Трофименко В. О.,
здобувач вищої освіти спеціальності 122 Комп'ютерні науки
Науковий керівник: Пархоменко О. Ю., к.ф.-м.н., доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій
Миколаївський національний аграрний університет,
м. Миколаїв

ЗАХИСТ ЦИФРОВОЇ ІНФРАСТРУКТУРИ АГРАРНИХ ПІДПРИЄМСТВ ЗА ДОПОМОГОЮ АНАЛІЗУ ЛОГІВ

Стрімка цифровізація аграрного сектору зумовлює зростання залежності підприємств від цифрової інфраструктури та інформаційних систем, що забезпечують автоматизацію виробничих процесів, моніторинг полів, облік ресурсів і логістику. Використання точного землеробства, систем дистанційного керування технікою, IoT-пристроїв і хмарних сервісів потребує надійного кіберзахисту, оскільки будь-які збої або зовнішні втручання можуть спричинити значні економічні втрати [1]. Одним із ключових інструментів забезпечення інформаційної безпеки є аналіз логів – систематичний процес збору, обробки та інтерпретації даних про події в IT-інфраструктурі підприємства.

Метою роботи є аналіз можливостей використання лог-аналізу та систем централізованого управління подіями безпеки для підвищення рівня кіберзахисту цифрової інфраструктури аграрних підприємств.

Для досягнення поставленої мети в роботі розглянуто основні джерела логів у цифровій інфраструктурі аграрних підприємств, проаналізовано типові кіберзагрози та визначено роль систем централізованого лог-менеджменту у процесі виявлення аномалій і реагування на інциденти безпеки. Дослідження ґрунтується на аналізі наукових публікацій, звітів міжнародних організацій та узагальненні практичних підходів до забезпечення кіберзахисту інформаційних систем.

Логи створюються всіма компонентами цифрової системи: серверами, мережевим обладнанням, SCADA-контролерами, датчиками, мобільними пристроями, програмним забезпеченням тощо. Вони фіксують інформацію про стан системи, дії користувачів, помилки, підозрілу активність і технічні аномалії. Саме тому аналіз логів дає можливість своєчасно виявити ознаки кіберзагрози, запобігти інцидентам або оперативно усунути їхні наслідки [2].

Залежно від функціонального призначення розрізняють системні, прикладні, мережеві та безпекові логи. Системні логи відображають стан операційних систем і серверного обладнання, прикладні – роботу спеціалізованого програмного забезпечення, мережеві – параметри передавання даних, а безпекові – події, пов'язані з автентифікацією, авторизацією та спробами порушення доступу. Комплексний аналіз різних типів логів дозволяє формувати цілісне уявлення про стан цифрової інфраструктури та своєчасно виявляти приховані загрози, які не завжди є очевидними при аналізі окремих компонентів системи.

Аграрні підприємства є потенційною мішенню для кіберзлочинців через використання IoT-пристроїв, недостатньо захищених мереж, віддалених технологічних майданчиків та великої кількості підрядників, які мають доступ до систем. Найпоширеними загрозами для таких підприємств є несанкціонований доступ до інформаційних систем, спроби підміни даних із сенсорів, шкідливе ПЗ, DDoS-атаки, фішинг, а також компрометація облікових записів працівників [3]. Більшість цих подій відображається у логах, що робить їхнім аналіз головним джерелом інформації для розпізнавання аномалій. Окрему увагу слід приділяти внутрішнім загрозам, пов'язаним із помилками персоналу, недотриманням політик безпеки або зловживанням правами доступу. Такі інциденти часто не супроводжуються явними ознаками атаки, однак можуть бути виявлені шляхом аналізу нетипових дій користувачів, змін конфігурацій або аномальної активності в робочий час. У цьому контексті лог-аналіз виступає важливим інструментом контролю та забезпечення прозорості роботи інформаційних систем.

