УДК 004.432
DOI https://doi.org/10.32689/maup.it.2024.4.3

Тетяна ВАВРИК
асистент кафедри інженерії програмного забезпечення,
Івано-Франківський національний технічний університет нафти і газу, vavruk1060@gmail.com
***ORCID:** 0000-0002-0612-0084*

Ліда ГОБИР
асистент кафедри інженерії програмного забезпечення,
Івано-Франківський національний технічний університет нафти і газу,
lidagobyr@gmail.com

ОПТИМІЗАЦІЯ ЗАХИСТУ ДАНИХ: ПРЕВЕНТИВНІ ТА РЕАКТИВНІ СТРАТЕГІЇ

Анотація. *У статті досліджуються ключові аспекти оптимізації захисту даних в умовах постійно зростаючих кіберзагроз. Автори виокремлюють дві основні категорії стратегій: превентивні, які спрямовані на запобігання інцидентам, та реактивні, що акцентують увагу на реагуванні на вже виниклі загрози.*

Мета роботи *дослідження основних підходів до забезпечення безпеки даних у сучасних інформаційних системах. Стаття розглядає ефективні превентивні стратегії для попередження витоків або несанкціонованого доступу до інформації, а також реактивні стратегії для відновлення систем та мінімізації наслідків кіберінцидентів.*

Методологія. *Огляд наукових публікацій, що стосуються стратегій захисту даних. Вивчення нормативних документів щодо захисту інформації.*

Це дозволить встановити сучасний стан проблеми та визначити найбільш ефективні превентивні і реактивні методи захисту. Аналіз превентивних стратегій використання методу порівняння різних підходів до захисту даних. Оцінка реактивних стратегій захисту таких як, відновлення після інцидентів, моніторинг атак та реагування на інциденти.

Наукова новизна. *Розробка методології оптимізації витрат на заходи з кібербезпеки. Це дозволяє визначити оптимальний баланс між проактивними і реактивними заходами безпеки. Введення комплексної оцінки, яка враховує не тільки витрати на реалізацію технологій, але й економічний ефект від зниження ризику безпеки та оперативного відновлення після атак.*

Висновки *дослідження підкреслюють важливість комплексного підходу до захисту даних, який поєднує превентивні та реактивні заходи, забезпечуючи більш надійний рівень інформаційної безпеки, а також зменшити ризики в умовах швидко змінюваного кіберпростору Це може бути корисними для фахівців у галузі інформаційних технологій, безпеки даних і стратегічного управління.*

Ключові слова: *захист даних, оптимізація, превентивні стратегії, реактивні стратегії, кібербезпека, політики безпеки.*

Tetiana VAVRYK, Lida HOBYR. OPTIMIZING DATA PROTECTION: PREVENTIVE AND REACTIVE STRATEGIES

Abstract. *The article examines key aspects of optimizing data protection in the face of ever-increasing cyber threats. The authors identify two main categories of strategies: preventive, which are aimed at preventing incidents, and reactive, which focus on responding to threats that have already occurred.*

The purpose of the work *is to study the main approaches to ensuring data security in modern information systems. The article considers effective preventive strategies to prevent leaks or unauthorized access to information, as well as reactive strategies to restore systems and minimize the consequences of cyber incidents.*

Methodology. *Review of scientific publications related to data protection strategies. Study of regulatory documents on information protection.*

This will allow to establish the current state of the problem and determine the most effective preventive and reactive protection methods. Analysis of preventive strategies using the method of comparing different approaches to data protection. Evaluation of reactive protection strategies such as, incident recovery, attack monitoring and incident response.

Scientific novelty*. Development of a methodology for optimizing costs for cybersecurity measures. This allows determining the optimal balance between proactive and reactive security measures. Introduction of a comprehensive assessment that takes into account not only the costs of implementing technologies, but also the economic effect of reducing security risk and rapid recovery after attacks.*

Conclusions. *The study's findings highlight the importance of a comprehensive approach to data protection that combines preventive and reactive measures, ensuring a more robust level of information security, as well as reducing risks in a rapidly changing cyberspace. This may be useful for professionals in the fields of information technology, data security, and strategic management.*

Key words: *data protection, optimization, preventive strategies, reactive strategies, cybersecurity, security policies.*

