УДК 004.056.5:004.75:004.8

Денега А.Р., здобувач,
Ящук В.І., к.екон.н., доцент,
Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

КОМПЛЕКСНИЙ ПІДХІД ДО ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Інсайдерські загрози становлять один із найнебезпечніших чинників порушення інформаційної безпеки, оскільки виникають усередині системи та часто маскуються під легітимну діяльність користувачів. Ефективний кіберзахист у таких умовах потребує поєднання поведінкової аналітики, технологічних інструментів моніторингу й організаційних заходів контролю доступу. Комплексний підхід базується на аналізі аномалій у діях користувачів, застосуванні машинного навчання, багаторівневих політиках автентифікації та принципах Zero Trust, що забезпечує підвищення кіберстійкості корпоративних мереж.

Більшість інцидентів інсайдерського характеру пов'язана не лише зі зловмисними намірами, а й із людськими помилками, низьким рівнем кіберобізнаності та нехтуванням політиками безпеки. У зв'язку зі зростанням цифрової складності організаційних інфраструктур ефективна протидія інсайдерам потребує поєднання технічних, поведінкових та організаційних методів контролю. Комплексний підхід до аналізу та запобігання інсайдерським загрозам дозволяє підвищити рівень кіберстійкості й забезпечує захист критичних даних у динамічному цифровому середовищі.

Інсайдерська діяльність здатна завдати системам значної шкоди через легітимність доступу та глибоке знання внутрішньої структури мережі. Типовими проявами таких загроз є несанкціоноване копіювання конфіденційних даних, ексфільтрація інформації через електронну пошту чи хмарні сервіси, маніпуляція критичними конфігураціями, зловживання привілейованими обліковими записами та маскування шкідливих дій у системних логах.

Ключову роль у своєчасному виявленні інсайдерської активності відіграють засоби поведінкової аналітики. Системи UEBA формують базові профілі нормальної діяльності користувачів і визначають відхилення, характерні для спроб порушення політик безпеки. Додаткову точність забезпечують SIEM-рішення, які корелюють події з різних сегментів мережі й фіксують послідовності дій, що не узгоджуються зі стандартними бізнес-процесами.

У складних інфраструктурах значущу роль відіграють алгоритми машинного навчання, здатні виявляти тонкі аномалії у патернах доступу, створювати прогнозні моделі ризику та зменшувати ймовірність хибних спрацьовувань. Важливим компонентом протидії є контроль доступу: принцип мінімальних привілеїв, сегментація мережі, регулярний аудит прав користувачів, управління привілейованими записами та застосування багатофакторної автентифікації. Zero Trust-архітектура доповнює ці механізми, оскільки передбачає постійну перевірку ідентичності користувачів, пристроїв і контексту їхніх дій.

Організаційні заходи також мають суттєвий вплив на зменшення ризиків інсайдерської активності. До них належать систематичне навчання персоналу принципам кібергігієни, моделювання соціотехнічних інцидентів, впровадження політик відповідальності та моніторинг інформаційних потоків усередині організації. Синергія технічних та організаційних інструментів створює стійку архітектуру безпеки, здатну протистояти різним формам інсайдерських загроз.

Інсайдерські загрози відзначаються високим рівнем складності через наявність у порушників легітимних прав доступу та можливість маскування шкідливої активності. Ефективна протидія вимагає застосування комплексної системи, що включає поведінкову аналітику, кореляційні механізми моніторингу, алгоритми машинного навчання, жорсткі політики контролю доступу та організаційні заходи формування культури безпеки. Інтегроване поєднання цих елементів забезпечує своєчасне виявлення аномалій, зменшує ризики витоку інформації та підвищує загальну кіберстійкість корпоративних мереж.

Список використаних джерел:

1. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations : NIST Special Publication 800-53. Gaithersburg : NIST, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2. National Institute of Standards and Technology. Zero Trust Architecture : NIST Special Publication 800-207. Gaithersburg : NIST, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final

3. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023. Athens : ENISA, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

4. Microsoft Security. Digital Defense Report 2023–2024. Microsoft Corporation, 2024. URL: https://www.microsoft.com/security/business/microsoft-digital-defense-report