Лунгол Ольга Миколаївна
к.пед.н., доц., доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки,
Торгало Павло Романович
рядовий поліції, курсант 109 н.вз. факультету підготовки фахівців для підрозділів кримінальної поліції,
Донецький державний університет внутрішніх справ,
м. Кропивницький, Україна

АНАЛІЗ ТА УПРАВЛІННЯ РИЗИКАМИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сфера інформаційної безпеки є ключовою для багатьох організацій та установ. Цифрова трансформація вимагає ефективних заходів із захисту конфіденційності, цілісності та доступності інформації, оскільки зі зростанням комплексності технологічного середовища підвищується і рівень ризиків. Аналіз та управління ризиками є важливою складовою стратегії інформаційної безпеки, спрямованою на забезпечення стійкості та витривалості організації.

Науковці Іванченко Н. та Подскребко О. [1] зазначають, що управління інформаційною безпекою є невід'ємною складовою загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу і вдосконалення заходів в області інформаційної безпеки. Вони відносять до цієї системи організаційні структури, інформаційну політика, дії з планування, обов'язки, процедури, процеси і ресурси. Костюк Ю. та Самойленко Ю. [2] до основних методів моніторингу інформаційно-комунікаційних систем та мереж для аналізу та управління ризиками відносять: активний та пасивний моніторинг, моніторинг мережі, заснований на маршрутизації та моніторинг за аномальною поведінкою. На важливості аналізу та управління ризиками в сфері інформаційної безпеки акцентують науковці Хохлачова Ю. [3], Гаврилова А. [3], Габорець О. [4] та Агішева А., і особливу увагу звертають на зростання частки злочинів, які вчиняються за допомогою Інтернет-мереж на державний і фінансовий сектор.

Під час аналізу ризиків у сфері інформаційної безпеки в першу чергу слід проводити ідентифікація ризиків в управлінні інформаційною безпекою. Ідентифікація ризиків – це систематичний процес визначення та описування можливих загроз і вразливостей, які можуть призвести до негативних наслідків для інформаційної безпеки організації. Цей етап є першим і ключовим кроком у процесі управління ризиками. Він має починатися зі збору інформації про різні аспекти діяльності організації, включаючи існуючі системи, процеси, персонал та зовнішнє середовище. Далі має здійснюватися ідентифікація можливих загроз, які можуть виникнути внаслідок взаємодії з інформаційними ресурсами

організації. Наприклад, технічні загрози (віруси, хакери), організаційні або людські аспекти. Важливо провести аналіз слабких місць в інформаційних системах, процесах чи практиках, які можуть бути використані зловмисниками для вчинення атак або порушення безпеки, можливих фінансових втрат, репутації та інших наслідків.

До інструментів ідентифікації ризиків можна віднести проведення аудитів безпеки, аналіз можливих сценаріїв інцидентів та їх можливих наслідків, співпраця з експертами в сфері інформаційної безпеки для виявлення загроз та вразливостей тощо.

Ідентифікація ризиків є важливим етапом в управлінні інформаційною безпекою, який дозволяє компаніям заздалегідь визначити потенційні проблеми та прийняти заходи для їх запобігання чи зменшення впливу. Вона створює основу для подальшого аналізу та розробки стратегії управління ризиками.

На основі аналізу ризиків визначається стратегія управління ризиками, яка може включати в себе уникання, зменшення, перенесення чи прийняття ризиків. Заходи для зменшення ризиків мають гармонійно поєднувати технічні, організаційні та правові заходи, спрямовані на покращення систем безпеки та зменшення можливості виникнення загроз. Сфера інформаційної безпеки постійно змінюється, тому важливо постійно моніторити ефективність прийнятих заходів та адаптувати стратегії управління ризиками відповідно до нових викликів.

Аналіз та управління ризиками в сфері інформаційної безпеки є постійним процесом, який дозволяє організаціям ефективно реагувати на зростаючі загрози та зберігати високий рівень безпеки своєї інформації. Аналіз та управління є важливими елементами стратегічного підходу до забезпечення стійкості організації в умовах зростаючих загроз та мінливого інформаційного середовища. З врахуванням високої динаміки технологічного прогресу, кількісного та якісного зростання кіберзагроз, важливість аналізу та управління ризиками є надзвичайно актуальною.

Список літератури

1. Іванченко Н., Подскребко О. Особливості реалізації системи управління інформаційною безпекою. Collection of Scientific Papers «SCIENTIA». March 24, 2023. Zagreb, Croatia, 19–21. Retrieved from https://previous.scientia.report/index.php/archive/article/view/813

2. Костюк Ю.В., Самойленко Ю.О. Моніторинг інформаційної безпеки в інформаційно-комунікаційних системах та мережах. *Матеріали II Міжнародної науково-практичної конференції «Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці»* (м. Київ, 7 грудня 2021 року). К.: ДУІТ, ХНУРЕ. 2021. С. 670–673.

3. Хохлачова Ю.Є., Гаврилова А.А. аналіз загроз безпеки інформації в сучасних інформаційно-комунікаційних системах і мережах. Challenges and threats to critical infrastructure. Detroit (Michigan, USA), 2023. С. 42–46.

4. Haborets O. Ensuring cybersecurity of Ukraine against cyberterrorism threats: a systematic approach. Наукові інновації та передові технології. №11 (25), 2023. С. 97–205. DOI: https://doi.org/10.52058/2786-5274-2023-11(25)-197-205