Вступ. Постановка проблеми. В сучасному цифровому світі, де обмін і зберігання інформації відбуваються в онлайн-режимі, захист конфіденційності, цілісності та доступності даних стає надзвичайно важливою задачею як для окремих користувачів так і для підприємств. Кіберзагрози стають все більш складними і руйнівними, змушуючи користувачів зосередитися на розробці та впровадженні ефективних стратегій захисту інформації. Розробка політики захисту даних дає змогу визначати межі ризику для кожної категорії інформації та забезпечити дотримання нормативно-правових вимог. Також ця

політика допомагає налаштувати автентифікацію й авторизацію, які визначають, кому потрібно надати доступ, до якої інформації та чому.

Важливим аспектом дослідження є порівняння ефективності превентивних та реактивних стратегій у мінімізації загроз і забезпеченні стійкості інформаційних систем. Превентивні стратегії спрямовані на попередження можливих загроз і запобігання інцидентам безпеки заздалегідь. З іншого боку, реактивні стратегії орієнтовані на виявлення інцидентів та реагування після їх виникнення.

Аналіз останніх досліджень і публікацій. Захист даних є одним із найважливіших аспектів у сучасному інформаційному суспільстві. Дослідження в цій сфері зосереджуються на розвитку стратегій, які можуть забезпечити безпеку інформаційних систем. Інтернет дав потужний поштовх для розвитку масової комунікації, торгівлі та обміну інформацією. Разом з тим сьогодні він є тією сферою, де здійснюється чимало правопорушень. Суттєве зростання кількості інцидентів у кіберпросторі обумовлює необхідність системного аналізу джерел виникнення загроз [1–3], на перше місце серед яких виходить фішинг. У роботі [2] отримано класифікатор та розглядаються можливості його використання для подальшого створення програмних рішень для розпізнавання фішингових сайтів [2].

Користувачі зараз використовують стратегію даних для покращення кібербезпеки за допомогою систем автоматичного реагування на наслідки (AMR), особливо в контексті боротьби зі складними загрозами. Дослідницька стаття [2] містить ретельний аналіз цього явища, вивчення його наслідків для операцій, розподілу ресурсів і довіри до автоматизації. Крім того, автори пропонує зрозуміти складності, пов'язані з управління хибними спрацьовуваннями, підкреслюючи необхідність ефективних механізмів перевірки [2].

Штучний інтелект і машинне навчання нещодавно зробили видатний внесок у продуктивність інформаційних систем і безпеку кібер-фізичних систем. У цій галузі було проведено безліч досліджень, що призвело до спалаху публікацій за останні два роки. Вибір правильного алгоритму для вирішення складної проблеми безпеки в дуже точному промисловому контексті є складним завданням. Автори статті [4] пропонують структуру рекомендацій щодо алгоритму навчання, яка для чітко визначеної ситуації керує вибором алгоритму навчання та наукової дисципліни (наприклад, RNN, GAN, RL, CNN тощо). Ця структура має перевагу в тому, що вона була створена на основі обширного аналізу літератури, як показано в цій статті для рекурентних нейронних мереж та їх варіацій [4].

У роботах [5–6] запропоновано інформаційну технологію моніторингу безпеки даних програмного забезпечення. Передбачається, що розроблена інформаційна технологія моніторингу безпеки даних програмного забезпечення набуде широкого використання не лише в комерційній розробці програмного забезпечення, але і в навчальному та науковому застосуванн [5, 7].

У роботах [8–10] виділені два дуже різні підходи до надання IT-підтримки. Неправильна стратегія може негативно вплинути на здатність служби підтримки оперативно вирішувати проблеми. Це може призвести до тривалих відключень і тривалого часу очікування вирішення проблеми . Реактивний підхід може змусити команду підтримки виправляти проблеми з наслідками, які впливають на загальне IT-середовище. Проактивні стратегії передбачають більш обережний і ефективний підхід до надання IT-підтримки. Проактивна стратегія передбачає розробку планів вирішення різних проблем ще до їх виникнення [10].

Метою статті є аналіз та оптимізація стратегій захисту даних в інформаційних системах, зокрема визначення ефективності превентивних і реактивних заходів у контексті запобігання і реагування на загрози безпеці. Дослідження також спрямоване на розробку рекомендацій щодо впровадження комплексного підходу до захисту даних, що дозволить підвищити стійкість до кібератак і забезпечити безпечнішу обробку інформації.

