УДК 004.052.3:004.773 DOI: 10.31673/2412-4338.2024.022128

Оксанич Ірина Миколаївна
Інститут проблем математичних машин і систем НАН України, м. Київ
ORCID ID: 0000-0002-1208-3427

Гречанінов Віктор Федорович
Науково-дослідний відділ ІПММС НАН України, Київ
ORCID ID: 0000-0001-6268-3204

Литвинов Валерій Андроникович
Інститут проблем математичних машин і систем НАН України, м. Київ
ORCID ID: 0000-0001-5568-7629

Складанний Павло Миколайович
Київський столичний університет імені Бориса Грінченко, Київ
ORCID ID: 0000-0002-7775-6039

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ТА КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНОГО ОБМІНУ В СКЛАДНИХ УМОВАХ

Анотація. *У статті розглянуто проблеми і задачі забезпечення стійкого інформаційного обміну (СІО) при реагування на інциденти підвищеної складності природнього та військового характеру, такі як землетруси, масштабні пожежі, виверження вулканів, інтенсивні бойові дії тощо. Специфікою надзвичайних подій є обмеження людського доступу у певні регіони, ускладнення СІО з центральними органами управління силами та засобами реагування на них внаслідок часткового руйнування або виходу з ладу інформаційної інфраструктури, потенційні загрози негативного впливу антропогенного характеру на гарантоздатність цієї інфраструктури. В цих умовах ключового значення набуває реалізація комплексу організаційно-технічних заходів в плані управління СІО, включаючи формування та втілення на етапі його проєктування відповідних вимог та реалізація певних завдань безпосередньо у ході інциденту. В роботі розглядаються два рівні управління реагуванням на інцидент – рівень центру управління реагуванням (ЦУР), як рівень головного СЦ, і рівень зони інциденту, де проводяться роботи з реагування та ліквідації наслідків надзвичайної ситуації. Для кожного з рівнів окреслені задачі що ними вирішуються. Головною ціллю СІО з ЦУР є побудова гарантоздатної кіберстійкої системи ситуаційної обізнаності та моделювання процесів, що відбуваються, і характеру їх подальшого протікання. Результатом такого моделювання можуть бути рекомендації для підтримки прийняття рішень особами, що приймають рішення (ОПР). На рівні ЦУР зберігається вся інформація про інцидент для її використання у майбутньому для реагування на інші можливі інциденти такого ж типу. Визначені засоби зв'язку і типи інформації, що передається. Основними задачами, що повинні вирішуватися на рівні інциденту є збір даних, перетворення даних, забезпечення безпечної передачі даних по мережі і використання відповідних протоколів. Зазначено, що попри всі види зв'язку, що можуть використовуватися в зоні інциденту, супутниковий зв'язок все ж таки лишається пріоритетним. Тому наголошено на необхідності використання хмарних технологій для СІО. Запропоновано використання роле-орієнтованого інтерфейсу користувача хмарних сервісів як засобу для розмежування доступу та додаткового (поряд з шифруванням) засобу посилення захисту інформації, що передається по мережі.*

Ключові слова. *ситуаційний центр, інформаційний обмін, гарантоздатність, кіберстійкість, захист інформації, розмежування доступу, роле-орієнтований інтерфейс, хмарні технології.*

Oksanych Iryna
Institute of Problems of Mathematical Machines and Systems of NAS of Ukraine, Kyiv
ORCID ID: 0000-0002-1208-3427

Grechaninov Viktor
Research Department of IPMS of NAS of Ukraine, Kyiv
ORCID ID: 0000-0001-6268-3204

Lytvynov Valerii
Institute of Problems of Mathematical Machines and Systems of NAS of Ukraine, Kyiv
ORCID ID: 0000-0001-5568-7629

Skladannyi Pavlo
Borys Grinchenko Kyiv Metropolitan University, Kyiv
ORCID ID: 0000-0002-7775-6039

