УДК 336.01-049.5
О. С. Марченко, д. е. н., проф.
проф. кафедри економічної теорії
Національного університету
«Юридична академія України імені Ярослава Мудрого»

ІНФОРМАЦІЙНА БЕЗПЕКА ФІНАНСОВОЇ СИСТЕМИ: ГОЛОВНІ СКЛАДОВІ ТА ЗАГРОЗИ

Формування економіки знань, провідними ресурсами якої є ресурси інформаційні, обумовлює необхідність забезпечення інформаційної безпеки людини, організації, держави,суспільства. Інформаційна безпека – це захищеність національних інтересів в інформаційній сфері, інформаційних ресурсів та інформаційного простору (середовища), прав і свобод громадян щодо збирання, накопичення, оброблення, збереження, використання і розповсюдження інформації.

Інформаційне убезпечення є однією з найважливіших умов ефективного функціонування як фінансової системи у цілому, так і її окремих структурних елементів. Інформаційна безпека фінансової сфери – це захищеність інформаційних ресурсів, процесів та технологій, що використовуються суб'єктами фінансових відносин у процесі їх діяльності. Це стан захищеності інформаційного середовища фінансової системи, її інформаційного простору.

Головними складовими інформаційної безпеки фінансової діяльності є:

1) безпека спеціальної інформації та її носіїв, до яких належать працівники фінансових установ, бази даних, комп'ютерні програми та ін. Це, по-перше, стан захищеності конфіденційної фінансової інформації від несанкціонованого розголошення, копіювання, використання конкурентами, втрати. По-друге, захищеність носіїв спеціальної інформації, що охоплює : а) інформаційну безпеку працівників фінансової установи та їх професійної діяльності шляхом створення

необхідних умов ефективного використання інформаційних ресурсів; б) безпеку баз даних та інших носіїв інформації;

2) безпека руху інформації у внутрішньому і зовнішньому середовищі фінансової організації як убезпечення інформаційних ресурсів фінансової діяльності, їх джерел та ретрансляторів і користувачів;

3) кібербезпека фінансової сфери – захищеність інформаційно-комунікаційних технологій (ІКТ)**,** значна роль якої у інформаційному суспільстві підкреслена у Конвенції Ради Європи про кіберзлочинність, яку Україна ратифікувала у 2005 році. Це захищеність від кіберзлочинності, пов’язаної з використанням новітніх ІКТ, спрямованим проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також захищеність від зловживання ними.

Інформаційна безпека фінансової системи залежить від стану інформаційної сфери в цілому,серед загроз якому треба виокремити:

– прояви обмеження свободи слова та доступу громадян до інформації, відмова від інформаційного обслуговування;

– поширення засобами масової інформації культу насильства, жорстокості, руйнування системи цінностей;

– комп’ютерна злочинність та комп’ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю;

– розкриття таємної, конфіденційної та іншої інформації з обмеженим доступом;

– маніпулювання суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації;

– несанкціоновані обмін та використання інформаційних ресурсів;

– порушення штатного режиму функціонування інформаційних мереж.

Загрози інформаційній безпеці фінансовій системі – це фактори або група факторів, що створюють небезпеку

інформаційним ресурсам, процесам, технологіям фінансової діяльності. Відповідно класифікації О.К. Юдіна і В. М. Богуша, можливо виокремити такі загрози інформаційній безпеці: неякісна інформація (недостовірна, фальшива, дезінформація), що обумовлює ризики нераціональних фінансових рішень та дій; несанкціонований і неправомірний вплив сторонніх осіб на інформацію та інформаційні ресурси; обмеження або порушення інформаційних прав і свобод особистості [1, с. 43-44]. Треба додати ще такий фактор загроз як опортуністична поведінка працівників фінансових закладів, негативними наслідками якої є розголошення конфіденційної інформації, її модифікація та фальсифікація, розкриття комерційної таємниці. Загрозами інформаційним ресурсам фінансової сфери є промисловий шпіонаж та недобросовісна конкуренція, інструментом якої може бути неправдива інформація про фінансову установу та її діяльність

Інформаційна безпека забезпечується менеджментом фінансової організації шляхом здійснення комплексу заходів:

а) техніко-технологічних – захист технічних засобів, комп'ютерних технологій, комунікацій тощо;

б) економіко-організаційних – система організації та управління витратами руху інформації;

в) мотиваційних – мотивація працівників фірм до збереження та захисту інформації;

г) правових – створення внутрішньофірмових правил і процедур використання інформації;

д)культурологічних – розвиток культури інтелектуальної організації, головним ресурсом якої є інформація.

