DOI: https://doi.org/10.32782/2524-0072/2021-23-23

УДК 658.1:005.8:001.891

ОСОБЛИВОСТІ ТЕХНІКО-ТЕХНОЛОГІЧНОГО МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ БІЗНЕС-СЕРЕДОВИЩА

FEATURES OF TECHNICAL AND TECHNOLOGICAL MANAGEMENT OF ENTERPRISE INFORMATION SECURITY IN THE BUSINESS ENVIRONMENT

Дячков Дмитро Володимирович
доктор економічних наук, доцент,
Полтавська державна аграрна академія
ORCID: https://orcid.org/0000-0002-2637-0099

Вовк Микола Олександрович
аспірант,
Полтавська державна аграрна академія
ORCID: https://orcid.org/0000-0001-8173-0918

Боскіна Марія Григорівна
здобувач вищої освіти,
Полтавська державна аграрна академія
ORCID: https://orcid.org/0000-0001-5395-4201

Diachkov Dmytro, Vovk Mykola, Boskina Mariya
Poltava State Agrarian Academy

У статті актуалізовано необхідність дослідження системи менеджменту інформаційної безпеки підприємства, зокрема в техніко-технологічній її частині. На основі проведених досліджень виділено основні рівні на яких відбувається забезпечення інформаційної безпеки: фізичний, програмний, нормативно-правовий, техніко-технологічний та організаційно-управлінський. Сформовано систему менеджменту техніко-технічного захисту інформації в інформаційних системах, яка включає суб'єкти (спеціальні суб'єкти системи захисту, керівництво, спеціалісти та персонал), об'єкти (бази даних, документація в електронному вигляді та на паперових носіях, відомості, що становлять комерційну таємницю, технологічна, технічна та виробнича інформація) та техніко-технологічні, апаратні, програмні, організаційно-управлінські інструменти управління захистом інформаційної системи. Зважаючи на пропоновану систему менеджменту техніко-технологічного захисту інформації в інформаційних системах, її функції, завдання, етапи здійснення та інші аспекти, виокремлено напрями та базові інструменти здійснення техніко-технологічного менеджменту інформаційної безпеки суб'єкту господарювання.

Ключові слова: аудит мережевої інфраструктури, інформаційна безпека, менеджмент інцидентів інформаційної безпеки, програмний захист, техніко-технологічний менеджмент, технологічний рівень захисту, фізичний рівень захисту.

В статье актуализирована необходимость исследования системы менеджмента информационной безопасности предприятия, в частности в технико-технологической ее части. На основе проведенных исследований выделены основные уровни, на которых происходит обеспечение информационной безопасности: физический, программный, нормативно-правовой, технико-технологический и организационно-управленческий. Сформирована система менеджмента технико-технической защиты информации в информационных системах, которая включает субъекты (специальные субъекты системы защиты, руководство, специалисты и персонал), объекты (базы данных, документация в электронном виде и на бумажных носителях, сведения, составляющих коммерческую тайну, технологическая, техническая и производственная информация) и технико-технологические, аппаратные, программные, организационно-управленческие инструменты управления защитой информационной системы. Учитывая предлагаемую систему менеджмента технико-технологической защиты информации в информационных системах, ее функции, задачи, этапы осуществления и

другие аспекты, выделены направления и базовые инструменты осуществления технико-технологического менеджмента информационной безопасности субъекта хозяйствования.

Ключевые слова: аудит сетевой инфраструктуры, информационная безопасность, менеджмент инцидентов информационной безопасности, программная защита, технико-технологический менеджмент, технологический уровень защиты, физический уровень защиты.

