УДК: 519.876.5
DOI: 10.36919/2312-7812.4.2022.61

В.В. Синявський

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Наприкінці минулого століття величезні зміни відбулися у всіх сферах та галузях економіки та науки, освіти та культури, нових технологій та інформаційних структур. Суспільство отримало назву інформаційного і даний термін, поряд з терміном інформатизація, отримав широке застосування, як серед професіоналів у галузі інформаційних технологій, так і фахівців інших напрямів. У інформаційному суспільстві щодня здійснюються всі види діяльності та накопичується інформація та дані, які вимагають захисту, оскільки саме дані визначають напрям та успіх професійної діяльності, як і багатьох інших аспекти життя.

Сучасна інформатизація суспільства та прискорення потоків інформації ведуть до появи нових способів обміну інформацією. Виникають загрози втрати важливої інформації та інформаційні атаки відбиваються на конкурентоспроможності та потребують удосконалення методів управління інформаційною безпекою в організаціях. На сучасному рівні інформаційна безпека характеризується переходом від традиційного розгляду захисту інформації з погляду техніки та технологій до широкого розуміння проблеми та впровадження. нових заходів.

Описуючи методи управління, підкреслено поступовість і поетапність впровадження політики інформаційної безпеки в організації.

Запропонований комплекс методів управління (адміністративні, інженерно-технічні, правові, теоретичні, економічні та соціально-психологічні) знаходиться в постійній динамічній рівновазі, де кожен компонент органічно доповнює інший і ігнорування одного з методів може призвести до втрати важливої інформації та негативно вплинути на конкурентоспроможність організації.

У статті розглянуто проблему захисту інформації в інформаційних системах організацій в умовах обмеженості наявних ресурсів. Показано, що традиційні моделі управління інформаційною безпекою не враховують зростальної кількості сучасних кіберзагроз, а також ризиків досягнення цілей. Запропоновано комплексну модель управління інформаційною безпекою та обґрунтовано необхідність її впровадження в організації. Сформульовано пропозиції щодо вдосконалення стратегічного управління інформаційною безпекою промислових організацій.

At the end of the last century, huge changes took place in all spheres and branches of economy and science, education and culture, new technologies and information structures. The society received the name information society and this term, along with the term informatization, was widely used both among professionals in the field of information technologies and specialists in other areas. In the information society, all kinds of activities are carried out every day and information and data are accumulated that require protection, since it is data that determines the direction and success of professional activity, as well as many other aspects of life.

Modern informatization of society and acceleration of information flows lead to the emergence of new ways of exchanging information. There are threats of loss of important information and information attacks affect competitiveness and require improvement of information security management methods in organizations. At the modern level, information security is characterized by a transition from the traditional consideration of information protection from the point of view of equipment and technologies to a broad understanding of the problem and implementation. new measures.

Describing the management methods, the gradual and phased implementation of the information security policy in the organization is emphasized.

The proposed complex of management methods (administrative, engineering-technical, legal, theoretical, economic and socio-psychological) is in a constant dynamic balance, where each component organically complements the other and ignoring one of the methods can lead to the loss of important information and negatively affect the competitiveness of the organization .

The article examines the problem of information protection in information systems of organizations in conditions of limited available resources. It is shown that traditional models of information security management do not take into account the growing number of modern cyber threats, as well as the risks of achieving goals. A comprehensive information security management model is proposed and the need for its implementation in the organization is substantiated. Proposals for improving the strategic management of information security of industrial organizations have been formulated.

Ключові слова: інформаційна безпека, інформаційна система, захист інформації, ділова репутація організації, кіберзагрози, інфраструктура організації, рівні захисту даних, внутрішнє середовище організації, зовнішнє середовище організації, управління інформаційною безпекою, модель управління інформаційною безпекою.

Keywords: information security, information system, information protection, business reputation of the organization, cyber threats, infrastructure of the organization, levels of data protection, internal environment of the organization, external environment of the organization, information security management, information security management model

Постановка проблеми. Система управління інформаційною безпекою спрямована на мінімізацію ризиків витоку інформації на підприємстві, а також на стале функціонування інформаційної структури підприємства.