FEATURES OF ENSURING WARRANTY AND CYBER RESISTANCE OF INFORMATION EXCHANGE IN COMPLEX CONDITIONS

Abstract. *The article examines the problems and tasks of ensuring sustainable information exchange (SIE) when responding to incidents of increased complexity of a natural and military nature, such as earthquakes, large-scale fires, volcanic eruptions, intense combat operations, etc. The specificity of emergency events is the restriction of human access to certain regions, the complication of SIE with the central bodies of force management and the means of responding to them due to the partial destruction or failure of the information infrastructure, potential threats of the negative impact of anthropogenic nature on the guarantee capacity of this infrastructure. In these conditions, the implementation of a set of organizational and technical measures in the management plan of the SIE, including the formation and implementation at the stage of its design of relevant requirements and the implementation of certain tasks directly during the incident, becomes of key importance. The work considers two levels of incident response management - the level of the response control center (RCC), as the level of the main SC, and the level of the incident zone, where work is carried out to respond and eliminate the consequences of an emergency situation. For each of the levels, the tasks to be solved are outlined. The main goal of SIE with the SDGs is to build a guarantee-capable cyber-resistant system of situational awareness and modeling of the processes taking place and the nature of their further course. The result of such modeling can be recommendations to support decision making by decision makers (DMPs). At the RCC level, all incident information is stored for future use to respond to other possible incidents of the same type. The means of communication and the types of information transmitted are defined. The main tasks that must be solved at the level of the incident are data collection, data transformation, ensuring secure data transmission over the network and the use of appropriate protocols. It is noted that despite all types of communication that can be used in the area of the incident, satellite communication still remains a priority. Therefore, the need to use cloud technologies for SIE is emphasized. The use of a role-oriented user interface of cloud services is proposed as a means of demarcating access and an additional (along with encryption) means of strengthening the protection of information transmitted over the network.*

Keywords: *situation center, information exchange, warranty capacity, cyber resistance, information protection, access control, role-oriented interface, cloud technologies.*

1. Вступ

Під час реагування на інциденти надзвичайної складності, які супроводжуються значними руйнуваннями та масовими людськими жертвами, як то інтенсивні бойові дії, землетруси, лавини, обвали, повені, цунамі, виверження вулканів тощо, важливість забезпечення стійкого інформаційного обміну (СІО) з центром управління силами та засобами реагування (ЦУР) на інциденти та між окремими загонами учасників вирішення проблем набуває дуже високого значення, і важливість такого обміну з часом, який витрачається на локалізацію та ліквідацію події, тільки зростає.

Обмін та управління інформацією необхідні також і для досягнення оперативних переваг під час планування операцій. Ефективний обмін миттєвими повідомленнями та подальша інформаційна перевага дозволяють підвищити ситуаційну обізнаність, підтримують більш ефективне прийняття рішень та більшу оперативну гнучкість. Корисна інформація, отримана вчасно, у потрібному місці та форматі, дає можливість максимізувати свободу дій,

розробити та відпрацювати плани дій у надзвичайних ситуаціях, що є запорукою ефективного використання ресурсів та резервів, які забезпечують свободу маневру при реагуванні.

2. Постановка проблеми.

Незважаючи на те, що у сфері впровадження та використання гарантоздатних кіберстійких інформаційно-комунікаційних технологій на даний час досягнуто значного прогресу, проблема зв'язку та обміну важливою інформацією на територіях, де виникають інциденти з важкими наслідками, залишається дуже актуальною.

3. Аналіз останніх досліджень і публікацій.

У публікації спільної доктрини JDP 6-00 «Комунікації та інформаційні системи. Підтримка спільних операцій» [1] наголошується, що для успішної підтримки проведення операцій комунікаційними і інформаційними системами по досягненню оперативних переваг, вимоги до обміну інформацією і управління нею є першочерговими. Такі інтегровані процеси дозволяють отримати корисну інформацію вчасно і у потрібному форматі, що дає змогу досягнути ситуаційної обізнаності командирів і штабів у плануванні ними спільних операцій. У документі наведено вимоги до ІО і планування інформаційних послуг.

У стратегічному плані «Національна модель обміну інформацією» [2] представлено бачення вирішення проблеми інформаційної сумісності при проведенні спільних операцій. Пропонується прийняти національну модель обміну інформацією (NIEM - National Information Exchange Model) у якості стандарту.

У Керівництві з планування місій у мережевому середовищі «Обмін цивільно-військовою інформацією» [3] зазначено, що при виникненні масштабних катастроф (землетрусів, цунамі, виверження вулканів, лісних пожеж, збройних конфліктів тощо), до ліквідації наслідків яких долучаються не тільки цивільні рятувальники, а й військовослужбовці, виникає необхідність у співпраці і, звісно, у обміні оперативною інформацією між штабами військових і цивільних рятувальників. У таких випадках інформація для обміну може бути як «відкритою» (несекретною), так і «закритою» з різними грифами секретності. Керівництво дає опис «кращих практик» та структури ІО, де зібрані вимоги та правила передачі інформації в складних умовах.