Виклад основного матеріалу дослідження

Превентивні стратегії захисту інформації. Превентивні стратегії захисту інформації спрямовані на запобігання потенційним загрозам та атакам заздалегідь. Їх основною метою є мінімізація ризиків та зменшення ймовірності виникнення вразливостей у системах та даних. Однією з основних переваг превентивних стратегій є їх здатність передбачити та попередити можливі загрози, що дозволяє організаціям підготуватися та вжити заходів у відповідь на них заздалегідь.

Превентивні стратегії захисту інформації включають широкий спектр заходів, спрямованих на запобігання можливим загрозам та атакам до їх виникнення. Ось деякі з основних компонентів превентивних стратегій:

1. Політика безпеки: Розробка чітких політик і стандартів безпеки для організації, що встановлюють правила щодо управління доступом, шифрування даних, регулярного оновлення програмного забезпечення тощо.

2. Шифрування даних: Застосування шифрування для захисту конфіденційної інформації від несанкціонованого доступу, забезпечуючи безпеку даних навіть у випадку втрати контролю над ними.

3. Управління доступом: Встановлення строгих прав доступу згідно принципу найменших привілеїв, що дозволяє обмежити доступ до даних лише для необхідних користувачів.

4. Регулярне оновлення програмного забезпечення: Вчасне встановлення патчів безпеки і оновлень програмного забезпечення для усунення вразливостей і запобігання атак.

5. Безпечне зберігання паролів: Використання безпечних методів зберігання паролів, таких як хешування та сіль.

6. Фізичний захист: Захист фізичного доступу до приміщень, серверних кімнат та інших просторів, де зберігається інформація.

7. Антивірусне програмне забезпечення та брандмауери: Використання програмних засобів для виявлення та запобігання вторгнень, включаючи віруси, шкідливі програми та несанкціонований доступ.

8. Захист мережі: Використання технічних засобів, таких як брандмауери та веб-фільтри, для моніторингу та блокування небажаного мережевого трафіку.

9. Резервне копіювання даних: Регулярне створення резервних копій даних і зберігання їх в безпечному місці для відновлення в разі втрати або пошкодження.

Реактивні стратегії захисту.

Реактивні стратегії, спрямовані на виявлення і реагування на загрози після їх виникнення. Ці стратегії спрямовані на реагування на інциденти безпеки, коли вони вже сталися, і їх мета – мінімізувати наслідки атак або порушень безпеки. Наприклад, регулярні аудити безпеки, моніторинг активності користувачів та вжиття заходів у разі виявлення атаки.

Моніторинг та виявлення загроз: Реактивні стратегії починаються з ефективного виявлення загроз. Для цього використовуються системи моніторингу і виявлення вторгнень (IDS), програми для аналізу аномалій в мережевому трафіку або на комп'ютерах, а також засоби для моніторингу безпеки. Чим раніше інцидент буде виявлений, тим швидше можна почати реагувати на нього. Постійний моніторинг систем та мереж для виявлення незвичайної або підозрілої активності, яка може вказувати на потенційні загрози.

Інцидентний відгук: Реагування на виявлені або підтверджені загрози шляхом запуску планів реагування на інциденти. Це може включати блокування атак, відключення компрометованих систем або зупинку небезпечних процесів. Також створення плану дій для команд безпеки, щоб оперативно і ефективно вирішувати проблему.

Відновлення після інциденту: Одна з основних цілей реактивної стратегії– швидке відновлення нормальної роботи після інциденту. Це може включати відновлення втрачених або пошкоджених даних з резервних копій, відновлення доступу до систем або перегляд безпекових налаштувань для запобігання повторним інцидентам.

Аналіз інциденту: Після того, як інцидент було ліквідовано, дуже важливо проаналізувати його і прийняти заходи для підвищення рівня безпеки в майбутньому. Це може включати коригування політик безпеки, оновлення програмного забезпечення, навчання персоналу щодо нових загроз або поліпшення методів моніторингу. Також аналіз слабких місць в системі, які дозволили інциденту статися, та внесення відповідних покращень.

