УДК 004.7

Слободянюк А.О., магістрант
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ТА РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ БАГАТОРІВНЕВОГО ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ

Стабільність функціонування локальних мереж є ключовою умовою безперервності роботи сучасних організацій, оскільки більшість бізнес-процесів прямо залежить від доступності сервісів та збереження цілісності інформації. Зростання кількості кіберзагроз і ускладнення методів атак підсилюють потребу у системах багаторівневого мережевого захисту, здатних забезпечити раннє виявлення порушень і мінімізувати ризики компрометації інфраструктури. Особливої уваги потребують гібридні атаки, які поєднують технічні та соціальні методи впливу й долають традиційні механізми захисту. Це підкреслює важливість систем, що дозволяють отримувати цілісне уявлення про стан мережевої безпеки.

Аналіз сучасних підходів до організації мережевої безпеки показує, що значна частина технічних засобів захисту застосовується ізольовано. Міжмережні екрани, системи моніторингу, IDS/IPS або SIEM-платформи часто працюють автономно, без узгодженого обміну даними. Це породжує фрагментацію захисту: фаєрволи забезпечують фільтрацію трафіку, але не мають контексту поведінкових подій, тоді як системи моніторингу фіксують загрози, однак не можуть самостійно вплинути на трафік або блокування доступу. Це призводить до того, що частина інцидентів фіксується лише після реалізації атаки, що значно збільшує час реагування та масштаби можливих наслідків.

Порівняльний аналіз функціональних можливостей міжмережних екранів та засобів моніторингу безпеки дає можливість виокремити їх ключові переваги й обмеження. Фаєрволи характеризуються високою ефективністю у контролі доступу, сегментації мережі та фільтрації пакетів, проте їхні можливості щодо аналітики обмежені. Натомість SIEM/IDS-системи забезпечують глибокий аналіз подій, кореляцію логів і виявлення потенційних атак, але не можуть самостійно виконувати превентивні дії на рівні мережевого трафіку. Основне протиріччя полягає в тому, що жоден із цих інструментів окремо не забезпечує комплексного захисту, тоді як їхня потенційно ефективна взаємодія на практиці залишається недостатньо узгодженою.

Результати аналізу показують, що найбільш ефективною є модель, у якій фаєрвол виконує функції первинної фільтрації та контролю

доступу, а система моніторингу забезпечує збір і кореляцію подій, виявлення аномалій та формування єдиного інформаційного поля безпеки. Такий підхід рекомендується для інтеграції систем, оскільки у ізольованих реалізаціях, взаємодія між компонентами відсутня, що обмежує швидкість реагування на інциденти та повноту інформації про загрози.

На основі проведеного аналізу сформульовано рекомендації щодо організації багаторівневого захисту локальної мережі:

– забезпечити логічну сумісність міжмережного екранування та систем моніторингу через уніфіковані політики безпеки;

– застосовувати централізований збір журналів подій із мережевих пристроїв, що підвищує повноту інформаційної картини;

– використовувати кореляцію подій для раннього виявлення загроз, які не фіксуються на рівні фільтрації трафіку;

– упроваджувати сегментацію мережі як базову передумову багаторівневого захисту;

– доповнювати систему моніторингу правилами поведінкового аналізу для виявлення складних та малопомітних атак.

Окремо слід розглянути впровадження регулярного аудиту безпеки та тестування політик доступу, оскільки це дозволяє оперативно виявляти конфігураційні помилки та зменшувати площу атаки.

Таким чином, результати аналітичного дослідження свідчать, що комбінований підхід до формування багаторівневої системи захисту є найбільш ефективним з погляду підвищення стійкості мережевої інфраструктури. Поєднання міжмережного екранування та моніторингу подій дозволяє мінімізувати обмеження кожного окремого інструмента й створити узгоджену систему протидії сучасним кіберзагрозам.

Перспективним напрямом подальших досліджень є впровадження адаптивних механізмів автоматизованого реагування та використання інтелектуальних методів аналізу поведінки мережі, що забезпечить вищий рівень автономності та точності виявлення інцидентів.

Список використаних джерел:

1. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. 3rd ed. Boston: Prentice Hall, 2014, 848 p.

2. Whitman M., Mattord H. Principles of Information Security. 7th ed. Boston: Cengage Learning, 2021. 672 p.

3. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання Cisco: навч. посіб. Київ: КНУТД, 2020. 168 с.