МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НАУКОВО-ПРАКТИЧНИЙ ВИМІР В УМОВАХ ВОЄННИХ ВИКЛИКІВ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 26 квітня 2024 року

Одеса
«Фенікс»
2024

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 15.05.2024 р.)

За загальною редакцією ***С. В. Ківалова***

Відповідальний за випуск ***М. Р. Аракелян***

Є 24 **Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів** : матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2024. – 1000 с.
ISBN 978-617-8430-05-4

У збірнику відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології в умовах повномасштабного військового вторгнення. Висвітлено питання загроз національній безпеці в їх конституційному вимірі у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов’язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики. Відображено наукові напрацювання у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових і науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)»364»»20»(062.552)

Матеріали видано в авторській редакції

ISBN 978-617-8430-05-4

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЕКЦІЯ 25. ПИТАННЯ МЕТОДИКИ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ, ТЕОРІЇ ТА ПРАКТИКИ ПЕРЕКЛАДУ ЯК ЗАСОБУ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ

чається навчання учасників освітнього процесу навичкам безпечного користування цифровими технологіями;
- аналіз законодавчої бази щодо захисту освітніх даних в умовах цифрової трансформації. Визначення недоліків та шляхів вдосконалення правового середовища для захисту освітніх даних;
- дослідження впливу соціальних мереж та онлайн-платформ на приватність та безпеку закладів освіти. Ідентифікація потенційних ризиків та шляхи їх запобігання в контексті використання соціальних мереж та онлайн-платформ у навчальних закладах.

Відповідно до цього, слід зробити висновок, що у сучасну цифрову епоху інформаційні технології є невід'ємною складовою сфери освіти, відкриваючи широкі можливості для покращення освітнього процесу. Зростання цифрової майстерності є важливим елементом сучасної освіти. Проте із цими перевагами постають значні безпекові виклики, що загрожують якості освіти та приватності учасників освітнього процесу. Розуміння та вирішення цих проблем вимагає комплексних заходів з підвищення кібербезпеки та розвитку цифрової грамотності серед учасників освітнього процесу.

Список використаних джерел

1. Концепція розвитку цифрових компетентностей : схвалено розпорядженням КМУ від 03.03.2021 р. № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text .

2. Безлєпкін Г. Є. Економічні засади імплементації цифрових інноваційній технології в сфері освіти. *Економіка та суспільство*. 2023. № 57. URL: https://doi.org/10.32782/2524-0072/2023-57-83.

Ключові слова: інформаційні технології, освіта, цифрова майстерність, безпекові виклики, кіберзлочинність, цифрові компетентності, кібербезпека, кібератаки, захист даних.Начало формы

Keywords: information technology, education, digital mastery, security challenges, cybercrime, digital competences, cyber security, cyber attacks, data protection.

Соловйов Артем Сергійович
Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій

ПРОБЛЕМАТИКА ФАЛЬСИФІКАЦІЇ СИСТЕМНИХ ЖУРНАЛІВ У ОПЕРАЦІЙНІЙ СИСТЕМІ LINUX

Системні журнали в операційній системі Linux відіграють важливу роль у забезпеченні безпеки та налагодженні системи. Лог-файли містять записи про події, що відбуваються в системі, такі як [1]:

- входи та виходи користувачів;
- запуски програм;
- зміни конфігурації;
- системні помилки;
- записи сторонніх програм.

Фальсифікація таких журналів може мати серйозні наслідки для безпеки та цілісності системи. Існує декілька методів фальсифікувати журнали:

- Пряме редагування: Зловмисник може мати отримати доступ до журналів та внести зміни до них.
- Використання спеціальних програм: Існує програмне забезпечення яке дозволяє фальсифікувати журнали

- Перехоплення системних викликів: Зловмисник може перехопити системні виклики, які використовуються для запису в журнал, та підміни даних.
- Наслідки які може мати фальсифікація системного журналу:
- Скриття зловмисних дій: Зловмисник може фальсифікувати записи, щоб приховати свою активність у системі.
- Ускладнення налагоджування: Фальсифікація запису можуть ускладнити діагностику проблем у системі [2].
- Підвищення ризику атаки: Фальсифікація журналу може допомогти зловмисникам обійти системи захисту системи.

Існує декілька заходів, які можна вжити для захисту від фальсифікації системних журналів. Заходи протидії проти фальсифікації системних журналів:

- Використання системних журналів з підтримкою цілісності: Такі системи дозволяють перевіряти, чи не дули записи в журналі змінені.
- Впровадження системного аудиту: системний аудит дозволяє відстежувати, хто вносив зміни до файлів журналу.
- Регулярний перегляд журналу: Регулярний перегляд журналів може допомогти виявити підозрілі дії та записи.

