перерахування грошей зі своїх рахунків на рахунки інших осіб, отримання грошей у готівковій формі в касах банків, пунктах обміну іноземної валюти уповноважених банків та через банківські автомати. Згідно зі ст. 11 цього Закону, СЕП НБУ – це державна система міжбанківських розрахунків. НБУ регламентує та забезпечує функціонування СЕП НБУ, гарантує її надійність і безпеку. НБУ здійснює контроль за діяльністю платіжних систем, що функціонують у межах України. Контроль за дотриманням учасниками платіжних систем нормативно — правових актів, що регламентують порядок проведення переказу, а також застосування відповідних заходів впливу, передбачених законодавством України, покладаються на НБУ. Банк, що обслуговує платника, та банк, що обслуговує користувача, несуть перед платником та користувачем відповідальність, пов'язану з проведенням переказу, відповідно до цього Закону та умов укладених між ними договорів. Платник несе перед банком або іншою установою – членом платіжної системи, що його обслуговують, відповідальність, передбачену умовами укладеного між ними договору. Стаття 38 цього Закону встановлює основні вимоги щодо захисту інформації:

1. Система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу грошей на усіх етапах її формування, опрацювання, передачі та зберігання.

2. Електронні документи, що містять інформацію, яка відноситься до банківської таємниці або є конфіденційною, мають бути зашифрованими під час передавання їх за допомогою телекомунікаційних каналів зв'язку.

3. Захист інформації забезпечується суб'єктами переказу грошей шляхом обов'язкового впровадження та використання відповідної системи захисту.

Система захисту інформації забезпечує виконання низки вимог:

1. Цілісність інформації, що передається у платіжній системі, та компонентів платіжної системи.

2. Конфіденційність інформації під час її опрацювання, передавання та зберігання у платіжній системі.

3. Неможливість відмови ініціатора від факту передавання та отримувачем від факту прийняття документа на переказ, документа за операціями із застосуванням засобів ідентифікації, документа на відкликання.

4. Забезпечення постійного та безперешкодного доступу до компонентів платіжної системи особам, які мають на це право або повноваження, визначені законодавством України, а також встановлені договором.

Згідно із ч. 2 ст. 55 Закону України № 2121-III від 7 грудня 2000 року «Про банки і банківську діяльність», банк зобов'язаний докладати максимальних зусиль для уникнення конфлікту інтересів працівників банку і клієнтів, а також конфлікту інтересів клієнтів банку. Згідно із ст. 60 цього Закону України, інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної, чи моральної шкоди клієнту, є банківською таємницею. Згідно зі ст. 1076 Цивільного Кодексу України № 435 від 16 січня 2003 року, банк гарантує таємницю банківського рахунку, операцій за рахунком і відомостей про клієнта. Відомості про операції та рахунки можуть бути надані тільки самим клієнтам або їх представникам. Іншим особам у тому числі органам державної влади, їхнім посадовим і службовим особам, такі відомості можуть бути надані виключно у випадках та в порядку, встановлених Законом України № 2121-IV від 7 грудня 2000 року «Про банки і банківську діяльність» [1].

Побудова надійної системи ІБ неможлива без попереднього аналізу можливих загроз безпеці системи. Цей аналіз повинен включати вирішення певних задач:

1. Оцінку цінності інформації, що зберігається в системі.
2. Оцінку затрат часу та засобів на проникнення в систему, допустимі для зловмисників.
3. Відокремлення найбільш небезпечних загроз.
4. Побудова моделі зловмисника (оцінка того, від кого треба захищатися).
5. Оцінка допустимих витрат часу, засобів та ресурсів системи на організацію її захисту.