The article actualizes the need to study the enterprise information security management system, in particular in its technical and technological part. On the basis of the conducted researches the basic levels at which there was maintenance of information security are allocated: physical, program, normative-legal, technical-technological and organizational-administrative levels. The system of management of technical and technical protection of information in information systems was formed, which includes subjects (special subjects of protection system, management, specialists and personnel), objects (databases, documentation in electronic form and on paper, information, constituting a trade secret, technological, technical and production information) and technical-technological, hardware, software, organizational and managerial tools for managing the protection of the information system. Taking into account the proposed management system of technical and technological protection of information in information systems, its functions, tasks, stages of implementation and other aspects, the directions and basic tools for technical and technological management of information security of the business entity were identified. The main directions of the management system of technical and technological protection of information were defined: management of information security incidents, regular updating of software security, access control and password policy control, audit of network infrastructure. The tools of technical and technological management of information security of the enterprise were characterized by: modules of trusted loading, analysis of security of information systems, protection against viruses and spam, DLP-systems, protection of virtual infrastructure, intrusion detection systems. Effective implementation of the system of technical and technological management of information security of the enterprise was proposed to implement on the basis of the model "Lifecycle Security", which regulates and describes the stages of building a corporate information security system and organizational modes of information system protection in general, means of information protection.

Keywords: information security incident management, information security, network infrastructure audit, physical level of protection, software protection, technical and technological management, technological level of protection.

Постановка проблеми. Інформаційна безпека підприємства є функціональним елементом системи забезпечення його стратегічного розвитку. Її основне завдання полягає у забезпеченні стабільності існування підприємства в умовах всеохоплюючої інформатизації та цифровізації, а також формування перспектив його сталого розвитку в майбутньому. У комплексній системі забезпечення інформаційної безпеки підприємств враховуються сучасні правові та організаційно-управлінські заходи, а також програмно-технічні засоби протидії зовнішнім і внутрішнім загрозам, що забезпечує стан захищеності інформації та перспективи розвитку інформаційних технологій.

Забезпечення безпеки інформації, яка циркулює на підприємстві, а також між підприємствами та державними установами – одна із головних умов формування ефективної загальної системи безпеки. Водночас це є багатоплановим та складним управлінським завданням, через те, що проблеми, пов'язані із забезпеченням інформаційної безпеки підприємства хоча і мають різнобічних характер, проте аналогічні за групами факторів впливу, серед яких: збільшення чисельності функціонування ПК та інших гаджетів в сучасному інформаційному просторі, що має міжнародну систему побудови і контролю; наявність великих обсягів інформації, яка накопичується, зберігається та обробляється за допомогою сучасної техніки та цифрових технологій; виникнення та вдосконалення програмних засобів й технологій, які потребують особливих технік та технологій захисту; недосконаліть міжнародних стандартів та законодавчої бази, що забезпечують необхідний рівень захисту інформації, особливо технологічної складової; створення єдиного інформаційного простору, який не забезпечує достатнього рівня інформаційної безпеки. Мінімізація негативного впливу зазначених факторів та різнорідних загроз інформаційній безпеці підприємства потребує формування сучасних теоретичних і практичної апробації наробок щодо визначення особливостей техніко-технологічного менеджменту інформаційної безпеки підприємства в умовах бізнес-середовища.

Отже, розвиток системи менеджменту інформаційної безпеки, зокрема в техніко-технологічній її частині є актуальним науковим завданням, вирішення якого потребує формування ґрунтовного теоретичного базису.

Аналіз останніх досліджень і публікацій. Доцільно відзначити, що дана предметна область дослідження не є новою та має теоретичну основу. Зокрема, окремим аспектам автоматизації технологічних процесів підпри-

ємств з урахуванням інформаційної безпеки присвячені праці Блінова А. М., Двойнішнікова Н. Е., Бойченка О. В., Шелудька Б. О. [3; 4; 6]. Водночас, організаційно-управлінським аспектам інформаційної безпеки підприємств присвячені наопрацювання Балановської А. В., Вовкодаєвої А. В., Ветрової Н. М., Гайсарової А. А., Дячкова Д. В., Маркіної І. А. [1; 5; 8; 10]. Програмній складовій забезпечення інформаційної безпеки присвячені праці Білозерова О. І., Топоркової І. І. [2]. Відтак, безпечність функціонування суб'єктів господарювання в умовах трансформації бізнес-середовища, захист систем управління виробничими, управлінськими, технологічними процесами, захищеність об'єктів інформаційної інфраструктури визнаються актуальними завданнями, які потребують формування теоретичного базису безпекології в сфері інформаційної захисту та практичної його реалізації.