Загроза захисту інформації зробила засоби забезпечення інформаційної безпеки однієї з обов›язкових показників інформаційної політики будь-якої компанії. Іншими словами, питання захисту інформації вирішуються для того, щоб ізолювати нормально що функціонує інформаційну систему від несанкціонованих керуючих впливів та доступу сторонніх осіб або програм до даних із метою розкрадання інформації Нехтування процесами управління інформаційними ризиками може спричинити втрату підприємством нематеріальних активів, що призведе до дестабілізації фінансового стану підприємства та неможливості підтримання ним власної конкурентоспроможності у майбутньому.

Аналіз останніх досліджень та публікацій. Вивченням питання інформаційної безпеки підприємства зймалися такі вчені, як: Абрамчук М., Богуш В, Герасименко А., Гуцу С., Деркач М., Дячков Д., Живко З., Захаркін О. та ін. Проте залишаються дискусійними питання сутнісних і змістовних характеристик інформаційної безпеки підприємств; не визначені підходи до її складових; не розроблено наукового положення щодо управління інформаційною безпекою підприємств в сучасних умовах господарювання.

Мета дослідження. Обґрунтування необхідності формування механізму управління інформаційними ризиками підприємства в процесі глобальних викликів сучасності.

Виклад основних матеріалів досліджень. Жодна система не може існувати без інформаційних потоків, порушення або їх недостатність призводить до збоїв та втрат в ефективності та рентабельності, зниження динаміки розвитку. Інформація є найважливішою складовою будь-якої економічної системи.

Стрімке зростання обсягів інформації, пов›язане з новим етапом науково-технічного прогресу, різким економічним наростанням конкуренції сприяли необхідності забезпечення інформаційної безпеки. Забезпечення інформаційною безпекою містить заходи щодо захисту процесів створення даних, їх введення, обробки, виведення та зберігання [3].

Інформація — найважливіший економічний ресурс кожної організації, без якого неможливий соціальний, економічний, технічний, технологічний, інтелектуальний та інший розвиток. Невід›ємною частиною здійснення програм співробітництва виступають територіальні комп›ютерні мережі: глобальні, локальні (регіональні, муніципальні, корпоративні), поява яких зумовлена досягненнями науково-технічного прогресу і пояснюється науковими потребами обміну інформацією для підвищення ефективності менеджменту [2]. Бо менеджмент має справу з економічними системами, то як правило, така взаємодія відбувається в рамках організації - стабільної формальної соціальної структури, яка отримує економічні ресурси із зовнішнього світу, що переробляє їх у готову продукцію або послуги з метою задоволення потреб фізичних або (і) юридичних осіб та отримання максимально можливого прибутку. В організації формуються дані, інформація, знання, утворюючи інформаційну піраміду менеджменту організації.

Представимо на рис. 1 підходи до визначення поняття «інформаційна безпека».

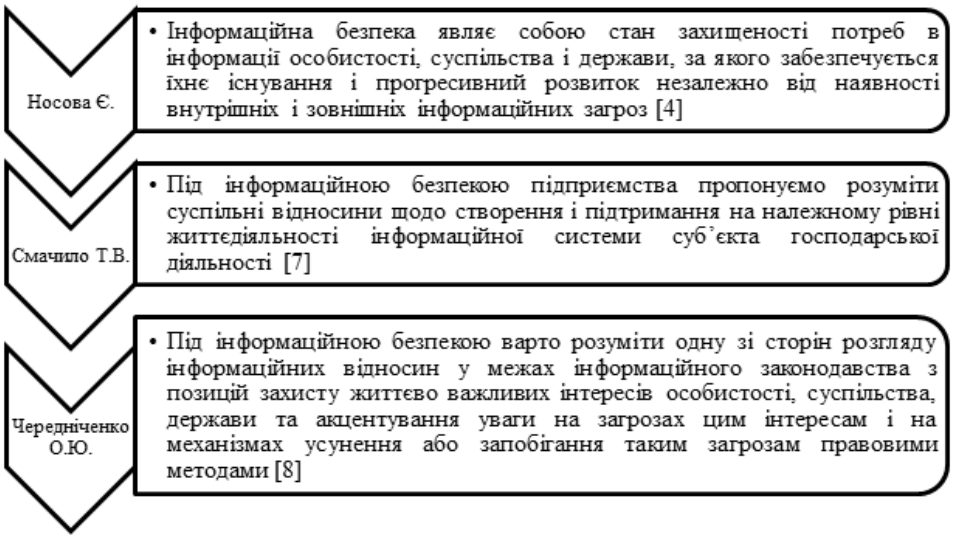

Рис.1. Підходи до визначення поняття «інформаційна безпека»
Джерело: узагальнено автором

Поняття «інформаційна безпека» слід розглядати як стан захищеності систем обробки та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення [6].