Навчання та підвищення свідомості: Після інциденту проводиться навчання персоналу та вдосконалення політик безпеки для підвищення стійкості до майбутніх атак. Інформування персоналу про інциденти та навчання їх, як уникати подібних ситуацій у майбутньому.

Політики та процедури відновлення: Визначення чітких політик та процедур для відновлення після інцидентів, включаючи регулярні аудити та оцінку ефективності.

Превентивні та реактивні стратегії захисту інформації мають різний підхід до забезпечення безпеки системи, і кожна з них має свої особливості, переваги та недоліки. Порівняємо ці підходи (табл. 1).

Тепер розглянемо недоліки кожної стратегії (рис. 1).

Пропонуємо наступну формулу, яка дозволить оцінити, наскільки ефективною є кожна стратегія захисту в контексті конкретного випадку, враховуючи як вигоди, так і витрати, пов'язані з її впровадженням та використанням.

$$E = \frac{(P_k \cdot P_b \cdot V_r \cdot T_c) - (P_l \cdot P_b \cdot V_c \cdot T_r)}{C_i \cdot C_P} \cdot F_r \cdot F_v \cdot F_a \cdot F_t$$

Де E – ефективність стратегії захисту інформації; P_k – потенційний ризик загрози; P_b – ймовірність виявлення загрози; V_r – вартість відновлення після загрози; T_c – тривалість кризового періоду; P_l – потенційний втрати від загрози; V_r – вартість відновлення після загрози; T_r – тривалість реагування на загрозу; C_i – вартість інвестицій у стратегію захисту; C_p – вартість захисту інформації; F_r – фактор ризику; F_v – фактор вразливості; F_a – фактор адаптивності; F_t – фактор часу;

Таблиця 1

Порівняльний аналіз кожної стратегії

Критерій	Превентивні стратегії	Реактивні стратегії
Основна мета	Запобігати виникненню загроз і атак	Виявлення та реагування на загрози та атаки після їх виникнення
Характер заходів	Попередні заходи, які призначені для мінімізації ризиків та запобігання атакам	Заходи, які вживаються після виникнення загрози або атаки для нейтралізації їх впливу та відновлення безпеки
Вартість	Зазвичай вимагає менших витрат, оскільки передбачається витрачання ресурсів перед подією	Може вимагати більших витрат, оскільки включає в себе відновлення після виникнення події
Ефективність	Може бути ефективнішою у запобіганні атак та мінімізації ризиків	Може бути менш ефективною у виявленні та нейтралізації загроз, але важлива для відновлення безпеки після події
Прогнозованість	Дозволяє заздалегідь приготуватися до можливих загроз та реагувати на них	Може бути менш передбачуваною, оскільки вимагає виявлення та реагування на непередбачені події
Превентивність	Запобігає загрозам до їх виникнення	Реагує на загрози після їх виникнення
Технічні засоби	Включає в себе використання технологічних засобів, таких як програмне та апаратне забезпечення	Може включати аудити безпеки та вирішення виявлених проблем
Організаційні аспекти	Включає в себе розроблення політик, процедур та навчання персоналу	Включає в себе впровадження політик безпеки та навчання персоналу з питань кібербезпеки
Орієнтація	Спрямована на передбачення майбутніх загроз та запобігання їм	Спрямована на виявлення та вирішення проблем після їх виникнення
Час	Вимагає часу на виявлення, відгук та відновлення після інциденту	Вимагає часу на встановлення та підтримку запобіжних заходів, але може заощадити час у майбутньому