Поява інформаційних загроз викликається рядом факторів:

1. Відсутність гарантії конфіденційності та цілісності передавання даних.
2. Недостатній рівень перевірки учасників з'єднання.
3. Недостатня реалізація або некоректна розробка політики ІБ.
4. Відсутність або недостатній рівень ІБ від несанкціонованого доступу.
5. Існуючі «прогалини» використовуваних ОС, ПЗ, СКБД, веб — систем, мережевих протоколів.
6. Непрофесійне та слабке адміністрування систем.
7. Проблеми при побудові міжмережевих фільтрів.
8. Перебої у роботі компонентів системи.

Основні види атак на фінансові повідомлення та фінансові трансакції такі:

1. Розкриття змісту.
2. Представлення документа від імені іншого учасника.
3. Несанкціонована модифікація.
4. Повтор переданої інформації.

Це приводить до крадіжки ключової інформації, підбору пароля, сканування жорстких дисків комп'ютера (сканування локального комп'ютера або розподілених ресурсів ЛОМ), прослуховування каналу (можливе лише в сегменті локальної мережі), перехоплення пакетів на маршрутизаторі, створення штучного маршрутизатора, нав'язуванню пакетів з недійсною зворотною адресою; на цій основі з'являються можливості перехопити дані, які банкомат відсилає в банк, щоб пересвідчитись в наявності запитуваної суми грошей на рахунку; для чого шахрай повинен підключитися до відповідного кабелю, при цьому не пошкоджуючи його, і зняти необхідні дані.

Для боротьби з інформаційною злочинністю банки, які активно займаються обслуговуванням підприємств з використанням пластикових карток, найближчим часом візьмуть на озброєння технологію електронної комерції. Спочатку в якості засобу для безготівкових розрахунків домінуючу роль будуть відігравати пластикові картки. Важливо відзначити існування міжнародних стандартів у галузі електро-

нної комерції. Наявність стандартів забезпечує сумісність програмних засобів різних виробників і є умовою для початку всезагального введення нової технології. На жаль, в галузі стандартизації протоколів проведення розрахунків за допомогою пластикових карток ще будуть відбуватися зміни. Це пов'язано із невтішним досвідом введення протоколу SET і з появою нового стандарту 3D Secure. Важливо, щоб цей стандарт уникнув помилок, зроблених при введенні SET. Пластикові картки з магнітною смугою не є ідеальним засобом розрахунків в Internet-комерції. На зміну їм прийдуть мікропроцесорні картки з надійними алгоритмами динамічної аутентифікації власника картки[1,5].

Таким чином, можна констатувати, що порушників інформаційної безпеки поділяють на внутрішніх та зовнішніх. До внутрішніх порушників потенційно відносяться співробітники підприємства та організацій із сфери інформаційних технологій, котрі надають підприємству телекомунікаційні та інші інформаційні послуги. Серед внутрішніх порушників визначають: безпосередніх користувачів та операторів ІС, у тому числі керівників; адміністраторів обчислювальних мереж та ІБ; прикладних та системних програмістів; працівників служби безпеки; технічний персонал з обслуговування приміщень та ЗОТ; допоміжний персонал та тимчасові працівники.

Серед зовнішніх правопорушників необхідно визначити: заказників, запрошених відвідувачів, представників конкуруючих організацій, співробітників органів відомчого контролю та управління, а також силових структур, порушників пропускного режиму, наглядачів за межами території охорони.

Злочини, які носять серійний, багатоепізодний характер, скоюються багаторазово, обов'язково супроводжуються діями щодо їх приховування. Їх найчастіше скоюють висококваліфіковані спеціалісти з вищою математичною, інженерно-технічною чи економічною освітою, які входять в організовані злочинні угрупування, добре забезпечені технічно, нерідко спеціальною технікою. На долю цієї групи злочинців приходиться більшість особливо небезпечних посадових злочинів, скоєних з використанням НІТ, привласнення грошових коштів в особливо великих розмірах тощо.

Вчинення злочину можна поділити на три етапи.

1. Підготовка до вчинення злочину - пошук, закупівля, отримання засобів та знарядь злочину; збирання інформації про систему захисту, підбір паролів, подолання системи захисту від несанкціонованого доступу до даних та комп'ютерної ІС, створення умов для вчинення злочину.

