УДК 657.221

ШПАК В. А.
д.е.н., професор,
Національна академія статистики,
обліку та аудиту

ОРГАНІЗАЦІЯ ЗАХИСТУ ОБЛІКОВОЇ ІНФОРМАЦІЇ

Актуальність проблеми. Забезпечення належного рівня економічної безпеки підприємства є однією з функцій системи бухгалтерського обліку. У внутрішніх нормативно-розпорядчих документах, що регулюють діяльність суб'єктів господарювання, вимоги щодо організації бухгалтерського обліку в частині зберігання та захисту облікової інформації, а також відповідальності за їх порушення повинні займати належне місце.

Аналіз останніх досліджень. Питання захисту облікової інформації знайшли своє відображення в наукових працях українських вчених: Ф.Ф.Бутинця, Б.І.Валуєва, В.В.Євдокимова, В.Ф.Палія, М.С.Пушкаря та ін.

Метою даної публікації є висвітлення проблемних питань організації захисту облікової інформації в системі економічної безпеки підприємства.

Виклад основного матеріалу. Система захисту інформації, і облікової зокрема, представляє собою комплекс технічних засобів, технологій, методів, організаційних заходів, які перешкоджають несанкціонованому (незаконному) доступу до інформації, що міститься у бухгалтерських документах.

Інформація бухгалтерських документів, належить до цінної інформації, значна частина якої складає комерційну таємницю. Конфіденційність такої інформації потребує захисту.

Необхідно підкреслити, що технологічні системи обробки і зберігання конфіденційних і відкритих бухгалтерських документів базуються на єдиній теоретико-методологічній основі. Вони єдині по структурі. Однак між ними спостерігаються деяка, різниця. Так, технологічна система обробки і зберігання відкритих документів (ручна, автоматизована або змішана) призначена для вирішення завдань в одній сфері – документального забезпечення управління. У свою чергу, технологічна система обробки і зберігання конфіденційній документів вирішує завдання не тільки у вказаній сфері, але й в сфері захисту інформації конфіденційних документів при роботі з ними персоналу. До цих завдань можна віднести наступні:

- попередження несанкціонованого доступу будь-якої особи до документу, його частин, варіантів, копій;
- забезпечення фізичного збереження документів і носіїв конфіденційної інформації;
- забезпечення збереження комерційної таємниці підприємства, цінної інформації, яка міститься в бухгалтерських документах.

Власник підприємства (інформації) особисто визначає не тільки склад цінної інформації, яка належить захисту**,** але й відповідні способи та засоби захисту. Одночасно ним розробляються заходи матеріального і морального стимулювання співробітників, які дотримуються порядку захисту цінної інформації, і відповідальність персоналу за розголошення таємниці підприємства. Система захисту інформації повинна бути багаторівневою з ієрархічним доступом до інформації, конкретизованою і прив'язаною до специфіки підприємства щодо методів та засобів захисту, відкритою для постійного оновлення, надійною як в звичайних, так і в екстремальних ситуаціях, не повинна створювати співробітникам підприємства незручності в роботі.

Комплексність системи захисту досягається її формуванням з різних елементів – правових, технічних, програмних та організаційних. Співвідношення елементів та їх зміст забезпечують індивідуальність системи захисту інформації підприємства і гарантують її надійність. Співвідношення елементів системи, їх склад та взаємозв'язок відображають, визначають не тільки її індивідуальність, але й конкретний заданий рівень захисту з врахуванням цінності інформації та вартості подібної системи.

Елемент правового захисту інформації передбачає:

- наявність в засновницьких та організаційно-правових документах підприємства, контрактах, що укладаються із співробітниками, і в посадових інструкціях положень та зобов'язань щодо захисту відомостей, які складають таємницю підприємства і її партнерів;
- формулювання і доведення до відома всіх співробітників підприємства механізму правової відповідальності за розголошення конфіденційних відомостей.

Елемент технічного захисту інформації включає:

- засоби захисту технічних каналів витоку інформації, що виникають під час роботи ЕОМ, засобів зв'язку, копіювальних апаратів, принтерів, факсів та інших приладів і обладнання;
- засоби захисту приміщень від візуальних та акустичних способів технічної розвідки;

- засоби охорони будівель і приміщень від проникнення сторонніх осіб (засоби спостереження, сповіщення, сигналізації, інформування та ідентифікації, інженерні споруди);
- засоби протипожежної охорони;
- засоби виявлення приладів і пристроїв технічної розвідки.

