



УДК 621.391:004.056.53 (045)

Гнатюк Сергій Олександрович

доктор технічних наук, доцент, провідний науковий співробітник

Національний авіаційний університет, Київ, Україна

OrcID 0000-0003-4992-0564

s.gnatyuk@nau.edu.ua

Кищенко Віталій Васильович

здобувач

Національний авіаційний університет, Київ, Україна

OrcID 0000-0004-3652-1524

vitaliy.kyschenko@gmail.com

Котелянець Віталій Володимирович

здобувач

Центральноукраїнський національний технічний університет, Кропивницький, Україна

OrcID 0000-0004-2152-3265

v.kotelianets@gmail.com

Бауиржан Мадіна

докторант PhD

Казахський національний дослідницький університет ім. К.І. Сатпаєва, Алмати, Республіка Казахстан

OrcID 0000-0003-2144-7845

madina890218@gmail.com

МЕРЕЖЕВО-ЦЕНТРИЧНИЙ МОНІТОРИНГ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ У СЕКТОРАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Анотація. Впровадження інформаційно-комунікаційних технологій у більшості сфер суспільного життя спрямований на підвищення ефективності бізнес-процесів, проте поява нових уразливостей та кіберзагроз породжує інциденти кібербезпеки, для локалізації та нейтралізації яких необхідні ефективні методи управління. Особливої актуальності та важливості ці процеси набувають в критичній інформаційній інфраструктурі держави, так як деструктивні впливи на об'єкти критичної інформаційної інфраструктури можуть завдати значних збитків державі (людські життя, матеріальні та іміджеві втрати). Відомі методи управління інцидентами не використовують конкретні компоненти і параметри кіберпростору, що ускладнює їх застосування в реальних інформаційно-комунікаційних системах. З огляду на це, в роботі розроблена концепція мережево-центричного моніторингу інцидентів, яка дозволяє визначити найбільш важливі об'єкти (реальні) захисту критичної інформаційної інфраструктури, а також прогнозувати категорії інцидентів кібербезпеки, які виникнуть внаслідок реалізації певної кібератаки, а також визначати рівень небезпеки. Далі, на основі розробленої концепції, можуть розроблятися інструментальні засоби для прогнозування інцидентів (характер і рівень їх збитків) в інформаційно-комунікаційних системах об'єктів критичної інфраструктури держави.

Ключові слова: інцидент, кібербезпека, мережево-центричний моніторинг, концепція, критична інфраструктура, CSIRT.

1. ВСТУП

Сьогодні, з огляду на динаміку розвитку та глобалізацію сучасних інформаційно-комунікаційних технологій (ІКТ), процес впровадження та використання ІКТ у

більшості сфер суспільного життя набув неабиякої актуальності. Серед іншого, цей процес включає в себе [1]:

- розвиток засобів інтерактивної комунікації та інформаційного обміну;
- інформатизацію та автоматизацію виробничих процесів і більшості сфер суспільного життя (побудова локальних (корпоративних) обчислювальних мереж;
- систематизація інформації в базах даних;
- платформи для сумісної роботи користувачів;
- загальний доступ до ресурсів;
- VoIP та відеозв'язок;
- електронний документообіг;
- системи управління взаємовідносинами з клієнтами (CRM);
- системи планування ресурсів підприємства (ERP);
- системи управління кібербезпекою (КБ);
- контроль та управління доступом;
- послуги Інтернет-банкінгу, електронну комерцію, миттєве переведення коштів.

Зазначені процедури, функціонування яких забезпечується ІКТ, є доволі критичними навіть для пересічного громадянина, в першу чергу, з точки зору інформації, яка в них циркулює. Особливої актуальності та важливості ці процеси набувають в критичній інформаційній інфраструктурі (рис. 1). Виникнення *інцидентів КБ* (подій, які можуть порушити КБ (конфіденційність, цілісність та доступність інформації у кіберпросторі) [2]) і, як наслідок, порушення штатного режиму функціонування всієї системи, може призвести до значних матеріальних збитків. Під виявленням, ідентифікацією, обробленням та розслідуванням інцидентів КБ будемо розуміти процедури відповідно до [3] – фактично, це складові процесу управління інцидентами КБ.



Рис. 1. Сектори критичної інфраструктури згідно IPREM

Більшість відомих систем управління інцидентами [4] базується на застосуванні сенсорів і зібраної статистики, проте такі системи не можливо використовувати в кіберпросторі з метою управління КБ, так як вони не оперують з реальними параметрами кіберпростору. З огляду на це, не є можливим прогнозування враження інцидентами КБ і конкретних складових ІКТ, як компонентів кіберпростору і, як наслідок, не можливе управління протидією (контрзаходами) та ліквідацією наслідків різних категорій інцидентів. Мережево-центрична (Network-centric) теорія управління

виникла у військовому середовищі не стільки в процесі теоретичних досліджень [5], скільки внаслідок систематичного аналізу результатів впровадження в збройні сили нових бойових засобів і підвищення рівня освіченості особового складу (рис. 2).

