УДК 65.012.8 : 004.01

Верескун М. В., *д. е. н., доцент, декан факультету інформаційних технологій ДВНЗ «Приазовський державний технічний університет», (Україна).*

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

У статті досліджено особливості побудови і функціонування системи забезпечення інформаційної безпеки промислового підприємства. Визначено, що теоретичною осново побудови системи інформаційної безпеки промислових підприємств мають стати системний, комплексний та процесний підходи до управління. Виявлено основні цілі, завдання, принципи побудови та види загроз. На їх основні сформовано методичний підхід до формування системи інформаційної безпеки промислових підприємств. В межах підходу основні його елементи віднесені до одного з чотирьох рівнів управління для кожного з яких визначені відповідальні за розробку та впровадження елементів системи інформаційної безпеки на кожному рівні. Використання розробленого підходу в практиці господарювання промислових підприємств допоможе підвищити ефективність розробки, впровадження та використання системи інформаційної безпеки та запобігти системних або методичних помилок на кожному з етапів.

Ключові слова: *інформаційна безпека, інформаційні технології управління, інформаційні системи.*
Рис. 2, літ. 4.

Верескун М. В.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ.

В статье исследованы особенности построения и функционирования системы обеспечения информационной безопасности промышленного предприятия. Определено, что теоретической основой построения системы информационной безопасности промышленных предприятий должны стать системный, комплексный и процессный подходы к управлению. Выявлены основные цели, задачи, принципы построения и виды угроз. На их основные сформирован методический подход к формированию системы информационной безопасности промышленных предприятий. В рамках подхода основные его элементы отнесены к одному из четырех уровней управления для каждого из которых определены ответственные за разработку и внедрение элементов системы информационной безопасности на каждом уровне. Использование разработанного подхода в практике хозяйствования промышленных предприятий поможет повысить эффективность разработки, внедрения и использования системы информационной безопасности и предотвращения системных или методических ошибок на каждом из этапов.

Ключевые слова: *информационная безопасность, информационные технологии управления, информационные системы.*

Vereskun M. V.

METHODOLOGICAL SUPPORT OF THE INFORMATION SECURITY SYSTEM OF INDUSTRIAL ENTERPRISE.

The peculiarities of construction and operation of the system of maintenance of information safety of industrial enterprises. It is determined that the theoretical basis for building information security systems of industrial enterprises should be systematic, comprehensive and process-based approaches to management. The basic goals, objectives, principles and types of threats. At their core formed methodical approach to developing the information security systems of industrial enterprises. Within the framework of its basic elements assigned to one of four levels of control for each of which is determined responsible for the development and implementation of elements of the system of information security at every level. The use of the developed approach the Holy Practice of management of industrial enterprises will help to increase the efficiency of development, implementation and use of information security and prevent system or methodological errors at each stage.

Keywords: *information security, information technology management, information systems.*

Постановка проблеми. На початку XXI століття основними макротенденціями сучасної світової економіки стали глобалізація, бурхливий розвиток інформаційних технологій (ІТ) і становлення інформаційної економіки. Інформаційні технології активно проникають в наше повсякденне життя, так і

в бізнес, стаючи необхідною умовою успішного функціонування все більшого числа промислових підприємств. Причому, із зростанням масштабів бізнесу, а особливо при переході до інтегрованим об'єднанням великих промислових підприємств, ефективне використання інформаційних технологій в таких сферах як матеріально-технічне постачання, логістика, планування, оперативне управління, контроль якості продукції і цілого ряду інших стають одним з найважливіших критеріїв, у кінцевому підсумку визначають конкурентоспроможність як окремого промислового підприємства, так і корпоративної групи в цілому.

Слід зазначити, що за останні п'ять років область застосування інформаційних технологій зазнала істотних зміни. Поряд з суттєвими конкурентними перевагами, наявні зміни привнесли в діяльність промислових підприємств і нові ризики. Так повсюдне впровадження і все більш активне використання інформаційних систем (ІС), насамперед у галузі управління, вимагає більш серйозної уваги до забезпечення безпеки їх функціонування на всіх рівнях, починаючи від кінцевих користувачів і закінчуючи національними урядами. При цьому основна частка відповідальності лягає на компанії, які займаються розробкою ІС, володіють правами на володіння ними, надають їх у користування, управляють і обслуговують їх.

