УДК 331.108.2:65.012.8

Мужанова Т.М., к.держ.упр.
Державний університет телекомунікацій

ОСОБЛИВОСТІ МЕНЕДЖМЕНТУ ПЕРСОНАЛУ У СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Проаналізовано особливості менеджменту персоналу у системі управління інформаційною безпекою підприємства. Визначено основні принципи роботи з персоналом, який працює з конфіденційною інформацією підприємства, та засади їх практичного застосування.

Постановка проблеми. Реалії сьогодення підтверджують потужний вплив «людського фактора» на стан інформаційної безпеки підприємства. Персонал генерує нові ідеї, впроваджує інновації, які прискорюють науково-технічний прогрес, сприяють удосконаленню системи управління інформаційною безпекою підприємства (СУІБ). Водночас, саме персонал є основним джерелом втрати цінної і конфіденційної інформації: близько 75% порушень у СУІБ підприємства відбуваються з вини його працівників [3].

У сучасних підприємницьких структурах практично кожен співробітник стає носієм цінних, конфіденційних відомостей, які становлять інтерес для конкурентів і кримінальних структур, що може стати передумовою виникнення бажання завдати шкоди організації, стати співучасником у недобросовісній конкуренції або кримінальних діях. З іншого боку існує загроза нанесення шкоди підприємству внаслідок недбалості, безвідповідальності, банального незнання правил роботи з конфіденційною інформацією та її захисту.

З огляду на зазначені чинники дослідження особливостей менеджменту персоналу, який поступово стає основним елементом побудови дієвої та ефективної СУІБ підприємства, є актуальним науковим завданням.

Аналіз останніх досліджень і публікацій. Основою для даного дослідження стали публікації вітчизняних та закордонних дослідників з організаційних питань управління інформаційною безпекою підприємства [3,4,5,10], а також праці, присвячені розгляду засад менеджменту персоналу у сфері інформаційної безпеки [2,6,7], кадрових вразливостей СУІБ [1], особливостей навчання персоналу [11] та формування корпоративної культури [9] як засобів забезпечення інформаційної безпеки підприємства. У роботі використані дані щодо світового досвіду менеджменту персоналу, що працює з конфіденційною інформацією [1].

Водночас особливості менеджменту персоналу у СУІБ підприємства, зокрема основні принципи роботи з персоналом, який працює з конфіденційною інформацією, та засади їх практичного застосування недостатньо досліджені в наукових працях, що обумовлює актуальність подальших досліджень у цьому напрямку.

Метою статті є аналіз особливостей менеджменту персоналу у системі управління інформаційною безпекою підприємства та визначення засад їх практичного застосування.

Викладення основного матеріалу. Основою стабільності функціонування та перспективного розвитку будь-якого підприємства є досягнення балансу між двома стратегічними завданнями: забезпечення прибутковості та процвітання бізнесу і гарантування добробуту працівникам фірми. Однак, у СУІБ підприємства, що має на меті забезпечення безпеки найважливішої корпоративної інформації; захист основних інформаційних активів і критичних бізнес-процесів організації; мінімізацію ризиків інформаційної безпеки при веденні операційної діяльності організації [5], менеджмент персоналу відіграє особливу роль. Системно та якісно організована робота з персоналом, яка спрямована на формування лояльності, відданості персоналу перешкоджає виникненню загроз для конфіденційних відомостей підприємства з боку його працівників.

Необхідність управління персоналом найтіснішим чином пов'язана із захистом комерційної таємниці, інших конфіденційних відомостей фірми, тому що персонал є одним з основних носіїв інформації, і, як вважають фахівці, ймовірність витоку відомостей через підкуп, переманювання співробітників складає 43%, а через вивідування - 24% [9].

