УДК 004.056
DOI: https://doi.org/10.36994/2788-5518-2024-01-07-11

АНАЛІЗ ІНДИКАТОРІВ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ЗА РЕЗУЛЬТАТАМИ ЗАСТОСУВАННЯ SIEM-СИСТЕМ

Писарчук О. О., *д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. https://orcid.org/0000-0001-5271-0248, platinumpa2212@gmail.com*

Кошара А. В., *аспірант, Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. https://orcid.org/0009-0000-8468-2704, artemkosharaa@gmail.com*

Анотація*. У статті проведено аналіз особливостей аналітичної обробки інформації для виявлення загроз інформаційній безпеці в інформаційно-телекомунікаційних системах за результатами застосування SIEM-систем. Зокрема, розглянуто актуальну проблему зростання кіберзагроз у світі, що посилюється з розвитком технологій штучного інтелекту. Наголошено на необхідності впровадження передових методів аналітики для ефективного виявлення загроз та оцінки ризиків, пов'язаних з інформаційною безпекою. Особливу увагу приділено впливу кіберзагроз на нацбезпеку держав, зокрема на державний сектор, який є однією з основних мішеней для кібератак. Відзначено, що кібератаки на держсектор можуть мати значні негативні наслідки, включаючи порушення функціонування критичної інфраструктури, витік конфіденційної інформації та підрив довіри до урядових органів. Застосовано поняття інфологічної моделі факторів, що дає змогу оцінити рівень захищеності інформаційно-телекомунікаційних систем від кіберзагроз за даними від SIEM. Модель включає аналіз різноманітних чинників, що можуть впливати на безпеку систем: технічних, організаційних, людських. У результаті застосування моделі можна отримати комплексну картину стану безпеки системи та виявити слабкі місця, які потребують додаткової уваги. Кіберзагрози класифіковано на три рівні: рівень соціальної інженерії, мережевий рівень та рівень кінцевої точки. Для кожного із цих рівнів надано детальний опис індикаторів, що дають змогу виявити загрози. Наголошено на важливості аналізу індикаторів ризиків інформаційної безпеки та окреслено перспективи подальших досліджень, спрямованих на формалізацію системи індикаторів загроз і багатофакторного оцінювання. Установлено ієрархію індикаторів загроз, яка базується на чинниках їх появи, що дає змогу ефективніше управляти безпекою інформаційно-телекомунікаційних систем та своєчасно реагувати на нові виклики.*

Ключові слова: *SIEM, індикатори, ризики, інформаційна безпека, багатофакторне оцінювання, державний сектор, аналіз.*

ANALYSIS OF INDICATORS OF INFORMATION SECURITY THREATS IN INFORMATION AND TELECOMMUNICATION SYSTEMS ACCORDING TO THE RESULTS OF THE APPLICATION OF SIEM SYSTEMS

Oleksii Pysarchuk, *Doctor of Technical Sciences, Professor, Professor of the Computer Engineering Department of the Faculty of Informatics and Computing, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine. https://orcid.org/0000-0001-5271-0248, platinumpa2212@gmail.com*

Artem Koshara, *postgraduate, Open International University of Human Development «Ukraine», Kyiv, Ukraine. https://orcid.org/0009-0000-8468-2704, artemkosharaa@gmail.com*

Abstract. *The article analyzes the features of analytical processing of information to identify threats to information security in information and telecommunication systems based on the results of the use of SIEM systems. In particular, the current problem of the growth of cyber threats in the world, which is increasing with the development of artificial intelligence technologies, is considered. It is emphasized the need to implement advanced analytical methods for effective threat detection and risk assessment related to information security. Special attention is paid to the impact of cyber threats on the national security of states, in particular on the public sector, which is one of the main targets for cyber attacks. It was noted that cyber-attacks on the public sector can have significant negative consequences, including disruption of critical infrastructure, leakage of confidential information and undermining of trust in government agencies. The concept of an infological model of*

factors is used, which allows you to assess the level of security of ITS against cyber threats based on data from SIEM. The model includes the analysis of various factors that can affect the security of systems: technical, organizational, and human factors. As a result of applying the model, you can get a comprehensive picture of the state of system security and identify weak points that require additional attention. Cyber threats are classified into three levels: the social engineering level, the network level, and the endpoint level. For each of these levels, a detailed description of indicators that allow detecting threats is provided. The importance of the analysis of information security risk indicators is emphasized and the prospects for further research aimed at formalizing the system of threat indicators and multifactorial assessment are outlined. A hierarchy of threat indicators has been established, which is based on the factors of their appearance, which allows for more effective management of the security of information and telecommunication systems and a timely response to new challenges.

