Практичне значення запропонованого методу полягає у можливості використання XGBoost у системах реального часу для виявлення ботнет-активності в корпоративних мережах без перевантаження аналітиків надмірною кількістю хибних тривог. У підсумку, запропонований підхід може бути використаний як основа для побудови масштабованих засобів мережевого моніторингу, у яких одночасно враховуються точність виявлення, контроль FPR та продуктивність обробки трафіку.

1. Samoilenko V., Gakhov S. Comparative Analysis of Machine Learning Methods for Detecting Botnet Activities in Corporate Networks. SSRN Electronic Journal. 2025. DOI: 10.2139/ssrn.5188775.
2. Sharafaldin I., Habibi Lashkari A., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. ICISSP 2018. P. 108–116. DOI: 10.5220/0006639801080116.
3. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System. Proc. of the 22nd ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining. 2016. P. 785–794. DOI: 10.1145/2939672.2939785.
4. Akiba T., Sano S., Yanase T., Ohta T., Koyama M. Optuna: A Next-generation Hyperparameter Optimization Framework. Proc. of the 25th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining. 2019. P. 2623–2631. DOI: 10.1145/3292500.3330701.

Ключові контролі стандартів інформаційної безпеки для захисту критичної інфраструктури

УДК 004.056.5

Сведенюк Олексій [1], Курій Євгеній [2]

Національний університет "Львівська політехніка",
oleksii.svedeniuk.asp.2025@lpnu.ua [1], yevhenii.o.kurii@lpnu.ua [2]

Актуальність та постановка проблеми. Об'єкти критичної інфраструктури (ОКІ) України перебувають під постійним тиском цілеспрямованих кібератак (APT). Конвергенція IT- та OT-технологій створює нові вектори загроз, де компрометація одного сегмента загрожує катастрофічними наслідками для національної безпеки. Складність традиційних підходів до захисту заважає їх швидкому впровадженню, що зумовлює необхідність виокремлення пріоритетних заходів контролю [1].

Мета роботи — визначити та обґрунтувати набір критичних контролів на основі міжнародних стандартів (NIST CSF, CIS Controls v8, ISO/IEC 27001), адаптованих для захисту активів вітчизняної критичної інфраструктури.

Наукова новизна. У роботі запропоновано адаптивну модель ієрархізації засобів захисту, яка враховує специфіку функціонування АСУ ТП (SCADA) та забезпечує безперервність критичних бізнес-процесів навіть в умовах обмежених ресурсів.

Виклад основного матеріалу. Аналіз фреймворків дозволяє виділити «фундаментальні контролі», що захищають від 85% поширених атак. Для ОКІ критичними є: 1) інвентаризація апаратних і програмних активів; 2) управління

вразливостями; 3) контроль привілейованих облікових записів; 4) сегментація IT/OT мереж; 5) аналіз журналів подій безпеки. Підхід «CIS Implementation Group 1» дозволяє ОКІ сформувати базову лінію захисту [2]. Особлива увага має приділятися механізмам MFA для віддаленого доступу до технологічних сегментів, що запобігає несанкціонованому втручанню в системи керування.

Висновки. Впровадження пріоритетних контролів безпеки стратегічно важливе для стійкості ОКІ, оскільки оптимізує витрати та прискорює реагування на інциденти. Подальші дослідження будуть спрямовані на автоматизацію перевірки відповідності цим контролям у реальному часі.

1. Сіденко В. П., Гнатюк С. О. Метод підвищення рівня захищеності критичних інформаційних систем держави. Кібербезпека: освіта, наука, техніка. – 2024. – Т. 4, № 24. – С. 138–154.
2. CIS Critical Security Controls Version 8. Center for Internet Security, 2021. 82 p.

Дослідження методів побудови постквантових крипто-кодових конструкцій на гіпереліптичних кодах

УДК 621.395.7 (043.2)

Сергій Євсеєв[1], Владислав Сокол[2]

Національний технічний університет «Харківський політехнічний інститут», [1]Serhii.Yevseiev@gmail.com, [2]Vladyslav.sokol@gmail.com

Фундаментальний зсув парадигми інформаційної безпеки у напрямку постквантової криптографії стимулює інтенсивний пошук нових алгебраїчних структур. Дослідження фундаментальних аспектів застосування гіпереліптичних кривих у сучасних системах криптографічного захисту інформації, наведені у [1], показують багатообіцяючі результати. Доведено, що такі багатовимірні алгебраїчні структури здатні забезпечити надзвичайно високий рівень безпеки при використанні значно коротших ключів порівняно з традиційними еліптичними аналогами завдяки більшій розмірності групи класів дивізорів нульового степеня. Але залишилися невирішеними питання, пов'язані з алгоритмічним забезпеченням швидкого та детермінованого підрахунку кількості раціональних точок для кривих довільного роду над довільними полями Галуа. Причиною цього явища виступають суттєві об’єктивні математичні труднощі, безпосередньо пов’язані з неминучим експоненційним зростанням обчислювальної складності в процесі безпосереднього розрахунку порядку Якобіана для складних типів кривих. Специфіка імплементації суворих методів багатофакторної автентифікації на основі модифікованих крипто-кодових систем у фінансовому секторі формалізована у [2]. Встановлено, що глибоко інтегровані механізми захисту, які органічно поєднують завадостійкість та криптографічну конфіденційність, є критично необхідними для безпечного проведення віддалених банківських транзакцій в умовах гібридних кіберзагроз. Але залишилися невирішеними питання, пов'язані з оптимізацією пропускної здатності комунікаційного каналу під час постійної передачі автентифікаційних токенів надто великого розміру. Варіантом