Управління інформаційною безпекою описує набір способів та процедурних засобів контролю, які ІТ та бізнес-організації впроваджують для захисту своїх інформаційних активів від загроз та ризиків. Відповідальність за інформаційну безпеку може бути покладена на директора з безпеки, головного технічного директора або керівника ІТ-операцій, до команди якого входять оператори ІТ та аналітики з безпеки. Незалежно від того, чи зберігаються ці дані у цифровому або фізичному форматі, процес управління інформаційною безпекою має вирішальне значення для захисту даних від несанкціонованого доступу чи крадіжки [3].

До основних інформаційних активів, якими може володіти організація, належать:

- стратегічна документація, що розробляється підприємством та документує довгострокові стратегічні та короткострокові тактичні цілі, які визначають цілі та бачення майбутнього. Ці цінні внутрішні документи містять секретну інформацію, до якої конкуренти захочуть отримати доступ;
- інформація про продукти (послуги) - критично важлива інформація, яка має бути захищена за допомогою управління інформаційною безпекою;
- інтелектуальна власність (патенти). Якщо компанія створює інтелектуальну власність, у тому числі розробляє програмне забезпечення, то можуть знадобитися засоби контролю інформаційної безпеки для її захисту, оскільки конкуренти можуть захотіти вкрасти вихідний код та використовувати його для перепроєктування продукту з метою конкуренції. У деяких країнах закони про авторське право або інтелектуальної власності не дотримуються, тим самим організації позбавляються засобів правового захисту;
- власні знання (комерційні секрети) - кожна організація генерує власні знання в процесі ведення бізнесу. Комерційні секрети — це унікальні ідеї, які дають бізнесу конкурентну перевагу;
- поточна проєктна документація складається із задокументованих деталей продуктів чи послуг, які перебувають у процесі запуску. Якщо конкуренти організації дізнаються, чим вона займається, вони можуть спробувати випустити конкурентний продукт швидше, ніж очікувалося, і навіть можуть порівняти його з новим продуктом, щоб витіснити організацію з ринку [8];
- дані про співробітників - відділи кадрів збирають та зберігають дані про всіх співробітників, включаючи огляди продуктивності, історію зайнятості, заробітну плату та іншу інформацію. Ці записи можуть містити конфіденційну інформацію, яку зловмисник може використовувати для шантажу працівників організації. Конкуруюча організація може використовувати ці дані для переманювання працівників
- конфіденційно представлені дані клієнтів, коли нездатність захистити дані від крадіжки спричинить втрату довіри ряду клієнтів, а в деяких випадках порушенням стандартів інформаційної безпеки чи законодавства.
- Інформаційна безпека на рівні організації зосереджена навколо тріади: конфіденційність, цілісність та доступність (рис. 2).

Конфіденційність. Збереження конфіденційності інформації означає, що тільки уповноважені особи можуть отримувати доступ до даних або змінювати їх. Для даних з підвищеним ризиком можуть бути реалізовані додаткові заходи для контролю конфіденційності.

Рис.2. Складові інформаційної безпеки підприємства
*Складено на основі наукових джерел [7]

Цілісність - управління інформаційною безпекою має справу з цілісністю даних шляхом впровадження засобів управління, які забезпечують узгодженість та точність збережених даних протягом всього їхнього життєвого циклу. Щоб дані вважалися безпечними, організація повинна гарантувати, що вони правильно зберігаються та не можуть бути змінені чи видалені без відповідних дозволів. Для підтримки цілісності даних можуть бути реалізовані такі заходи, як контроль доступу користувачів [1].

Доступність – управління інформаційною безпекою має справу з доступністю даних шляхом впровадження процесів та процедур, які забезпечують доступність важливої інформації для авторизованих користувачів за потреби.

Типові дії включають обслуговування та ремонт обладнання, встановлення виправлень та оновлень, а також реалізацію процесів реагування на інциденти та аварійного відновлення для запобігання втраті даних у разі кібератаки.