Key words: *SIEM, indicators, risks, information security, multi-factor assessment, public sector, analysis.*

Вступ

Досвід сьогодення переконливо доводить актуальність та нагальність питань забезпечення інформаційної безпеки (ІБ) інформаційно-телекомунікаційних систем (ІТС). Особливо ці питання загострюються для сектору державних ІТС. Державний сектор залишається однією з основних мішеней для зловмисників. Так, лише протягом цього року зафіксовано 12 217 інцидентів (позначено синім кольором на рис. 1), із них 1 085 – із підтвердженим оприлюдненням/компрометацією інформації, що захищалася [1].

	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	30,458	919	1,298	28,241	10,626	617	986	9,023
Accommodation (72)	220	16	9	195	106	16	9	81
Administrative (56)	28	7	7	14	21	6	4	11
Agriculture (11)	79	5	0	74	56	4	0	52
Construction (23)	249	17	6	226	220	12	5	203
Education (61)	1,780	82	630	1,068	1,537	56	618	863
Entertainment (71)	447	16	2	429	306	10	1	295
Finance (52)	3,348	75	122	3,151	1,115	54	87	974
Healthcare (62)	1,378	54	21	1,303	1,220	41	18	1,161
Information (51)	1,367	79	62	1,226	602	49	19	534
Management (55)	22	4	1	17	19	4	1	14
Manufacturing (31–33)	2,305	102	81	2,122	849	62	49	738
Mining (21)	30	1	2	27	20	1	1	18
Other Services (81)	462	13	5	444	417	8	5	404
Professional (54)	2,599	205	102	2,292	1,314	124	73	1,117
Public Administration (92)	12,217	56	115	12,046	1,085	39	27	1,019
Real Estate (53)	432	35	5	392	399	29	2	368
Retail (44–45)	725	90	47	588	369	55	32	282
Transportation (48–49)	260	21	38	201	138	17	12	109
Utilities (22)	191	17	11	163	130	12	6	112
Wholesale Trade (42)	76	22	21	33	54	17	14	23
Unknown	2,243	2	11	2,230	649	1	3	645
Total	30,458	919	1,298	28,241	10,626	617	986	9,023

Рис. 1. Кількість інцидентів із ІБ за галуззю

Об'єктами атаки є ІТС елементів критичної інфраструктури держави: системи державного управління, сектор безпеки і оборони, енергетика, зв'язок, банківська сфера тощо [2]. Метою інформаційного впливу є порушення цілісності, конфіденційності та/або доступності інформації, що циркулює в ІТС критичної інфраструктури. Таким чином, *забезпечення ІБ в ІТС об'єктів критичної інфраструктури загалом та державного сектору зокрема є важливим і нагальним завданням*.

Практика забезпечення ІБ в ІТС може здійснюватися з використанням інструментів SIEM – систем забезпечення управління інформаційною безпекою ІТС [3]. Це забезпечує отримання, акумуляцію та можливість комплексного аналізу даних про процеси функціонування компонент ІТС: програм, комп'ютерних систем, мережевого обладнання тощо в реальному масштабі часу в різних умовах поточної обстановки. Базовим функціоналом SIEM-системи будь-якого типу є: акумуляція даних та керування журналами подій; відстеження інцидентів і реагування на них; виявлення підозрілих дій користувачів та ін.

