УДК 004.75:004.49 https://doi.org/10.32515/2664-262X.2025.11(42).2.63-69

О. Б. Гуральник, **О. С. Савенко,** проф., д-р техн. наук
Хмельницький національний університет, м. Хмельницький, Україна
e-mail: gurualexua@gmail.com, savenko_oleg_st@ukr.net

Оброблення критичної інформації в корпоративних мережах на основі комбінованого підходу DLP системи з системою виявлення ботнетів

У статті досліджено сучасні методи та засоби оброблення критичної інформації в корпоративних мережах. Розглянуто технології Data Loss Prevention (DLP) як ключовий механізм захисту даних, особливості використання ботнетів для викрадення критично важливої інформації в корпоративних мережах. Запропоновано комбінований підхід, що інтегрує систему DLP з системою виявлення ботнет трафіку. Розроблено гібридну архітектуру моніторинг - виявлення - реагування - захист та реалізовано прототип, який блокує ексфільтрацію критичних даних, знижуючи хибно позитивні спрацювання до 2 %. Експериментальні результати підтверджують ефективність моделі та вказують на необхідність комплексного підходу до інформаційної безпеки.
ботнет, DLP, ексфільтрація даних, критична інформація, корпоративні мережі

Постановка проблеми. Сьогодні робота підприємств нерозривно пов’язана з інформаційними технологіями, а отже, обсяги даних, що циркулюють і зберігаються в корпоративних мережах, стрімко зростають. Це дає бізнесу ширші можливості для аналітики, оптимізації процесів та ухвалення управлінських рішень на основі достовірної інформації. Водночас збільшення масиву даних суттєво підвищує ризик їхнього витоку, який може завдати компанії серйозної шкоди.

Критичні відомості здатні зникнути як через необережність співробітників, так і внаслідок умисних дій зловмисників. Наслідком стає розкриття конфіденційної інформації, утрата інтелектуальної власності чи фінансових даних, що призводить до прямих фінансових втрат, підриву довіри клієнтів і партнерів та потенційних юридичних санкцій.

Упродовж останніх років в корпоративних мережах відбувається зміна характеру витоків даних. На заміну класичним каналам ексфільтрації (електронна пошта, хмарні сховища, знімні носії) дедалі частіше відбувається зараження вузлів мережі ботнет орієнтованим шкідливим програмним забезпеченням (ШПЗ). В 2024 році за допомогою цієї категорія ШПЗ було інфіковано 23 млн хостів і викрадено 2,1 млрд облікових даних, причому 70 % заражень припали на корпоративні системи [1].

Зростає, також, швидкість операцій з викрадення даних. У 45 % інцидентів дані виводяться менш ніж за добу після первинної компрометації, а медіанне вікно між зломом і ексфільтрацією скоротилося до двох діб [2].

Ботнети еволюціонують у багатофункціональні платформи. Дослідження [3] показало, що у 2024 році найбільший активний ботнет налічував 227 000 пристроїв, а спектр його застосування включав не лише DDoS, а й масштабні кампанії з викрадення конфіденційних файлів та облікових даних. У результаті традиційні DLP системи, сконцентровані на контролі вихідного трафіку, виявляються неефективними проти фрагментарного й шифрованого витоку, що відбувається всередині ботнет каналу керування й обміну.

Таким чином, наукова й прикладна проблема полягає у створенні комбінованого підходу, що інтегрує механізми DLP з високоточним виявленням ботнет активності на рівні мережевої поведінки й телеметрії кінцевих точок. Розв'язання цього завдання критично важливе для захисту критичної інформації підприємств від стрімкого, малопомітного витоку. Скорочення часу реакції SOC-підрозділів до рівня, коли ексфільтрація ще не завершена. Підвищення стійкості корпоративних мереж до складних комбінованих атак, у яких ботнет є початковим або проміжним елементом.