Задачі та проблеми CIO при здійсненні морських операцій визначені у [4] , а у [5] дано опис та порівняння військових мереж передачі даних, що можуть бути використані для вирішення відповідних завдань, зокрема, типів Link 11, Link 16, Link 22.

З метою утворення умов спільної роботи над плануванням безпеки та стійкості критично важливих інфраструктурних послуг, включаючи системи інформаційного обміну, на тлі різноманітних загроз і змін кіберландшафту Американське агентство CISA [6] розробило структуру планування стійкості інфраструктури (*Infrastructure Resilience Planning Framework* – IRPF), що фактично уніфікує відповідні підходи для локацій, регіонів і приватного сектору та визначає методологічні засади протидії кіберзагрозам стійкості.

У [7] проаналізовано актуальну проблему зловживання привілеями в комп'ютерних системах інформаційного обміну, що утворює передумови потенційного витоку інформації внаслідок легітимного доступу до неї. Як механізм зменшення ризиків інформаційної безпеки та реалізації загроз інсайдерської діяльності персоналу організації, що має привілейований доступ, рекомендовано застосування PAM – рішення.

У [8] досліджені кібератаки типу підробленої точки доступу та з використанням фішингової сторінки, на підставі проведених експериментів визнано необхідним опрацювання методик підвищення рівня обізнаності користувачів та блокування потенційних атак на об'єкти інформаційної діяльності.

Процес реалізації моделі швидкісної стійкої до завад та розривів сенсорної мережі описано у [9]. Стійкість інформаційного обміну досягається шляхом побудови розподіленої мережі, в якій всі вузли передають повідомлення всім доступним вузлам.

З метою підвищення кіберстійкості технологічної системи в [10] запропоновано використовувати PLM схеми, які здатні змінювати внутрішню алгоритмічну структуру. При цьому реконфігурацію структури мікроконтролерної системи запропоновано здійснювати за результатами самодіагностування,

В [11] проведено аналіз побудови ефективних рішень задля підвищення рівня кібербезпеки інформаційних систем державного рівня в умовах зброї агресії та потужних кібератак на критичну інфраструктуру. Запропонована модель загроз безпеки з урахуванням концепції Zero Trust, а також візуалізовано моделі загроз, що сприяє визначенню потенційних вразливостей існуючих рішень. У [12] розглянуто концептуальні основи синтезу системи управління та проаналізовано мережу інформаційного обміну військового призначення, як об'єкт управління, а також описано мобільну та стаціонарну компоненти системи зв'язку.

В [13], [14] запропоновані та обґрунтовані оригінальні рішення щодо побудови децентралізованої системи розмежування доступу та модель гарантоздатності та кіберзахисту в інформаційних системах ситуаційного центру

Метою статті є напрацювання технологічних рішень щодо надійного інформаційного обміну, які можуть бути застосовані при побудові СІО у кризисних (ситуаційних) центрах, які залучаються до реагування на природні інциденти або до вирішення конфліктів високої складності.

4. Методологічні засади дослідження.

4.1. Задачі стійкого інформаційного обміну

Під час реагування на складні конфлікти обмін інформацією між центром управління та учасниками реагування стає не простою технічною вимогою, а й критично важливим механізмом, який може істотно вплинути на результат проведення операцій з реагування на інцидент, що виник. У такому випадку одним з головних завдань СІО є забезпечення ситуаційної обізнаності (СО), тобто повного розуміння у ЦУР подій, що розгортаються, що, у свою чергу, дає змогу особам, що приймають рішення (ОПР), вести скоординовані дії та краще розподіляти ресурси. Така СО забезпечується миттєвим доступом до даних про подію у реальному часі, що, у свою чергу, веде до необхідності забезпечення миттєвої передачі даних. Розв'язання цієї проблеми тягне за собою вирішення ряду задач.

Розглянемо більш детально ці задачі.

На рис. 1 зображено умовно два рівні управління реагуванням на інцидент: 1) рівень центру управління (ЦУР); 2) рівень управління, що знаходиться в зоні інциденту (рівень штабу або командного пункту).

