УДК 658:004.056

# ФОРМУВАННЯ СИСТЕМИ ПРОТИДІЇ ЗАГРОЗАМ ВТРАТИ ІНФОРМАЦІЇ

# FORMATION OF A SYSTEM TO COUNTERACT THREATS TO INFORMATION LOSS

**Мозгова Г.В.**
кандидат економічних наук, доцент, доцент кафедри маркетингу та менеджменту зовнішньоекономічної діяльності,
Харківський національний університет імені В.Н. Каразіна

**Сквіра І.О.**
студентка,
Харківський національний університет імені В.Н. Каразіна

*Стаття присвячена теоретико-методичному обґрунтуванню системи протидії загрозам втрати інформації. Визначено основні види загроз інформаційній безпеці на підприємстві. Виділено категорії інформації, яка не підлягає розголошенню. Обґрунтовані основні напрями захисту інформації. Встановлено, що використання сучасних інформаційних систем є одним з інструментів інформаційної безпеки підприємства, оскільки вони дозволяють зберегти від втрачання важливий інформаційний ресурс – корпоративні знання.*

***Ключові слова:*** *інформаційна безпека, загрози втрати інформації, комерційна таємниця, захист інформації, збереження інформаційних ресурсів.*

*Статья посвящена теоретико-методическому обоснованию системы противодействия угрозам потери информации. Определены основные виды угроз информационной безопасности на предприятии. Выделены категории информации, не подлежащей разглашению. Обоснованы основные направления защиты информации. Установлено, что использование современных информационных систем является одним из инструментов информационной безопасности предприятия, поскольку они позволяют сохранить от потери важный информационный ресурс – корпоративные знания.*

***Ключевые слова:*** *информационная безопасность, угрозы потери информации, коммерческая тайна, защита информации, сохранность информационных ресурсов.*

*The article is devoted to the theoretical and methodological justification of the system for countering threats to information loss. Identified the main types of threats to information security in the enterprise. Identified the categories of information that can not be divulged. Substantiated the main directions of information protection. It is established that the use of modern information systems is one of the tools of information security of the enterprise, since they allow saving from loss an important information resource – corporate knowledge.*

***Keywords:*** *information security, threats of loss of information, trade secrets, information protection, safety of information resources.*

**Постановка проблеми.** Інформація є активним елементом відтворювальних відносин і капіталом підприємства, здатним приносити дохід і забезпечувати ефективний результат на макро- і мікрорівнях. Як капітал підприємства, що приносить йому доход, інформаційно-ресурсний потенціал вміщений у загальну систему економічного аналізу й управління, а значить повинен мати систематичну фінансово-управлінську підтримку для оновлення, поповнення, оцінки корисності [1, с. 17]. Крім того, постає проблема захисту конфіденційної інформації, попередження її витоку, захисту програмних продуктів із метою забезпечення стабільного функціонування та динамічного розвитку підприємства. Це призводить до необхідності формування та підтримки системи протидії загрозам втрати інформації.

**Аналіз останніх досліджень і публікацій.** Питанню безпеки інформації присвячено багато робіт вітчизняних та зарубіжних учених. Серед них В. Бузмаков, В. Домарева, Т. Замкова, М. Зубок, Б. Кормич, А. Корченко, В. Лужецький, А. Литвинюк, Л. Маккарті, А. Печенюк, О. Степанова, А. Шумський, В. Фурашев, В. Цимбалюк та інші. Проте разом із швидким розвитком інформаційних технологій отримання, обробки, збереження, передачі інформації, з'являються і

нові загрози втрати інформаційного капіталу, що потребують подальшого дослідження та визначення інструментів захисту інформації.

**Метою статті** є теоретико-методичне обґрунтування системи протидії загрозам втрати інформації: визначення основних видів загроз інформаційної безпеки на підприємстві, встановлення інформації, яка не підлягає розголошенню і на цій основі формулювання основних напрямів захисту інформації.