Процеси забезпечення інформаційної безпеки є суттю антагоністичного конфлікту порушника та суб'єкта забезпечення інформаційної безпеки. Це виявляється у постійній модифікації способів та сценаріїв нападу на інформацію з формуванням заходів протидій на досвіді успішних інцидентів за апріорною невизначеністю потенційних та реальних загроз. Тому реалізують динамічний процес управління інформаційною безпекою, тобто реагування на загрози в реальному часі з використанням заздалегідь побудованої та відкритої до модифікації системи забезпечення ІБ в ІТС.

Апріорна невизначеність про конкретику методів і способів нападу на інформацію в ІТС потребує організації адаптивного аналітичного аналізу інформації від SIEM-систем суб'єктами забезпечення ІБ (фахівцями із кібербезпеки) в реальному масштабі часу. Тобто маємо ергатичну (за участю людини) автоматизовану систему управління інформаційною безпекою. Її недоліки полягають у відносній інертності прийняття рішень, обмеженій пропускній здатності, залежності результатів від психофізіологічного стану людини та її підготовки. Тому *важливим є розроблення автоматизованої системи підтримки прийняття рішень (СППР) (класу smart ERP), яка б моделювала аналітичну діяльність суб'єкта забезпечення ІБ за даними від SIEM-систем.*

Реалізація процесу автоматизації прийняття рішень про інформаційні загрози в ІТС має базуватися на математичному моделюванні аналітичної діяльності суб'єкта забезпечення ІБ за даними від SIEM-систем. Це можливо з використанням методів машинного навчання, зокрема багатокритеріального scoring-у (оцінювання) [4; 5].

Для застосування багатокритеріального scoring-у необхідно описати предметну сферу прийняття рішень – аналітичну роботу суб'єкта забезпечення ІБ у взаємозв'язку факторів, показників та критеріїв загроз. Зазначене має відображати інфологічну модель предметної сфери виявлення загроз ІБ за результатами роботи SIEM-систем. Тобто необхідно створити scoring-гову карту індикаторів загроз ІБ, на якій на рівні *образів* у ментальності «як найкраще, як найгірше» сформувати сценарії можливих загроз. Це дасть змогу в подальшому «навчити» *smart ERP-систему ідентифікувати загрози ІБ за індикаторами від SIEM-систем.* Де факто надати суб'єкту забезпечення ІБ компетентне рішення про загрози для управління ІБ. *Образи* мають формувати дійсні експерти-професіонали у сфері ІБ, що підвищує ефективність синергетичного об'єднання дій пересічного суб'єкта забезпечення ІБ та smart ERP-системи виявлення загроз ІБ.

Таким чином, метою статті є перший етап створення інфології загроз ІБ – аналіз індикаторів загроз інформаційній безпеці в інформаційно-телекомунікаційних системах за результатами застосування SIEM-систем.

Із позицій методології завдання ідентифікації загроз ІБ полягає у бінарній класифікації/кластеризації за множиною (вектором) ознак. У такій інтерпретації відома доволі значна кількість методів машинного навчання, зокрема [6–9]: k-Means / Hard-c-means / k-середніх; метод «найближчого сусіда» / k-nearest neighbors algorithm / k-NN; метод опорних векторів (support vector machine – SVM); ієрархічна кластеризація; дискримінантний аналіз; логістична регресія; наївний байесовский класифікатор; методи глибинного навчання із застосуванням штучних нейронних мереж; багатофакторний/багатокритеріальний скоринговий аналіз.

Зазначені підходи, безумовно, мають свої переваги та недоліки та практику успішного використання в багатьох прикладних задачах. У ході досліджень буде використаний багатофакторний/багатокритеріальний скоринговий аналіз. Причинами цього є таке: можливість відносно більшої адекватності відображення міркувань суб'єкта забезпечення ІБ у формуванні образів загроз на рівні ментальних суджень «як найкраще, як найгірше»; можливість отримання рішень, оптимальних за Парето; відносна невелика обчислювальна складність; структурна відкритість підходу до додавання індикаторів загроз; пропорційність інтегрованого скору загроз ІБ імовірності їх виявлення; реалізація схеми навчання без учителя, що спрощує вимоги до вхідних даних.