Виділення невирішених раніше частин загальної проблеми. Заважаючи на значне наукове підґрунтя зазначеної проблематики, поза увагою залишаються особливості управління техніко-технологічною складовою інформаційної безпеки підприємства в умовах бізнес-середовища.

Формулювання цілей статті – обґрунтування особливостей техніко-технологічного менеджменту інформаційної безпеки підприємства в умовах бізнес-середовища.

Виклад основного матеріалу дослідження. Порушення інформаційної безпеки підприємства призводить до зростання соціальних, економічних, екологічних втрат. Відтак, забезпечення інформаційної та цифрової безпеки суб'єктів господарювання на різних рівнях є пріоритетним завданням для керівників різних рівнів.

На основі проведених досліджень доцільно виділити основні рівні на яких відбувається забезпечення інформаційної безпеки (рис. 1).

Безпека інформаційної системи залежить від оточення, в якому вона функціонує, що вимагає, в першу чергу, вжиття заходів для захисту будівель, прилеглої території, підтримуючої інфраструктури, обчислювальної техніки, носіїв даних. Основний принцип «фізичного захисту», дотримання якого слід постійно контролювати, формулюється як «безперервність захисту в просторі і часі». На основі проведених досліджень доцільно виділити наступні напрямки фізичного захисту: фізичне управління доступом; протипожежні заходи; захист підтримуючої інфраструктури; захист від перехоплення даних; захист комунікаційних систем. Заходи фізичного управління доступом дозволяють контролювати, та за необхідності обмежувати, вхід й вихід співробітників, відвідувачів до або з приміщень, які містять інформацію, інформаційні ресурси, технології обробки даних, апаратні засоби, інформаційну інфраструктуру тощо. Контролюватися може як будівля організації загалом, так і окремі приміщення, наприклад, ті, де розташовані сервери, комунікаційна апаратура тощо. Більшість теоретиків та практиків наголошують, що при проектуванні та реалізації заходів фізичного управління доступом доцільно застосовувати об'єктний підхід, який дозволяє:

по-перше, визначити периметр безпеки, що обмежує контрольовану територію. На цьому рівні деталізації визначається зовнішній інтерфейс організації – порядок входу/виходу штатних співробітників та відвідувачів, техніки, інформаційних ресурсів тощо. Все, що не входить до зовнішнього інтерфейсу, має бути інкапсульоване, тобто захищене від нелегальних проникнень;