**Виклад основного матеріалу дослідження.** У сучасному українському турбулентному ринковому середовищі, в умовах нестачі матеріальних ресурсів, головними факторами розвитку підприємств стають люди зі своїми знаннями та здібностями приймати рішення, технології, що дають можливість ефективно керувати діяльністю підприємств та процеси, які є набором взаємопов'язаних дій, що перетворюються на результат. Усі ці фактори реалізують свій ресурсний потенціал через інформацію.

Інформація як ресурс не замикається безпосереднім процесом виробництва. Переплетення і з'єднання потоків інформації не просто супроводжують, а спрямовують і координують рух ресурсів і продуктів, тобто є направляючим чинником у процесі управління [1, с. 8]. Тому від унікальності інформаційного ресурсу залежить рівень конкурентоспроможності підприємства. Це призводить до необхідності формування системи протидії загрозам втрати інформації.

У результаті дослідження інформації як ресурсу і капіталу підприємства, загроз її втрати та сучасних технологій формування та збереження, було запропоновано дві складові системи протидії загрозам втрати інформації:

1. Підсистема безпеки інформації – є відповіддю на зростання бажання конкурентів отримати цінний інформаційний ресурс, тобто є системою захисту інформації від зловмисників.

2. Підсистема збереження інформації – визначається наявністю в компанії неформалізованого, але дуже цінного інформаційного ресурсу у вигляді знання та досвіду працівників компанії, які можна втратити в разі звільнення фахівця, а також корпоративної інформації, яка отримується в процесі життєдіяльності компанії та може бути втрачена за умов відсутності систематичного підходу до її оновлення та збереження. Тобто є системою формування корпоративного знання.

У межах нашого дослідження ці дві підсистеми будуть проаналізовані окремо.

Безпека інформації – це стан збереження і захищеності інформаційних ресурсів, і процес при якому забезпечуються їх конфіденційність, доступність і цілісність. Безпека інформації на підприємстві – це сукупність заходів, що забезпечує безпеку даних клієнтів і співробітників, важливих електронних документів і комерційних таємниць [2]. Поширені види загроз інформаційної безпеки на підприємстві представлені в таблиці 1.

Аналіз інформації, представлений у таблиці 1, показує, що зовнішні загрози, як правило, визначені діями зловмисника, який шукає уразливості в інформаційній структурі, що можуть дати йому доступ до сховищ даних підприємства, ключових вузлів внутрішньої мережі, локальних комп'ютерів співробітників. При цьому зловмисник може користуватися таким інструментом, як шкідливе програмне забезпечення (віруси, трояни, комп'ютерні хробаки). Це призводить до необхідності використання підприємствами спеціально розроблених програми для захисту інформації. Тобто повинна

Таблиця 1

**Види загроз інформаційній безпеці на підприємстві**

| Зовнішні загрози | Внутрішні загрози |
|---|---|
| Використання вірусів для розвалу програмних операцій | Крадіжка і продаж конфіденційної інформації |
| Фізичне виведення з ладу комп'ютера або ліквідація встановленого програмного забезпечення | Кримінальні дії з використанням інфраструктури роботодавця |
| Заборона або блокування роботи користувачів системи програмними засобами | Поширення інформації обмеженого доступу |
| Виявлення, перехоплення і крадіжка секретних кодів і паролів | Без офіційного дозволу комунікації з пресою та конкурентами |
| Використання чутливості компонентів для злому програмного захисту з метою отримання несанкціонованих прав читання, копіювання, зміни та знищення інформаційних ресурсів, а також порушення прав їх доступності | Змови з метою отримання додаткової грошової винагороди |
| | Крадіжка інформаційних або матеріальних активів роботодавця |
| | Нелояльна поведінка співробітників |
| Прослуховування каналів передачі даних | Зловживання доступом співробітниками |
| Розвідувальна діяльність конкурентів | |
| Неправильна політика фірми в галузі безпеки | |

*Джерело: складено за [2–5]*

бути впроваджена система безпеки інформації, яка буде спрямована на усунення зовнішніх загроз.