2. Замах на злочин (шляхом маніпуляції даними, що зберігаються у пам'яті банківської ІС, та її управляючих програмах організується несанкціонований рух грошових коштів на користь злочинця або третьої особи, приховуються сліди злочину).

3. Закінчення злочину (вже завершені всі несанкціоновані транзакції, злочинець має можливість скористатися плодами свого злочину).

Для запобігання зловживань в інформаційному просторі системи рекомендується:

− шифрування змісту документа;
− контроль авторства документа;
− контроль цілісності документа;
− нумерація документів;
− проведення сесій на рівні захисту інформації; динамічна аутентифікація;
− забезпечення збереженості таємних ключів;
− надійна процедура перевірки клієнта при реєструванні у прикладній системі;
− використання електронного сертифікату клієнту;
− створення надійного з'єднання клієнта із сервером.

Відносно технічних засобів захисту Інтернет-сервісів, фахівці називають такі:

• брандмауер (міжмережевий екран) − програмна або апаратна реалізація;
• системи виявлення атак на рівні мережі;
• антивірусні засоби;
• захищені ОС, що забезпечують рівень B2 за класифікацією захисту комп'ютерних систем та додаткові засоби кон-

тролю цілісності програм та даних;

• захист на рівні додатків (applications): протоколи безпеки, шифрування, ЕЦП, цифрові сертифікати;

• захист засобами системи управління БД;

• захист компонентів програмного забезпечення, що передаються по мережі;

• моніторинг ІБ та виявлення спроб вторгнення, адаптивний захист мережі, активний аудит дій користувачів;

• шахрайські (стосовно хакерів) системи;

• коректне управління політикою ІБ.

Крім того, при проведенні електронного документообігу повинні виконуватися:

− аутентифікація документа при його створенні;

− захист документа при його пересиланні;

− аутентифікація документа при опрацюванні, збереженні та виконанні;

− захист документа при доступі до нього із навколишнього середовища.

Для забезпечення високого рівня ІБ обчислювальних систем фахівці рекомендують проводити наступні процедури при організації роботи власного персоналу:

− фіксувати у трудових, цивільно-правових угодах обов'язки персоналу щодо дотримання конфіденційності у тому числі осіб, які працюють за сумісництвом;

− розподіляти основні функції між співробітниками так, щоб жодна операція не могла бути виконана однією людиною від початку до кінця;

− забезпечити суворий режим пропуску та порядку в службових приміщеннях, встановити жорсткий порядок використання засобів зв'язку та передавання інформації;

− регулярно проводити оцінку наявної інформації та виокремлювати з неї конфіденційну з метою її захисту;

− мати нормативно-правові документи з питань захисту інформації;

− постійно підвищувати кваліфікацію співробітників, знайомити їх з новими методами забезпечення ІБ;

− створити БД для фіксування спроб несанкціонованого доступу до конфіденційної інформації;

− проводити службові розслідування у кожному випадку порушення політики ІБ.

Основними принципами захисту комп'ютерної інформації є такі: не підключайте комп'ютери, що містять критичну інформацію до Internet; не завантажуйте і не проглядайте електронні повідомлення, в яких ви не впевнені. Для попередження злочину проти ІС необхідно проводити спеціальну підготовку персоналу, підтримувати здоровий мікроклімат у колективі, проводити профільний набір найманих працівників, своєчасно виявляти зловмисників. Фахівці у галузі інформаційних технологій рекомендують звертати особливу увагу на прийнятих на роботу співробітників таких професій: адміністратори, програмісти, фахівці в галузі комп'ютерної техніки та захисту інформації. Відомі випадки прийняття на роботу людей, які працюють на конкурентів, або хакера-одинака чи представника хакерської групи, особливо якщо вони увійшли у зговір з керівництвом підрозділів та СБ підприємства або з організованими злочинними угрупуваннями.