Загрози інформаційній безпеці можуть бути класифіковані за різними ознаками (рис. 3):

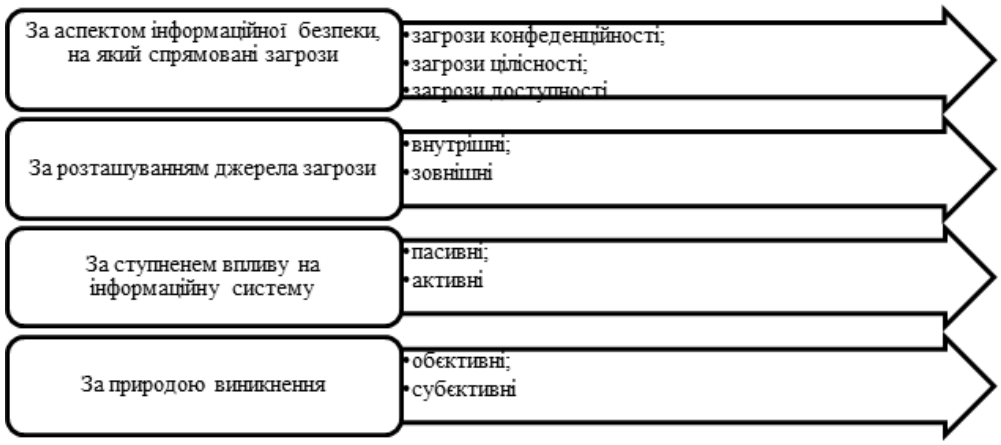

Рис.3. Класифікація загроз інформаційної безпеки підприємства
*Складено на основі наукових джерел [3, 4]

Існує великий спектр дій, що застосовуються для захисту інформації від вищезазначених загроз. Проте слід зазначити, що засоби захисту мають бути застосовані

комплексно. Для цього використовується комплексна система управління інформаційною безпекою, за якою інформаційна безпека являє собою необхідний рух потоку інформації, призначений для надання певного рівня функціонування систем.

Можна перерахувати кілька підходів до управління інформаційною безпекою: організаційний, кібернетичний, процесний, теорія ухвалення рішень, оптимізаційний.

Під організаційним методом управління розуміють систему внутрішнього документообігу, відповідно до напряму діяльності підприємства. У кібернетичному підході описується застосування моделі чорної скриньки, що являє собою процес роботи системи у зовнішньому середовищі [1].

За допомогою теорії прийняття рішень можна розробити систему ухвалення рішень. Результатом застосування процесного підходу є надання безперервної роботи, комплексного функціонування управлінських процесів. Оптимізаційний підхід служить для коригування застосовуваних процесів управління інформаційною безпекою, головною метою якої є ефективне керування.

Сучасні системи управління вирішують певні завдання, комплексні. На якість роботи систем управління позитивно впливають проведення аудитів та планування стратегії розвитку компанії.

Важливими складовими досягнення та оцінки конфіденційності, цілісності та доступності інформації є облік змін, їх оцінка, класифікація ризикових подій, мінливість системи управління інформаційної безпеки внаслідок зовнішніх і внутрішніх чинників.

Систематизувати всю зібрану інформацію, оцінити поточний стан системи менеджменту інформаційної безпеки та мети організації можна тільки із застосуванням спеціальних методів, результатом використання яких буде вище та грамотне прогнозування очікуваних результатів процесів та керування ними на основі фактів та даних (рис. 4).

Рис.4. Класифікація методів управління інформаційної безпеки підприємства
*Складено на основі наукових джерел [2]

Організаційні методи — це група методів, що включає аспекти, які ґрунтуються на принципі відповідальності та прихильності керівництва у сфері інформаційної безпеки. Застосування методів включає аналіз вимог до інформаційної безпеки, розробку плану виконання цих вимог, управління та адміністративний контроль [5] над реалізованою системою інформаційної безпеки, визначення цілей та політики розробка стратегії в галузі ІБ та управління ризиками.

Ризикоорієнтовані методи - група методів, спрямованих на координацію діяльності з управління та контролю за організацією щодо ризиків. Методи містять основні підходи до оцінки ризиків та способи управління ними з урахуванням напряму діяльності організації та її організаційної структури.

