ТАВРІЙСЬКИЙ ДЕРЖАВНИЙ
АГРОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ДМИТРА МОТОРНОГО

УДОСКОНАЛЕННЯ ОСВІТНЬО-ВИХОВНОГО ПРОЦЕСУ В ЗАКЛАДІ ВИЩОЇ ОСВІТИ

ЗБІРНИК НАУКОВО-МЕТОДИЧНИХ ПРАЦЬ

Таврійський державний агротехнологічний
університет імені Дмитра Моторного

Удосконалення освітньо-виховного процесу в закладі вищої освіти

збірник науково-методичних праць

Запоріжжя
2024

УДК 821.161.2.09 (062.552)
У45

Удосконалення освітньо-виховного процесу в закладі вищої освіти: збірник науково-методичних праць / Таврійський державний агротехнологічний університет імені Дмитра Моторного. Запоріжжя : ТДАТУ, 2024. Вип. 27. 478 с.

Рекомендовано до друку Вченою радою
Таврійського державного агротехнологічного університету імені Дмитра Моторного
протокол №11 від 28.06.2024 р.

У збірнику подано матеріали науково-методичної конференції ТДАТУ «Удосконалення освітньо-виховного процесу в закладі вищої освіти» (31 травня 2024 р., м. Запоріжжя).

Публікації присвячені питанням розвитку вищої освіти в умовах дистанційного навчання, використання інноваційних технологій в освітньому процесі, неформальної освіти та її ролі в підготовці майбутніх фахівців, упровадження результатів наукових досліджень з пріоритетних напрямів у фахову підготовку здобувачів освіти технічних спеціальностей, провідним тенденціям суспільно-гуманітарної та економічної освіти.

Збірник буде корисним науково-педагогічним працівникам, учителям-практикам, аспірантам та здобувачам вищої освіти.

Статті опубліковано мовою оригіналу

Адреса редакції**:** 69600, ТДАТУ, пр-т Соборний, 226,
м. Запоріжжя, Запорізька обл.
e-mail: nnc@tsatu.edu.ua
Навчально-науковий центр університету

ЗМІСТ

УДК 004.056.5

Мірошниченко М.Ю., к.тех.н., ст. викл.
Таврійський державний агротехнологічний університет
імені Дмитра Моторного
Чернова Г.В., к.пед.н., доцент
Харківський національний університет імені В.Н. Каразіна

СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ: АНАЛІЗ ЕФЕКТИВНОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Анотація. *У публікації представлені сучасні технології захисту інформації, зокрема аналізується їх ефективність та перспективи розвитку. У дослідженні приділяється увага як традиційним методам криптографії, так і новітнім підходам, таким як блокчейн технології та машинне навчання в сфері кібербезпеки. Розглядаються питання нормативно-правового забезпечення захисту інформації, оскільки правові аспекти відіграють важливу роль у створенні безпечного інформаційного середовища. Аналізуються сучасні загрози та тенденції у сфері кібербезпеки, що дозволяє виявити ключові напрями розвитку технологій захисту інформації.*

Ключові слова: *захист інформації, сучасні технології, перспективи розвитку, інформація, сучасний простір.*

Постановка проблеми. У сучасному світі інформація стала одним із найцінніших ресурсів, що обумовлює необхідність її ефективного захисту. З розвитком інформаційних технологій та зростанням обсягу цифрових даних виникають нові виклики у сфері безпеки [1, с. 70]. Технологічний прогрес відкриває нові можливості для захисту інформації, але водночас створює й нові загрози. Дослідження охоплює теоретичні аспекти та практичні приклади застосування сучасних технологій захисту інформації у різних галузях, зокрема в банківській справі, охороні здоров’я, державному секторі та індустрії розваг. Це дозволяє отримати цілісне уявлення про поточний стан і майбутні перспективи розвитку технологій у сфері захисту інформації [2, с. 98].

Аналіз останніх досліджень і публікацій. Дослідження сучасних технологій захисту інформації проводиться багатьма вченими та експертами у сфері інформаційної безпеки. Питання організації самостійної діяльності здобувачів вищої освіти засобами ІКТ вивчали Гладких Г.В. та Шарова Т.М. Аспекти новітніх технологій в інформаційному суспільстві, у сільському господарстві, у Збройних Силах України представлено у дослідженнях Голубовської В.С., Наконечний О.І., Сороківська О.А., Гевко В.Л., Крачок Л.І., Малик Я.Й., Лаврут О.О., Лаврут Т.В., Климович О.К., Здоренко Ю.М. Натомість питання напрямків використання інтелектуальних систем в освітньому процесі займаються сучасні вчені Лубко Д.В. та Шаров С. В. У наукових дослідженнях вчені Терещенко Г., Кириченко І. представляють аналіз і обґрунтування використання наявних блокчейн-рішень для захисту цифрових активів.