Типи правопорушників можуть суттєво відрізнятися, поділятися за складом, можливостями та поставленою метою (наприклад, може бути хакер-одинак або об'єднана хакерська група; може бути підприємство-конкурент; найбільш небезпечними є корумповані представники різних структур відомчого рівня та спецслужби різних країн). Стосовно двох останніх необхідна організація захисту інформації на дуже високому рівні, що пов"язано із суттєвими витратами.

В Україні створені авторські курси, спрямовані виключно на вирішення реальних проблем, для різних категорій користувачів − від керівників вищої ланки до системних адміністраторів. Розробниками є «Информзащита», «Специалист», «Ланит», «Ай Ти». Проходячи два рази на рік необхідні тренінги (вивчаються міжнародні стандарти управління ІБ, зокрема 150-17799) можна вирішувати конкретні за-

вдання − від обґрунтування необхідності вкладення коштів в ІБ до аудиту ІС та підсумкової перевірки корпоративної системи на відповідність світовим стандартам. Так, І5О-17799 − це міжнародний стандарт управління ІБ, розроблений і прийнятий у 2000 році міжнародним інститутом стандартів (150), який має світове визнання. Цей стандарт містить практичні правила з управління ІБ і може бути використаний для оцінки механізмів ІБ організаційного рівня, у тому числі адміністративних, процедурних та фізичних заходів захисту. Перевагою цього стандарту є простота застосування та адаптація на практиці. Крім того, він не залежить від конкретних ЗОТ та рішень, що забезпечує свободу вибору платформ, обладнання, виробників і т. ін. Він несе в собі інформацію про комплексний підхід до забезпечення захисту інформації. До недоліків стандарту можна віднести поверховий огляд матеріалу, що дозволяє лише визначити галузі ІБ, не конкретизуючи їх.

1. Максимальне обмеження об'єму мережі. Чим більша мережа (географічно та за числом комп'ютерів), тим важче її захистити.

2. Якщо мережа АБС має вихід в Internet, то завдання організації її захисту суттєво ускладнюється; цс обумовлюється тим, що в цьому випадку будь-який користувач Internet має фізичний доступ до мережі; якщо в системі захисту мережі АБС є помилка − в ПЗ або політиці безпеки, її може використати будь-який користувач Internet, якщо ізолювати мережу від Internet неможливо, адміністратори цієї мережі повинні приділяти особливу увагу обмеженню доступу до мережі користувачів Internet.

У реальній практиці намітився перехід від формального захисту певних об'єктів до завдання більш високого рівня − «керування безпекою». Мета керування безпекою полягає в наступному: постійна модифікація системи до змін в загрозах та в об'єкті, що захищається; контроль стану засобів, що забезпечують необхідний сервіс безпеки; контроль доступу користувачів до інформаційних ресурсів та відповідність політики доступу адміністративній політиці. Крім того, необхідно здійснювати процес виявлення та оцінки ризиків, визначення їх впливу та засобів контролю для зменшення та уникнення ризиків (стосовно використання ІТ). Успіх аналізу ризиків залежить від підтримки та участі керівництва підприємства. Специфічними завданнями керівництва в цьому процесі є: підбір групи учасників та їх керівника; визначення повноважень та обов'язків групи; прийняття остаточних рішень у зв'язку із введенням заходів безпеки.

Далі процес аналізу ризиків відбувається за таким планом [2,3,4].

1. Ідентифікація, групування та ієрархізація інформаційних ризиків (побудова макету інформаційної інфраструктури організації; визначення пріоритетів захисту ресурсів).

2. Виявлення ризиків та асоціювання ризиків з ресурсами (перелік ризиків для кожного ресурсу, опис цих ризиків та засобів захисту).

3. Оцінка ризиків та надання рекомендацій (прийняття рішень щодо усунення ризиків та фінальний звіт).

4. Моніторинг ризиків.