Одним із найефективніших інструментів захисту є системи централізованого лог-менеджменту, зокрема SIEM-рішення (Security Information and Event Management). Вони дозволяють збирати логи з усіх джерел, автоматично корелювати події, формувати сповіщення та будувати поведінкові моделі для виявлення відхилень у роботі систем. Наприклад, система може ідентифікувати підозрілу активність, якщо спостерігається аномальний обсяг трафіку між польовими датчиками та сервером або повторні невдалі спроби входу в систему GPS-навігації техніки [4]. Важливою перевагою SIEM-систем є можливість масштабування та адаптації до специфіки конкретного підприємства. Вони підтримують налаштування правил кореляції подій, що дозволяє враховувати особливості технологічних процесів аграрного виробництва, сезонність робіт та географічну розподіленість об'єктів. Це підвищує точність виявлення інцидентів і знижує кількість хибних спрацювань, що є критично важливим для підприємств із обмеженими ресурсами кібербезпеки.

Для підприємств, діяльність яких напряму залежить від безперервного функціонування обладнання (наприклад, поливних комплексів, температурних сенсорів, систем живлення в тваринництві), аналіз логів також є інструментом моніторингу працездатності та діагностики. Регулярний перегляд журналів дозволяє своєчасно виявляти технічні несправності: збої датчиків, переривання передачі даних, нестабільність мережевих з'єднань, перевантаження серверів тощо [5]. Це сприяє зменшенню простоїв обладнання та стабілізації технологічних процесів.

З метою підвищення рівня кіберзахисту аграрним підприємствам доцільно впроваджувати комплексну систему лог-аналізу, що включає:

– визначення джерел логів і встановлення політик їхнього зберігання;
– централізований збір та автоматичну обробку подій;
– використання SIEM-платформ для кореляції та аналізу;
– регулярний аудит журналів безпеки;
– навчання персоналу та розробку внутрішніх протоколів реагування.

Таким чином, в умовах стрімкої цифровізації аграрного сектору та зростання залежності підприємств від інформаційних і телекомунікаційних технологій проблема забезпечення кібербезпеки набуває особливої актуальності. Використання систем точного землеробства, IoT-пристроїв, автоматизованих комплексів управління технікою й хмарних сервісів значно підвищує ефективність виробничих процесів, однак одночасно розширює поверхню можливих кібератак і технічних збоїв. У цьому контексті аналіз логів виступає одним із базових інструментів забезпечення безпеки та стабільності функціонування цифрової інфраструктури аграрних підприємств.

Аналіз журналів подій дозволяє не лише своєчасно виявляти ознаки несанкціонованого доступу, шкідливої активності чи порушень політик безпеки, але й забезпечує можливість глибшого розуміння поведінки інформаційних систем і користувачів. Завдяки централізованому збору та кореляції подій із різних джерел лог-аналіз сприяє підвищенню рівня керованості IT-інфраструктури, скороченню часу реагування на інциденти та мінімізації потенційних економічних втрат.

Використання сучасних SIEM-рішень дозволяє автоматизувати процеси моніторингу, аналізу та реагування на події безпеки, що є особливо важливим для аграрних підприємств із розгалуженою інфраструктурою та віддаленими об’єктами управління. Крім того, регулярний аналіз логів може виконувати функцію превентивного контролю, сприяючи ранньому виявленню технічних несправностей, деградації обладнання або нестабільності мережевих з’єднань, що позитивно впливає на безперервність виробничих процесів.

Отже, впровадження комплексної системи лог-аналізу є важливим кроком на шляху до підвищення кіберстійкості аграрних підприємств. Такий підхід сприяє не лише зміцненню інформаційної безпеки, а й загальному підвищенню ефективності управління цифровими ресурсами. Подальші дослідження у цьому напрямі можуть бути спрямовані на розробку спеціалізованих методів аналізу логів з урахуванням галузевої специфіки аграрного виробництва та інтеграцію інтелектуальних алгоритмів для прогнозування кіберзагроз.

Список використаних джерел

1. ENISA. Cybersecurity in the Agriculture Sector. European Union Agency for Cybersecurity, 2022. URL: https://www.enisa.europa.eu (дата звернення: 04.11.2025.)

2. Behl A., Behl K. Cyberwarfare: Threats, Risks and Responses. New York : Oxford University Press, 2017. 270 p.

3. FAO. Cybersecurity in Agriculture: Risks and Challenges. Rome, 2022. URL: https://www.fao.org (дата звернення: 04.11.2025.)

4. Stallings W. Network Security Essentials: Applications and Standards. 7th ed. Boston : Pearson, 2021. 432 p.

5. IoT Security Foundation. IoT Security Compliance Framework. 2020. URL: https://www.iotsecurityfoundation.org (дата звернення: 04.11.2025.)