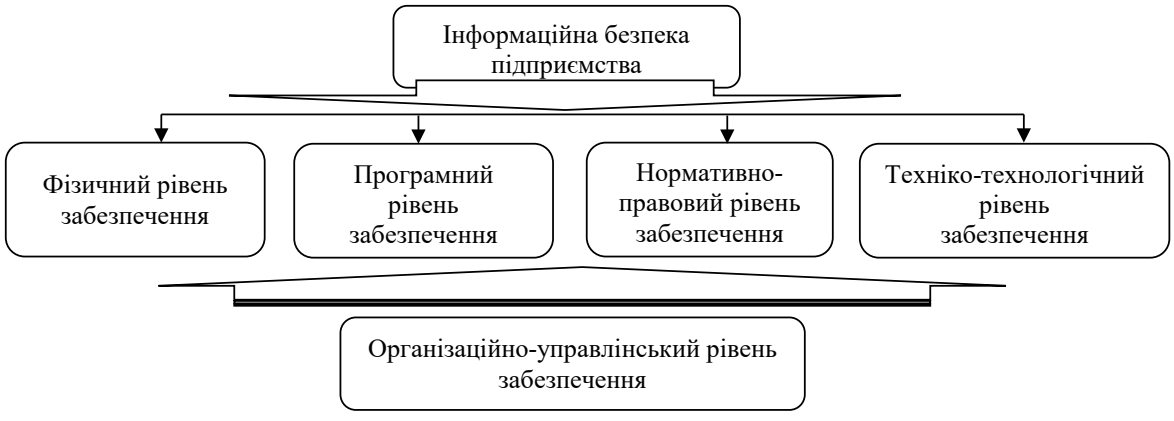

Рис. 1. Рівні забезпечення інформаційної безпеки підприємства

Джерело: сформовано авторами

по-друге, провести декомпозицію території підприємства, визначити об'єкти інформаційного захисту та комунікаційного зв'язку. При такій, більш глибокій деталізації слід виділити серед об'єктів інформаційного та цифрового захисту найбільш критичні з точки зору безпеки та забезпечити їм підвищений рівень захисту [7].

Заходи захисту програмного рівня засновані на використанні спеціальних програм та відповідних апаратних засобів, які самостійно або в комплексі з іншими засобами виконують функції інформаційного захисту, зокрема: ідентифікацію та аутентифікацію користувачів; розмежування доступу до ресурсів; реєстрацію подій; криптографічні перетворення; перевірку цілісності системи; перевірку відсутності шкідливих програм; програмний захист переданої інформації та каналів зв'язку; захист системи від наявності та появи небажаної інформації; створення фізичних перешкод на шляху проникнення порушників; моніторинг та своєчасну сигналізацію дотримання правильності роботи системи; створення резервних копій цінної інформації тощо.

Правове забезпечення захисту інформації визначене на міжнародному і державному рівнях та регулюється міждержавними договорами, конвенціями, деклараціями, реалізується за допомогою патентів, ліцензій, авторських прав тощо. На державному рівні правовий захист регулюється державними та відомчими актами. Відомчі нормативні акти визначаються наказами, інструкціями, положеннями та інструкціями, які видаються самими відомствами, організаціями, а також підприємствами, що діють в рамках певних структур. Цілями захисту інформації з позиції нормативно-правового забезпечення є: запобігання розголошенню, витоку і несанкціонованого доступу до інформації та інформаційних ресурсів; запобігання протиправних дій з модифікації, знищення, перекручення, блокування та копіювання інформації; запобігання інших форм протизаконного втручання в інформаційні системи та інформаційні ресурси; забезпечення для документованої інформації правового режиму як для об'єкта власності; захист прав громадян, забезпечених конституцією, на збереження особистої таємниці та конфіденційність персональних даних, які є в інформаційних системах; забезпечення конфіденційності документованої інформації та збереження державної таємниці відповідно до чинного законодавства; забезпечення прав суб'єктів в усіх інформаційних процесах, а також при розробці, виробництві і використанні інформаційних технологій, систем і засобів їх забезпечення та інші.

Технічний та технологічний захист інформації являє собою найбільший комплекс робіт: від обладнання приміщень засобами обмеження доступу, шифрування даних, інформування колективу та виявлення передбачуваних каналів витоку до постійного оновлення засобів й способів підтримки безпеки. Технічне забезпечення інформаційної безпеки спрямоване, перш за все, на підвищення захисту технологічних процесів збереження даних, ноу-хау, інформації з патентів, власних напрацювань або придбаних методик, ліцензій. Слід зауважити, що методами й засобами технічного захисту забезпечується інформаційна безпека відомостей про фінансові операції підприємства, зокрема його кредити, інформацію про контрагентів, персональні дані керівництва та співробітників. Відповідно до зазначеного, об'єктами системи техніко-технічного захисту інформації на підприємстві є: бази даних з інформацією про партнерів, клієнтів, постачальників (послуг, товарів, ресурсів); документація в електронному вигляді (у тому числі в системах електронного документообігу) і на паперових носіях; будь-які відомості, що становлять комерційну таємницю (зазвичай це фінансові дані: активи та пасиви підприємства, кредити й дебіторська заборгованість, розміри заробітної плати ключових співробітників); технологічна, технічна та виробнича інформація – специфіка виробничих процесів, ноу-хау, склад обладнання й топологія технологічних ланцюжків. Відтак, небезпеку для об'єктів технічного захисту інформації представляють: зовнішні джерела – конкуренти, власні співробітники (в тому числі й керівництво), зловмисники [9].