Аналіз останніх досліджень і публікацій. У роботі [4] запропонували багатокласову AI-систему виявлення ботнетів у зашифрованому трафіку, яка поєднує гібридну модель KNN + Random Forest із методами Explainable AI (SHAP, LIME). Завдяки глибокому препроцесингу (PCA, SMOTE) й оптимізації гіперпараметрів автори досягли точності 0,99 на наборі CICIDS-2017 та понад 99 % у сценаріях стекінгу на CTU-NCC. Робота демонструє, що перехід від бінарної до багатокласової класифікації істотно підвищує детекції ботнету, а інтеграція XAI робить рішення інтерпретованим для аналітиків SOC, знижуючи хибні спрацювання.

В [5] дослідили виявлення ботнет атаки в IoT середовищі, запропонувавши гібридну процедуру відбору ознак, яка генерує оптимальні підмножини ознак для класифікації трафіку. Автори порівняли п'ять моделей (DT, RF, KNN, AdaBoost, Bagging) і засвідчили, що при бінарній класифікації AdaBoost досягає 99,28 % точності з 18 ознаками, тоді як у мультикласовому сценарії RF демонструє 86,62 % точності з 22 ознаками. Використання запропонованого гібридного відбору ознак підвищило показники всіх моделей у середньому на 3 %, а найкраще рішення (RF) забезпечило 95,11 % (binary) та 83,96 % (multi-class) виявлення ботнетів. Робота підтверджує ефективність комбінованого аналізу ознак і ансамблевих моделей для IoT.

Дослідження [6] зосередилося на мережевій протидії мобільним ботнетам і представили MONDEO-Tactics5G - багатоступеневий алгоритм, який працює прямо у 5G-інфраструктурі оператора й не потребує ПЗ на кінцевих пристроях. Механізм корелює сигнали DNS-тунелювання, DoH-трафіку та C2-beaconing, забезпечуючи високу точність виявлення шкідника FluBot й адаптивне управління зараженими абонентами. Трафік інфікованого ґаджета обмежують так, щоб знизити ризик DDoS атаки, але не розривати активні сеанси та не погіршувати користувацький досвід. Дослідження демонструє, що мережеві контролі на рівні оператора можуть ефективно стримувати мобільні ботнети без участі користувача.

У статті [7] представлено підхід до виявлення ботнету для розподілених систем. Він базується на розробленій трирівневій моделі, яка включає компоненти ботнету: центр управління, центри управління, основні елементи ботнету (боти). Нова структура дає змогу виявляти відомі та невідомі ботнети та складається з рівнів хоста та мережі.

У роботі [8] запропоновано новий метод виявлення DDoS ботнетів на основі аналізу мережевих характеристик ботнетів. Він використовує напівконтрольоване (semi-supervised) нечітке кластерування fuzzy c-means. Аналіз здійснюється на основі характеристик, вилучених із мережевого трафіку, які можуть вказувати на наявність DDoS ботнетів у мережі.

Автори [9] запропонували нову двошарову систему виявлення зашифрованого шкідливого трафіку без дешифрування, що поєднує глибоку (DL) і класичну (ML) обробку ознак та вводить спеціалізований набір цифрових відбитків пакета, орієнтованих саме на шкідливий зашифрований трафік. Автори детально проаналізували існуючі методики формування ознак, сформували власну, а також склали комплексний датасет із публічних джерел для повноцінного навчання DL моделі. У порівняльних експериментах їхня дворівнева архітектура перевершила ResNet і Random Forest, що підтверджує ефективність комбінованого підходу.

В [10] запропоновано нову інформаційну технологію виявлення ботнетів на основі аналізу поведінки ботнетів у корпоративній мережі. Виявлення ботнетів виконується двома способами: за допомогою аналізу на рівні мережі та на рівні хосту. Один підхід дозволяє аналізувати поведінку програмного забезпечення на хості, що може вказувати на можливу присутність бота безпосередньо в хості та ідентифікувати шкідливе програмне забезпечення, а інший передбачає моніторинг та аналіз DNS трафіку, що дозволяє зробити висновок про зараження хостів мережі ботом ботнету.

