

О.Д. Азаров
І.С. Колесник
В.М. Зарічний

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ КОМЕРЦІЙНИХ ПІДПРИЄМСТВ

Вінницький національний технічний університет

Анотація

Комплексна система захисту комерційних підприємств охоплює сукупність організаційних, технічних, правових та кадрових заходів, спрямованих на забезпечення безпеки майна, інформації, фінансів і персоналу підприємства. Її основне завдання — запобігання загрозам, мінімізація ризиків та забезпечення безперервності діяльності компанії. У роботі розглянуто основні елементи комплексного захисту, принципи його побудови та практичні заходи, що застосовуються на сучасних підприємствах.

Ключові слова: безпека підприємства; інформаційна безпека; фізична охорона; ризики; захист інформації; комерційна діяльність; комплексна система захисту.

Abstract

The comprehensive security system of commercial enterprises includes a set of organizational, technical, legal, and personnel measures aimed at protecting property, information, finances, and employees. Its main task is to prevent threats, minimize risks, and ensure the uninterrupted functioning of the company. This paper examines the main components of comprehensive security, principles of its development, and practical measures used in modern enterprises.

Keywords: enterprise security; information security; physical protection; risks; data protection; commercial activity; comprehensive security system.

Вступ

Сучасні комерційні підприємства працюють у надзвичайно конкурентному й водночас ризикованому середовищі, де кожен елемент діяльності може стати об'єктом посягання або зовнішнього втручання. Поширення цифрових технологій, зростання обсягів комерційної інформації, активний розвиток електронного бізнесу та збільшення кількості кіберзагроз роблять питання безпеки одним із ключових для будь-якої організації, незалежно від масштабів її діяльності. Окрім загроз цифрового характеру, сучасний бізнес стикається з фізичними ризиками, такими як крадіжки, несанкціоноване проникнення, пошкодження майна, а також з внутрішніми викликами — недобросовісністю персоналу, витоком конфіденційних даних, порушенням регламентів і необізнаністю співробітників щодо правил безпеки.

У цих умовах підприємство не може обмежитись використанням окремих заходів, спрямованих лише на захист інформації або фізичної інфраструктури. Необхідним є створення комплексної, багаторівневої системи, що охоплює всі напрями діяльності підприємства: організаційний, технічний, правовий, кадровий, інформаційний, фінансовий та операційний. Така система покликана не тільки реагувати на вже існуючі загрози, а й передбачати їх, забезпечуючи стабільну, безперебійну та передбачувану роботу бізнесу. Саме тому актуальність формування цілісної системи безпеки постійно зростає, а підприємства все частіше розглядають її як стратегічний елемент управління, що забезпечує конкурентні переваги, підтримує довіру партнерів та зберігає цінні ресурси.

Основна частина

Комплексна система захисту комерційних підприємств являє собою поєднання взаємопов'язаних заходів, методів і механізмів, спрямованих на запобігання зовнішнім і внутрішнім загрозам, а також на мінімізацію їх наслідків у разі виникнення. Її основу становить стратегія безпеки, що визначає політику доступу, порядок обробки інформації, принципи взаємодії між підрозділами та норми поведінки персоналу. Важливою складовою є організаційний компонент, який формує структуру управління безпекою, розподіляє відповідальність, встановлює процедури контролю та регулює всі внутрішні процеси, пов'язані із захистом ресурсів. Без чітко визначених правил та їх дотримання будь-які технічні або правові засоби втрачають ефективність.

Особливе місце в системі безпеки займає фізичний захист підприємства. Сюди належить облаштування охоронних систем, встановлення відеоспостереження, використання механізмів контролю доступу, створення пропускового режиму та забезпечення охорони матеріальних цінностей. Ці заходи покликані не тільки перешкоджати проникненню сторонніх осіб, а й мінімізувати ризики крадіжок, псування майна чи диверсій. Ефективна фізична безпека також передбачає правильне планування території, організацію освітлення, ведення журналів доступу та контроль роботи охоронного персоналу.

Не менш важливою є інформаційна безпека, оскільки більшість комерційних процесів тісно пов'язані з використанням електронних даних. Підприємства зобов'язані захищати свої інформаційні ресурси від кібератак, несанкціонованих змін, викрадення комерційної таємниці та поширення конфіденційних відомостей. Для цього необхідно впроваджувати системи шифрування, антивірусний захист, брандмауери, засоби контролю доступу, резервне копіювання та моніторинг мережевої активності. Важливу роль відіграє навчання персоналу, оскільки людський фактор часто стає найслабшим місцем у системі. Поінформовані співробітники здатні правильно реагувати на фішингові атаки, уникати небезпечних дій та дотримуватися політик безпеки.