Формулювання цілей статті. Основною метою статті є дослідження сучасних технологій захисту інформації, аналіз їх ефективності та перспектив розвитку.

Виклад основного матеріалу досліджень. Вивчення сучасних технологій захисту інформації охоплює широкий спектр питань, які можна класифікувати за різними аспектами інформаційної безпеки [10, с. 112]. Основні питання для вивчення в цій галузі включають: криптографічні методи, аутентифікація та управління доступом, блокчейн-технології, машинне навчання та штучний інтелект, нормативно-правове регулювання, інтернет речей (IoT) та мобільна безпека, хмарні технології та віртуалізація, аналіз загроз та управління інцидентами, а також приватність та захист персональних даних [8, с. 92].

Відомо, що Advanced Encryption Standard (AES) є одним із найбільш поширених симетричних алгоритмів шифрування, який використовується для захисту конфіденційної інформації. Він забезпечує високу швидкість шифрування та декодування, завдяки чому широко застосовується в різних галузях, включаючи фінансові системи та комунікаційні мережі. AES підтримує різні розміри ключів (128, 192 та 256 біт), що дозволяє балансувати між безпекою та продуктивністю. Досить часто таким методом шифрується інформація Збройних Сил України [4, с. 91].

Натомість RSA (Rivest-Shamir-Adleman) є одним із перших асиметричних криптографічних алгоритмів, що широко використовується для захисту даних, особливо в електронних підписах та безпечному обміні

ключами. На відміну від симетричних алгоритмів, RSA використовує пару ключів: відкритий ключ для шифрування та закритий ключ для розшифрування. Квантова криптографія використовує принципи квантової механіки для забезпечення високого рівня безпеки. Одним із ключових методів квантової криптографії є протокол квантового розподілу ключів (QKD). QKD дозволяє двом сторонам створити спільний секретний ключ, використовуючи властивості квантових частинок, наприклад, фотонів. Будь-яка спроба перехоплення ключа призводить до його зміни, що одразу виявляється учасниками обміну.

SHA-3 (Secure Hash Algorithm 3) є останнім членом родини алгоритмів хешування, розроблених Національним інститутом стандартів і технологій США (NIST). SHA-3 забезпечує високу криптографічну стійкість і використовується для генерування хеш-значень, які є унікальними представленнями вихідних даних. Алгоритми хешування застосовуються для забезпечення цілісності даних, створення цифрових підписів і зберігання паролів у захищеному вигляді. Вивчення цих методів є ключовим для розуміння сучасних технологій захисту інформації. Кожен з них має свої особливості, переваги та сфери застосування, що дозволяє вибирати найбільш підходящі рішення залежно від конкретних вимог безпеки [9, с. 117].

Однак питання аутентифікація та управління доступом на сьогодні є досить важливим. Паролі є найбільш розповсюдженим методом аутентифікації. Їхньою перевагою є простота використання, але недоліком є уразливість до атак, таких як брутфорс, фішинг та соціальна інженерія. З метою підвищення безпеки рекомендується використовувати довгі та складні паролі, а також змінювати їх регулярно [13, с. 136]. Біометричні методи аутентифікації використовують унікальні фізичні характеристики людини, такі як відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока або голосу. Біометрична аутентифікація забезпечує високий рівень безпеки, оскільки ці характеристики важко підробити. Однак, існують занепокоєння щодо конфіденційності та можливих помилок і відмов у доступі [3, с. 224].

Двофакторна аутентифікація (2FA) поєднує два різні методи для перевірки особи користувача. Зазвичай це поєднання пароля (що ви знаєте) і другого фактору, такого як код, надісланий на мобільний телефон (що ви маєте), або біометричні дані (що ви є). 2FA значно підвищує рівень безпеки,

оскільки для успішної аутентифікації необхідно пройти два незалежних етапи перевірки.