У статті [11] представлено метод виявлення ботнетів у корпоративних мережах. Він заснований на використанні алгоритмів штучної імунної системи. Запропонований підхід дозволяє відрізнити нешкідливий мережевий трафік від шкідливого за допомогою алгоритму клонального відбору з урахуванням особливостей присутності ботнету в мережі.

В роботі [12] автори акцентують, що поширення хмарних сервісів, вимоги privacy-by-design та Zero-Trust архітектур підвищують попит на DLP, але одночасно ускладнюють менеджмент таких проєктів. Вміщення продуктивності в рамки політик безпеки, точна класифікація даних і мінімізація ризику від інсайдерів залишаються ключовими перешкодами. Як перспективні напрямки огляд виділяє інтеграцію DLP з XDR платформами, використання ML для динамічних політик і появу cloud-native DLP, що підтримує гібридні та хмарні сценарії.

У дослідженні [13] запропонували метод запобігання витокам даних у блокчейн-орієнтованій енергомережі IoT, який поєднує NER підхід DeBERTa-BiLSTM-CRF із традиційними регулярними виразами для виявлення чутливої інформації як у структурованих, так і в неструктурованих повідомленнях між платформою мережі та сторонніми системами. Модель, натренована на наборі CLUENER 2020, досягла F1 = 81,26 %, що демонструє значне поліпшення порівняно з класичними regexp правилами та розширює сферу застосування DLP-технологій до складних галузевих даних.

Автори [14] розвинули ідею статистичного підходу до DLP, запропонувавши модель класифікації документів на основі вдосконаленого градієнтного бустингу (IGBCA), що використовує TF-IDF векторизацію та машинне навчання для оцінки ризику витоку до надання доступу. Автори доводять, що IGBCA підвищує точність класифікації порівняно зі стандартними методами (regex, fingerprinting) і дозволяє ефективно захищати дані.

Постановка завдання. Метою дослідження є розробка та оцінка ефективності комбінованого підходу, який інтегрує механізми DLP системи з виявленням ботнет активності у корпоративних мережах, забезпечуючи контроль руху критичної інформації й автоматизоване блокування каналів екфільтрації в реальному часі.

Основні завдання дослідження: 1) синтезувати гібридну архітектуру детекції; 2) розробити механізми автоматизованого моніторингу, виявлення, реагування та захисту критичної інформації; 3) провести експериментальне дослідження і перевірити ефективність запропонованого рішення.

Виклад основного матеріалу. Запропонована архітектура системи оброблення критичної інформації складається з шести основних вузлів (рисунок 1).

Кінцева станція є джерелом і споживачем інформації. На ній користувач створює, копіює чи передає файли, а також ініціює мережеві з'єднання. Агент DLP, що працює на цій станції на рівні операційної системи або драйвера файлової системи, аналізує вміст документів, маркує їх за ступенем конфіденційності, фіксує дії користувача і формує події про потенційний витік. Сенсор ботнетів відслідковує мережевий трафік і розпізнає підозрілі шаблони обміну даними, характерні для ботнета. Консоль інцидентів отримує повідомлення від обох сенсорів, об'єднує їх у єдину часову стрічку подій, додає контекст про користувача, пристрій і клас даних, надає оператору візуалізацію та забезпечує API для автоматичних дій. Модуль політик

інтерпретує ці події через заздалегідь задані правила та адаптивні порогові моделі, визначає, чи слід блокувати, шифрувати або лише журналювати інцидент. Модуль реагування отримує рішення від політик, перетворює його на конкретні технічні дії. Він надсилає агенту команду блокування або шифрування файлів, вносить правило до міжмережевого екрана чи проксі, аби перервати ботнет канал. Після виконання захисних дій він повертає підтвердження у консоль для аудиту системи.