Технічні методи містять різні практики управління інформаційною безпекою (засоби управління) для досягнення цілей управління у разі виникнення ризику. Захисні заходи дозволяють забезпечити інформаційну безпеку, зменшити вразливості, обмежити вплив інцидентів та полегшити відновлення активів. Технічні методи є інструментарієм для здійснення організаційних та ризикоорієнтованих методів, оскільки мають на увазі комплекс дій, механізмів, які спрямовані на захист інформаційної безпеки технічними способами [4].

Правові методи допомагають підтримувати функціонування системи інформаційної безпеки на основі реалізації правових норм з інформаційної безпеки.

Аналіз інформаційної безпеки здійснювали на прикладі АТ «Київський радіозавод». АТ «Київський радіозавод» здійснює роботи з проєктування та виробництва ліфтів, ескалаторів та ліфтових шахт різної складності, монтажу та модернізації ліфтів, гарантійне та післягарантійне обслуговування ліфтів та ескалаторів власного виробництва [5].

На даний час структура підприємства складається з Керуючого підприємства та 6 підрозділів, які займаються виробництвом готової продукції й наданням послуг промислового і непромислового характеру.

Дана структура надає всім відділам рівною мірою доступ до всієї інформації, що є у базі даних (БД), що призводить до неправильної роботи самої БД, і навіть можливості надання закритої інформації особам, які не повинні мати доступ до неї.

Відповідно можна зробити висновок, що дана схема організації доступу до даних має велику кількість потенційних загроз інформаційної безпеки та для поліпшення захисту даних необхідно розмежувати доступ до даної системи.

Управління безпекою в АТ «Київський радіозавод» є конфліктним процесом. Конфлікти відбуваються через перетин інтересів різних категорій посадових осіб, які працюють з інформаційною системою організації [5].

На підприємстві можна виділити три категорії посадових осіб, які стосуються забезпечення інформаційною безпекою: співробітники підрозділу інформатизації (системні, мережеві адміністратори, адміністратори баз даних тощо); підрозділи захисту інформації (служба безпеки); керівники структурних підрозділів.

Співробітники підрозділу інформатизації обслуговують комунікаційне обладнання, сервери баз даних, встановлені операційні та прикладні системи. Їхнє основне завдання — забезпечення безперебійного функціонування того обладнання та програмного забезпечення, за яке вони відповідають.

Співробітники підрозділу інформатизації мають розширений набір привілеїв для виконання своїх обов›язків та зацікавлені у максимальному полегшенні роботи користувача системи, що зазвичай суперечить положенням політики безпеки організації та інтересам власника інформаційної системи.

Служба безпеки покликана забезпечити надійний захист інформації в організації, незалежно від того, за допомогою якого обладнання та програмного забезпечення вона обробляється. Вони повинні впливати на процес призначення прав доступу співробітників до інформаційних ресурсів, контролювати зміни, що відбуваються в системі та контролювати дії співробітників, які здійснюються в рамках виконання ними службових обов›язків. Інтереси адміністраторів безпеки найповніше відображають інтереси власника системи.

Керівники структурних підрозділів відповідають за рішення функціональних завдань. Саме для цих підрозділів і створюється інформаційна система. Тільки керівник знає, що має робити той чи інший його підлеглий. Однак, зазвичай, ці відомості він може передати службі безпеки тільки в вигляді деяких неформальних побажань, що важко піддаються аналізу та практичній реалізації.

В результаті: фахівці, які володіють засобами управління системою, не знають, які права доступу та привілеї потрібні тому чи іншому співробітнику для виконання своїх функціональних обов›язків.

Водночас співробітники та адміністратори безпеки самостійно не можуть ефективно використовувати захисні можливості системи та забезпечити контроль за станом усієї ІС. А керівники структурних підрозділів не можуть подати свої вимоги адміністратору службі безпеки у формі, що дозволяє однозначно інтерпретувати їх. У такій ситуації застосування будь-яких (у тому числі найсучасніших) засобів управління безпекою не призведе до розв›язання проблеми, оскільки сама проблема криється у неефективності взаємодії різних підрозділів організації між собою.

Вивчення сфери діяльності організації дозволило виявити такі інформаційні активи:

- інформація / дані (проєктна документація організацій, особисті дані клієнтів тощо);
- апаратні засоби (комп›ютери, сховища даних, оргтехніка);
- програмне забезпечення, включаючи прикладні програми (в т.ч. засоби САПР);
- документи у паперовому вигляді (у т.ч. договори, скани проєктів, витяги з державних реєстрів тощо).