Як свідчить практика, основними умовами, що сприяють неправомірному оволодінню інформацією, є:

- розголошення (зайва балакучість співробітників) - 32% випадків;
- несанкціонований доступ шляхом підкупу і схиляння до співпраці з боку конкурентів і злочинних угрупувань - 24%;
- відсутність на фірмі належного контролю і жорстких умов забезпечення інформаційної безпеки - 14%;
- традиційний обмін виробничим досвідом - 12%;
- безконтрольне використання інформаційних систем - 10%;
- наявність передумов виникнення серед співробітників конфліктних ситуацій, а також відсутність високої трудової дисципліни, психологічна несумісність, випадковий підбір кадрів, слабка робота кадрів по згуртуванню колективу - 8% [6].

Саме для уникнення таких інцидентів за участю персоналу необхідним є дотримання основних засад менеджменту персоналу у СУІБ підприємства. Принципи, покладені в основу ефективного управління персоналом, досить різноманітні. Система управління персоналом підприємства, задіяним у сфері інформаційної безпеки, має здійснюватися у відповідності як із загальними принципами управління персоналом, так і зі спеціальними принципами, які відображають специфіку роботи корпоративної СУІБ (Рис.1.).

Серед, загальних принципів управління персоналом виділяють, зокрема, принцип науковості, системності, плановості, адаптивності, єдиноначальності, централізації і децентралізації, соціального партнерства та демократизму, гласності, економічної доцільності, послідовності, безперервності та узгодженості, врахування об'єктивних закономірностей розвитку виробничих та невиробничих (персонал) систем підприємства.

Деякі із зазначених принципів набувають особливої ваги у контексті управління інформаційною безпекою. Так, дотримання принципу адаптивності означає постійне оновлення методів та підходів до менеджменту персоналу в СУІБ з урахуванням розвитку як гуманітарних, так і інформаційних технологій та нових ризиків антропогенного характеру для інформаційної безпеки підприємства.

Принцип єдиноначальності відображає таку специфіку роботи з персоналом в СУІБ як обов'язкове підпорядкування підрозділів із забезпечення інформаційної безпеки одному керівнику, при чому це, як правило, безпосереднє підпорядкування директору або його заступнику, що відповідає за питання безпеки. Побудова менеджменту персоналу на основі принципів соціального партнерства та демократизму створює міцні передумови для формування «фірмового» патріотизму та відданості працівників підприємства.

Рис. 1. Принципи менеджменту персоналу у системі УІБ підприємства.

Для системи менеджменту персоналу підприємства у сфері інформаційної безпеки характерні також спеціальні принципи.

Важливим є дотримання принципу підбору і добору кадрів за спеціальною процедурою, яка передбачає оцінювання претендентів не тільки за діловими і моральними якостями, а і з урахуванням їх професійної та психологічної

придатності для роботи з конфіденційною інформацією.

На думку фахівців-психологів, потенційний співробітник служби інформаційної безпеки чи інших служб, що мають справу з конфіденційними даними, має володіти такими особистими якостями як порядність, чесність, принциповість і сумлінність, старанність, дисциплінованість, емоційна стійкість (самовладання), прагнення до успіху і порядку в роботі. Також претенденту мають бути характерні самоконтроль у вчинках і діях, правильна самооцінка власних можливостей і здібностей, помірна схильність до ризику, вміння зберігати таємниці, тренована увага та хороша пам'ять, здібності до порівняльної оцінки фактів та інше.

Натомість не сприяють збереженню таємниць такі особисті якості: емоційна неврівноваженість, розчарування в собі і своїх здібностях, відчуження від колег по роботі, невдоволення своїм службовим становищем, нечесність, ображене самолюбство, надмірно егоїстична поведінка, недостатня розсудливість, небажання і нездатність захищати інформацію, фінансова безвідповідальність. Негативним фактором є виявлення у претендента ознак вживання наркотиків та алкоголю, що може призвести до балакучості, необдуманих вчинків тощо [1].

Крім використання традиційних засобів (аналіз документів, співбесіда, опитування на службі і осіб, які знають кандидата тощо) для більш повного ознайомлення з особистістю кандидата на зайняття посади у СУІБ підприємство може звернутися до органів внутрішніх справ: довідатися про наявність (відсутність) судимості кандидата й про осіб, що перебувають у розшуку, залучити працівників приватних детективних агентств для збору повних відомостей про кандидата. Така практика широко застосовується у США [9].