До внутрішніх загроз належать будь-які дії з інформацією, які можуть бути ініційовані співробітниками підприємства або іншими особами, що мають законний доступ до інформаційної системи. Самі співробітники також можуть передавати інформацію головним конкурентам. Тому на підприємстві на всіх рівнях важливо правильно організувати і впровадити систему менеджменту безпеки інформації.

Аналіз сучасного менеджменту безпеки інформації на українських підприємствах показав, що ще багато керівників не вважають за необхідне турбуватися про можливий витік інформації. Однією з причин є існування думки, що важливої інформації на підприємстві немає. Але це є помилкою, оскільки навіть процес переговорів із клієнтами повинен супроводжуватися заходами з захисту інформації. Другою поширеною помилкою є підхід крайньої інформаційної закритості підприємства. Це теж може призводити до негативних наслідків, адже брак достатньої відкритої інформації про підприємство може призвести до падіння довіри з боку клієнтів.

Такі помилки в менеджменту безпеки інформації спричинені, зокрема тим, що не має чіткої уяви з боку керівництва підприємств, що таке конфіденційна інформація, яка інформація справді повинна не підлягати розголошенню.

Конфіденційна інформація – це інформація, доступ до якої здійснюється строго обмеженим і відомим колом осіб з умовою, що інформація не буде передана третім особам без згоди власника інформації. У цій статті в категорію конфіденційної інформації містить інформацію, що підпадає під визначення комерційної таємниці.

Комерційна таємниця – режим конфіденційності інформації, що дозволяє її власникові при наявних обставинах збільшити доходи, уникнути невиправданих витрат, зберегти положення на ринку товарів і послуг або отримати іншу комерційну вигоду [4]. Під комерційною таємницею підприємства розуміють відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, розголошення або витік яких може завдати шкоди його інтересам. Інформація, яка не підлягає розголошенню на підприємстві, систематизована в таблиці 2.

Підприємство може забезпечити юридичний захист своєї інформації, що становлять комерційну цінність тільки в разі встановлення на підприємстві режиму комерційної таємниці та проведення всіх необхідних заходів щодо забезпечення захисту інформації. Якщо такий режим не введений, то це означає, що компанія не зробила необхідних дій для захисту власних секретів і не може претендувати на юридичний захист власних інтересів із боку держави.

Також останнім часом згадки про витік інформації з самих різних комерційних та некомер-

Таблиця 2

**Інформація, яка не підлягає розголошенню на підприємстві**

| Види інформації | Характеристика |
|---|---|
| Загальна інформація | Документи про комерційні переговори. |
| | Зведені звіти по фінансовій діяльності підприємства. |
| | Методи ціноутворення. |
| | Відомості про організацію праці та про добір працівників. |
| | Інформація про умови зберігання документів. |
| | Документи, пов'язані з маркетинговими дослідженнями. |
| | Бізнес-плани розвитку організації. |
| | Відомості про контракти підприємства: кредитні договори з банками; договори купівлі і продажу. |
| | Інформація про постачальників і клієнтів. |
| | Аналітичні дані про ринок. |
| | Інформація про перспективне географічне положення просування продукції підприємства. |
| | Заходи, які використовують конкуренти щодо своїх супротивників. |
| | Інформація про місце зберігання вантажів, часу і маршрутах їх перевезення. |
| Інформація особистого характеру | Розклад і адреси зустрічей – ділових і особистих. |
| | Інформація про людські слабкості. |
| | Дані про друзів, подруг, місцях проведення дозвілля, способи і маршрутах пересування. |
| | Інформація про цінності. |
| | Проблеми в родині. |

*Джерело: складено за [4; 5]*

ційних організацій у новинах стають фактично щоденними. У зв'язку із зростанням таких випадків зростає інтерес до систем, які могли б запобігти подібного роду інцидентам.