Актуальність теми дослідження обумовлюється також тим фактом, що проблеми інформаційної безпеки промислових підприємств виходять на перший план незважаючи на постійне вдосконалення технологій і інструментів захисту даних. Про це свідчить невтішна динаміка порушень інформаційної безпеки та зростання важкості її наслідків. Так, у світі загальна кількість порушень інформаційної безпеки щорічно збільшується більш ніж удвічі, а в Україні тільки виявлена кількість злочинів в сфері ІТ зростає щорічно на 150%. Аналіз статистичних даних за останні роки свідчать також, що оприлюднення важливої внутрішньої інформації у 60% випадків веде до банкрутства підприємств. Наведені данні свідчать про наявність низки чинників, що визначають необхідність підвищення уваги до зазначеної проблеми. Основними з них є постійно зростаюча кількість видів інформаційних загроз та пов’язаних з ними ризиків, а також недостатній рівень інформаційної безпеки інформаційних систем існуючих промислових підприємств.

Аналіз результатів розвитку промислових підприємств України свідчить, що керівництво постійно приймає та удосконалює заходи щодо захисту корпоративної інформації, проте ці дії не носять системного характеру, оскільки спрямовані на усунення локальних конкретних загроз, які найчастіше одного разу вже були реалізовані.

Таким чином наукові дослідження, присвячені розробці загальних методичних рекомендацій щодо формування системи інформаційної безпеки промислових підприємств є актуальними.

Стан вивченості проблеми. Проблемам забезпечення інформаційної безпеки підприємств присвячені роботи таких вчених, як А. Абросимов, Ст. Адріанов, А. Афоничкин, С. Ашмаріна, А. Баутов, А. Голів, М. Давлетханов, А. Добрянин, Д. Дияконів, А. Еляков, А. Курило, В. Лазарєв, А. Макарова, Тобто Мешайкина, Р. Наса-кін, Р. Нижньогородців, А. Павлов, А. Пастюшков, П. Покровський, Ст. Савельєв, С. Симонов, Тобто Смирнов, Н. Столяров, В. Стрілець, Б. Татарських, Тобто Терехова, Ф. Удалов, В. Філіппова, Р. Хайретдінов, Ст. Ярочкин та ін.

Серед дослідників, які розглядали проблему інформаційної безпеки з точки зору вищого керівництва підприємств, найбільший внесок внесли Дж. Албаниз, С. Беринато, Ст. Галатенко, Дж. Джейсінг, Р. Лавджой, А. Лукацький, Дж. Міллер, А. Міцці, М. Мішель, Д. Моррилл, Дж. Різ, Ст Сонненрих, Б. Шнайер, Р. Уітті, А. Уилхайи і деякі інші.

Проте слід зазначити, що переважна більшість наявних робіт присвячені насамперед техніко-технлогічним проблемам формування системи інформаційної безпеки, вирішувати які повинні спеціалісти в галузі ІТ. Сучасні дослідження в галузі інформаційної безпеки вкрай рідко порушують питання організаційного та економічного характеру. В сучасних дослідженнях розгляд цих факторів носить епізодичний, позасистемний характер, проте зростання масштабів проблеми та вагомість можливих негативних наслідків потребують проведення комплексних досліджень.

Мета статті полягає в обґрунтуванні теоретичних і методичних положень формування і розвитку системи забезпечення інформаційної безпеки промислових підприємств.

Викладення результатів досліджень. Під інформаційною безпекою (ІБ) промислового підприємства розуміються всі елементи системи управління підприємством, пов’язані з визначенням, досягненням конфіденційності, цілісності, доступності, неспростовності, підзвітності, автентичності та достовірності інформації або засобів її обробки.