Для формування інфологічних моделей предметної галузі існує практика унітарного чи комбінаторного використання аналітичних, евристичних та експериментальних підходів. Для виявлення взаємозв'язку факторів та показників загроз ІБ за індикаторами від SIEM-систем природно використати на первинному етапі (реалізовано в статті) аналітичний, евристичний аналіз.

Виконання досліджень

Забезпечення ІБ – це комплексне поняття, що характеризується різноманітними індикаторами (потенційні та/або реальні факти (прямі, непрямі), ризики тощо). Залежно від комбінаторики цих індикаторів визначається тип загроз та їхній рівень (severity). Задля визначення рівня загроз та захищеності ІТС за даними від SIEM на основі таких індикаторів необхідно сформувати інфологічну модель факторів, показників та критеріїв загроз інформаційній безпеці. Водночас рішення про включення категорії індикаторів до інфологічної моделі має базуватися на прагматиці та суті аналітичної обробки індикаторів для виявлення загроз ІБ. Тому, перш за все, слід розглянути суть процесів аналітичної обробки інформації від SIEM-системи, які визначатимуть зміст скорингової карти інфологічної моделі. Надалі слід сформувати головні категорії показників загроз ІБ в ІТС.

І. Опис процесів аналітичної обробки інформації SIEM-системами.

Функціонування SIEM-систем орієнтовано на реалізацію суб'єкта забезпечення ІБ: агрегація та моніторинг реєстрації користувачів ІТС (логування) у реальному часі; зіставлення подій безпеки;

аналіз атрибутів доступу користувачів і звітність щодо відповідності вимогам; виявлення шкідливого програмного забезпечення; аналіз мережевого трафіку та інформаційне сприяння проведенню розслідувань; оцінювання вразливостей ІТС; аналітика поведінки користувачів ІТС. Зазначені процеси спрямовані на виявлення підозрілих дій та запобігання інформаційним потенційним інтендантам, локалізація та призупинення інцидентів, що сталися, ліквідація їхніх наслідків та розслідування подій. Зазначені процеси реалізуються на множині індикаторів, які можна узагальнити в три головні категорії: *індикатори атак соціальної інженерії (наприклад, фішинг); індикатори мережевого рівня; індикатори рівня кінцевої точки.* Кожен із них має прямі та опосередковані індикатори, які об'єктивно визначаються SIEM-системою та аналізуються суб'єктом забезпечення ІБ. Їх аналітична обробка передбачає комплексний аналіз часткових індикаторів зазначених груп. Цей процес базується на врахуванні та порівнянні поточної ситуації з ретроспективним досвідом інцидентів що відбулися на об'єкті інформаційної діяльності, оприлюднені іншими фахівцями та за досвідом суб'єкта забезпечення ІБ. При цьому типові загрози ІБ виявляються за допомогою імплантованих до SIEM-систем алгоритмів. Складності в аналітиці виникають відносно апріорно невідомих сценаріїв дій зловмисників відносно ІТС. А отже, це і є предметом автоматизації за допомогою smart ERP-системи ідентифікації загроз ІБ, для якої формуються причинно-наслідкові зв'язки факторів, показників та критеріїв виявлення загроз. Конкретика аналізу наводиться в описі категорій загроз ІБ.

ІІ. Головні категорії показників загроз ІБ в ІТС.

Індикатори атак соціальної інженерії. Атаки соціальної інженерії через засоби комунікації можуть бути класифіковані за ознаками: мета, спосіб доставки, тип умісту, ступінь персоналізації тощо. Але всі вони мають спільну ознаку в меті – використати користувачів ІТС для цілей атаки. Наприклад, отримати корисні дані через шкідливе посилання, що переадресує користувача на сторінку, для викрадення облікових даних (логін, пароль), текстовий файл (документ пакету Office, PDF-файл тощо), що міститиме посилання або шкідливий макрос для завантаження шкідливого навантаження та розгортання на пристрої. За допомогою SIEM-систем суб'єкт забезпечення ІБ аналізує отримані індикатори загроз із поштового сервера, що містяться в метаданих листа: невідповідність доменів, електронних адрес, IP-адрес, підписів, умісту, вкладень, підписів SPF, DKIM і DMARC тощо.