Загрозам інформаційної безпеки, які визначені в статті, можна протистояти за допомогою спеціальних заходів. Основні напрями захисту безпеки інформації на підприємстві представлено в таблиці 3.

Підсистема збереження інформації повинна формуватися виходячи з визначення інформаційних ресурсів підприємства.

Таблиця 3

**Основні напрями захисту безпеки інформації на підприємстві**

| Напрям | Опис загрози | Інструменти подолання загроз |
|---|---|---|
| Контроль і захист робочих місць | У будь-якій організації співробітники використовують для роботи безліч пристроїв – стаціонарні комп'ютери, ноутбуки. | Захист усіх робочих пристроїв.<br>Контроль робочих місць.<br>Контроль або заборона використання зйомних пристроїв.<br>Безпека доступу до Інтернету.<br>Шифрування інформації, яка зберігається на пристроях.<br>Контроль програм, які використовують. |
| Захист від цільових атак | Цілеспрямована атака завжди призначена для заподіяння шкоди конкретній організації. Викрадення або маніпуляції з даними, порушення бізнес-процесів. | Перешкоджання – посилення системи безпеки, підвищення інформованості співробітників про чинні загрози.<br>Виявлення вразливостей у системі безпеки і спроб проникнення в мережу.<br>Негайна реакція на атаку і зменшення пов'язаної з нею шкоди.<br>Прогнозування – оцінка ризиків для безпеки в поточній діяльності. |
| Захист центрів обробки даних | В організації може використовуватися приватний або комерційний центр обробки даних. Постає завдання щодо забезпечення безпеки і цілісності інформації, що зберігається в ньому. | Захист для найбільш поширених програм, які одночасно виконують кілька операційних систем на одному і тому ж комп'ютері.<br>Захист різних систем зберігання корпоративного рівня без зниження швидкості доступу. |
| Захист віртуальних засобів | Технології віртуалізації підвищують ефективність і продуктивність. Віртуалізація охоплює все більше ділянок бази, тому віртуальне середовище стає складніше. | Встановлення захисного програмного забезпечення на віртуальному пристрої – це забезпечить захист всіх віртуальних машин, що працюють на ньому. |
| Захист мобільного та онлайн-банкінгу | Клієнти все більше здійснюють банківські операції, використо-вуючи комп'ютер або телефон. Вони деколи поводяться легковажно щодо безпеки їх комп'ютерів і мобільних пристроїв. | Встановлення програми, яка блокує доступ до онлайн-систем клієнтів банку, у яких заражений пристрій. |
| Безпека мобільних пристроїв | Кіберзлочинці все частіше атакують мобільні пристрої, які легко втратити. Зловмисники можуть дістати несанкціонований доступ до корпоративних систем і даним. | Захист мобільних пристроїв – технології мобільної безпеки забезпечують багаторівневий захист від новітніх загроз.<br>Управління мобільними пристроями – управління функціями мобільного пристрою, дозволяє віддалено управляти пристроєм у разі його зникнення. |
| Експертиза в галузі кібербезпеки | Постійно з'являються нові складні загрози, прийоми для обходу існуючих технологій захисту. Фахівці з інформаційної безпеки повинні знати передові методи захисту, які лежать в основі ефективної корпоративної стратегії протидії кіберзагрозам. | Тренінги й онлайн-навчання, яке містить: тестування на проникнення, аналіз захищеності додатків дозволяє виявити уразливості в них будь-якого типу, розслідування інцидентів та аналіз шкідливого програмного забезпечення дозволяють відтворити детальну картину інциденту інформаційної безпеки. |
| Упровадження технічних засобів захисту інформації | Можливість витоку інформації з основних каналів. | Електромагнітні засоби – установка спеціального обладнання для запобігання знімання індуктивних наводок.<br>Віброакустичні засоби – захист приміщень від прослуховування всіма засобами віброакустичного знімання інформації. |

*Джерело: складено за [3; 5; 6]*

Інформаційні ресурси можна охарактеризувати, як весь наявний обсяг інформації в інформаційній системі [7]. Вони складаються з внутрішньої та зовнішньої інформації. До внутрішньої належить інформація про: співробітників підприємства, асортимент продукції, витрати, технологічні процеси, техніку продажу, методи розподілу продукції. До зовнішньої належить інформація про: ситуацію на внутрішньому і міжнародному ринку, наявних і потенційних конкурентів, тенденції розвитку в діловому середовищі країни, покупців, попит, потреби клієнтів, зміни в законодавстві.