Для забезпечення ефективного функціонування всіх вище визначених елементів необхідно використання комплексного підходу. Це означає, насамперед, що в межах системи управління не може бути створено окремої підсистеми, яка б відповідала за інформаційну безпеку, при повному збереженні існуючих на промисловому підприємстві бізнес-процесів. Звісно, в системі управління мають бути створені окремі підрозділи, основною функцією яких буде забезпечення і підтримка на необхідному рівні інформаційної безпеки. Проте, їх діяльність призведе до суттєвих змін у роботі практично кожного

елементу в системі управління. При цьому не виключається можливість створення нових бізнес-процесів та ліквідація частини існуючих.

Численні публікації останніх років показують, що зловживання інформацією, що циркулює в ІС або передається по каналах зв'язку, удосконалювалися не менш інтенсивно, ніж заходи захисту від них. В даний час для забезпечення захисту інформації потрібно не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних заходів протидії і т. д.). Комплексний характер захисту виникає з комплексних дій зловмисників, які намагаються будь-якими засобами добути важливу для них інформацію. Сьогодні можна стверджувати, що народжується нова сучасна технологія - технологія захисту інформації в комп'ютерних інформаційних системах і мережах передачі даних.

Проведені дослідження дозволили визначити, що для ефективного виконання такого завдання необхідна система відповідного методичного забезпечення. Основними елементами такої системи є принципи побудови системи ІБ, цільові характеристики системи, її завдання, основні загрози та заходи щодо нейтралізації загроз.

Одним з базових, основних елементів системи інформаційної безпеки промислових підприємств виступають принципи, які мають бути покладені в основу її побудови. Для промислових підприємств основними принципами ІБ є наступні: простоти, повного контролю, загальної заборони, відкритої архітектури, розмежування доступу, мінімальних привілеїв, достатньої стійкості, мінімізації дублювання. Розглянемо принципи ІБ докладно:

1. Простота. Цей принцип ІБ наголошує на тому, що простота використання інформаційної системи здатна забезпечити мінімізацію помилок. Процес експлуатації інформаційної системи обов’язково супроводжується ненавмисними помилками з боку користувачів та адміністраторів системи, результатом яких може стати зниження рівня ІБ. Зрозуміло, що ускладнення здійснюваних користувачами та адміністраторами операцій і процедур призводить до зростання кількості таких помилок. Для зниження кількості помилок простота використання системи є необхідною умовою. Проте, простота використання не означає простоту архітектури і зниження вимог до функціональності системи ІБ.

2. Повний контроль. Виконання цього принципу передбачає організацію безперервного контролю за станом ІБ та моніторинг всіх подій, що впливають на ІБ. Передбачає таку архітектуру системи ІБ, яка б дозволяла здійснювати контроль доступу до будь якого об’єкту ІС, блокувати небажані дії та швидко відновлювати нормальні параметри інформаційної системи.

3. Загальна заборона. Заборонено все, на що немає дозволу. Доступ до об’єктів ІС можливий тільки при наявності відповідного дозволу, який надається у відповідності до діючих нормативних документів щодо організації роботи ІС. Проте важливо усвідомлювати, що система ІБ спрямована на надання дозволу, а не заборони будь яких дій. Означений принцип передбачає, що в ІС можливо виконання тільки відомих безпечних дій. Система не налаштовується на пошук та розпізнавання будь-якої загрози, оскільки такий шлях побудови системи ІБ є дуже ресурсномістким, та унеможливлює забезпечення достатнього рівня ІБ.

4. Відкрита архітектура ІС.

Цей принцип інформаційної безпеки полягає у тому, що безпека повинна забезпечуватися через неясність. Спроби захистити інформаційну систему від комп'ютерних загроз шляхом ускладнення, заплутування і приховування слабких місць ІС, опиняються в кінцевому підсумку неспроможними і тільки відстрочують успішну хакерську, вірусну чи інсайдерську атаку.

5. Розмежування доступу. Даний принцип ІБ полягає в тому, що кожному користувачеві надається доступ до інформації і її носіїв у відповідності з його повноваженнями. При цьому виключена можливість перевищення повноважень. Кожній ролі/посади/групі можна призначити свої права на виконання дій (читання/редагування/видалення) над певними об'єктами ІС.

6. Мінімальні привілеї. Принцип мінімальних привілеїв полягає у виділенні користувачеві найменших прав і доступу до мінімуму необхідних функціональних можливостей програм. Такі обмеження, тим не менш, не повинні заважати виконанню роботи.