Елемент програмного захисту інформації включає:

- регламентацію доступу до електронних документів персональними паролями, що ідентифікуються командами та іншими найпростішими методами захисту;
- регламентацію спеціальних засобів і продуктів програмного захисту;
- регламентацію криптографічних методів засобів захисту інформації в ЕОМ та мережах, шифрування тексту під час передачі його по каналах звичайного та факсимільного зв'язку, під час пересилки поштою.

Елемент організаційного захисту включає в себе:

- формування і регламентацію діяльності служби безпеки підприємства, забезпечення цієї служби нормативно-методичними документами з організації і технології захисту інформації;
- регламентацію та постійне оновлення переліку (списку) цінної, конфіденційної інформації, яка підлягає захисту, складання і ведення переліку конфіденційних документів підприємства;
- регламентацію системи (ієрархічної схеми) обмеження доступу персоналу до конфіденційної інформації;
- регламентацію технології захисту і обробки конфіденційних документів підприємства;
- побудова захищеного паперового або безпаперового документообігу;
- побудова технології документування цінної інформації, складання, оформлення, виготовлення конфіденційних документів;
- побудова технологічної системи обробки і збереження конфіденційних документів;
- організацію архівного зберігання конфіденційних документів;
- регламентацію захисту цінної інформації підприємства від несанкціонованих дій персоналу;
- порядок і правила роботи персоналу з конфіденційними документами і інформацією, контроль за виконанням всіма співробітниками цього порядку і правил;
- відбір персоналу для роботи з конфіденційною інформацією, навчання та інструктування співробітників;

- ліцензування технічних систем і засобів захисту інформації та охорони;
- регламентацію пропускного режиму на території і приміщеннях підприємства, ідентифікацію персоналу та вантажу;
- регламентацію системи охорони території, приміщень, обладнання, грошових коштів, транспорту і персоналу підприємства;
- регламентацію організаційних питань експлуатації технічних засобів захисту інформації і охорони;
- регламентацію роботи по управлінню системою захисту інформації підприємства.

Елемент організаційного захисту є тією ланкою, яка зв'язує в одну систему всі інші елементи.

Центральною проблемою при розробці організаційних заходів захисту інформації є формування дозвільної (обмежувальної) системи доступу персоналу до конфіденційних відомостей, документів і баз даних. Важливо чітко і однозначно встановити: хто, кого, до яких, відомостей, коли, на який період і як допускає.

Дозвільна система доступу вирішує наступні завдання:

- забезпечення співробітників всіма необхідними для роботи документами і інформацією;
- обмеження кола осіб, які допускаються до конфіденційних документів;
- виключення (недопущення) несанкціонованого ознайомлення з конфіденційним документом.

Ієрархічна послідовність доступу реалізується за принципом "чим вища цінність конфіденційних відомостей, тим менша чисельність співробітників можуть їх знати". У відповідності із цим визначається необхідний ступінь посилення захисних заходів, структура рівнів (ешелонів) захисту інформації.

Доступ співробітника до конфіденційних відомостей, який здійснюється у відповідності з дозвільною системою, називається санкціонованим. Дозвіл (санкція) на доступ до цих відомостей завжди є персоніфікованим і оформлюється керівником в письмовому вигляді: наказом, що затверджує схему посадового чи іменного доступу до інформації, резолюцією на документі, списком-дозволом в картці видачі справи або на обкладинці справи ознайомлення з документом.

Технологія захисту документованої інформації безпосередньо пов’язана із документообігом. Документообіг як об'єкт захисту представляє собою сукупність (мережу) каналів розповсюдження документованої конфіденційної інформації серед споживачів у процесі управлінської та виробничої діяльності. Рух документованої інформації не

можна розглядати тільки як механічне переміщення документів за адресатами. Основною характеристикою такого руху є його технологічна комплексність, тобто з'єднання в єдине ціле завдань щодо управління, діловодства та технічного забезпечення руху документів. В процесі руху документів (в тому числі електронних) за технологічною послідовністю оброблення та споживання інформації виникають потенційні загрози втрати цієї інформації внаслідок розширення числа джерел, що володіють цінною інформацією. Загрози документам в документопотоках включають:

- викрадення, втрату документу або його окремих частин (додатків, примірників, листів та ін.);
- копіювання паперових і електронних документів і баз даних;
- підміну документів, носіїв і їх окремих частин з метою фальсифікації або приховування факту втрати, викрадення;
- несанкціоноване ознайомлення з документами і базами даних, передавання інформації зловмиснику;
- дистанційний перегляд документів за допомогою спеціальних технічних засобів;
- помилкові дії персоналу під час роботи з документами (порушення дозвільної системи, порядку обробки документів, правил роботи з документами і т.д.);
- випадкове або зловмисне знищення цінних документів і баз даних, їх несанкціонована модифікація, спотворення і фальсифікація;
- зчитування даних в чужих масивах за рахунок роботи з залишковою інформацією на копіювальній стрічці, папері, дискам ЕОМ;
- маскування під зареєстрованого користувача;
- витік інформації через технічні канали під час обговорення і диктування тексту документа, виготовлення копій документів.