Можливим є також перевірка на поліграфі, хоча проведення такого тестування пов’язано з певними складнощами. Застосування поліграфа в Україні не узаконено, але й не заборонено. Небезпідставно керуючись даним принципом, керівники багатьох організацій вважають застосування поліграфа цілком виправданим і корисним [4].

Ще одним засобом перевірки працівника є проведення випробувального терміну, під час якого проходить вивчення особистих, моральних і професійних якостей працівника, навчання правилам роботи з конфіденційною інформацією і документами, інструктажі, перевірка знань і за підсумками якого приймається остаточне рішення про працевлаштування.

Варто відзначити, що ускладнені процедури прийому на роботу, пов’язану з володінням конфіденційною інформацією підприємства, дають можливість всебічно оцінити кандидата на посаду. З іншого боку, вони дають можливість керівництву підприємства і самому кандидату оцінити ситуацію і без поспіху прийняти правильне рішення щодо працевлаштування.

Як свідчить практика, тільки вміле поєднання традиційних кадрових процедур і психологічних методів оцінки претендента дозволяє зробити достатньо обґрунтовані висновки про придатність даної особи для заміщення вакантної посади, пов'язаної з володінням конфіденційною інформацією.

Аналогічно ускладненою є процедура звільнення працівників СУІБ, яка включає встановлення причини звільнення і бажано місця передбачуваної роботи

працівника; здачу всіх закріплених за працівником, що звільняється, документів, носіїв конфіденційної інформації, перевірка їх комплектності, повноти та оформлення прийому відповідним актом, здача співробітником пропуску, ключів і печаток; підписання зобов'язання про нерозголошення ним конфіденційних відомостей після звільнення. Не рідко в зобов'язання щодо нерозголошення конфіденційної інформації, яке підписує співробітник, що звільняється, включається попередження, що принаймні протягом року після звільнення з підприємства за його діяльністю буде здійснюватися спостереження.

Ефективним засобом запобігання розголошення фірмових таємниць є укладення угоди про надання співробітником, що звільняється, консультативних послуг підприємству протягом кількох років (переважно терміну дії грифу конфіденційності відомих йому відомостей) з виплатою платні, близької за розмірами до зарплати. Така система діє в США [8].

Обов’язковим є виконання принципу нормативного закріплення обов’язку працівника нерозголошення конфіденційної інформації: включення пункту про нерозголошення конфіденційної інформації підприємства в трудовий договір, правила внутрішнього розпорядку та посадові інструкції працівників, зайнятих у цій сфері. Часто міститься пункт про обов'язки співробітника повідомляти в службу безпеки про всі спроби сторонніх осіб отримати у нього конфіденційну інформацію. В обов'язковому порядку включається пункт про обов'язки співробітника негайно повідомляти безпосередньому керівнику і службі безпеки про втрату носіїв конфіденційної інформації, документів, справ тощо. У заключній частині вказується ступінь відповідальності за розголошення таємниці підприємства або недотримання правил захисту інформації.

Зобов'язання про нерозголошення конфіденційної інформації та збереження таємниці підприємства претендент підписує до того, як йому буде повідомлено склад конфіденційних відомостей, з якими йому доведеться працювати, і порядок захисту цих відомостей. Вважається, що зобов'язання про нерозголошення таємниці підприємства не дають повної гарантії збереження цих відомостей, однак істотно знижують ризик розголошення персоналом цих відомостей, ризик незаконного їх використання, а також число спроб конкурентів впровадити на фірму свою агентуру.

Принцип розподілу обов'язків передбачає такий розподіл ролей і відповідальності, щоб один працівник не міг порушити критично важливий для організації процес, а принцип мінімізації привілеїв - виділення користувачам тільки тих прав доступу, які необхідні їм для виконання службових обов'язків. Призначення цього принципу - зменшити збиток від випадкових або навмисних некоректних дій [11].