Усі активи компанії можна розглянути з позиції цінності та розташувати їх у порядку зростання:

1. системне програмне забезпечення;
2. особисті відомості про співробітників;
3. особисті дані клієнта;
4. проєктна документація, плани комунікацій у т.ч. стратегічного призначення;
5. проєктна документація, отримана від замовника;
6. проєктна документація, розроблена організацією

Таким чином, у компанії виявлено безліч активів, пов›язаних з інформаційними даними.

Відповідно для них можуть бути виділені наступні загрози: дії зловмисників; вихід з ладу апаратного забезпечення (АЗ);нестача ресурсів АЗ; конструктивні недоліки

програмного забезпечення (ПЗ);вихід з ладу ПЗ; нестача ресурсів ПЗ; викрадення під час передачі по лініях зв›язку (ЛЗ); підміна під час передачі по ЛЗ; відмова в обслуговуванні ЛЗ; помилки користувача; розголошення конфіденційної інформації; недбале ставлення до інформаційної безпеки; саботаж; виникнення непереборної сили; обставини непереборної сили.

Загрози інформаційної безпеки підприємства можуть мати природний чи людський чинник, загрози можуть виникнути як випадково, так і навмисно. Для підприємства необхідно і вкрай важливо не пропустити жодної загрози інформаційній безпеці, тому що можливі збитки можуть бути дуже значними, але й наголошувати на незначних загрозах не треба, тому що може бути залучено вкрай багато коштів, а збитків підприємству може бути не завдано.

Після того як виявлено можливе джерело загрози та сектор, схильний до загрози (об›єкт загрози), треба визначити можливість і розміри здійснення загрози. Для цього необхідно врахувати аналітичні дані, такі як: частоту виникнення загрози; мета загрози, використовувані ресурси та можливості здійснення тієї чи іншої загрози; наскільки привабливий ресурс, на який впливає загроза; наскільки можливі виникнення випадкових загроз, пов›язаних з географічним фактором, реалізацією яких може бути природна або техногенна катастрофа. Для проведення аналітики за загрозою, що виникла, необхідно скористатися статистичними даними, якщо такі є.

У АТ «Київський радіозавод» є уразливі інформаційні активи, які потрібно захищати. А для більш правильного вибудовування політики інформаційної безпеки необхідно визначити основні проблеми та завдання захисту інформації на промисловому підприємстві [5].

На підприємстві при роботі з великим обсягом конфіденційних даних стоїть першочергове завдання організації захисту інформації, тобто визначення заходів, спрямованих на створення, забезпечення та підтримку інформаційної безпеки.

Об›єкт захисту інформації являє собою інформацію або інформаційний процес, який вимагає забезпечення захисту від несанкціонованого доступу, порушення цілісності та структурованості даних.

Ефективність захисту інформації дозволяє визначити рівень відповідності результатів використовуваної системи захисту даних поставленим цілям. Виділяють такі основні види захисту інформації:

1. Захист інформації від витоків — це заходи, спрямовані на збереження та цілісність конфіденційних даних, що використовуються у внутрішньому та зовнішньому документообігу підприємства.

2. Захист даних від розголошень - це заходи, направлення на запобігання від необережних, навмисних дій співробітників або інших осіб, які оголосили конфіденційну інформацію, що може призвести до подальшої передачі даних.

3.Захист даних від несанкціонованого доступу (НСД) — це заходи, спрямовані на заборону доступу до комп'ютерної мережі внаслідок застосування комплексу інженерно-технічних, програмних та організаційних засобів.

Проблеми захисту нині пов›язані з що дестабілізує впливом зовнішніх і внутрішніх загроз, що виникають у компанії і впливають на її функціонування.

Належні служби АТ «Київський радіозавод» виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової безпеки підприємства.

До основних завдань інформаційної безпеки даних АТ «Київський радіозавод» відносяться:

- забезпечення конфіденційності, цілісності та структурованості інформації;
- організація своєчасного виявлення та запобігання зовнішніх та внутрішніх загроз;
- впровадження організаційних, інженерно-технічних, апаратно-програмних методів, що дозволяють посилити захист даних;
- розробка та вдосконалення політики безпеки з урахуванням сучасних тенденцій розвитку апаратного та програмного забезпечення.