Багатофакторна аутентифікація (MFA) включає більше двох факторів для перевірки особи користувача. Це може бути комбінація паролів, біометричних даних, смарт-карток, одноразових паролів (OTP) або інших методів. MFA забезпечує ще вищий рівень безпеки, оскільки ускладнює можливість несанкціонованого доступу навіть у разі компрометації одного з факторів. Вивчення цих методів аутентифікації та моделей управління доступом дозволяє забезпечити належний рівень безпеки в інформаційних системах та ефективно захищати конфіденційні дані від несанкціонованого доступу [5, с. 231].

Блокчейн у сучасному просторі є розподіленим реєстром, який зберігає дані у вигляді послідовних блоків, зв’язаних між собою криптографічними хешами. Кожен блок містить транзакції або записи, а його хеш залежить від вмісту блоку та хеша попереднього блоку. Це забезпечує незмінність даних: будь-яка зміна в одному блоці впливає на всі наступні блоки, що робить блокчейн стійким до підробок. Однак, блокчейн працює на основі розподіленої мережі, де кожен вузол (учасник мережі) зберігає повну копію реєстру. Це забезпечує високу надійність та безпеку, оскільки відсутній центральний контрольний пункт, який міг би бути атакований або скомпрометований [12, с. 164].

Завдяки криптографічному захисту та децентралізації, дані у блокчейні захищені від несанкціонованого доступу та підробок. Використання консенсусних алгоритмів (наприклад, Proof of Work, Proof of Stake) забезпечує достовірність та цілісність даних. Блокчейн дозволяє відстежувати всі транзакції та дії в реєстрі, що забезпечує високу прозорість. Це особливо корисно для систем, де важливо мати відкритий і доступний для перевірки запис всіх дій, наприклад, в державному управлінні, логістиці та фінансах.

Криптовалюти, такі як Bitcoin та Ethereum, використовують блокчейн для зберігання та захисту фінансових транзакцій. Кожна транзакція підписується приватним ключем власника, що забезпечує автентичність та запобігає несанкціонованому доступу. Багато криптовалют забезпечують певний рівень анонімності транзакцій, використовуючи псевдоніми (адреси), замість реальних імен користувачів. Однак для підвищення конфіденційності розробляються криптовалюти, такі як Monero та Zcash,

які використовують додаткові методи шифрування для приховування деталей транзакцій.

Смарт-контракти – це програми, які автоматично виконуються, коли виконуються певні умови. Вони зберігаються в блокчейні, що забезпечує їхню незмінність та прозорість. Смарт-контракти можуть автоматизувати широкий спектр угод, від фінансових транзакцій до управління ланцюгами постачання. Смарт-контракти виконуються автоматично і не потребують довіри до третьої сторони, оскільки код контракту забезпечує дотримання умов угоди. Однак розробка безпечних смарт-контрактів вимагає ретельного аналізу та тестування, щоб уникнути вразливостей, таких як ті, що були виявлені в DAO (Decentralized Autonomous Organization) на платформі Ethereum.

У сучасному інформаційно-комунікаційному просторі відомо, що машинне навчання дозволяє створювати моделі нормальної поведінки користувачів і систем. Відхилення від цих моделей можуть сигналізувати про можливі кіберзагрози або атаки. Такі моделі можуть автоматично оновлюватися та адаптуватися до нових загроз. Алгоритми машинного навчання можуть аналізувати великий обсяг даних у реальному часі, виявляючи аномалії, які можуть вказувати на наявність шкідливої активності. Завдяки аналізу історичних даних, системи на основі машинного навчання можуть передбачати ймовірність майбутніх атак. Машинне навчання та штучний інтелект значно покращують можливості виявлення та запобігання кіберзагрозам. Однак важливо забезпечити захист самих алгоритмів від можливих атак, щоб зберегти їхню ефективність та надійність у довгостроковій перспективі.

Не кожна людина, яка користується персональним комп’ютером та віртуальним простором, знає нормативно-правові документи, що можуть забезпечити їй конфіденційність у напрямку захисту даних та інформації, яку вона має. Та, наприклад, загальний регламент про захист даних Європейського Союзу (GDPR) є одним із найважливіших нормативних актів, що регулює обробку персональних даних. Він встановлює жорсткі вимоги до збору, зберігання, обробки та передачі персональних даних. Вимога отримання явної згоди на обробку даних, право суб’єктів даних на доступ до своїх даних і на їх видалення (право на забуття), обов’язок повідомлення про порушення безпеки даних протягом 72 годин, вимоги до

забезпечення безпеки даних за допомогою відповідних технічних та організаційних заходів.