Відповідно, якщо перевірка індикаторів SPF, DKIM і DMARC провалилася – це одна з ознак фішингу, що впливатиме на оцінку загроз (до scor-у мають додаватися бали до рівня ризику). На рис. 2 наведено ілюстрацію успішної перевірки SPF та DKIM – IP-адреса відповідає заявленому домену відправника.

Received-SPF	pass (google.com: domain of icct@uu.kyiv.ua designates 178.20.159.40 as permitted sender) client-ip=178.20.159.40;
Authentication-Results	mx.google.com; dkim=temperror (no key for signature) header.i=@uu.kyiv.ua header.s=dkim header.b=MrSpcoEy; spf=pass (google.com: domain of icct@uu.kyiv.ua designates 178.20.159.40 as permitted sender) smtp.mailfrom=icct@uu.kyiv.ua
DKIM-Signature	v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=uu.kyiv.ua; s=dkim; h=Content-Transfer-Encoding:Content-Type:MIME-Version:Subject: Message-ID:Date:From:To:Sender:Reply-To:Cc:Content-ID:Content-Description: Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc:Resent-Message-ID: In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:List-Subscribe: List-Post:List-Owner:List-Archive; bh=9jzPyymu9+vYwlDW5Jy0xSg7DAD3/7pMHxaddZEYlJ8=; b=MrSpcoEyHkAMjPZg2qTecqmxbH qAiS/C4jwCfjHSWl3pqDC4DxwO6mX26sQMyp+4GyRwGM394xyZgQIN6fdgi7yXctgaZr8RfconPVR rItoT77BPrdfqmfJBjThH1pySlC9lDZBcjy7YPTd7Q2m4cXiZRj+5ol+6uXL+Vmm4NV0=;

Рис. 2. Аналіз індикаторів електронного листа на наявність перевірок SPF, DKIM, DMARC

Індикатори мережевого рівня. Під час мережевої комунікації або спроб такої комунікації SIEM-системи здатні «підсвічувати» аномальний мережевий трафік, якщо отримують дані з мережевого обладнання. Індикаторами загроз інформаційної безпеки мережевого рівня доречно визначити: протоколи, порти, репутацію IP-адреси, уміст пакету та успішність мережевої комунікації. На рис. 3 зображено результат перевірки IP-адреси, що має вкрай негативну репутацію на сервісі IBM X-Force Exchange і тісну інтеграцію з SIEM Qradar. Відповідно, результат розрахунку оцінки загроз – scor має бути більш відповідним у бік високих ризиків ІБ.

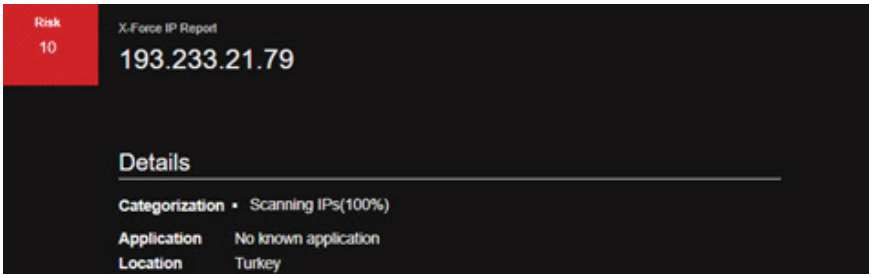

Рис. 3. Результат перевірки репутації IP-адреси, що має негативну репутацію

Індикатори рівня кінцевої точки. Серед індикаторів загроз даного рівня доцільно визначити такі: актуальність версії програмного забезпечення, результати перевірки файлів системи антивірусними засобами, їх контрольних сум (хешів) серед існуючих баз шкідливих файлів, зміни реєстру, зафіксована аномальна активність процесів на кінцевому пристрої. SIEM-системи в інтеграції з такими системами сканування файлів, як VirusTotal, здатні перевіряти репутацію програм, файлів хешів. На рис. 4 зображено результат пошуку за хешем файлу у базі знань VirusTotal. За результатами перевірки встановлено, що файл має негативну репутацію серед більшості існуючих антивірусних систем захисту.