Головним напрямом захисту документованої інформації (документів) від всіх видів загроз є формування захищеного документообігу і використання в обробці і зберіганні документів технологічної системи, що забезпечує безпеку інформації на будь-якому типі носія. За рахунок цього досягається можливість контролю конфіденційної інформації на етапах її формування і розповсюдження.

Окрім загальних підходів щодо захисту інформації захищений документообіг базується на виконанні додаткових правил:

- персональної відповідальності співробітників за збереження носія і таємницю інформації;
- обмеження ділової необхідності доступу персоналу до документів, справ і базам даних;

- операційному обліку документів і контролю за їх збереженням у процесі руху, розгляду, виконання і використання;

- жорсткій регламентації порядку роботи з документами, справами і базами даних для всіх категорій персоналу.

У великих підприємницьких структурах зі значним обсягом документів в потоках захищеність документообігу досягається за рахунок:

- формування самостійних, ізольованих потоків конфіденційних (з грифом) документів і, нерідко, додаткового дроблення їх на ізольовані потоки у відповідності з рівнем конфіденційності (рівнем грифу) документів, що переміщаються;

- використання централізованої автономної технологічної системи обробки і зберігання конфіденційних документів, ізольованої від системи обробки інших документів;

- організації самостійного підрозділу (служби) конфіденційної документації або аналогічного підрозділу, що входить у склад служби безпеки, аналітичної служби фірми.

В підприємницьких структурах з невеликим складом штатних співробітників та обсягом опрацьованих документів (наприклад, в малому бізнесі), а також в структурах, основний масив документів в яких є конфіденційним (наприклад, в банках, страхових компаніях), конфіденційні документи можуть не виділятися з загального документопотоку і оброблятися в межах єдиної технологічної системи. Підрозділ конфіденційної документації в таких підприємницьких структурах зазвичай не створюється.

При будь-якому варіанті побудови захищеного документообігу для безпеки інформації заходи не повинні збільшувати терміни руху та виконання документів. Однією з найважливіших вимог до захищеного документообігу є вибірковість у доставці і використання персоналом цінної інформації. Вибірковість призначена не тільки для забезпечення оперативності в отриманні користувачем цінної інформації, але й обмеження у доставці йому тієї інформації, робота з якою дозволена у відповідності з його функціональними обов'язками. В основі вибірковості в доставці і використанні конфіденційних документів лежить діюча на підприємстві дозвільна система доступу персоналу до конфіденційної інформації (документам, справам і базам даних). Система в даному випадку передбачає цілеспрямоване дроблення конфіденційної інформації між співробітниками на складові елементи, кожний з яких окремо значної цінності не представляє. Захист документованої інформації в потоках досягається одночасним використанням як дозвільних заходів, так і комплексом технологічних процедур і операцій, які входять в систему обробки і зберігання документів, що забезпечує розгляд, виконання,

використання і рух документів. В захищеному документообігу у більшості випадків використовується традиційна (не автоматизована) технологічна система обробки і зберігання конфіденційних документів. В окремих випадках автоматизуються (при збереженні традиційного обліку документів) довідкові та пошукові завдання, контроль виконання.

Висновки. Облікова інформація є ключовим фактором у забезпеченні економічної безпеки підприємства. Захист облікової інформації є умовою об'єктивного відображення реальної дійсності суб'єкта господарювання, що сприятиме вчасному виявленню внутрішніх і зовнішніх загроз та можливих розрахунків альтернативних рішень щодо їх усунення чи попередження. Тому питанню захисту облікової інформації має приділятися належна увага при організації бухгалтерського обліку на конкретному підприємстві.

Список використаних джерел:

1. Асєєв Г. Методологія електронного документообігу: динамічні архіви //Вісник Книжкової палати. – 2005. –№ 11. – С. 22 -25.

2. Євдокимов В. В. Надійність бухгалтерської інформації як передумова забезпечення економічної безпеки підприємства //Вісник ЖДТУ. – 2011. – № 3 (57). – С.46-50.