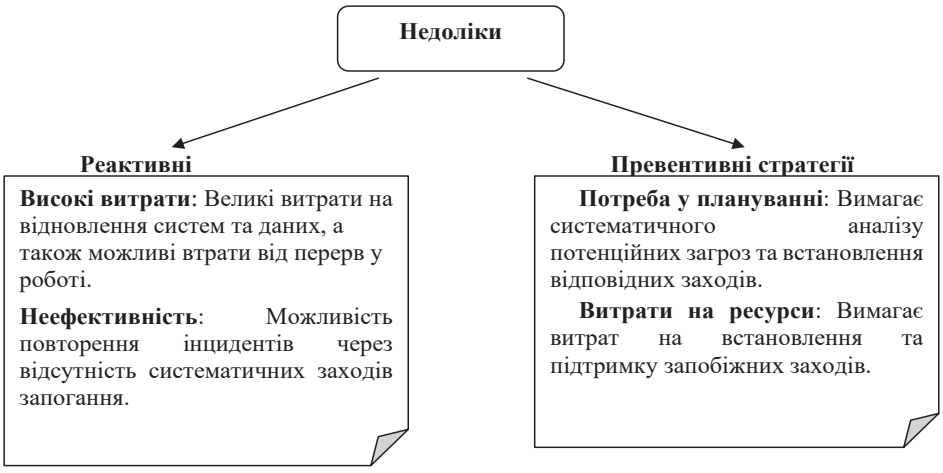

Рис. 1. Недоліки превентивної та реактивної стратегії захисту

Ця формула дозволяє врахувати різноманітні аспекти, такі як ризики, втрати, вартість та інші фактори, що впливають на ефективність стратегії захисту інформації у складних інформаційних середовищах.

Висновки даного дослідження і перспективи подальших розвідок у даному напрямку. Захист даних вимагає комплексного підходу, який включає як превентивні, так і реактивні стратегії. Порівняльний аналіз надає загальний огляд переваг та обмежень превентивних та реактивних стратегій захисту інформації. Порівнюючи превентивні та реактивні стратегії захисту інформації, можна зазначити, що обидва підходи мають свої переваги та обмеження. Успішний захист інформації вимагає поєднання як превентивних, так і реактивних стратегій. Комбінування цих стратегій дозволяє створювати комплексну систему захисту інформації, яка ефективно впорається з сучасними кіберзагрозами. Перспективи подальших досліджень можуть бути зосереджені на вдосконаленні існуючих методів та розробці нових, зокрема в контексті розвитку технологій, таких як штучний інтелект та машинне навчання. Використання сучасних методів аналізу та штучного інтелекту для виявлення аномалій і прогнозування загроз може значно підвищити ефективність реактивних стратегій.

Список використаних джерел:

1. Куперштейн Л., Луцишин Г., Кренцін М. Інформаційна технологія моніторингу безпеки даних програмного забезпечення. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. 3(23), 71–84. URL: https://doi.org/10.28925/2663-4023.2024.23.7184

2. Штонда Р., Черниш Ю., Терещенко Т., Терещенко К., Цикало Ю., Поліщук С. Класифікація та методи виявлення фішингових атак. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. 4(24), 69–80. URL: https://doi.org/10.28925/2663-4023.2024.24.6980

3. Alam, Mohammad Nazmul, et al. Phishing attacks detection using machine learning approach. In: *2020 third international conference on smart systems and inventive technology (ICSSIT)*. IEEE, 2020. 1173–1179.

4. Barreto C., Koutsoukos X. Design of Load Forecast Systems Resilient Against Cyber-Attacks. In Lecture Notes in Computer Science 2019. (pp. 1–20). *Springer International Publishing*. URL: https://doi.org/10.1007/978-3-030-32430-8_1

5. CHANTI S., CHITHRALEKHA T. A literature review on classification of phishing attacks. *International Journal of Advanced Technology and Engineering Exploration*, 2022, 9.89: 446–476.

6. Christophe Feltus. Optimizing Data Strategy for Automated Mitigation Response Security – Ransoware Case Study URL: https://www.researchgate.net/publication/380464686_Optimizing_Data_Strategy_for_Automated_Mitigation_Response_Security_-_Ransoware_Case_Study

7. Detecting Phishing Emails URL: https://meu.edu.jo/uploads/1/590422b4d5dd81.pdf Detecting Phishing Emails Using Machine Learning Techniques

8. Feltus C. Learning algorithm recommendation framework for IS and CPS security: Analysis of the RNN, LSTM, and GRU contributions. *International Journal of Systems andSoftware Security and Protection (IJSSSP)* 13, no. 1 (2022): 1–23.

9. Holmes D., Papathanasaki M., Maglaras L., Ferrag M. A., Nepal S., Janicke H. (2021, September). Digital twins and cyber security – solution or challenge? 2021 *6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Preveza, Greece. URL: https://doi.org/10.1109/SEEDA-CECNSM53056.2021.9566277

10. Optimizing IT Support: Proactive vs. Reactive Strategies. URL: https://vastitservices.com/blog/optimizing-it-support-proactive-vs-reactive-strategies/