У зоні інциденту для СІО між учасниками ліквідації наслідків інциденту та ЦУР поширеним є використання таких технічних систем зв'язку:

–Супутниковий зв'язок;

–Цивільні сотові та транкінгові та системи мобільного зв'язку;

–Системи відомого радіозв'язку;

–IP – кабельні та безпроводові системи (Інтернет-зв'язок);

–Фіксований телефонний зв'язок.

Оскільки управління реагуванням на інцидент відбувається на обох вищезазначених рівнях, то і СІО здійснюється як між рятувальниками безпосередньо у зоні інциденту, так і між обома рівнями управління. У той час, як на рівні інциденту відбувається в основному підготовка інформації, на рівні ЦУР здійснюється її опрацювання з метою вироблення рішень для ОПР.

Розглянемо коротко задачі, які вирішуються на рівні ЦУР, і більш детально задачі, які вирішуються на рівні інциденту.

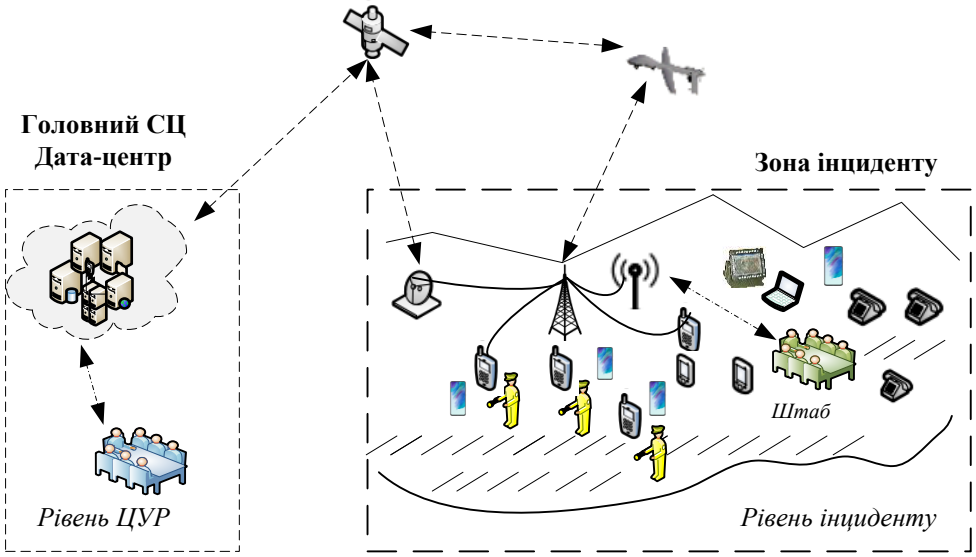

Рис. 1. Рівні управління реагуванням на інцидент, що стався

На рівні ЦУР вирішуються такі задачі:

–збереження отриманих з рівня інциденту даних у базах даних дата-центру;

–злиття даних (Data Fusion) - об'єднання різних даних в цілісну картину;

–інтелектуальний аналіз отриманих даних з використанням методів штучного інтелекту, машинного навчання та алгоритмів глибинного аналізу, який дає змогу перетворювати дані на інформацією та накопичені знання;

–моделювання можливих ситуацій і варіантів зв'язаних з ними рішень;

–прийняття рішень по ліквідації наслідків інциденту за результатами моделювання;

–пересилка підготовлених варіантів рішень на рівень інциденту.

Результатом обробки даних на рівні ЦУР є загальна картина ситуаційної обізнаності, прогноз її подальшого розвитку та різні варіанти рішень розв'язання надзвичайної ситуації, які пропонуються аналітичними системами.

На рівні інциденту вирішуються такі задачі:

–збір первинних даних про інцидент, що стався;

–підготовка (перетворення) даних для пересилки на рівень ЦУР;

–безпечна пересилка даних по мережі;

–використанням відповідних протоколів для пересилки по мережі.

Розглянемо більш детально ці задачі.

Задача збору даних про інцидент вирішується за допомогою всіх доступних способів зв'язку, і отримані дані зберігаються на пристроях, які є у наявності (смартфони, планшети, ноутбуки тощо). Це такі типи даних - графічні, текстові, табличні, аеро, фото та космічні знімки, аудіо, відео, показання різних датчиків, сигнали, повідомлення тощо, дубльовані, зашумлені, спотворені, можливо (або навмисно) помилкові дані у різних форматах з різних джерел.