У СУІБ підприємства діє принцип персональної відповідальності керівництва і персоналу, оскільки робота з конфіденційними відомостями вимагає з одного боку чіткого визначення категорій інформаційних ресурсів з обмеженим доступом, і з іншого – розмежування відповідальності щодо їхнього використання.

Необхідним є також здійснення жорсткого обліку та контролю за використанням та зберіганням, знищенням працівником конфіденційної

інформації. У разі встановлення фактів невиконання працівниками вимог щодо захисту конфіденційної інформації до них в обов'язковому порядку і своєчасно застосовуються заходи осуду і покарання відповідно до правил внутрішнього трудового розпорядку: оголошення догани, пониження в посаді, позбавлення премії, відсторонення від роботи з конфіденційною інформацією, звільнення.

Засобом реалізації зазначених вище чотирьох принципів розподілу обов'язків та мінімізації привілеїв, персональної відповідальності та контролю діяльності персоналу виступає дозвільна (розмежувальна) система доступу до конфіденційної інформації підприємства, яка є сукупністю правових норм і вимог, що встановлюються керівництвом підприємства з метою забезпечення правомірного ознайомлення та використання працівниками конфіденційних відомостей, необхідних їм для виконання службових обов'язків.

Основними завданнями дозвільної системи є: обмеження і регламентація складу співробітників, функціональні обов'язки яких вимагають знання конфіденційних відомостей та роботи з їх носіями; строгий вибірковий і обгрунтований розподіл документів та інформації між працівниками; забезпечення співробітників всім необхідним для реалізації їхніх службових функцій (документами, справами, базами даних, інформацією, технічними засобами тощо); безперешкодний прохід персоналу в приміщення (режимну зону), до своїх робочих місць; виключення можливості для сторонніх осіб несанкціонованого ознайомлення з конфіденційною інформацією в процесі роботи працівників та безконтрольного використання ними інформації, яка підлягає захисту (колективний контроль за роботою співробітників) [5].

Дозвільна система включає в себе дві складові частини: допуск співробітника до конфіденційної інформації і безпосередній його доступ до конкретних відомостей.

Дослідження показують, що порушення інформаційної безпеки підприємства у 55% відбувається внаслідок помилок персоналу (недостатнього рівня кваліфікації) і тільки у 20% - це цілеспрямовані дії персоналу [3]. З огляду на таку ситуацію необхідним є забезпечення принципу регулярного навчання та підвищення кваліфікації персоналу, задіяного у роботі з конфіденційними даними підприємства, через проведення тренінгів, інструктажів, стажувань з актуальних питань інформаційної безпеки з урахуванням прискореного розвитку IT, технологій захисту інформації, а також протиправних методів нанесення шкоди СУІБ підприємства. Такий підхід зменшує ризики виникнення загроз для інформаційної безпеки підприємства внаслідок некомпетентності персоналу, відсутності навичок та дотримання вимог практичної роботи з конфіденційною інформацією.

Навчання і підвищення кваліфікації персоналу у сфері інформаційної безпеки організовується за кількома основними блоками:

- характер і склад конфіденційної інформації;
- порядок роботи з конфіденційними відомостями і документами;
- структури системи захисту, вимоги і правила захисту конфіденційної інформації, в тому числі інтелектуальної власності;

- потенційні загрози конфіденційним відомостям, канали їх об'єктивного поширення та канали втрати, методи роботи зловмисників;
- способи виявлення і запобігання неправомірним діям інших працівників;
- загальні та спеціальні методи розпізнавання шахрайських дій з боку третіх осіб (партнерів, клієнтів, постачальників тощо);
- колективні й індивідуальні дії в екстрених ситуаціях [12].

Окремим напрямом навчання та підвищення кваліфікації може бути розвиток у персоналу компанії навичок протидії методам т.зв. соціальної інженерії, які мають на меті за допомогою маніпулятивних прийомів спонукати людину виконати певні дії чи розголосити конфіденційну інформацію.