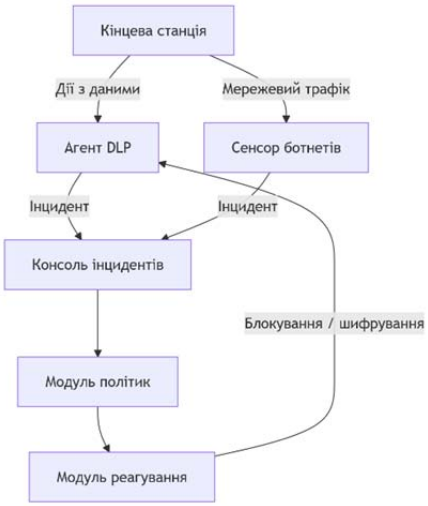

Рисунок 1 – Архітектура системи

Джерело: розроблено авторами

Алгоритм роботи системи. На кінцевій станції користувач працює з файлами й водночас генерує мережевий трафік. Обидва потоки даних рухаються до різних компонентів. Локальні операції одразу фіксує агент DLP, який оцінює, наскільки чутливим є контент і чи відповідають дії політикам безпеки. Тим часом копія мережевого трафіку надходить до сенсора ботнетів, що аналізує його й сигналізує про можливу активність. Контентний і мережевий модулі формують події та надсилають їх у консоль інцидентів, де інформація зводиться в єдиний запис і збагачується контекстом про користувача й систему. Далі консоль передає зведений інцидент у модуль політик, який визначає рівень ризику й ухвалює, чи слід втручатися. Прийняте рішення потрапляє до модуля реагування, який у разі потреби надсилає агенту на станції команду заблокувати або зашифрувати файл і одночасно додає правило блокування адреси чи домену на мережевому рівні. Після виконання дії підтвердження повертається назад у консоль, закриваючи цикл і забезпечуючи повний журнал подій для аудиту й подальшого вдосконалення системи.

Експериментальне дослідження ефективності. Для оцінки працездатності комбінованої системи створюється ізольоване лабораторне середовище з кількома віртуальними робочими станціями, які виконують звичайні офісні сценарії та одночасно відтворюють інфіковану поведінку. На кожному хості встановлюється агент DLP, а копія мережевого трафіку спрямовується на сенсор ботнетів. У межах експерименту генерується два типи діяльності. Перший - легітимна діяльність, редагування документів різних класів конфіденційності, збереження їх у мережевій папці, надсилання електронною поштою та синхронізація з хмарним сховищем. Другий - контрольовані атаки, відбувається імітація роботи ботнета, який намагається ексфільтрувати файли, попередньо позначені агентом як критичні. Система фіксує, скільки часу минає від моменту запуску шкідливого каналу до появи інциденту у консолі, яку дію обирає модуль політик і як швидко модуль реагування блокує передачу. Паралельно ведеться підрахунок хибних спрацювань, перевіряється чи не потрапили в карантин допустимі операції користувача і чи не був заблокований легітимний мережевий ресурс. Після серії з кількох сотень ітерацій обчислюються

середні показники, істинно позитивна та хибно позитивна частка, середній час виявлення і середній час до фактичного блокування.

Завершальний етап полягає у спробі вручну передати критичний файл за каналом, який система щойно заблокувала. Передача не відбувається, а файл на станції заблокований, експеримент підтверджує, що інтегрований підхід успішно перериває витік навіть за умов активного ботнет трафіку. Результати експериментів представлено в таблиці 1.

Таблиця 1 – Результати експериментів

Сценарії	Кількість подій	Спрацювання системи	Істинно позитивні, %	Хибно позитивні, %	Середній час виявлення, с	Середній час блокування, с
Легітимні дії користувача	400	6	-	1.5	-	-
Витік тільки через DLP канал (без ботнетів)	120	118	98.3	1.7	0.72	1.2
Ботнет трафік без критичних файлів	100	96	96	4.0	0.81	-
Витік критичних файлів через ботнет	80	79	98.8	1.2	0.85	1.35
Підсумок по всіх сценаріях	700	299	97.8	2.2	0.79	1.28

Джерело: розроблено авторами

Для ботнет трафіку без критичних файлів система не виконує блокування файлу, тому параметр «час блокування» не вимірювався.

