Саврацький О.О.
аспірант кафедри кібербезпеки
НУ«ОЮА»
м.Одеса, Україна

НОРМАТИВНО-ПРАВОВИЙ ФУНДАМЕНТ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ПІДПРИЄМСТВА

Однією з характерних рис інформаційного суспільства є те що питання безпеки в кіберсередовищі стають одними із найважливіших в усіх сферах людської діяльності. Якщо мова йде про економічну сферу, можна стверджувати, що зростаюча залежність від інформаційних технологій та мережевих систем робить сучасні підприємства вразливими до кіберзагроз. Адже, без належного захисту, кібератаки та інші форми втручання можуть призвести до значних фінансових втрат, погіршення репутації та низки прямих юридичних наслідків. Керівництво підприємств може самостійно побудувати власну систему кібербезпеки або звернутися до зовнішніх консультантів, які проаналізують ситуацію та розроблять стратегію захисту на випадок різних інцидентів [3, с. 146]. При цьому відповідні заходи потрібно вживати не тільки для самого підприємства , але й для всього ланцюга контрагентів, включаючи аутсорсингові компанії.

У цьому контексті належний нормативно-правовий фундамент відіграє ключову роль у формуванні ефективної стратегії управління кібербезпекою. Кінцева мета при цьому полягає у забезпеченні конфіденційності, цілісності та доступності (в тому числі й контексті зручності) інформації, що зберігається та обробляється в комп'ютерних системах. Дотримання законодавчих вимог, впровадження міжнародних стандартів та постійне вдосконалення внутрішніх процесів дозволяють підприємствам не лише мінімізувати ризики, але й підвищити свою конкурентоспроможність на ринку.

Саме нормативно-правове регулювання встановлює обов'язкові вимоги та стандарти, яких повинні дотримуватися підприємства для забезпечення належного рівня кібербезпеки основних бізнес-процесів. Воно визначає правові рамки, у межах яких організації можуть розробляти та впроваджувати політики, процедури та технологічні рішення, спрямовані на захист інформаційних ресурсів.

Насамперед, управління інформаційною та кібербезпекою здійснюється із дотриманням міжнародних стандартів, таких як ISO/IEC 27001. Вони допомагають підприємствам ідентифікувати ризики, розробляти відповідні заходи контролю та реагування на інциденти, постійно вдосконалювати власну систему безпеки. Дотримання зазначених стандартів сприяє підвищенню довіри з боку партнерів та клієнтів, а також полегшує доступ до міжнародних ринків.

Національні законодавчі акти визначають специфічні вимоги до захисту інформації та кібербезпеки в межах конкретної країни. Наприклад, в Україні діє Закон «Про основні засади забезпечення кібербезпеки України», який встановлює правові та організаційні основи державної політики у сфері кібербезпеки. Саме він визначає обов'язки суб'єктів господарювання щодо захисту критичної інформаційної інфраструктури та забезпечення стійкості інформаційних систем. [5]

Ще одним важливим об'єктом регулювання в контексті забезпечення кібербезпеки є персональні дані. Слід зауважити, що Європейський Загальний регламент про захист даних (GDPR) встановлює достатньо суворі вимоги до обробки та зберігання персональних даних громадян ЄС. Зокрема, підприємства, що працюють з цими даними, повинні забезпечувати їхню конфіденційність, цілісність та доступність, а також дотримуватися принципів законності, прозорості та обмеження мети обробки. [1] Паралельно із цим окремі галузі економіки мають й власні специфічні нормативні вимоги щодо питань кібербезпеки. Зокрема, у фінансовому секторі діють стандарти PCI DSS щодо захисту платіжних карток, а в енергетичній сфері — нормативи щодо захисту критичної інфраструктури. Вказані акти

встановлюють додаткові вимоги до підприємств, враховуючи особливості їхньої діяльності та потенційні ризики і вразливості. [6]

В усьому світі недотримання нормативно-правових вимог до кібербезпеки призводить до серйозних юридичних наслідків для підприємств. Це можуть бути фінансові штрафи, кримінальна відповідальність керівництва та співробітників, а також репутаційні втрати. Тому на рівні менеджменту підприємствам важливо не лише розуміти вимоги законодавства, але й активно впроваджувати їх у повсякденну діяльність. На локальному рівні ефективне управління кібербезпекою вимагає розробки внутрішніх політик та процедур, які б відповідали нормативно-правовим вимогам та специфіці діяльності підприємства. Ці документи регулюють питання доступу до інформаційних систем, реагування на інциденти безпеки, управління ризиками та інші критичні аспекти. [2]

Останнім часом найслабшою ланкою в системі кібербезпеки виступає людський фактор. В цьому сенсі регулярне навчання та підвищення обізнаності співробітників щодо актуальних загроз, політик безпеки та нормативних вимог допомагає зменшити кіберризики, пов'язані з помилками або недбалістю персоналу. Серед конкретних заходів можна виокремити консультування співробітників з питань захисту інформації, моніторинг рівня ризиків та безпеки, формування механізмів реагування на інциденти, налаштування окремих елементів системи безпеки, створення команд безпеки та керування технічними фахівцями.

Участь окремих підприємств у професійних спільнотах та їхня співпраця з державними органами мають надати додаткові ресурси та знання для покращення кіберзахисту. Вказана співпраця включає доступ до інформації про нові загрози, методи їхнього запобігання та можливість впливати на формування нормативно-правового середовища.

Відтак нормативно-правовий фундамент є критично важливим для ефективного управління кібербезпекою підприємства. Він надає необхідні рамки та стандарти, що дозволяють організаціям захищати свої інформаційні ресурси від сучасних та майбутніх загроз. Дотримання міжнародних стандартів, таких як ISO/IEC 27001, та національного законодавства забезпечує не лише юридичну відповідність, але й підвищує довіру з боку клієнтів і партнерів [4]. Розуміння важливості кібербезпеки та інтеграція її в загальну стратегію розвитку підприємства є невід'ємними складовими успіху в сучасному цифровому середовищі. Не слід забувати, що кіберзагрози постійно еволюціонують, тому підприємства повинні регулярно проводити аудити безпеки, моніторити відповідність вимогам законодавства та оновлювати свої політики та процедури. Лише комплексний та проактивний підхід до управління кібербезпекою забезпечить стійкість та розвиток підприємства в умовах постійно зростаючих кіберзагроз і швидких технологічних змін.

Література:

1. ISO/IEC 27001:2013. Інформаційні технології — Системи управління безпекою інформації — Вимоги. URL: https://dnaop.com/html/62498/doc-%D0%94%D0%A1%D0%A2%D0%A3_ISO_IEC_27001_2015

2. Payment Card Industry Data Security Standard (PCI DSS) Version 3.2.1, May 2018. URL: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

3. Горбаченко С. А. Місце менеджменту кібербезпеки у сучасній управлінській науці та практиці. *Сталий розвиток економіки*. 2024. № 1(48). С. 144-149.

4. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 27.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. Дата оновлення : 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

6. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року щодо захисту фізичних осіб у зв'язку з обробкою персональних даних та щодо вільного переміщення таких даних (GDPR). URL: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX%3A32016R0679