Зважаючи на вищезазначене, система менеджменту техніко-технічного захисту інформації в інформаційних системах на підприємстві має вигляд відображений на рис. 2.

Техніко-технологічне забезпечення безпеки захисту конфіденційної і комерційної інформації є сукупністю заходів, спрямованих на вирішення трьох завдань:

закритість для сторонніх осіб будівель та приміщень, де зберігаються носії важливих відомостей;

уникнення псування або знищення інформаційних носіїв як в результаті дій зловмисників, так і в разі виникнення стихійних лих;

запобігання розкраданню конфіденційних відомостей по технічних каналах.

Рис. 2. Структура системи менеджменту техніко-технологічного захисту інформації в інформаційних системах на підприємстві

Джерело: розроблено авторами

З метою забезпечення ефективного здійснення зазначених завдань системи менеджменту техніко-технологічного захисту інформації в інформаційних системах на підприємствах доцільно виділити наступні етапи робіт:

підготовчий – оцінка загроз для приміщень, де зберігаються дані, розташовано технічно-апаратну частину інформаційної системи; визначення категорії даних, які захищаються; затвердження бюджету на інженерно-технічні розробки;

проектувальний – встановлення програмного забезпечення та визначення вимог до апаратних засобів захисту;

фінальний – ввід в експлуатацію та визначення методів подальшого супроводу з оновленням систем безпеки.

Основними заходами формування системи менеджменту технічного й технологічного захисту інформації в інформаційних системах на підприємстві є: створення служби (відділу) інформаційної безпеки; використання спеціальних технічних пристроїв; моніторинг «слабкої ланки» для отримання неконтрольованого доступу до інформаційних сигналів; розробка системи та методів технічного захисту інформації; оцінка «вузьких місць» копіювання, зміни, знищення інформаційних ресурсів та аналіз каналів витоку фінансової, комерційної та технологічної інформації.

Зважаючи на пропоновану систему менеджменту техніко-технологічного захисту інформації в інформаційних системах, її функції, завдання, етапи здійснення та інші аспекти, доцільно виокремити напрями та базові інструменти здійснення техніко-технологічного менеджменту інформаційної безпеки суб'єкту господарювання (рис. 3).

Менеджмент інцидентів інформаційної безпеки передбачає документування та подальший перегляд подій інформаційної безпеки, на основі якого здійснюється розробка плану та програми заходів з аудиту інформаційної безпеки. Відсутність менеджменту інцидентів інформаційної безпеки та регламенту реагування на події інформаційної безпеки ускладнює оперативне виявлення критичних подій, що призводить до зростання рівня інформаційної небезпеки.

Аудит мережевої інфраструктури, особливо якщо він здійснюється в реальному часі (моніторинг), дозволяє визначити техніко-технологічні проблеми функціонування мережевого обладнання, але не дає можливості визна-

Рис. 3. Напрями та базові інструменти здійснення техніко-технологічного менеджменту інформаційної безпеки підприємства

Джерело: сформовано авторами

чити, висловити події чи інцидент інформаційної безпеки. За відсутності засобів виявлення вторгнення та засобів запобігання інформаційні атаці, об'єкти системи техніко-технологічного менеджменту інформаційної безпеки підприємства не мають можливості визначити тип та рівень небезпеки. А відповідно і своєчасно протидіяти. Використовувати техніко-технологічні засоби виявлення вторгнення та засоби запобігання атаці, необхідно у взаємозв'язку із відповідним програмно-апаратним забезпеченням інформаційної безпеки підприємства.

Регулярне оновлення програмного забезпечення інформаційної безпеки Програмні методи захисту реалізуються за допомогою засобів програмного та апаратного забезпечення. Технічні методи захисту передбачають використання засобів програмно-технічного характеру, спрямованих, передусім, на обмеження доступу користувача, який працює з інформаційними системами підприємства до закритої тієї інформації [9]. Програмні засоби захисту необхідні, перш за все, для виконання логічних та інтелектуальних функцій захисту.