Система продемонструвала високу стійкість. Із 700 протестованих подій вона коректно ідентифікувала 97,8 % небезпечних ситуацій, утримавши частку хибно позитивних спрацювань на рівні 2,2 %. Середній час між появою шкідливої активності й формуванням інциденту склав 0,79 с, а повне припинення ексфільтрації критичних даних відбувалося за 1,28 с. Лише шість разів система помилково спрацювала на легітимні дії користувача, що є прийнятним для реальних корпоративних середовищ. Показники підтверджують, що комбінований підхід де взаємодія мережевих ботнет ознак із класифікацією DLP ефективно блокує витоки даних й майже не заважає законній роботі співробітників.

Висновки. Проведене дослідження довело, що інтеграція DLP системи з системою виявлення ботнетів забезпечує високий рівень захисту корпоративних даних. Запропонована архітектура формує єдиний цикл моніторинг - виявлення - реагування - захист і здатна задіяти захисну дію за півтори секунди після початку ексфільтрації, зберігаючи при цьому помірну, у межах двох відсотків частку хибних спрацювань. Кореляція мережевих індикаторів керування ботнетом із класом чутливості даних дозволяє пріоритезувати інциденти й перекривати саме ті канали, які несуть максимальний ризик для організації.

Попри отримані результати, залишаються напрями, що потребують подальших досліджень. Особливої уваги потребує мобільний і IoT сегмент, поява ботнетів типу FluBot показала, що пристрої поза периметром компанії стають плацдармом для витоку.

Отже, щоб надійно захистити критично важливі дані, компанії мають впроваджувати комплексну багатошарову стратегію, яка поєднує сучасні технології, детально прописані правила безпеки, безперервний моніторинг і системне підвищення кваліфікації співробітників. Інтегруючи актуальні DLP□платформи з іншими інструментами кіберзахисту, організація суттєво зменшує ймовірність витоку та

зберігає стійкість своїх інформаційних ресурсів у середовищі зростаючих цифрових загроз.