Особливо важливого значення для забезпечення інформаційної безпеки підприємства набуває принцип стимулювання і мотивації працівників, що володіють конфіденційною інформацією, як засобів забезпечення стабільності персоналу і зменшення ризиків витоку інформації обмеженого доступу.

У системі матеріального стимулювання працівників першочерговим стає обґрунтоване й справедливе матеріальне заохочення, участь у доходах підприємства, достатні соціальний захист та медичне страхування. Крім матеріального стимулювання обов’язковим елементом є нематеріальна мотивація, наприклад залучення підлеглих до обговорення поточних питань, а також прийняття стратегічних рішень, справедливе оцінювання досягнутих результатів й відповідне заохочення, просування по службових сходах, підвищення рівня професійної компетентності працівників через навчання та перепідготовку, заохочення ініціативи та творчого підходу до виконання поставлених завдань [7].

Принцип стабільності персоналу (націленість та забезпечення довгострокової роботи працівників на підприємстві) формує орієнтацію працівників на лояльність до організації. Подолання плинності кадрів підвищує ефективність роботи і зменшує ризики витоку конфіденційної інформації підприємства.

Формування лояльності, відданості персоналу є одним із ключових, основоположних завдань менеджменту персоналу у СУІБ. Як показали опитування, серед основних факторів формування лояльності персоналу виділяють такі: матеріальна винагорода, цікава робота, кар’єрне та професійне зростання, репутація компанії та корпоративна культура, умови роботи, психологічна атмосфера в колективі, особистість та поведінка керівника [2]. Отже, фактично дотримання двох попередніх принципів: навчання персоналу як засобу забезпечення його професійного зростання та використання стимулювання та мотивації працівників, - якраз і є передумовою формування відданості персоналу підприємства.

Однак, для досягнення цього завдання необхідним є також здійснення виховання працівників на основах взаємної довіри, взаєморозуміння і турботи, створення комфортних умови праці та відпочинку, підвищення загального добробуту персоналу, формування сприятливого психологічного клімату в колективі, що створює серйозний бар'єр на шляху будь-якого зловмисника, який намагається отримати конфіденційні відомості підприємства.

Одним із завдань є формування корпоративної культури як системи базових уявлень, цінностей і норм організації, що визначає правила поведінки її

персоналу, діловий стиль, традиції тощо. Саме ці складові корпоративної культури мобілізують внутрішні ресурси, єднають і мотивують персонал, надають зміст його праці і надихають на максимальну самовіддачу [10]. У процесі формування корпоративної культури персоналу прищеплюються стійкі мотиваційні моделі поведінки в тій чи іншій ситуації, пов'язаній із забезпеченням недоступності інформації стороннім особам, уникненням можливості несанкціонованого доступу цих осіб до конфіденційних відомостей.

Загалом процес виховної роботи повинен регулярно відслідковуватися і коригуватися. Основними результатами всієї виховної роботи мають стати: зростання продуктивності праці, прибутку, помітне поліпшення життєвого рівня персоналу, нормалізація психологічного клімату в колективі, поява у працівників почуття фірмової гордості, причетності до спільної справи, зменшення або ліквідація плинності кадрів, зниження негативних наслідків людського фактора в СУІБ, зменшення числа ймовірних порушників вимог інформаційної безпеки серед персоналу підприємства тощо [2].

Висновки та перспективи подальших досліджень. Таким чином, менеджменту персоналу у СУІБ підприємства притаманні такі особливості, пов’язані зі специфікою роботи з відомостями обмеженого доступу та їх захисту: здійснення найму і звільнення кадрів за спеціальною процедурою; дотримання принципу розподілу обов'язків та мінімізації привілеїв; встановлення персональної відповідальності та нормативне закріплення обов’язку нерозголошення конфіденційної інформації; функціонування системи допуску та доступу працівників до інформації обмеженого доступу; впровадження жорсткого обліку та контролю за дотриманням персоналом підприємства вимог інформаційної безпеки; проведення навчання та регулярного підвищення кваліфікації працівників з метою оновлення їхніх умінь та навичок щодо протидії інформаційним загрозам; забезпечення стабільності та формування відданості підприємству з боку його працівників з використанням економічних та морально-психологічних засобів.