Контроль управління доступом та парольною політикою передбачає отримання фізичний доступ до інформаційних ресурсів або доступ до інформаційної системи в цілому. Мотивація суб'єктів системи техніко-технологічного захисту інформаційної системи, в даному випадку передбачає те, що вони виконують вимогу неперервності технологічного процесу: процедури ідентифікації та аутентифікації користувачів інформаційних ресурсів підприємства. Важливим взаємозв'язком із зазначеними напрямами інформаційного захисту, за даної ситуації, виступає організація пропускного та внутрішньооб'єктного режимів (багаторівненва аутентифікація, біометрична система контролю та управління доступом), застосування елементів соціальної інженерії, а також антивірусні програми захисту.

Інструментами реалізації зазначених напрямів є:

модулі довіреного завантаження – це програмні або програмно-апаратні засоби, за допомогою яких здійснюється завантаження операційної системи з довірених носіїв інформації. Подібні пристрої контролюють цілісність програмного забезпечення (системних файлів, директорій операційної системи), тех-

нічних параметрів, відіграють роль аутентифікаційних і ідентифікаційних засобів;

DLP-системи є спеціальними програмними рішеннями, що забезпечують захист внутрішніх мереж підприємства від витоків даних. Системи зазначеного типу формують захищений цифровий периметр підприємства, проводять аналіз всієї вихідної та вхідної інформації. В якості даних, які знаходяться під контролем, може виступати не тільки вебтрафік, але і інші інформаційні потоки (наприклад, документи, винесені за межі контуру інформаційного захисту на зовнішніх носіях, паперові носії, носії інформації, які передаються каналами Wi-Fi, Bluetooth або іншим способом);

аналіз захищеності інформаційних систем передбачає процес, під час якого перевіряється інфраструктура, зокрема й інформаційна, підприємства на наявність вразливостей та проблем в мережевому периметрі, віртуальній інфраструктурі, пов'язаних з помилками конфігурації, програмного забезпечення, вихідним кодом додатків. Тобто, в процесі аналізу захищеності виконується перевірка безпеки інформаційних систем (зовнішніх і внутрішніх);

захист віртуальної інфраструктури підприємства передбачає використання рішень та засобів, які будуть ефективні саме для неї. Спеціалізовані організації, які надають послуги в цій сфері, використовують особливі підходи до захисту віртуальної інфраструктури, які базуються на поглибленому аналізі кіберзагроз та використанні найбільш відповідних програмних продуктів, за допомогою яких буде виконана ефективна нейтралізація загроз, а також сформована комплексна система захисту віртуального середовища, що функціонує у взаємозв'язку з традиційними рішеннями;

захист від вірусів та спаму забезпечується здебільшого використанням відповідного антивірусного програмного забезпечення. У кожному виді такого програмного забезпечення можуть застосовуватися різні методи виявлення та «лікування» заражених файлів. До основних різновидів антивірусного програмного забезпечення варто віднести: сканери, монітори (сторожі), «поліфаги», «блокувальними», ревізори. Залежно від різновиду загрози (відомої або невідомої для певного антивірусу), програмне забезпечення може виконувати реактивний або проактивний захист;

міжмережеве екранування виконується через брандмауер який являє собою локальне (однокомпонентне), або функціонально-розподілене програмне забезпечення або програмно-апаратний засіб (комплекс засобів), основне завдання якого полягає в контролюванні інформації, що надходить в інфосистему і/або виходить за її межі. За допомогою міжмережевого екранування забезпечується захист інформаційної системи завдяки фільтрації інформації (її аналізу по комбінації критеріїв та прийнятті рішення про її поширення на основі заданих правил);

системи виявлення вторгнень передбачає програмні та апаратні засоби, які призначені для виявлення фактів несанкціонованого доступу до інформації, що захищається системою або мережою, будь-якого неправомірного, несанкціонованого управління нею. Системи виявлення вторгнень застосовуються для забезпечення додаткового рівня захисту системи інформаційної безпеки.