Список літератури

1. Kapko M. Infostealers fueled cyberattacks and snagged 2.1B credentials last year. *CyberScoop*. 2025. 18 March. URL: https://cyberscoop.com/infostealers-cybercrime-surged-2024-flashpoint/ (дата звернення: 02.04.25).
2. Whitmore W. Today's Attack Trends - Unit 42 Incident Response Report. *Palo Alto Networks*. 2024. 28 February. URL: https://www.paloaltonetworks.com/blog/2024/02/unit-42-incident-response-report/ (дата звернення: 02.04.25).
3. Barry C. Top threats of the 2024 botnet landscape. *Barracuda*. 2025. 21 March. URL: https://blog.barracuda.com/2025/03/21/top-threats-of-the-2024-botnet-landscape (дата звернення: 02.04.25).
4. Patel, V., Shukla, H., Raval, A. Enhancing botnet detection with machine learning and explainable AI: a step towards trustworthy AI security. *IJFMR*. 2025. 7(2). 39353 URL: https://doi.org/10.36948/ijfmr.2025.v07i02.39353 (дата звернення: 03.04.25).
5. Alshaeaa, H. Y., Ghadhban, Z. M. Developing a hybrid feature selection method to detect botnet attacks in IoT devices. *Kuwait Journal of Science*. 2024. 51(3). 100222. URL: https://doi.org/10.1016/j.kjs.2024.100222 (дата звернення: 03.04.25).
6. Sousa, B., Dias, D., Antunes, N., Cámara, G., Wagner, R., Schmerl, B., Garlan, D., Fidalgo, P. MONDEO-Tactics5G: Multistage botnet detection and tactics for 5G/6G networks. *Computer Security*. 2024. 140. 103768. URL: https://doi.org/10.1016/j.cose.2024.103768 (дата звернення: 03.04.25).
7. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., Vasylkiv, N. Botnet detection approach based on the distributed systems. *International Journal of Computing*. 2020. 19(2). 190-198. URL: https://doi.org/10.47839/ijc.19.2.1761 (дата звернення: 03.04.25).
8. Lysenko, S., Savenko, O., Bobrovnikova, K. DDoS botnet detection technique based on the use of the semi-supervised fuzzy c-means clustering. 2018. *CEUR-WS*. 2104. 688-695. URL: https://ceur-ws.org/Vol-2104/paper_251.pdf
9. Wang, Z., Thing,V. Feature mining for encrypted malicious traffic detection with deep learning and other machine learning algorithms. 2023. *Computers & Security*. 128. 103143. URL: https://doi.org/10.1016/j.cose.2023.103143 (дата звернення: 03.04.25).
10. Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A., Savenko, B. Information technology for botnets detection based on their behaviour in the corporate area network. in: Gaj, P., Kwiecień, A., Sawicki, M. (eds) Computer Networks. CN 2017. *Communications in Computer and Information Science*. 2017. vol 718. Springer, Cham. URL: https://doi.org/10.1007/978-3-319-59767-6_14 (дата звернення: 05.04.25).
11. Lysenko, S., Bobrovnikova, K., Savenko, O. A botnet detection approach based on the clonal selection algorithm. *Proceedings of the IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. 2018. Kyiv Ukraine. 424-428. URL: https://doi.org/10.1109/DESSERT.2018.8409171 (дата звернення: 05.04.25).
12. Noman, A. Advancements and best practices in data loss prevention: A comprehensive review. *ResearchGate*. 2024. URL: https://www.researchgate.net/publication/387325365_Advancements_and_Best_Practices_in_Data_Loss_Prevention_A_Comprehensive_Review (дата звернення: 05.04.25).
13. Miao, W., Zhao, X., Zhang, Y., Chen, S., Li, X., Li, Q. A deep learning-based method for preventing data leakage in electric power industrial internet of things business data interactions. *Sensors*. 2024. 24(13). 4069. URL: https://doi.org/10.3390/s24134069 (дата звернення: 05.04.25).
14. Gupta, K., Kush, A. A learning oriented DLP system based on classification model. *arXiv*. 2023. URL: https://doi.org/10.48550/arXiv.2312.13711 (дата звернення: 05.04.25).

References

1. Kapko, M. (2025, March 18). Infostealers fueled cyberattacks and snagged 2.1B credentials last year. *CyberScoop*. https://cyberscoop.com/infostealers-cybercrime-surged-2024-flashpoint/
2. Whitmore, W. (2024, February 28). Today's attack trends: Unit 42 incident response report. *Palo Alto Networks Blog*. https://www.paloaltonetworks.com/blog/2024/02/unit-42-incident-response-report/
3. Barry, C. (2025, March 21). Top threats of the 2024 botnet landscape. *Barracuda Blog*. https://blog.barracuda.com/2025/03/21/top-threats-of-the-2024-botnet-landscape
4. Patel, V., Shukla, H., & Raval, A. (2025). Enhancing botnet detection with machine learning and explainable AI: A step towards trustworthy AI security. *International Journal for Multidisciplinary Research, 7*(2), Article 39353. https://doi.org/10.36948/ijfmr.2025.v07i02.39353
5. Alshaeaa, H. Y., & Ghadhban, Z. M. (2024). Developing a hybrid feature selection method to detect botnet attacks in IoT devices. *Kuwait Journal of Science, 51*(3), Article 100222. https://doi.org/10.1016/j.kjs.2024.100222