Правова складова комплексного захисту забезпечує юридичну захищеність підприємства. Створення договорів про нерозголошення комерційної інформації, визначення відповідальності за порушення правил доступу, дотримання вимог законодавства щодо обробки персональних даних та захисту інформації — усе це формує правові рамки, у межах яких підприємство може ефективно протидіяти загрозам і притягувати винних до відповідальності. Юридична підтримка також допомагає захищати інтереси компанії в судах, укладати безпечні контракти з партнерами та уникати недобросовісних дій контрагентів.

Не можна недооцінювати й кадрову безпеку, яка охоплює всі аспекти роботи з персоналом — від перевірки кандидатів при прийомі на роботу до забезпечення внутрішнього контролю у процесі трудової діяльності. Співробітники можуть бути як найважливішим ресурсом підприємства, так і потенційним джерелом загроз. Тому необхідно контролювати рівень їх доступу до комерційної інформації, проводити інструктажі з безпеки, оцінювати ризики, пов'язані з кадровими переміщеннями, та формувати корпоративну культуру, що стимулює відповідальне ставлення до безпеки.

Комплексна система захисту не може існувати без принципів, що забезпечують її цілісність і ефективність. Вона повинна бути безперервною, постійно діючою та здатною адаптуватися до нових форм загроз. Рівень захисту має відповідати рівню ризиків, а всі заходи повинні бути економічно доцільними, що показано на рисунку 1, [1]. Водночас система не повинна ускладнювати діяльність підприємства — її завдання полягає у підтриманні стабільної роботи бізнесу, а не у створенні додаткових перешкод.



Рисунок 1 – Схема економічного захисту підприємства

Також необхідно враховувати характер загроз, що постійно еволюціонують. Підприємства стикаються з кібератаками, шахрайством, витоком даних, зловмисними діями співробітників, порушенням поставок, форс-мажорними обставинами та іншими ризиками. Для мінімізації наслідків впроваджуються системи реагування на інциденти, проводиться регулярний аудит безпеки, здійснюється аналіз ризиків та формуються плани відновлення роботи після надзвичайних ситуацій. Ефективний захист завжди має превентивний характер, тобто спрямований не тільки на реагування, але й на попередження загроз.

Висновки

Комплексна система захисту є ключовою умовою стабільного функціонування сучасних комерційних підприємств. Її багаторівнева структура забезпечує взаємодію організаційних, технічних, правових, інформаційних та кадрових механізмів, що разом формують надійний захисний комплекс. Реалізація такої системи дозволяє підприємству протистояти як зовнішнім, так і внутрішнім загрозам, зберігати матеріальні й цифрові ресурси, підтримувати безперервність бізнес-процесів та забезпечувати конкурентні переваги на ринку. У сучасних умовах, коли ризики стають дедалі складнішими й різноманітнішими, важливість комплексного підходу до безпеки лише зростає, роблячи його невід’ємною частиною стратегії будь-якого успішного підприємства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Система управління економічною безпекою підприємства веб-посібники ВНТУ
2. Delta Guard – Система безпеки підприємства
3. <http://www.economy.nayka.com.ua/?op=1&z=4497K>
4. Resit - Методи захисту інформації для підприємства

Науковий керівник: **Азаров Олексій Дмитрович**, доктор технічних наук, професор, завідувач кафедри ОТ, Вінницький національний технічний університет, м. Вінниця, e-mail: azarov2@vntu.edu.ua

Колесник Ірина Сергіївна – к.т.н., доцент, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця.

Зарічний Віктор Миколайович, студент групи ІСП-236, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця zvitmirs@gmail.com

Academic supervisor **Azarov Olexiy D.**, Doctor of Technical Sciences, Professor, Head of the Department of Computer Engineering, Vinnitsa National Technical University, Vinnitsia, e-mail: azarov2@vntu.edu.ua

Iryna S. Kolesnyk – PHD, candidate of engineering sciences, associate professor of department of the computing engineering, Vinnytsya national technical university, Vinnytsya.

Zarichnyy Victor M., student of group 2SP-23B, faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, zvitmirs@gmail.com