Задача підготовки (перетворення) даних застосовується до даних, отриманих безпосередньо з місця події з метою їх підготовки до пересилки по мережі та включає такі етапи:

–первинна перевірка даних (перевірка достовірності, усунення надмірності, дублювання тощо);

–фільтрація даних (видалення неважливих, помилкових, безглуздих даних та шуму);

–перевірка семантики та приведення опису даних до загальновживаних і зрозумілих на рівні ЦУР термінів;

–додавання метаданих (джерела, власника, території, часу, опису події тощо);

−форматування даних, приведення до використовуваних для передачі по мережі і на рівні ЦУР форматів;

Треба зазначити, що для ефективного СІО важливими є також кількість інформації, що передається і її семантика. Інформація для обміну повинна бути не дуже великого об'єму, щоб не викликати втому, не затемнювати критичні моменти у даних, не навантажувати системи зв'язку і, одночасно, достатньо вичерпною і достовірною для прийняття рішень ОПР.

Інформація, яка передається повинна мати описову характеристику, яка визначає, наскільки така інформація є повною, які вона має невизначеності для прийняття рішень ОПР.

Етап перевірки і виправлення семантики даних також є важливим особливо при проведенні взаємних військово-цивільних операцій. Для виправлення семантики даних рекомендовано створювати тезауруси, що містять терміни та визначення і відповідають найбільш ймовірним масштабним катастрофам.

Інформація, що передається, має бути точною, повною і своєчасною. Чим динамічніше оперативне середовище (тобто швидке наступне стихійне лихо), тим більша потреба в точному обміні інформацією, який дозволить реагуючим ОПР (військовим та гуманітарним) визначити найкращий курс дій для задоволення потреб населення.

Задача безпечної пересилки даних по мережі

Інформація, яка передається по мережі, може мати різні позначки обмеження доступу, наприклад, «секретно», «конфіденційно», «для службового користування» та інші. Тому для СІО її треба розділяти по цих рівнях. Так, для СІО у несекретному середовищі (голосовий зв'язок, електронна пошта, відеоконференції, публікації в інтернеті) використовується несекретна та інформація для загального користування. З отриманих даних пропонується видаляти деякі дані для пониження рівня їх секретності.

Для СІО секретними даними доцільно використовувати визначені законодавством системи спеціального зв'язку та допущені встановленим порядком системи шифрування даних.

Задача використанням відповідних протоколів для пересилки по мережі

Визначення протоколів потрібно, в основному, для СІО інформацією з обмеженим доступом. Такі протоколи визначають типи даних, формати, розмір та шифрування даних, а також частоти, та час передачі.

4.2. Використання хмарних сервісів

Незважаючи на декілька видів зв'язку, що можуть використовуватися при управлінні реагуванням на масштабні інциденти і які перераховані вище, треба відмітити, що основним все-таки залишається супутниковий зв'язок. Тому можна стверджувати, що використання хмарних сервісів є очікуваним.

Як схематично показано на рис.1, обробка даних, що надходять до ЦУР, відбувається у хмарній інфраструктурі (ХІ), яка, по великому рахунку, може бути доволі складною та багаторівневою. Така ХІ дозволяє зберігати, обробляти та архівувати великі об'єми даних, перетворюючи їх на знання, що знадобляться для прийняття рішень при управлінні реагуванням на подібні інциденти у майбутньому. Окрім того, структура ХІ дозволяє надійно зберігати дані, використовуючи процедури розподілення та реплікації.

Навпаки, у зоні інциденту збігання великих об'ємів даних є проблемою, оскільки вони можуть бути знищені наслідками події. Крім того, зв'язок у такому регіоні може бути нестійким та ненадійним. Тому тут доцільно застосовувати різні види зв'язку. Загалом, у термінах хмарних обчислень, обчислення у зоні інциденту можна віднести до периферійних (туманних) обчислень, які розподілені по зоні інциденту, виконуються на особистих пристроях, обробляють невеликі об'єми даних та мінімізують затримку їх передачі і навантаження основної мережі.

