

СУЧАСНІ ТЕХНОЛОГІЇ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ

Вінницький національний технічний університет

Анотація

У роботі розглянуті сучасні технології моніторингу та реагування на кіберзагрози, їх функціональні можливості, виклики впровадження та значення для забезпечення кібербезпеки, зокрема у військовій сфері.

Ключові слова: кібербезпека, моніторинг кіберзагроз, система моніторингу безпеки хоста, виявлення загроз, тестування на проникнення, управління виправленнями, захист кінцевих точок, нульова довіра, військові операції, інформаційна безпека.

Abstract

The paper examines modern technologies for monitoring and responding to cyber threats, their functionality, implementation challenges, and significance for ensuring cybersecurity, particularly in the military sphere.

Key words: cybersecurity, cyberthreatmonitoring, hostsecuritymonitoringsystem, threatdetection, penetrationtesting, patchmanagement, endpointprotection, zerotrust, militaryoperations, informationsecurity.

Вступ

У сучасному світі кіберзагрози стали невід'ємною частиною інформаційного середовища, що створює нові виклики як для окремих організацій, так і цілих держав. Постійне ускладнення методів атак потребує застосування передових технологій для моніторингу, виявлення та запобігання загрозам. Ці технології є ключовими у забезпеченні безпеки, оскільки дають змогу оперативно реагувати на інциденти, мінімізувати ризики та посилювати загальний рівень захисту. Особливе значення ці підходи мають у військовій сфері, де від своєчасного виявлення кіберзагроз залежить ефективність операцій та безпека держави. Саме тому інтеграція автоматизованих інструментів, навчання персоналу та стратегічне планування стають критичними елементами сучасної кібероборони.

Результати дослідження

Технології моніторингу кіберзагроз охоплюють автоматизовані та ручні інструменти для виявлення, аналізу і запобігання загрозам, які, будучи розгорнутими, дозволяють організаціям знизити ризик кібератак, швидко реагувати на інциденти та підвищити загальний рівень кібербезпеки. Ключові технології містять: виявлення загроз – інструменти для виявлення потенційних атак, аналізу поведінки зловмисників та запобігання вторгненням; моніторинг – безперервний моніторинг стану безпеки та відстеження активності в інформаційних системах для своєчасного реагування на підозрілу поведінку; тестування на проникнення – реальна загроза; моделювання – перевірка стійкості системи до атак. Це допомагає виявити слабкі місця та посилити захист.

Управління виправленнями – систематичне виявлення вразливостей та їх усунення шляхом встановлення оновлень та виправлень. Захист кінцевих точок – забезпечення контролю доступу та захисту від кіберзагроз до таких пристроїв, як ноутбуки, мобільні телефони та інші гаджети. Контроль доступу та захист від кіберзагроз. Технології інтегровані в комплексну систему кіберзахисту, яка автоматизує багато функцій безпеки, що дає змогу командам зосереджуватися на стратегічних завданнях. Водночас, ручні методи, як-от навчання персоналу та моделювання інцидентів, можуть допомогти підвищити обізнаність працівників та сформувати культуру кібергігієни [1].

Система моніторингу безпеки хоста – це програмно-апаратний комплекс, що відстежує, аналізує та реагує на загрози, які пов'язані з такими кінцевими пристроями в мережі, як сервери, робочі станції та ноутбуки. Основні функції системи моніторингу безпеки хоста в режимі реального часу –

моніторинг активності, виявлення підозрілої поведінки, контроль змін у системних файлах, управління виправленнями, ведення журналів подій та автоматизоване реагування на загрози. Система складається з агента на кінцевому пристрої для зборуданих, центрального сервера для обробки інформації, інтерфейсу адміністратора для управління політикою безпеки та модуля аналізу з алгоритмами машинного навчання для виявлення аномалій.

Ключові технології, що використовуються в HSMS, містять інструменти для виявлення загроз та реагування на них, поведінковий аналіз для виявлення аномалій, хмарні рішення для віддаленого управління, а також підходи нульової довіри, які вимагають перевірки всього доступу, незалежно від джерела. Основними проблемами при впровадженні таких систем є складність їх інтеграції у великі мережі, потенційне навантаження на пристрої, хибні спрацьовування та необхідність захисту самої системи від атак [2].

У сучасних умовах ведення війни важливість кібербезпеки неможливо переоцінити. Інформаційні технології стали невід'ємною частиною військових операцій, а ціна помилок і недооцінки кіберзагроз може бути надто високою. Для військових, які діють на передовій, знання і дотримання вимог кібербезпеки мають бути такими ж стандартними, як озброєння і стратегічне планування. Кібератаки є особливо небезпечними, оскільки можуть паралізувати командування і управління збройними силами, порушити зв'язок і призвести до жертв. Однак технічний захист і превентивні заходи часто відходять на другий план через постійну напруженість і необхідність вирішувати інші нагальні проблеми. Водночас, інструкції та настанови з кібербезпеки мають бути знаннями для всіх, хто задіяний в обороні країни, адже виявлення та нейтралізація кібератак вимагає своєчасного реагування та обізнаності кожного військовослужбовця. Такі заходи не лише допоможуть захистити військові об'єкти та дані, але й підвищать загальний рівень обороноздатності країни, оскільки кіберпростір став критично важливим полем битви за національну безпеку на кожному кроці [3].

Висновки

Дослідження методів моніторингу кіберзагроз показують важливість інтеграції автоматизованих і ручних інструментів для виявлення, аналізу та запобігання кіберзагрозам. Ці інструменти можуть допомогти зменшити ризик атак, швидко реагувати на інциденти та підвищити рівень кібербезпеки. Ключові технології містять виявлення загроз, моніторинг, тестування на проникнення, моделювання атак, управління виправленнями та захист кінцевих точок. Системи моніторингу безпеки хостів забезпечують моніторинг активності в режимі реального часу, виявлення підозрілої поведінки й управління виправленнями, інструменти і використання принципів нульової довіри посилюють захист, але також створюють проблеми складної інтеграції, накладних витрат на пристрої і хибно позитивних спрацьовувань. Кібербезпека має вирішальне значення у військових операціях. Кібератаки можуть паралізувати командування і мати серйозні наслідки. Військова підготовка з кібербезпеки має важливе значення для забезпечення національної безпеки в умовах сучасної війни.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Чотири елементи сильної стратегії кібербезпеки від фахівців BDO в Україні – BDO. *Міжнародна аудиторська компанія BDO – BDO*. URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/four-elements-of-a-strong-cybersecurity-strategy>.
2. Михайлишин Д. А. Система моніторингу безпеки кінцевих пристроїв/ Hostsecuritymonitoringsystem. *Кваліфікаційна робота*. URL: <http://dspace.wnu.edu.ua/bitstream/316497/46655/1/Михайлишин.pdf>
3. Кібербезпека як важлива складова всієї системи захисту держави / Міністерство оборони України. URL: <https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html>.

Оболонська Яна Олександрівна, студентка групи ІБС-22б, факультету інформаційних технологій та комп'ютерно інженерії та Кафедри військової підготовки, Вінницький національний технічний університет, Вінниця, e-mail: vn.oyana@gmail.com

Віщун Ігор В'ячеславович, викладач Кафедри військової підготовки, Вінницький національний технічний університет, м. Вінниця, e-mail: vishchunihor@gmail.com

Obolonska Yana Oleksandrivna, student of group 1BS-22b, Faculty of Information Technologies and Computer Engineering and Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: vn.oyana@gmail.com

Vishchun Igor Vyacheslavovich, Lecturer, Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: vishchunihor@gmail.com