7. Достатня стійкість. Цей принцип інформаційної безпеки виражається в тому, що потенційні зловмисники повинні зустрічати перешкоди у вигляді досить складних обчислювальних завдань. Наприклад, необхідно, щоб злом паролів доступу вимагав від хакерів неадекватно великих проміжків часу і/або обчислювальних потужностей.

8. Мінімізація дублювання. Передбачає мінімізацію ідентичних процедур. Цей принцип інформаційної безпеки полягає в тому, що в системі ІБ не повинно бути загальних для декількох користувачів процедур, таких як введення пароля. У цьому випадку масштаб можливої хакерської атаки буде менше.

Побудована за наведеними принципами система ІБ має бути налаштована на досягнення

визначених цілей, специфіка яких буде великою мірою визначати як структуру системи так і основні параметри її функціонування. Для промислового підприємства основними цілями досягнення високого рівня інформаційної безпеки є забезпечення конфіденційності, цілісності, доступності, достовірності та неспростовності інформації.

Розглянемо кожну цільову характеристику інформації докладно:

1. Конфіденційність - це стан доступності інформації тільки авторизованим користувачам, процесів і пристроїв. Необхідно підкреслити, що конфіденційність є однією з основних цільових характеристик інформації, а її забезпечення – найголовнішою функцією системи інформаційної безпеки. Категорія конфіденційності є особливо важливою для промислових підприємств на етапі проведення НДДКР та впровадження інновацій. Зрозуміло, що з плином часу всі технологічні новинки, технічні та дизайнерські рішення стануть здобутком загалу, проте передчасне оприлюднення такої інформації, або навіть її частин може призвести не тільки до величезних збитків, а й взагалі до краху компанії. Така ситуація пояснюється тим, що в сучасному інтегрованому і консолідованому світі технологічні, технічні або дизайнерські ноу-хау з одного боку, є одним з основних чинників конкурентоспроможності, з іншого – термін їх «життя» в якості конкурентної переваги постійно скорочується. Наприклад, якщо у 80-х роках XX століття промислова компанія мала у своєму розпорядженні якусь суттєву техніко-технологічну конкурентну перевагу, то вона могла не хвилюватися щодо можливостей копіювання протягом наступних 4-5 років. Сьогодні цей термін скоротився до 4-5 місяців. В таких умовах передчасне оприлюднення інформації можуть призвести до величезних втрат.

Основними методами забезпечення конфіденційності інформації є: закриття, шифрування, приховування та подрібнення.

Закриття інформації передбачає розмежування прав доступу до неї, а також заборону неавторизованим користувачам, процесам або пристроям використовувати інформацію. Шифрування інформації передбачає приведення її у нечитаний вигляд для тих, хто не має спеціального ключа або коду. Приховування інформації має на меті зробити невідомим сам факт існування інформації. Найчастіше для цього використовують різні методи стенографії. Подрібнення інформації призводить до того, що вона розділюється на окремі частини таким чином, щоб знання однієї з них не дозволяло відновити всю її в цілому.

2. Цілісність - це відсутність неправомочних спотворень, доповнень або знищення інформації. Гарантія цілісності особливо важлива в тих випадках, коли інформація представляє велику цінність і не повинна бути втрачена, а також коли дані можуть бути навмисно змінені з метою дезінформації одержувача. Як правило, від стирання інформацію захищають методами, що забезпечують конфіденційність, і резервним копіюванням, а відсутність спотворень перевіряють з допомогою хешування.

3. Доступність - це забезпечення своєчасного і надійного доступу до інформації і інформаційних сервісів. Типовими випадками порушення доступності є збій в роботі програмних/апаратних засобів і розподілена атака типу «відмова в обслуговуванні» (DDoS). Від збоїв інформаційну систему захищають усуненням причин збоїв, а від DDoS-атак - відсіканням паразитного трафіку.

4. Справжність або автентичність - можливість однозначно ідентифікувати автора/джерело інформації. Автентичність електронних даних часто засвідчується таким засобом, як електронно-цифровий підпис.