При використанні для СІО хмарних сервісів з огляду на їх загальну доступність, постає питання обмеження доступу до чутливої інформації, що передається. Для вирішення цієї проблеми доцільно використовувати, окрім засобів захисту інформації, роле-орієнтований

інтерфейс користувача сервісу, який забезпечує розмежування доступу до інформації у відповідності до наданих йому ролей (наприклад, «пожежник-рятувальник», «медик», «зв'язківець», «пошуковець-рятувальник» тощо). Крім розмежування доступу та регламентування об'єму інформації, що надається користувачу, такий інтерфейс не потребує прив'язки до конкретної людини та її місця знаходження, і при втраті комп'ютерного пристрою, на якому працює користувач (або неможливості подальшої роботи користувача), інший пристрій (користувач) може продовжити роботу з даною роллю, якщо в нього будуть на це повноваження. Використання роле-орієнтованого інтерфейсу користувача наряду з загальними засобами захисту інформації (захищений зв'язок, спеціальні захищені протоколи передачі даних, шифрування інформації тощо) додатково сприяє посиленню захисту інформації, що передається по мережі.

5. Висновки та перспективи подальших досліджень.

У роботі розглянуто проблеми і задачі стійкого інформаційного обміну (СІО) при реагуванні на інциденти, які відбуваються в складних умовах. Такими умовами є руйнівні стихійні лиха (землетруси, лавини, обвали, повені, цунамі, виверження вулканів тощо) та інтенсивні бойові дії, що супроводжуються значними руйнуваннями та людськими жертвами. СІО в таких умовах, як правило, є утрудненим, особливо при спілкування і обміні з центральними органами управління реагуванням.

Розглядається два рівня управління реагуванням на інцидент – рівень центру управління реагуванням (ЦУР) і, власне, рівень інциденту. Визначені задачі, які повинні вирішуватися на кожному з рівнів. Зазначено, що, незважаючи на різні види зв'язку між учасниками ліквідації, супутниковий зв'язок все ж таки лишається необхідним, і тому використання хмарних сервісів може бути доцільним. У зв'язку з цим пропонується у хмарних сервісах використання роле-орієнтованого інтерфейсу користувача, як засобу обмеження інформаційного навантаження на нього та додаткового розмежування доступу до інформації.

Подальші дослідження побудови СІО уявляється доцільним сконцентрувати на актуальної задаче забезпеченні можливості автоматизованого розмежування доступу до різних видів конфіденційної та секретної інформації під час її обробки взаємодіючими структурами.

Список використаної літератури

1. Joint Doctrine Publication (JDP) 6-00 Communications and Information Systems Support to Joint Operations (3rd Edition) dated January 2008. URL: https://assets.publishing.service.gov.uk/media/5a78d1e840f0b6324769a6ad/20111221JDP600_Ed3_inc_Chg1.pdf.

2. National Information Exchange Model (NIEM). Military Operations Domain Strategic Plan. Aug, 2017. URL: http://niem.github.io/community/milops/educational/MilOpsStraPlanv7.pdf.

3. Civilian-Military Information Sharing Guidebook for Mission Planning in a Federated Mission Networking Environment. MCDC 2017-2018: CMIS Guidebook. URL: https://www.cimic-coe.org/resources/handbooks/final-cmis-guidebook-oct2018-cek.pdf.

4. D. Taylor. The evolution of real-time data-sharing in naval warfare. *Military Embedded Systems*, September 06, 2023. URL: https://militaryembedded.com/comms/communications/the-evolution-of-real-time-data-sharing-in-naval-warfare.

5. What are military data links. Bundeswehr, 2023. URL: https://www.bundeswehr.de/en/military-data-links-5676750#:~:text=Military%20data%20links%20are%20special,and%20command%20and%20control%20systems.

6. Infrastructure Resilience Planning Framework (IRPF). CISA (March 25, 2024) URL: https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf

7. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Порівняльний аналіз рішень для забезпечення контролю та управління привілейованим доступом в іт-середовищі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(16), 98–112.

8. Sokolov, V. Y., & Kurbanmuradov, D. M. (2018). Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(1), 6–16.

9. Vladymyrenko, M., Sokolov, V., & Astapenya, V. (2019). Дослідження стійкості роботи однорангових безпроводових мереж із самоорганізацією. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(3), 6–26.

10. Толюпа, С., Самохвалов, Ю., Хусаінов, П., & Штаненко, С. (2023). Самодіагностування як спосіб підвищення кіберстійкості термінальних компонентів технологічної системи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 134–147.

11. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроєктні рішення щодо побудови системи авторизації на основі концепції Zero Trust. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242.