У подальших дослідженнях доцільно детальніше проаналізувати особливості роботи з персоналом на окремих його етапах, зокрема основні підходи до добору та відбору кадрів, засоби діагностики морально-психологічних, ділових якостей кандидатів на зайняття посади у СУІБ, засади організації систем стимулювання та мотивації персоналу, навчання та підвищення кваліфікації працівників, що працюють з конфіденційною інформацією тощо.

Список використаних джерел

1. Астахова Л. В. Кадровые уязвимости информационной безопасности организации: методика оценки [Електронний ресурс] / Л. В. Астахова. – Режим доступу : http://cyberleninka.ru/article/n/problema-identifikatsii-i-otsenki-kadrovyh-uyazvimostey-informatsionnoy-bezopasnosti-organizatsii

2. Гаврюшин Е. И. Человеческий фактор в обеспечении безопасности конфиденциальной информации [Електронний ресурс] / Е. И. Гаврюшин. – Режим доступу : http://bre.ru/security/16248.html

3. *Журавель М. М. Проблеми захисту інформації [Електронний ресурс] / М. М. Журавель, С. В. Паршуков. – Режим доступу : http://informatika.udpu.org.ua/?page_id=1173*
4. *Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч.1 / С. В. Кавун, В. В. Носов, О. В. Мажай. – Харків : Вид. ХНЕУ, 2008. – 352 с.*
5. *Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 747 с.*
6. *Основы информационной безопасности: учеб. пособие / А. Н. Данилов, С. А. Данилова, А. А. Зорин. – Пермь : Изд-во Перм. гос. техн. ун-та, 2008. – 556 с.*
7. *Скляренко А.К. Забезпечення виконання персоналом політики інформаційної безпеки [Електронний ресурс] / А. К. Скляренко. – Режим доступу : http://analiz.at.ua/publ/informacija/zakhist_informaciji/zabezpechennja_ vikonannja_personalom_politiki_informacijnoji_bezpeki/3-1-0-34*
8. *Степанов Е. А. Информационная безопасность и защита информации / Е. А. Степанов, И. К. Корнеев. – М . : ИНФРА-М, 2001. - 304 с.*
9. *Столяров Н. С. Зарубежный опыт защиты информации в процессе организации работы с кадрами (на примере США) [Електронний ресурс] / Н. С. Столяров. – Режим доступу : http://bre.ru/security/19485.html*
10. *Тарасова О. В. Корпоративна культура як інструмент ефективного менеджменту підприємства. / О. В. Тарасова, С. С. Марінова // Економіка харчової промисловості. – 2013. – № 3(19). – С. 28–32.*
11. *Хорошко В. О. Основи інформаційної безпеки / В. О.Хорошко, В. С. Чередниченко, М. Є. Шелест. – К.: ДУІКТ, 2008. – 186 с.*
12. *Чумарин И. Г. Укрепление безопасности компании через обучение сотрудников [Електронний ресурс] / И. Г. Чумарин. – Кадры предприятия. – 2004. - № 3. – Режим доступу : http://kapr.ru/articles/2004/10/3558.html*

Мужанова Татьяна. Особенности менеджмента персонала в системе управления информационной безопасностью предприятия. *В статье проанализированы особенности менеджмента персонала в системе управления информационной безопасностью предприятия. Определены основные принципы работы с персоналом, работающим с конфиденциальной информацией предприятия, и основы их практического применения.*

Muzhanova Tetyana. Specificity of personnel management within information security management system of company. *A specificity of personnel management within the information security management system of company is considered in the article. The key principles of personnel management at the information security sphere and its practical applying are analyzed.*