Рис. 4. Результат пошуку за хешем у базі знань VirusTotal

Таким чином, виходячи наведених міркувань, можливо встановити головні категорії показників загроз ІБ в ІТС та на їх підставі сформувати систему часткових показників (табл. 1). Зазначена структура скорингової карти є основою для формування інфологічної моделі факторів, показників та критеріїв виявлення загроз ІТС за даними від SIEM-систем.

Таблиця 1

Головні категорії показників загроз ІБ в ІТС

Рівень	Індикатори загроз	Позначення
Соціальна інженерія	Інсайдерська загроза, фішинг	F_{soc}
Мережевий рівень	Комунікація з IP	F_{ip}
	Комунікація з URL	F_{url}
	Застосування експлойтів мережевих служб, баз даних, застосунків	F_{ex}
Рівень кінцевої точки	Брутфорс	F_{b}
	Актуальність версії ПЗ	F_{s}
	Використання неліцензійного ПЗ	F_{lic}
	Стан роботи модулів антивірусної системи захисту	F_{mal}
	Адміністративний доступ у звичайного користувача	F_{adm}
	Виявлення шкідливого файлу	F_{mf}

Інформаційні складові табл.1 дозволяють сформувати вектор індикаторів загроз ІБ в ІТС за даними від SIEM-систем:

$$D = \left[F_{soc} F_{ip} F_{url} F_{ex} F_{b} F_{s} F_{lic} F_{mal} F_{adm} F_{mf} \right]^{T} \quad (1)$$

Таким чином, маємо первинний рівень класів індикаторів загроз ІБ в ІТС. У подальшому буде реалізовано: декомпозицію класів на унітарні часткові показники; установлення джерел даних, порядку їх розрахунку; ревізію індикаторів на всебічність відображення загроз ІБ; аналіз на співвідношення об'єктивних/суб'єктивних індикаторів; установлення вимог екстремуму – формування критеріїв виявлення загроз ІБ в ІТС за даними від SIEM-систем. Запропонована структура відріз-

няється комплексним підходом до всіх груп показників з урахуванням поточних технічних можливостей SIEM-систем.

Висновки

Аналіз проблематики забезпечення ІБ в ІТС, що здійснюється за даними від SIEM-систем, показав таке. Для реакції на актуальні загрози реалізується контур управління ІБ із залученням ергатичного складника – суб'єкта забезпечення ІБ (фахівці у сфері кібербезпеки). Рішення про конкретику загроз ІБ приймається суб'єктивно, на підставі аналітичної обробки множини індикаторів, що отримується за даними від SIEM-систем. Недоліки автоматизованих систем спонукають до розроблення та впровадження smart ERP-систем ідентифікації загроз ІБ за індикаторами від SIEM-систем. Розроблення такої системи має базуватися на методах багатофакторного/багатокритеріального scoring-у, що, своєю чергою, потребує побудови інфологічної моделі факторів, показників та критеріїв ІБ в ІТС за даними від SIEM-систем. У ході досліджень запропоновано головні категорії показників загроз ІБ в ІТС (див. табл. 1 та вир. (1)).

У подальших дослідженнях передбачається уточнення запропонованої структури до унітарних часткових показників та доведення їх до рівня критеріїв.

Література

1. Verizon. 2024 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/T500/reports/2024-dbir-data-breach-investigations-report.pdf

2. РНБО. Стратегія кібербезпеки України (2021–2025 роки). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

3. Gómez, E.C.F., Almeida, O.X.B., & Arévalo Gamboa, L.M. (2022). Analysis of centralized computer security systems through the alienvault ossim tool. *[Espacios: Revista de Gestión Empresarial y Perspectivas Tecnológicas (https://dx.doi.org/10.46480/esj.6.1.181)*, 6(1).

4. Писарчук О.О. Оцінювання ефективності інформаційних систем за вектором критеріїв. *Збірник наукових праць ЖВІ НАУ*. 2010. Вип. 3. С. 117–123.