12. Бовда Е.М. Концептуальні основи синтезу автоматизованої системи управління зв'язком військового призначення / Ю.А. Плуговий, В.А Романюк // Збірник наукових праць ВІТІ - 2016. - № 1. – С. 6 -18.

13. Grechaninov, V., et al. (2021). Decentralized Access Demarcation System Construction in Situational Center Network. In Cybersecurity Providing in Information and Telecommunication Systems II, 3188 (2), 197–206.

14. Grechaninov, V., et al. (2022). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. In Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149,107–117.

15. Оксанич І.М. Використання онтологій для побудови роле-орієнтованого інтерфейсу користувача в автоматизованих системах сервіс-орієнтованої архітектури. Proceedings of the XV International Scientific and Practical Conference "The main directions of the development of scientific research" (April 18 – 21, 2023) Helsinki, Finland. Pp. 375-377. URL: https://isg-konf.com/the-main-directions-of-the-development-of-scientific-research/.

References

1. Joint Doctrine Publication (JDP) 6-00 Communications and Information Systems Support to Joint Operations (3rd Edition) dated January 2008. URL: https://assets.publishing.service.gov.uk/media/5a78d1e840f0b6324769a6ad/20111221JDP600_Ed3_inc_Chg1.pdf .

2. National Information Exchange Model (NIEM). Military Operations Domain Strategic Plan. Aug, 2017. URL: http://niem.github.io/community/milops/educational/MilOpsStraPlanv7.pdf.

3. Civilian-Military Information Sharing Guidebook for Mission Planning in a Federated Mission Networking Environment. MCDC 2017-2018: CMIS Guidebook. URL: https://www.cimic-coe.org/resources/handbooks/final-cmis-guidebook-oct2018-cek.pdf.

4. D. Taylor. The evolution of real-time data-sharing in naval warfare. Military Embedded Systems, September 06, 2023. URL: https://militaryembedded.com/comms/communications/the-evolution-of-real-time-data-sharing-in-naval-warfare.

5. What are military data links. Bundeswehr, 2023. URL: https://www.bundeswehr.de/en/military-data-links-5676750#:~:text=Military%20data%20links%20are%20special,and%20command%20and%20control%20systems .

6. Infrastructure Resilience Planning Framework (IRPF). CISA (March 25, 2024) URL: https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf

7. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Comparative analysis of solutions to ensure control and management of privileged access in the IT environment. Electronic specialized scientific publication "Cybersecurity: education, science, technology", 4(16), 98–112.

8. Sokolov, V. Y., & Kurbanmuradov, D. M. (2018). Methods of countering social engineering at the objects of information activity. Electronic professional scientific publication "Cybersecurity: education, science, technology", 1(1), 6–16.

9. Vladymyrenko, M., Sokolov, V., & Astapenya, V. (2019). Study of stability of peer-to-peer wireless networks with self-organization. Electronic professional scientific publication "Cybersecurity: education, science, technology", 3(3), 6–26.

10. Tolyupa, S., Samokhvalov, Yu., Husainov, P., & Shtanenko, S. (2023). Self-diagnosis as a way to increase the cyber resistance of the terminal components of the technological system. Electronic specialized scientific publication "Cybersecurity: education, science, technology", 2(22), 134–147.

11. Kryuchkova, L., Skladanniy, P., & Vorohob, M. (2023). Pre-project solutions for building an authorization system based on the Zero Trust concept. Electronic specialized scientific publication "Cybersecurity: education, science, technology", 3(19), 226–242.

12. Bovda E.M. Conceptual bases of the synthesis of the automated military communication control system / Yu.A. Plugovyi, V.A Romanyuk // Collection of scientific works of VITI - 2016. - No. 1. – pp. 6-18.

13. Grechaninov, V., et al. (2021). Decentralized Access Demarcation System Construction in Situational Center Network. In Cybersecurity Providing in Information and Telecommunication Systems II, 3188 (2), 197–206.

14. Grechaninov, V., et al. (2022). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. In Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149,107–117.

15. I.M. Oksanych Using ontologies to build a role-oriented user interface in automated systems of service-oriented architecture. Proceedings of the XV International Scientific and Practical Conference "The main directions of the development of scientific research" (April 18 - 21, 2023) Helsinki, Finland. pp. 375-377. URL: https://isg-konf.com/the-main-directions-of-the-development-of-scientific-research/.