Найбільш важливим рівнем забезпечення інформаційної безпеки підприємства організаційно-управлінський рівень забезпечення, від ефективності якого залежить результативність захисту інформації та інформаційної системи на інших рівнях.

Особливість організаційно-управлінського рівня інформаційної безпеки підприємства полягає в створенні надійного механізму захисту інформації на адміністративно-правовій та організаційно-технічній основі, що виключало б (або зводило до мінімуму) можливість виникнення небезпеки доступу до конфіденційної інформації. Несанкціоноване використання конфіденційних відомостей підприємства в значній мірі обумовлюються не технічними аспектами, а зловмисними діями і халатністю користувачів або фахівців щодо їх захисту. Саме тому від людського фактору залежить ефективність здійснення захисту на фізичному, програмному, нормативно-правовому, техніко-технологічному рівнях.

Висновок. Таким чином, ефективність функціонування системи інформаційного захисту на підприємстві залежить від різних рівнів забезпечення цього захисту, особливої уваги серед яких заслуговує організаційно-управлінський рівень. Оскільки, технічний та технологічний захист інформації являє собою найбільший комплекс робіт, то управління ним є складним завданням, що і актуалізувало формування структури системи менеджменту техніко-технологічного захисту інформації в інформаційних системах на підприємстві, а також визначення напрямів та базових інструментів здійснення техніко-

технологічного менеджменту інформаційної безпеки підприємства. Зазначене дозволило охарактеризувати суб'єкти, об'єкти, особливості, функції, завдання, інструменти техніко-технологічного менеджменту інформаційної безпеки підприємства. Ефективну реалізацію системи техніко-технологічного менеджменту інформаційної безпеки підприємства пропонується реалізувати на основі моделі «Lifecycle Security», яка регламентує та описує етапи побудови корпоративної системи захисту інформації та організаційних режимів здійснення захисту інформаційної системи в цілому, що дозволяє систематично оцінювати ефект від дії технічних та організаційних засобів захисту інформації.

Перспективними напрямами досліджень є характеристика моделі «Lifecycle Security» та адаптація її застосування в межах системи менеджменту техніко-технологічного захисту інформації в інформаційних системах на підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Балановская А. В., Волкодаева А. В. Организационно-экономические механизмы обеспечения эффективности управления информационной безопасностью промышленных предприятий : монография. Самара : САГМУ, 2012. 248 с.

2. Белозеров О. И., Топоркова И. И. Программно-технические аспекты функционирования систем обеспечения информационной безопасности. *Вопросы науки и образования*. 2018. № 10(22). С. 45–47.

3. Блинов А. М. Некоторые аспекты автоматизации технологических процессов предприятий с учетом информационной безопасности. *Записки Горного института*. 2011. Т. 192. С. 136–139.

4. Бойченко О. В., Шелудько Б.А. Технологические аспекты информационной защиты объекта информатизации. Мировая наука: проблемы и инновации : материалы VIII Международной научно-практической конференции МЦНС «наука и просвещение». 2017. С. 55–58.

5. Ветрова Н. М., Гайсарова А. А. Особенности менеджмента информационной безопасности на современном этапе. *Экономика строительства и природопользования.* 2017. № 1(2). С. 64–69.

6. Двойнишников Н. Э. Технологические особенности проблем обеспечения информационной безопасности автоматизированных систем управления, являющихся объектами критической информационной инфраструктуры. *Международный журнал прикладных наук и технологий «Integral»*. 2019. № 1. С. 127–132.

7. Домарев В.В. Программно-технические методы и средства защиты информации. URL: http://www.bezpeka.com/files/lib_ru/bookdomarev03/ch_ 09.pdf (дата звернення: 19.12.2020).

8. Дячков Д. В. Стратегічні напрями управління інформаційною безпекою підприємств агропродовольчої сфери. *Український журнал прикладної економіки.* 2019. Том 4. № 4. С. 70–78.

9. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес*. 2015. № 3. С. 87–92.

10. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва : зб. наук. пр. Харківського національного автомобільно-дорожнього університету.* Харків : ХНАДУ, 2016. № 3(14). Т. 1. С. 80–88.