5. Неспростовність - неможливість зречення від авторства інформації, а також факту її відправки або отримання. Неспростовність можна гарантувати електронно-цифровим підписом та іншими криптографічними засобами і протоколами. Неспростовність актуальна, наприклад, у системах електронних торгів, де вона забезпечує відповідальність друг перед іншому продавців і покупців.

Також на промислових підприємствах система інформаційної безпеки може бути спрямована на забезпечення специфічних властивостей інформації, наприклад підзвітність, адекватність та інші.

Для досягнення названих цілей система ІБ повинна бути спроможною виконувати наступні завдання:

- забезпечення захищеного зберігання інформації на різних носіях;
- захист даних, що передаються по каналах зв'язку;
- розмежування доступу до різних видів документів;
- створення резервних копій, післяаварійне відновлення інформаційних систем.

Забезпечення інформаційної безпеки підприємства можливо тільки при системному і комплексному підході до захисту. В системі ІБ повинні враховуватися всі актуальні комп'ютерні загрози та вразливості [1].

Загрози інформаційній безпеці - це можливі дії або події, які можуть вести до порушень ІБ. Вони також є кінцевими цілями (або результатами) діяльності її порушників. Види загроз інформаційної безпеки дуже різноманітні і мають безліч класифікацій. За результатами проведеного дослідження

запропонованан класифікація загроз інформаційної безпеки, яки є найбільш актуальними по відношенню саме до промислових підприємств.

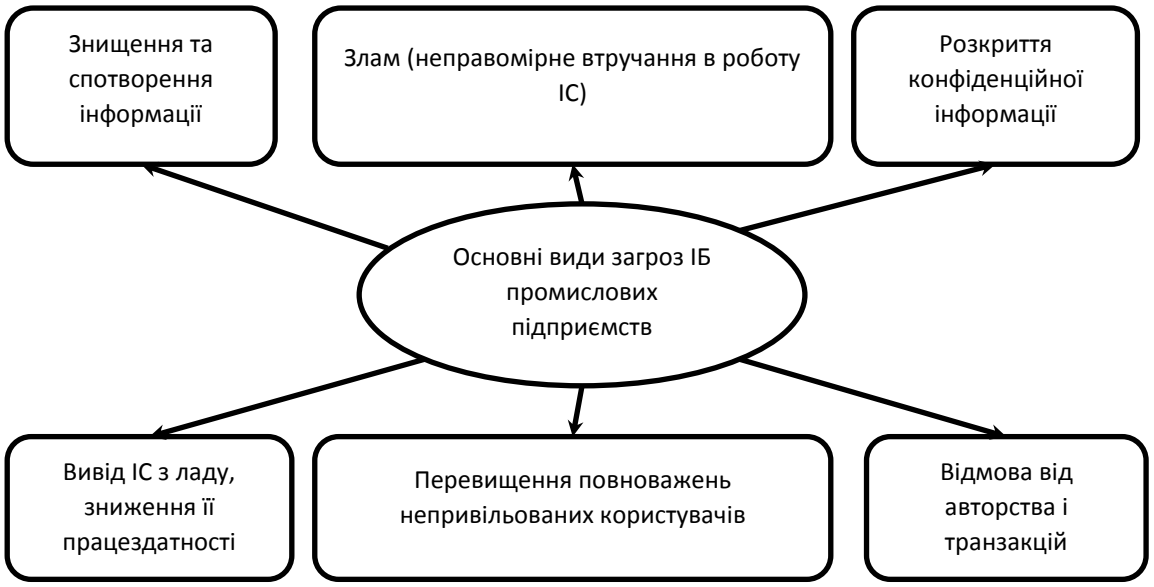

Рис. 1. Загрози інформаційній безпеці промислових підприємств.

Повноцінна інформаційна безпека підприємств і організацій передбачає безперервний контроль в реальному часі всіх важливих подій і станів, що впливають на безпеку даних. Захист має здійснюватися цілодобово і цілорічно і охоплювати весь життєвий цикл інформації - від її надходження або створення до знищення або втрати актуальності.

На рівні підприємства за інформаційну безпеку відповідають відділи інформаційних технологій, економічної безпеки, кадрів та інші служби [2].