Важливим є застосування управлінських технологій, які реалізують принципи індивідуалістичних, едхократичних і партисипативних організацій. Ідивідуалістичні організації (на відміну від корпоративних) – це відкриті організації, одиницею управління в яких є особистість; едхократичні орієнтуються на вільні дії працівників, їх компетенцію і вміння самостійно приймати рішення; партисипативні спираються на участь працівників в управлінні. Сполучення індивідуалізації, волі,

самостійності, участі в управлінні, довіри, співробітництва і культури – фундамент ефективного управління творчою працею, подолання загроз інформаційній безпеці фірми.

Важливе значення має мотивація персоналу фінансової установи до збереження та захисту конфіденційної інформації. З цією метою у системі заходів забезпечення інформаційної безпеки треба широко використовувати такий інструмент, як оплата праці. Необхідно створити умови для реалізації з метою забезпечення інформаційної безпеки такої специфічної функції оплати праці, як функція закріплення (збереження) глибоко спеціалізованих інтелектуальних трудових ресурсів, їх «монополізації» фірмою.

По-перше, висококваліфіковані працівники, як правило, є носіями конфіденційної спеціальної інформації. Їх закріплення (збереження) – важливе завдання управління інформаційною безпекою, на вирішення якого повинна бути націлена внутрішньофірмова система оплати праці. По-друге, фінансова установа несе значні витрати і втрати, пов'язані з опортуністичною поведінкою персоналу відносно інформаційних ресурсів. Тому, запобігання цим втратам диктує необхідність використання фірмою різних засобів її подолання, одним із яких і є належна оплата праці. По-третє, оплата праці виступає для фірми інструментом конкурентної боротьби за працівників-носіїв спеціальної інформації, оскільки її конкуренти заінтересовані у її залученні та використанні у власних цілях. Отже, використання оплати праці як інструмента закріплення (збереження) працівників фінансової організації – це дієвий засіб подолання загроз інформаційній безпеці.

Мотивація працівників – носіїв спеціальної інформації базується також на реалізації принципів організації оплати інтелектуальної праці: індивідуалізованість, багатофакторність, гарантованість, гнучкість і комплексність. Вимір абсолютно нематеріальних результатів інтелектуальної праці набуває форму оцінки працівника, його місця й ролі у виробничому процесі, ступеня специфічності його знань і навичок, рівня

реалізації творчого потенціалу. Ось чому, оцінка праці і її оплата повинні бути індивідуалізованими, відображати індивідуальні особливості працівників і їх трудової діяльності. Реалізація принципу індивідуалізованості диктує необхідність багатофакторного аналітичного підходу до оцінки і оплати праці, що поряд із традиційними критеріями враховує статус фахівця в організації, їх внесок у створення і збільшення інформаційної бази, участь у внутрішньофірмовому русі інформації з та ін. Гарантованість певного рівня індивідуалізованої оплати праці виступає дійовим чинником закріплення у фірмі працівника, а принцип гнучкості забезпечує реалізацію стимулюючої функції заробітної плати.

Таким чином, інформаційна безпека фінансової системи та її складових, що охоплює безпеку спеціальної інформації та її носіїв, безпеку руху інформації у внутрішньому і зовнішньому середовищі фінансової організації, кібербезпеку, забезпечується системою заходів: техніко-технологічних, економіко-організаційних, правових, культурологічних, здійснення яких є завданням менеджменту організації. Запобігання опортуністичній поведінці працівників-носіїв спеціальної інформації повинно також базуватися на реалізації специфічної функції оплати праці – функції закріплення таких працівників в організації.

Використані джерела:

1. Юдін О. К. Інформаційна безпека держави : навч. посібн. / О. К. Юдін, В. М. Богуш. – Х.: Консум, 2005. – 576 с.