Відомо, що організації несуть відповідальність за захист персональних даних, які вони обробляють. Це включає впровадження відповідних заходів безпеки, проведення оцінки ризиків і забезпечення безпеки систем та процесів. У разі порушення безпеки даних організації зобов'язані повідомляти про це відповідні органи та постраждалих осіб у встановлені строки (наприклад, протягом 72 годин за вимогами GDPR). Організації зобов'язані проводити оцінку впливу на захист даних для ідентифікації та мінімізації ризиків для приватності та безпеки даних, особливо при впровадженні нових технологій або процесів. Організації повинні укладати угоди з обробниками даних, щоб забезпечити дотримання вимог щодо захисту даних та встановити відповідальність сторін [7, с. 13].

Законодавство, таке як GDPR, накладає обмеження на передачу персональних даних за межі ЄС, дозволяючи такі передачі лише за наявності відповідного рівня захисту даних у країні-отримувачі або на основі відповідних договорів (наприклад, стандартних договірних положень). Нормативно-правове регулювання в сфері захисту інформації встановлює чіткі вимоги до обробки та захисту персональних даних, а також відповідальність організацій за дотримання цих вимог. Важливо, щоб організації ретельно дотримувалися відповідних законодавчих та нормативних вимог, щоб уникнути значних штрафів і забезпечити надійний захист даних.

Оскільки IoT-пристрої часто обмежені в обчислювальних ресурсах, важливо використовувати легкі шифрувальні алгоритми для захисту даних під час передачі та зберігання. Впровадження надійних методів аутентифікації, таких як багатофакторна аутентифікація (MFA) для підтвердження правомірності доступу до IoT-пристроїв. Використання ролей та політик доступу для обмеження прав доступу до ресурсів та даних лише для авторизованих користувачів і пристроїв. Розуміємо, що безпека в хмарних середовищах є критично важливою складовою, оскільки дані користувачів зберігаються та обробляються на віддалених серверах. Дані, які зберігаються в хмарі, повинні бути зашифровані. Це можна досягти за допомогою алгоритмів шифрування, таких як AES (Advanced Encryption Standard). Дані, які передаються між користувачем та хмарним сервісом,

повинні бути захищені за допомогою протоколів шифрування, таких як TLS (Transport Layer Security) [11, с. 32].

Шифрування під час використання (Data-in-Use) – це відносно нова технологія, яка включає використання таких методів, як гомоморфне шифрування, щоб забезпечити безпеку даних під час їх обробки. Віртуалізація дозволяє запускати кілька віртуальних машин (VM) або контейнерів на одному фізичному сервері, що підвищує ефективність використання ресурсів. Забезпечення безпеки в хмарних середовищах і віртуалізованих середовищах вимагає комплексного підходу, включаючи шифрування даних, управління доступом, моніторинг і регулярне оновлення систем. Використання цих методів допомагає захистити дані і ресурси від несанкціонованого доступу та потенційних загроз.

Ідентифікація та класифікація кіберзагроз є основоположними елементами ефективної кібербезпеки [14, с. 237]. Вони дозволяють організаціям вчасно виявляти потенційні загрози та розробляти відповідні стратегії для їх нейтралізації. Під час моніторингу мережевого трафіку (Network Traffic Monitoring) передбачено використання інструментів для аналізу мережевого трафіку з метою виявлення аномалій або підозрілої активності, що можуть вказувати на наявність загроз. Доречним буде аналіз логів (Log Analysis), що зводиться до регулярного перегляду і аналізу журналів подій та активності для виявлення несанкціонованих дій чи збоїв.

Системи виявлення вторгнень (Intrusion Detection Systems, IDS) стосуються здебільшого інструментів, які відслідковують і аналізують мережевий трафік для виявлення підозрілої активності або потенційних атак. Використання інтелекту про загрози (Threat Intelligence) включає в себе збір та аналіз даних про загрози з різних джерел, включаючи звіти про загрози, інформацію від партнерів та спеціалізовані служби, щоб розпізнати та класифікувати нові загрози. Забезпечення приватності даних є ключовим аспектом для захисту персональної інформації. Два основні методи для досягнення цієї мети – анонімізація та псевдонімізація. Дослідження цих питань дозволяє сформувати комплексне розуміння сучасних технологій захисту інформації та забезпечити їх ефективне застосування у різних галузях [6, с. 305].