Оперативна реалізація заходів з розробки та охорони інформаційної складової безпеки АТ «Київський радіозавод» здійснюється послідовним виконанням певного комплексу робіт за напрямками в рамках вищезазначених завдань:

- збирання різних видів необхідної інформації;
- обробка та систематизація одержаної інформації;
- аналіз одержаної інформації;
- захист інформаційного середовища підприємства, що традиційно охоплює: заходи для захисту суб'єкта господарювання від промислового шпіонажу з боку конкурентів або інших юридичних і фізичних осіб; технічний захист приміщень, транспорту, кореспонденції, переговорів, різної документації від несанкціонованого доступу зацікавлений юридичних і фізичних осіб до закритої інформації; збирання інформації про потенційних ініціаторів промислового шпіонажу та проведення необхідних запобіжних дій з метою припинення таких спроб; зовнішня інформаційна діяльність.

На підприємстві функціонує служба безпеки. До завдань служби безпеки АТ «Київський радіозавод» належать наступні (рис. 5):

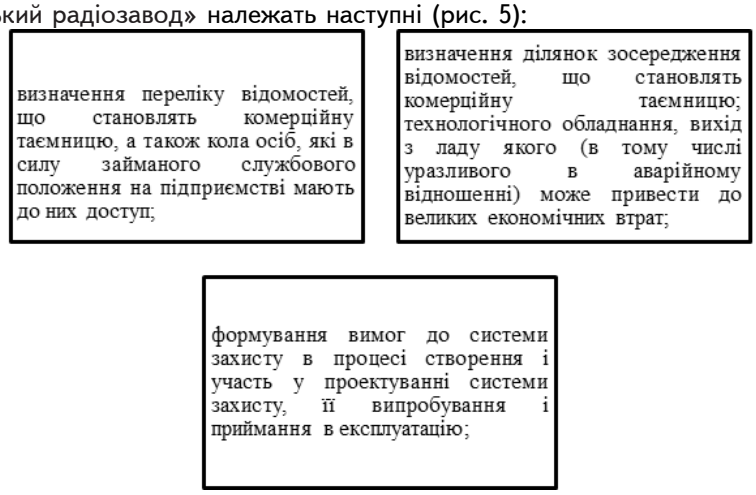

Рис.5. Основні завдання Служби безпеки АТ «Київський радіозавод»
*Складено на основі наукових джерел [5]

Додатково до обов'язків співробітників СІБ в АТ «Київський радіозавод» входить виконання директив вищестоящого керівництва, участь у виробленні рішень з усіх питань, пов'язаних з процесом обробки інформації з точки зору забезпечення його захисту.

Результати обстеження об›єкта щодо наявності інформаційної безпеки внесено до таблиці 1.

Таблиця 1

Аналіз виконання основних завдань щодо забезпечення інформаційної безпеки АТ «Київський радіозавод»

Основні завдання щодо забезпечення інформаційної безпеки	Рівень виконання
Забезпечення безпеки діяльності, захист інформації та відомостей, що є комерційною таємницею;	Низький
Організація роботи з правового, організаційного та інженерно-технічного (фізичного, апаратного, програмного та математичного) захисту комерційної таємниці;	Середній
Організація спеціального діловодства, що виключає несанкціоноване отримання відомостей, що є комерційною таємницею	Відсутня
Запобігання необґрунтованому допуску та відкритому доступу до відомостей та робіт, що становлять комерційну таємницю;	Низький
Виявлення та локалізація можливих каналів витоку конфіденційної інформації в процесі повсякденної виробничої діяльності та в екстремальних ситуаціях	Не проводиться

*Складено автором за даними [5]

З таблиці 1 видно, що рівень підприємства стосовно стандартів захисту дуже низький, тобто у разі розкрадання даних компанія може зазнати колосальних втрат. Дані, зазначені в таблиці, показують, що обраний напрямок розробки інформаційної безпеки є актуальним і вкрай необхідним.

В процесі дослідження прийшли до наступних висновків: основною проблемою є необхідність забезпечення необхідного рівня захисту, при якому необхідно враховувати, що інформація, що передається комп›ютерною мережею, може бути отримана зловмисником і передана каналами зв›язку; головною метою стандартизації є підвищення довіри, рівня стабільності роботи мережі, виконання необхідних заходів щодо захисту інформації від загроз і впровадження методів для зниження ризиків; також необхідно розробити документи, які становитимуть основу політики інформаційної безпеки.