REFERENCES:

1. Balanovskaya, A., & Volkodayeva, A. (2012). *Organizatsionno-ekonomicheskiye mekhanizmy obespecheniya effektivnosti upravleniya informatsionnoy bezopasnost'yu promyshlennykh predpriyatiy* [Organizational and economic mechanisms for ensuring the effectiveness of information security management of industrial enterprises]. Samara: SAGMU, 248. (in Russian)

2. Belozerov, O., & Toporkova, I. (2018). Programmno-tekhnicheskiye aspekty funktsionirovaniya sistem obespecheniya informatsionnoy bezopasnosti [Software and technical aspects of the functioning of information security systems]. *Voprosy nauki i obrazovaniya – Science and education issues,* 10(22), 45–47. (in Russian)

3. Blinov, A. (2011). Nekotoryye aspekty avtomatizatsii tekhnologicheskikh protsessov predpriyatiy s uchetom informatsionnoy bezopasnosti [Some aspects of automation of technological processes of enterprises taking into account information security]. *Zapiski Gornogo instituta – Notes of the Mining Institute,* 192, 136–139. (in Russian)

4. Boychenko, O., & Shelud'ko, B. (2017). Tekhnologicheskiye aspekty informatsionnoy zashchity ob"yekta informatizatsii [Technological aspects of information protection of the object of informatization]. *Mirovaya nauka: problemy i innovatsii: materialy VIII Mezhdunarodnoy nauchno-prakticheskoy konferentsii MTSNS «nauka i prosveshcheniye» – World Science: Problems and Innovations: Proceedings of the VIII International Scientific and Practical Conference of the ICNS «Science and Education»*, 55–58. (in Russian)

5. Vetrova, N., & Gaysarova, A. (2017). Osobennosti menedzhmenta informatsionnoy bezopasnosti na sovremennom etape [Features of information security management at the present stage]. *Ekonomika stroitel'stva i prirodopol'zovaniya – Economics of construction and environmental management*, 1(2), 64–69. (in Russian)

6. Dvoynishnikov, N. (2019). Tekhnologicheskiye osobennosti problem obespecheniya informatsionnoy bezopasnosti avtomatizirovannykh sistem upravleniya, yavlyayushchikhsya ob"yektami kriticheskoy informatsionnoy infrastruktury [Technological features of the problems of ensuring information security of automated control systems that are objects of critical information infrastructure]. *Mezhdunarodnyy zhurnal prikladnykh nauk i tekhnologiy «Integral» – International journal of applied sciences and technologies "Integral",* 1, 127–132. (in Russian)

7. Domarev, V. (n.d.) Programmno-tekhnicheskiye metody i sredstva zashchity informatsii [Software and technical methods and information security tools]. Retrieved from: http://www.bezpeka.com/files/lib_ru/bookdomarev03/ch_09.pdf (in Russian)

8. Dyachkov, D. (2019). Stratehichni napryamy upravlinnya informatsiynoyu bezpekoyu pidpryyemstv ahroprodovol'choyi sfery [Strategic directions of information security management of agro-food enterprises]. *Ukrayins'kyy zhurnal prykladnoyi ekonomiky – Ukrainian Journal of Applied Economics,* 4(4), 70–78.

9. Lehominova S. (2015). Teoretychni zasady informatsiynoyi bezpeky pidpryyemstva [Theoretical principles of information security of the enterprise]. *Ekonomika. Menedzhment. Biznes – Economy. Management. Business,* 3, 87–92.

10. Markina I., & Dyachkov D. (2016). Osnovy formuvannya systemy menedzhmentu informatsiynoyi bezpeky pidpryyemstva [Fundamentals of formation of information security management system of the enterprise]. *Problemy i perspektyvy rozvytku pidpryyemnytstva: zb. nauk. pr. Kharkivs'koho natsional'noho avtomobil'no-dorozhn'oho universytetu – Problems and prospects of business development: coll. science.* Kharkiv: KHNADU, 3(14), 80–88.