6. Sousa, B., Dias, D., Antunes, N., Cámara, G., Wagner, R., Schmerl, B., Garlan, D., & Fidalgo, P. (2024). MONDEO-Tactics5G: Multistage botnet detection and tactics for 5G/6G networks. *Computers & Security, 140*, Article 103768. https://doi.org/10.1016/j.cose.2024.103768
7. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., & Vasylkiv, N. (2020). Botnet detection approach based on the distributed systems. *International Journal of Computing, 19*(2), 190–198. https://doi.org/10.47839/ijc.19.2.1761
8. Lysenko, S., Savenko, O., & Bobrovnikova, K. (2018). DDoS botnet detection technique based on the use of the semi-supervised fuzzy c-means clustering. *CEUR Workshop Proceedings, 2104*, 688–695. https://ceur-ws.org/Vol-2104/paper_251.pdf
9. Wang, Z., & Thing, V. (2023). Feature mining for encrypted malicious traffic detection with deep learning and other machine learning algorithms. *Computers & Security, 128*, Article 103143. https://doi.org/10.1016/j.cose.2023.103143
10. Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A., & Savenko, B. (2017). Information technology for botnets detection based on their behaviour in the corporate area network. In P. Gaj, A. Kwiecień, & M. Sawicki (Eds.), *Computer Networks: CN 2017* (Communications in Computer and Information Science, 718). Springer. https://doi.org/10.1007/978-3-319-59767-6_14
11. Lysenko, S., Bobrovnikova, K., & Savenko, O. (2018). A botnet detection approach based on the clonal selection algorithm. In *Proceedings of the IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 424–428). IEEE. https://doi.org/10.1109/DESSERT.2018.8409171
12. Noman, A. (2024). Advancements and best practices in data loss prevention: A comprehensive review. *ResearchGate*. https://www.researchgate.net/publication/387325365_Advancements_and_Best_Practices_in_Data_Loss_Prevention_A_Comprehensive_Review.
13. Miao, W., Zhao, X., Zhang, Y., Chen, S., Li, X., & Li, Q. (2024). A deep learning-based method for preventing data leakage in electric power industrial internet of things business data interactions. *Sensors, 24*(13), 4069. https://doi.org/10.3390/s24134069
14. Gupta, K., & Kush, A. (2023). A learning oriented DLP system based on classification model. *arXiv*. https://doi.org/10.48550/arXiv.2312.13711

Oleksandr Huralnyk, **Oleg Savenko**, Prof., Doctor of Technical Sciences
Khmelnytskyi National University, Khmelnytskyi, Ukraine

Processing Critical Information in Corporate Networks Based on a Combined Approach of a DLP System with a Botnet Detection System

This paper aims to develop a multi-layered cyber defense concept that combines content-aware data loss prevention and botnet detection. The goal is to provide full visibility into critical data flows in corporate networks, block leakage channels in real time, and maintain an acceptably low false positive rate. To achieve this goal, we synthesize a hybrid monitoring-detection-response-protection architecture and verify its performance in a controlled laboratory environment.

As a result of the study, an architecture of six logical nodes was formed. The end station became both a source and a consumer of data; users generated files and network sessions on it. The installed DLP agent successfully classified documents by confidentiality level, recorded actions, and generated events about a possible leak. The deployed botnet sensor timely detected characteristic anomalies in the traffic. Both event streams were consolidated into a single incident console, where they were supplemented with user, device, and data class context. The policy engine then correctly assessed the risk based on adaptive thresholds and made decisions on blocking, encrypting, or logging. The response engine implemented this decision, sent an order to the agent to block or encrypt files, and synchronously set network rules that interrupted the botnet channel. After performing the actions, the system returned confirmation to the console, ensuring a complete audit cycle.

The integrated solution correctly processed 97.8% of malicious events, while keeping false positives at 2.2%. The median detection time remained below 0.8 seconds, and full containment of critical data occurred within 1.3 seconds of the attack. The results confirm that correlating botnet behavior with data classification context dramatically reduces noise and speeds up response. By integrating up-to-date DLP platforms with other cybersecurity tools, an organization significantly reduces the likelihood of leakage and maintains the resilience of its information resources in an environment of growing digital threats.

botnet, DLP, data exfiltration, critical information, corporate networks

Одержано (Received) 02.05.2025 *Прорецензовано (Reviewed) 05.05.2025*
Прийнято до друку (Approved) 06.05.2025