В ході аналізу визначається рівень ризику ІС або інформаційного процесу. Виходячи з рівня ризику визначають вимоги до ІБ та захисту інформації. На підставі проведеного аналізу розробляються технічні та організаційні методи контролю та зниження ризиків .

Аналіз рівня ризику системи включає такі заходи: 1)регулярний аудит журналу змін у системі; 2) періодичний аналіз прав користувачів у системі; 3)періодичний аналіз захищеності системи; 4)періодичний аналіз практики менеджменту, процедур, положень і т. ін.

В якості головних ризиків слід враховувати наступне: 1) ризик підробки документів є одним із найбільш суттєвих; відноситься до операційних ризиків; 2) ризик відмови від документу відноситься до операційних ризиків (у разі неправильного використання клієнтом банківських послуг або помилки при опрацюванні документів як клієнтом, так і працівником банку, що

може призвести до відповідальності (адміністративної або кримінальної); у разі збоїв у роботі клієнтського забезпечення, за функціонування якого відповідає банк (наприклад, Internet-Клієнт); 3) ризик законодавчий є характерним у випадках недостатнього обліку нормативних документів, стандартів; 4) ризик втрати репутації.

До заходів забезпечення інформаційної безпеки треба віднести: інформаційно-аналітична розвідувальна діяльність щодо виявлення та прогнозування можливих загроз виробничим структурам; контрольні заходи щодо боротьби з агентурним економічним шпигунством, запобігання збору конфіденційної інформації технічними засобами, а також через персонал у внутрішньому середовищі; забезпечення безпеки фінансово-економічної діяльності від економічних злочинів, афер, шахрайства, зловживань персоналу, партнерів, акціонерів, сторонніх організацій; організаційні заходи для забезпечення таємності та конфіденційності внутрішньої та комерційної інформації; фізичний, технічний та «електронний» захист будівель та приміщень комерційних структур та їх співробітників, розробка та забезпечення контрольно-пропускних режимів, виконання охоронно-постових та патрульно-караульних функцій; охорона керівників комерційних структур, а також осіб, що прибувають для зустрічей та переговорів з інших міст, районів, у тому числі із-за кордону; генерація та реалізація антикризових планів діяльності комерційних структур, що передбачають вихід з різних типових надзвичайних ситуацій; кадрово-адміністративні, режимні, нормативні та спеціальні заходи при підборі, перевірки, підготовці, перепідготовці, розміщенні, звільненні персоналу; перехоплення інформації на різних частотних каналах внутрішньої та зовнішньої зв'язках комерційних структур.

Таким чином, особливо привабливою є бізнес середовище для скоєння інформаційних злочинів. У цій системі чиниться велика кількість фінансових афер, здійснюваних частіше за все під час банківських операцій. Злочини, що скоюються у бізнес-системі, відносяться до найбільш небезпечних економічних злочинів, оскільки їх негативний вплив відбивається як на самій системі, так і на інших суб'єктах економічної діяльності та на всій фінансової системі держави.

Література

1. Головко В.І., Мінченко А.В., Шаманська В.М. Фінансово-економічна діяльність підприємства: контроль, аналіз та безпека.. – К.: Центр навчальної літератури, 2006 . – 448 с.

2. Бюджетна сфера: нормативна база/Уклад. Маргорська Л., Пироженко О. – Х : Фактор, 2003. – 208 с.

3. Кирсанова К.А., Малявина А.В., Попов Н.В. Информационная безопасность. – М.: МАЭП, ИИП «Калита», 2000. – 56с.

4. Зайцев Л.Г., Соколова М.И. Стратегический менеджмент. – М.: Юрист, 2002. – 103 с.

5. Банківські операції / А.М. Мороз, М.І. Савлук, М.Ф. Пудовкіна та ін.; За ред.. А.М. Мороза. – К:КНЕУ 2002. – С.104-109

Статья поступила в редакцию 20.12.2007