Висновки. Сучасні технології захисту інформації є невід’ємною частиною цифрової дійсності, де кожен кілобайт даних має свою вагу. У наш час, коли кіберзлочинність швидко набирає обертів, важливо знати про

існуючі засоби захисту від небажаних втручань та крадіжок інформації. У світі, де обмін даними відбувається миттєво, важливою перешкодою на шляху до безпеки є віртуальні загрози та ризики. Тому, розуміючи ключові аспекти використання новітніх технологій для захисту конфіденційної інформації, можна уникнути кібератак та зберегти цілісність даних.

Література

1. Гладких Г.В., Шарова Т.М. Організація самостійної діяльності здобувачів вищої освіти засобами ІКТ. *Педагогіка формування творчої особистості у вищій і загальноосвітній школах*. 2020. Т. 2. №69. С. 70–74.
2. Голубовська В.С. Інформаційне суспільство: можливості, проблеми та перспективи розвитку. *Інформація і право.* №2. 2013. С. 98–104.
3. Крачок Л.І. Новітні технології у сільському господарстві: проблеми і перспективи впровадження. *Сталий розвиток економіки*. №3. 2013. С. 224–231.
4. Лаврут О.О., Лаврут Т.В., Климович О.К., Здоренко Ю.М. Новітні технології та засоби зв'язку у Збройних Силах України: шлях трансформації та перспективи розвитку. *Наука і техніка Повітряних Сил Збройних Сил України.* №1 (34). 2019. С. 91–101.
5. Лубко Д.В., Мірошниченко М.Ю. Аналіз сучасних підходів та методик в області захисту інформації та даних. *Вісник ХНТУ*. Серія: Інформаційні технології. 2024. №1. С. 231–236.
6. Лубко Д.В., Шаров С.В. Напрямки використання інтелектуальних систем в освітньому процесі. *Українські студії в європейському контексті*. 2021. №3. С. 305–310.
7. Малик Я.Й. Інформаційна безпека України: стан та перспективи розвитку. *Ефективність державного управління*. 2015. №44 (1). С. 13–20.
8. Мінгальова Ю.І. Дослідження сучасних криптографічних методів захисту інформації. *Нові перспективи: економіка, транспорт, інформаційні технології, екологія, редакторська та журналістська майстерність*. 2012. С. 92–94.
9. Наконечний О. Технології захисту інформації на підприємстві. *Вісник студентського наукового товариства «ВАТРА» Вінницького*

торговельно-економічного інституту ДТЕУ. Вінниця : Редакційно-видавничий цент. С. 117.

10. Павленко О.М., Шаров С.В., Москальова Л.Ю., Шарова Т.М., Коваленко А. С. Реалізація дистанційної форми навчання засобами платформи Moodle у процесі підготовки майбутніх філологів. *Інженерні та освітні технології.* 2019. Т. 7. № 3. С. 106–121.

11. Сороківська О.А., Гевко В.Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету*. 2010. №2.2. С. 32–35.

12. Терещенко Г., Кириченко І. Аналіз і обґрунтування використання наявних блокчейн-рішень для захисту цифрових активів. *Сучасний стан наукових досліджень та технологій в промисловості.* 2024. №1 (27). С. 164–178.

13. Шаров С.В. Сучасний стан розвитку штучного інтелекту та напрямки його використання. *Українські студії в європейському контексті*. 2023. №6. С. 136–144.

14. Шарова Т.М. Освітній портал як ефективний засіб забезпечення дистанційного навчання здобувачів вищої освіти. *Українські студії в європейському контексті:* зб. наук. пр. 2022. №5. С. 237–244.

Miroshnichenko M., Chernova G. Modern information protection technologies: analysis of efficiency and prospects of development

Summary. *The publication presents modern information protection technologies, in particular analyzes their effectiveness and development prospects. The research focuses on both traditional cryptography methods and emerging approaches such as blockchain technology and machine learning in the field of cybersecurity. Issues of regulatory and legal provision of information protection are also considered, since legal aspects play an important role in creating a secure information environment. Modern threats and trends in the field of cyber security are analyzed, which makes it possible to identify the key areas of development of information protection technologies.*

Key words: *information protection, modern technologies, development prospects, information, modern space.*

Для нотаток