5. Писарчук О.О., Соколов К.О., Гудима О.П. Розроблення багатокритеріальної методики ситуаційного управління структурою і параметрами системи забезпечення інформаційної безпеки. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2016. № 3. С. 24–32.

6. P. Yuan, Y. Chen, H. Jin, L. Huang. MSVM-kNN: Combining SVM and k-NN for Multi-class Text Classification. *Proceedings of the 2008 IEEE World Congress on Services*, (1), 384–389. https://dx.doi.org/10.1109/WSCS.2008.36

7. H. Xiao, F. Sun, Y. Liang. A Fast Incremental Learning Algorithm for SVM Based on K Nearest Neighbors. *Proceedings of the 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI)*, (1), 157–161. https://dx.doi.org/10.1109/AICI.2010.207

8. S. Lahmiri, R. Saadé, D. Morin, F. Nebebe. Learning Analytics based on Bayesian Optimization of Support Vector Machines with Application to Student Success Prediction in Mathematics Course. *Proceedings of the 2020 International Conference on Cloud Technologies and Applications (CloudTech)*, (1), 1–4. https://dx.doi.org/10.1109/CloudTech49835.2020.9365915

9. Pacheco W.D.N., López F.R.J. Tomato classification according to organoleptic maturity (coloration) using machine learning algorithms K-NN, MLP, and K-Means Clustering. *Proceedings of the 2019 24th Symposium on Signal Processing, Images and Computer Vision (STSIVA)*, (1), 1–6. https://dx.doi.org/10.1109/STSIVA.2019.8730232

References

1. Verizon. 2024 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/T500/reports/2024-dbir-data-breach-investigations-report.pdf

2. NSDO Cybersecurity Strategy of Ukraine (2021-2025) Resource access mode: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

3. Gómez, E.C.F., Almeida, O.X.B., & Arévalo Gamboa, L.M. (2022). Analysis of centralized computer security systems through the alienvault ossim tool. *[Espacios: Revista de Gestión Empresarial y Perspectivas Tecnológicas (https://dx.doi.org/10.46480/esj.6.1.181)*, 6(1).

4. Pysarchuk O.O. Evaluation of the effectiveness of information systems by a vector of criteria // Zbirnyk naukovyx pracz ZhVI NAU - Collection of scientific works of ZVI NAU vol 3. 2010. P. 117–123.

5. Pysarchuk O.O., Sokolov K.O., Gudyma O.P. Development methods multi situational management structure and parameters of information security system / O.O. Pysarchuk, Collection of scientific works of the Center for Military and Strategic Research of the National University of Defense of Ukraine Ivan Chernyakhovskyi. - 2016. No. 3. P. 24–32.

6. P. Yuan, Y. Chen, H. Jin, L. Huang. MSVM-kNN: Combining SVM and k-NN for Multi-class Text Classification. *Proceedings of the 2008 IEEE World Congress on Services*, (1), 384-389. https://dx.doi.org/10.1109/WSCS.2008.36

7. H. Xiao, F. Sun, Y. Liang. A Fast Incremental Learning Algorithm for SVM Based on K Nearest Neighbors. *Proceedings of the 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI)*, (1), 157-161. https://dx.doi.org/10.1109/AICI.2010.207

8. S. Lahmiri, R. Saadé, D. Morin, F. Nebebe. Learning Analytics based on Bayesian Optimization of Support Vector Machines with Application to Student Success Prediction in Mathematics Course. *Proceedings of the 2020 International Conference on Cloud Technologies and Applications (CloudTech)*, (1), 1–4. https://dx.doi.org/10.1109/CloudTech49835.2020.9365915

9. Pacheco W.D.N., López F.R.J. Tomato classification according to organoleptic maturity (coloration) using machine learning algorithms K-NN, MLP, and K-Means Clustering. *Proceedings of the 2019 24th Symposium on Signal Processing, Images and Computer Vision (STSIVA)*, (1), 1–6. https://dx.doi.org/10.1109/STSIVA.2019.8730232