Основними завдання формування і розвитку інформаційних ресурсів є:

– підвищення якості одержуваної інформації з мікро- та макросередовища;

– підвищення швидкості обробки і надання інформації, необхідної для прийняття рішень на всіх рівнях управління;

– підвищення якості бази корпоративного знання.

Знання – це форма існування результатів пізнавальної діяльності людини [8]. Структура знання містить у собі: теоретичні знання, емпіричні та корпоративні. Корпоративні знання характеризуються системою накопичення і передачі технологічної, виробничої, організаційної, функціональної, ділової та іншої інформації серед співробітників із метою розвитку і вдосконалення підприємства. Корпоративні знання формуються з:

– знань бізнес-процесів підприємства: фінансова, юридична документація, навички і досвід персоналу;

– знань корпоративної культури: корпоративні стандарти взаємодії персоналу з клієнтами підприємства в різних ситуаціях;

– навичок застосування інформаційних технологій для автоматизації діяльності підприємства;

– особистих знань співробітників.

Зростаючі об'єми інформації, яка супроводжує процеси розробки, прийняття та реалізації рішень, призводять до необхідності формування підсистеми збереження інформації за допомогою сучасних автоматизованих інформаційних систем. На кожному підприємстві використовують інформаційні системи, які відрізняються за ступенем автоматизації, можливістю задовольнити інформаційні потреби управління підприємством.

Таблиця 4

**Приклади програмних продуктів, які дозволять автоматизувати підсистему збереження інформації**

| Програмний продукт | Характеристика |
|---|---|
| OneDrive для бізнесу | За допомогою цього продукту кожен відділ може створювати свої окремі захищені сховища в хмарному сервісі OneDrive, де зберігаються всі документи, презентації, фото і відео файли, і всі, кому це потрібно, мають доступ до сховища з будь-якого місця і пристрою. Є можливість не переписувати інформацію з ноутбука на флешку, з флешки на ноутбук, а просто викладати все на OneDrive, переглядати і редагувати ці файли вдома, на зустрічі з клієнтом або у відрядженні. |
| SharePoint | Використовується для зберігання процесів і знань. На її базі може функціонувати «бібліотека підприємства», а також система дистанційного навчання персоналу. SharePoint має зручний інтерфейс і юзабіліті, надає широкі можливості для роботи і зберігання всієї необхідної документації.<br>У бібліотеці зберігається вся документація (положення, процедури). Система дозволяє зберігання кожної редакції документа, роботу відразу декількох користувачів над редагування змісту. |
| Cobra++ | Об'єднує можливості документообігу та переваги технології workflow для інформаційної підтримки корпоративних систем управління підприємством. Ключовим елементами системи є інформаційна підсистема, що дозволяє швидко і якісно створювати інформаційні ресурси. Має такі підсистеми: моделювання та управління бізнес-процесами; формування потоку завдань на кожному робочому місці підприємства; обміну даними з іншими системами; аналізу накопичених даних, забезпечення спільної роботи співробітників підприємства за встановленим регламентом. |
| Microsoft Dynamics CRM | Характеризується поєднанням додатків, необхідних для ефективного ведення бізнесу з ядром у вигляді CRM-системи. Дозволяє управляти сервісом, продажами, соціальними мережами та маркетингом. Управління сервісом представляє механізм автоматизованого обслуговування клієнтів, який містить у собі управління черговістю обробки запитів, планування необхідних ресурсів, а також формування ресурсу у вигляді бази знань. Microsoft Dynamics CRM забезпечує менеджерів із продажу швидким доступом до потрібних даних у режимах онлайн і оффлайн, тому вони можуть працювати ефективніше. |

*Джерело: розроблено за [8–12]*

У таблиці 4 приведено приклади програмних продуктів, які дозволять автоматизувати підсистему збереження інформації та надана їх коротка характеристика.