Необхідно також відзначити, що рівень загроз і, відповідно рівень інформаційної безпеки промислового підприємства, постійно змінюються під дією різних факторів. Найбільш впливовими з них є наступні:

- розширення співпраці підприємства з партнерами;
- автоматизація бізнес-процесів на підприємстві;
- розширення кооперації виконавців при побудові і розвитку інформаційної інфра-структури підприємства;
- зростання обсягів інформації підприємства, яка передається по відкритих каналах зв'язку;
- ріст комп'ютерних злочинів.

Для досягнення задовільного рівня інформаційної безпеки на промисловому підприємстві необхідно застосування комплексу організаційних і технічних заходів, спрямованих на захист корпоративних даних. **Організаційні заходи** включають документовані процедури і правила роботи з різними видами інформації, IT-сервісами, засобами захисту і т. д. **Технічні заходи** полягають у використанні апаратних і програмних засобів контролю доступу, моніторингу витоків, антивірусного захисту, міжмережевого екранування, захисту від електромагнітних випромінювань і ін.

При виборі програмно-технічних рішень із забезпечення ІБ підприємства, перевага віддається рішень, що забезпечує дотримання основних принципів ІБ, а також відповідаючих наступним **критеріям:**

- підтримка міжнародних, національних, промислових та Інтернет стандартів (перевага віддається міжнародним стандартам).
- підтримка найбільшою мірою інтеграції з корпоративними програмно-апаратними платформами і використовуваними СЗІ;
- уніфікація розробників і постачальників використовуються продуктів;
- уніфікація засобів і інтерфейсів управління підсистемами ІБ.

Таким чином, за результатами проведених досліджень, можна сформувати методичний підхід до побудови системи інформаційної безпеки промислових підприємств (рис. 2).

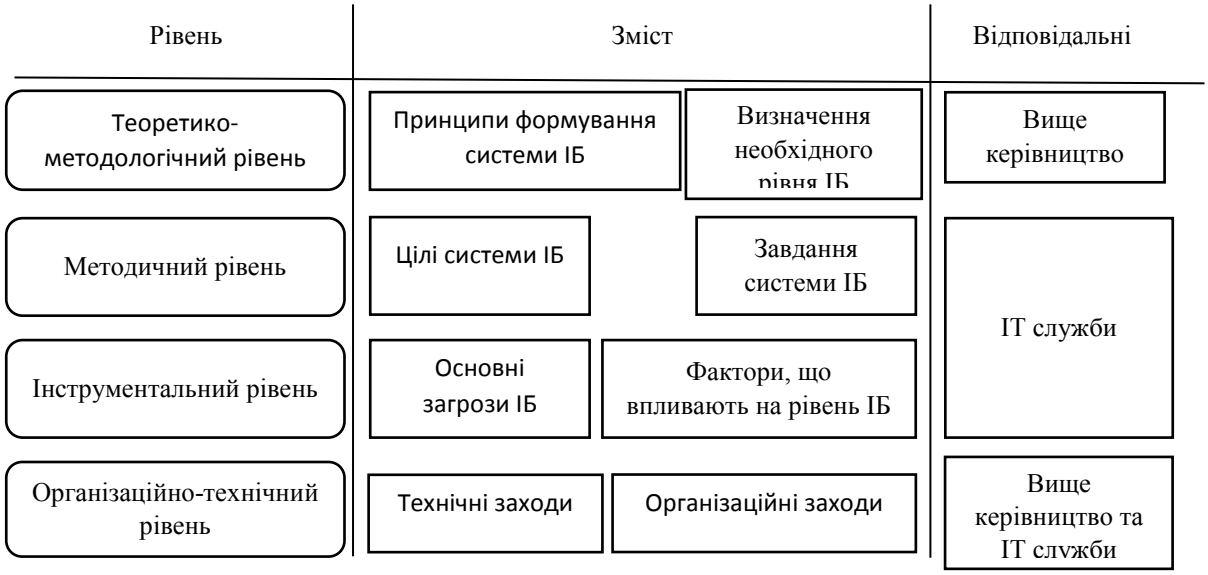

Рис. 2. Методичний підхід до формування системи ІБ промислових підприємств.