При побудові інформаційної безпеки підприємства використовуються міжнародні стандарти інформаційної безпеки ISO17799 («Норми та правила щодо забезпечення безпеки інформації»). Дані стандарти описують рекомендації загального характеру щодо забезпечення інформаційної безпеки, що забезпечують основний рівень інформаційної безпеки систем. Аналіз інформаційної безпеки АТ «Київський радіозавод» показав, що на підприємстві не дотримані основні положення вищенаведеного стандарту.

Крім того, документообіг на підприємстві не повністю автоматизований. Тобто реалізуються функції з автоматизації традиційних діловодних процесів і передбачають паралельне функціонування електронного і паперового документообігу. Водночас підприємство може успішно здійснювати повноцінний електронний документообіг.

На відміну від традиційного програмного забезпечення – систем орієнтованих на автоматизацію конкретних ділянок бізнесу (бухгалтерія, складський облік, кадри та ін.) системи автоматизації документообігу пропонують розв›язання задач менш очевидних і більш комплексних.

Підприємство використовує систему оперативного управління підприємством «Мотив». Можна інтегрувати систему з електронною поштою або корпоративним порталом. Така інтеграція дозволить керівництву та службі безпеки отримувати необхідну інформацію щодо переміщення інформації між співробітниками. Крім того, підприємство не проводить оцінку стану інформаційної безпеки, що є обов'язковою умовою підвищення її рівня. Саме тому, одним з головних заходів підвищення ефективності управління інформаційною безпекою є впровадження щорічної оцінки стану інформаційної безпеки для виявлення її потенційних загроз та забезпечення сталого розвитку.

Висновки. В процесі дослідження встановлено, що забезпечення інформаційної безпеки є одним із найважливіших напрямів розвитку. Для коректного управління інформаційною безпекою на підприємстві варто впорядкувати обробку конфіденційної інформації, систематизувавши її. Таким чином, в нових реаліях, коли інформаційні технології набувають глобального характеру, інформаційна безпека є невід'ємним складником системи економічної безпеки підприємства й економічної безпеки держави загалом. Своєю чергою, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку окремого підприємства. Щоб зберегти бізнес, його розвивати та бути конкурентоспроможним, необхідно створити ефективну систему інформаційною безпекою. Сутність викладеного дає підстави стверджувати, що в нових реаліях, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку.

1. *Бакай В.Й.* Нові виклики та особливості створення системи інформаційної безпеки підприємства. Вісник Хмельницького національного університету. Економічні науки. 2020. № 5.URL: http://nbuv.gov.ua/UJRN/Vchnu_ekon_2020_5_6; 2. Інформаційна безпека. Економічний енциклопедичний словник. URL: http://zalik.org.ua/index.php?newsid=25011; 3. *Маркіна І.А.* Інформаційна безпека підприємства та організаційні заходи її забезпечення. Український журнал прикладної економіки. - 2019. - Т. 4, № 4. URL: http://nbuv.gov.ua/UJRN/ujae_2019_4_4_26; 4. *Носова Є.* Інформаційна складова у механізмі фінансової безпеки підприємства. Зовнішня торгівля: економіка, фінанси, право. 2021. № 3. URL: http://nbuv.gov.ua/UJRN/uazt_2021_3_11; 5. Офіційний сайт АТ «Київський радіозавод» URL: http://krz.kiev.ua/about-ua/; 6. Про інформацію: Закон України від 02.10.1992 № 2658-XII. Відомості Верховної Ради України. 1992 № 48. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text; 7. *Смачило Т.В.* Теоретичні засади управління системою інформаційної безпеки підприємства. Молодий вчений. 2016. № 12.1. URL http://nbuv.gov.ua/UJRN/molv_2016_12; 8. *Чередніченко О.Ю.* Інформаційно-аналітичні критерії забезпечення систем управління економічною безпекою підприємства. Вісник економіки транспорту і промисловості. - 2018. - № 62 дод.. URL: http://nbuv.gov.ua/UJRN/Vetp_2018_62dod

1. *Bakay V.Y.* Novi vyklyky ta osoblyvosti stvorennya systemy informatsiynoyi bezpeky pidpryyemstva. Visnyk Khmel'nyts'koho natsional'noho universytetu. Ekonomichni nauky. 2020.