Також фальсифікувати данні системного журналу можливо для захисту системи, від зловмисників та шкідливого програмного забезпечення що аналізує лог-файли системи. Для такої фальсифікації можна виконати такі дії [3]:

- Шифрування: Якщо вам потрібно зберегти конфіденційні дані у системному журналі, можна використати шифрування. Зазвичай це досягається завдяки інструментів шифрування файлової системи, наприклад eCryptfs або EncFS.
- Анонімізація: Якщо потрібно приховати конкретні дані в лог-файлах, можна використати інструменти анонімності, щоб змінити конфіденційні дані на загальні або випадкові значення.
- Змінення налаштування логування: Можна налаштувати систему таким чином, щоб вона не записувала певні типи подій або не записувати певні данні в системні журнали. Наприклад можна відключити аудит подій, пов'язаний з входом користувачів, якщо потрібно приховати власну активність у системі.
- Аудит системних журналів: Адміністратори постійно перевіряють лог-файли для виявлення аномальної діяльності або потенційної загрози безпеки. Приховання вашої діяльності можуть викликати підозри і привести до подальших розслідувань [4].

Важливо зазначити, що будь яке приховання присутності у системному журналі повинно виконуватися з обережністю, бо кожне урізання інформації для запису у системному журналі може ускладнити пошук можливих помилок та проблем у операційній системі.

Загальні принципи забезпечення приватності та приховання присутності у системних журналах полягає у збалансованому підході між забезпеченням конфіденційності та забезпеченням безпеки системи. Важливо розуміти, що приховання присутності може бути використано як зловмисниками так і користувачами, і відповідно заходи безпеки повинні бути призначенні для захисту системи від обох видів загроз. Для дозволу фальсифікації системних журналів для звичайних користувачів треба розуміти такі моменти як:

- Врахування потенційних наслідків: перш ніж приймати рішення щодо приховання присутності, важливо усвідомлювати можливі наслідки. Дії користувачів можуть викликати підозрілі управління системою, або вони можуть порушити правила користування системою, що може призвести до негативних наслідків, включно втрату доступу до системи або правові наслідки.
- Легальність та етика: Приховування присутності має бути здійснене в рамках законів та правил, що регулюють використання комп'ютерних систем. Заборонені дії, такі як

злам або незаконне вторгнення, можуть мати серйозні правові наслідки. Будьте впевнені, що ваші дії відповідають вимогам закону та етики.

- Користування захисними заходами: Використовуйте захисні заходи, такі як файрволи, системи виявлення вторгнень та програмне забезпечення антивірусного захисту, для захисту системи від незаконної або шкідливої активності [5].

Фальсифікація системних журналів є серйозною проблемою, яка може мати значні наслідки для безпеки та цілісності системи. Недотримання правил безпеки системи на системних журналів може призвести до великих страт даних, та іншої важливої інформації. Дотримуючись рекомендацій системних адміністраторів та правил користування системою можна знизити ризики фальсифікації системних журналів зловмисниками, та захистити свою систему від атак.

Список використаних джерел

1. What is Log Tampering? URL: https://www.geeksforgeeks.org/what-is-log-tampering/
2. Chintan Gurjar. Computer forensics investigation: A case study. 2018. URL: https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-investigation-case-study/
3. Troubleshooting with Linux Logs. 2022. URL: https://www.loggly.com/ultimate-guide/troubleshooting-with-linux-logs/
4. How to Prevent Data Tampering In Your Business. 2020. URL: https://www.cypressdatadefense.com/blog/data-tampering-prevention/
5. Most Common Linux Logging Issues. 2023. URL: https://linuxstans.com/common-linux-logging-issues/

Ключові слова: Фальсифікація, системні журнали, лог файли, операційна система, програмне забезпечення, вразливості.

Keywords: Tampering, system logs, log files, operating system, software, vulnerabilities.

Дика Анастасія Іванівна
Національний університет «Одеська юридична академія»,
аспірантка кафедри інформаційних технологій
Трофименко Олена Григорівна
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій, кандидат технічних наук, доцент

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ЗАСОБАМИ CHATGPT ДЛЯ ТЕСТУВАННЯ БЕЗПЕКИ ВЕБЗАСТОСУНКІВ

Вебзастосунки нині є невіддільною частиною сучасного цифрового світу. Зростання їх популярності не в останню чергу зумовило актуалізацію вимог до їх безпеки. Потенційно вебзастосунки можуть піддаватися різноманітним загрозам: атакам з використанням вразливостей, витокам конфіденційної інформації, атакам з метою отримання несанкціонованого доступу до системи тощо. Тестування безпеки вебзастосунків є важливою складовою процесу їх розробки, оскільки дозволяє виявити й усунути потенційні вразливості перед введенням програмного забезпечення в експлуатацію.

З появою штучного інтелекту стало можливим його використання й у сфері інформаційної безпеки, наприклад, для тестування безпеки вебзастосунків. Моделі глибокого навчання, зокрема GPT (Generative Pre-trained Transformer), дозволяють створювати системи, здатні аналізувати текстові дані, що відкриває широкі можливості їх застосування для тестування безпеки. Дослідники [1] звернули увагу на можливості застосування ChatGPT для автоматизації процесу тестування безпеки вебзастосунків, завдяки його здатності розуміти контекст