Із наведеного рисунку видно, що основні елементи методичного підходу до формування системи управління ІБ розділені на чотири рівні, кожному з яких відповідає визначений рівень управління промисловим підприємством. Так, принципи формування системи ІБ, що віднесені до теоретико-методологічного рівня запропонованого підходу, є тим елементом системи, за формування якого відповідає вище керівництво промислового підприємства. Також на цьому рівні мають бути сформовані основні вимоги до необхідного промисловому підприємству рівня ІБ. Далі ІТ служби відповідають за виконання заходів, віднесених до методичного та інструментального рівня, тобто вони повинні сформулювати основні цілі та завдання системи ІБ, а також визначити основні загрози ІБ та фактори, що впливають на її рівень. Після цього, ІТ служби мають розробити план технічних ат організаційних заходів, спрямованих на досягнення визначеного рівня ІБ. Після цього план погоджується вищим керівництвом підприємства і розпочинаються роботи по його практичному впровадженню. Особливо слід відзначити необхідність обов'язкової участі вищого керівництва підприємства у реалізації заходів організаційно-технічного рівня. На цьому етапі керівництво промислового підприємства повинно зрозуміти, що просте впровадження «додаткових заходів» без зміни всієї системи управління не забезпечить необхідного рівня ІБ. Важливою умовою ефективного функціонування системи інформаційної безпеки є її повна інтеграція в оперативну діяльність компанії. Її впровадження неодмінно буде вимагати коригування, а іноді і докорінної зміни більшості бізнес процесів. Можлива поява принципово нових бізнес-процесів, пов'язаних із забезпеченням функціонування системи ІБ. Це вимагає внесення змін в описі бізнес-процесів, регламентацію всіх нововведень та визначення нових меж відповідальності виконавців. Також необхідно ввести в практику постійні навчання та тренування з питань ІБ.

Висновки. Таким чином, проведені дослідження особливостей формування і розвитку системи забезпечення інформаційної безпеки промислових підприємств дозволяють зробити наступні висновки.

1. Формування системи інформаційної безпеки промислових підприємств є складним управлінським процесом, який потребує використання системного та комплексного підходів до управління. Для успішного впровадження на промислових підприємствах ефективної системи інформаційної безпеки необхідне відповідне методичне забезпечення цього процесу.
2. В роботі запропоновано новий методичний підхід до формування системи інформаційної безпеки промислових підприємств до складу якого входять основні принципи формування системи інформаційної безпеки, цілі та завдання цієї системи, основні загрози ІБ та фактори, що впливають на її рівень, а також основні заходи, спрямовані на її реалізацію. Основною особливістю запропонованого підходу є віднесення визначених елементів до одного з чотирьох рівнів управління (теоретико-методологічного, методичного, інструментального та організаційно-технічного) і визначення відповідальних за ефективність розробки, впровадження та функціонування системи ІБ на кожному з рівнів.
3. Результатом дослідження є також визначення основних складових кожного з елементів запропонованого підходу та опис особливостей його впровадження та використання.

Вважаємо, що удосконалення та пристосування розробленого методичного підходу до особливостей функціонування промислових підприємств конкурентних галузей національного господарства є перспективним напрямом подальших досліджень.

СПИСОК ДЖЕРЕЛ

1. Обеспечение информационной безопасности предприятия [Електронний ресурс]. Режим доступу: http://www.arinteg.ru/articles/informatsionnaya-bezopasnost-predpriyatiya-25799.html

2. Коновал Д. Комплексный подход к организации системы защиты информации на предприятии: основные вопросы и технологи. [Електронний ресурс]. Режим доступу: http://www.epam-group.ru/aboutus/news-and-events/articles/2009/aboutus-ar-gaz-prom-09-01-2009.html#sthash.qruifGvr.dpuf

3. Принципы информационной безопасности . [Електронний ресурс]. Режим доступу: http://www.arinteg.ru/articles/printsipy-informatsionnoy-bezopasnosti-26490.html.

4. Цели и методы ИБ. [Електронний ресурс]. Режим доступу: http://www.arinteg.ru/articles/tseli-informatsionnoy-bezopasnosti-26725.html