Застосування будь-якого програмного продукту надає такі можливості у збереженні та відновленні інформації:

– єдина точка входу – співробітник завжди знає, де знайти необхідну інформацію, зручний інтерфейс, мінімум витрат часу;

– підвищення знань співробітників із продуктів, процесів, документообігу;

– підвищення ефективності процесів продажів у режимі онлайн;

– підвищення рівня залученості і задоволення співробітників;

– внутрішня соціальна мережа, яка допомагає співробітникам спілкуватися, ділитися інформацією та ідеями.

**Висновки.** Отже, інформаційна безпека підприємства є складною проблемою, яка вимагає сучасних рішень. Можна стверджувати, що для успішного функціонування підприємства питання формування системи протидії загрозам втрати інформації повинно вирішуватися вже на стадії створення компанії.

Оптимальною формою побудови системи протидії загрозам втрати інформації може стати система, яка має дві складові: підсистему безпеки інформації та підсистему збереження інформації, що передбачає визначення основних видів загроз інформаційній безпеці на підприємстві, встановлення категорії інформації, яка не підлягає розголошенню, впровадження організаційних та технічних інструментів подолання загроз, використання сучасних інформаційних систем.

**БІБЛІОГРАФІЧНИЙ СПИСОК:**

1. Мозгова Г. Регулювання інформаційного середовища маркетингу : автореф. дис. на здобуття наук. ступеня к. е. н. : спец. 08.02.03 «Організація управління, планування і регулювання економікою» / Г. Мозгова. – Харків, 2006. – 19 с.

2. Батюк А. Інформаційні системи в менеджменті : підручник / А. Батюк, З. Двуліт, К. Обельовська, І. Огороднік, Л. Фабрі. – Львів : Інтелект-Захід, 2004. – С. 343–384.

3. Біленчук П. Комп'ютерна злочинність : навчальний посібник / П. Біленчук, Б. Романюк, В. Цимбалюк. – Київ : Атіка, 2002. – 240 с.

4. Зубок М. Безпека банківської діяльності : навчальний посібник / М. Зубок. – К. : КНЕУ, 2002. – 190 с.

5. Кормич Б. Інформаційна безпека : організаційно-правові основи : навчальний посібник / Б. Кормич. – К. : Кондор, 2005. – 382 с.

6. Лужецький В. Інформаційна безпека : навчальний посібник / В. Лужецький, О. Войнович, А. Дудатьєв. – Вінниця : Універсум-Вінниця, 2009. – 240 с.

7. Новаківський І. Інформаційні системи в менеджменті : системний підхід : навчальний посібник / І. Новаківський, І. Грибик, Т. Федак. – Львів : Видавництво «Національний університет Львівська політехніка», 2010. – 202 с.

8. Зацихайло Д. Корпоративне управління : навчальний посібник / Д. Зацихайло, О. Кібенко, Г. Назарова. – Х. : Ескада, 2003. – 688 с.

9. Програмний продукт OneDrive для бізнесу [Електронний ресурс]. – Режим доступу : https://onedrive.live.com.

10. Програмний продукт SharePoint інструменти для командної роботи [Електронний ресурс]. – Режим доступу : https://products.office.com/ru-ru/sharepoint/collaboration.

11. Програмний продукт Cobra++ [Електронний ресурс]. – Режим доступу : http://www.scregul.ru/.

12. Програмний продукт FreshOffice [Електронний ресурс]. – Режим доступу : http://www.freshoffice.ru/.

13. Програмний продукт Microsoft Dynamics CRM [Електронний ресурс]. – Режим доступу : http://crm.ua/.