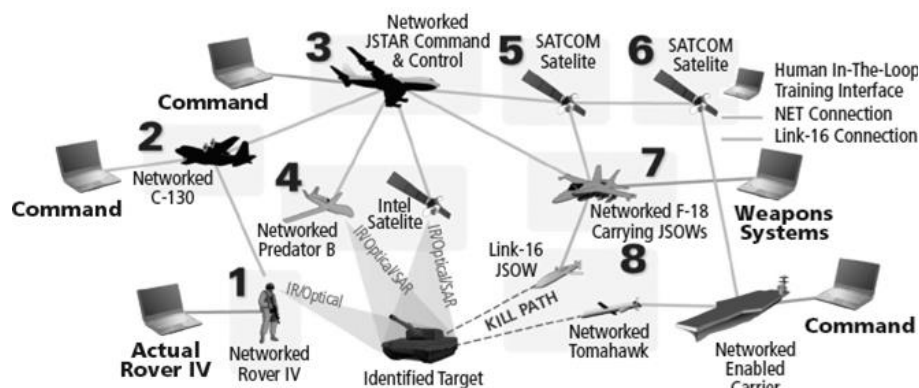


Рис. 2. Мережево-центрична концепція військового середовища

Останнім часом термін «мережево-центричний» все частіше використовується в різних цивільних галузях, пов'язаних з використанням ІКТ у сфері управління, наприклад у [6] пропонується мережево-центричне управління кластерами ІКТ, а в [7] розглядається мережево-центричний підхід до ліквідації наслідків надзвичайних ситуацій. Проте, не зважаючи на очевидну аналогію із зазначеними галузями системи управління інцидентами КБ, на сьогодні відсутня загальна концепція і відповідні методи, моделі та системи мережево-центричного управління інцидентами. З огляду на це, **метою** роботи є розробка концепції мережево-центричного моніторингу інцидентів, яка, на основі обробки динамічно змінюваних параметрів кіберпростору, дозволить визначати об'єкти захисту та прогнозувати рівень небезпеки інцидентів.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Нова версія стандарту з інцидент-менеджменту [3] визначає місце управління інцидентами в системі управління інформаційною безпекою таким чином (рис. 3):

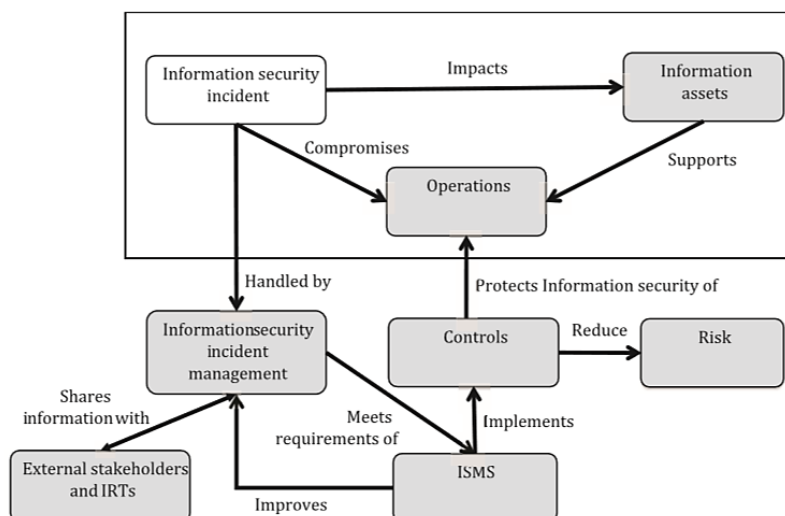


Рис. 3. Модель життєвого циклу процесу управління інцидентами

Також, відповідно до [3], основою функціонування всіх процесів системи управління інформаційною безпекою та КБ є модель PDCA. Процес управління інцидентами, теж підпорядковується зазначеній моделі (рис. 4) [4].

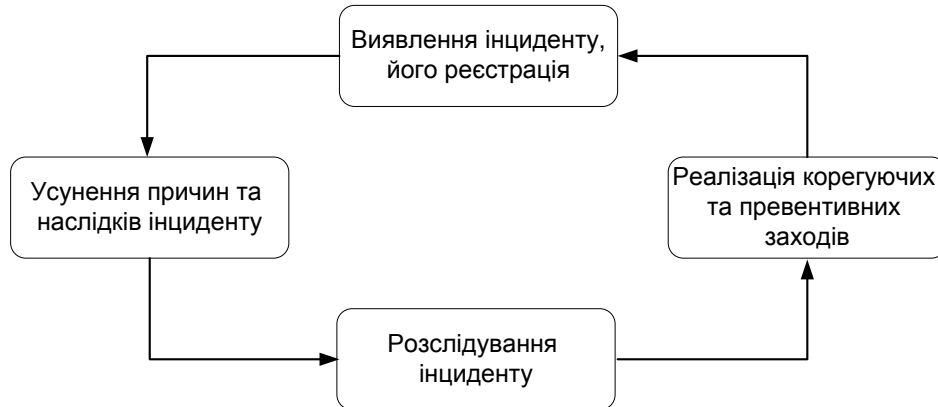


Рис. 4. Модель життєвого циклу процесу управління інцидентами

Розглянемо основні етапи згідно рис. 4:

1. Виявлення та реєстрація інциденту

Інцидент КБ може помітити користувач або адміністратор системи. Як правило, адміністратори знають, що слід робити у випадку виявлення інцидентів, чого не завжди можна сказати про користувачів. Для користувачів доцільно розробити інструкцію, яка буде містити опис, в якому вигляді співробітник повинен повідомити про виникнення інциденту, координати відповідальних осіб, а також перелік дій, які співробітник може виконати самостійно (або попереджений, що виконувати будь які дії самостійно заборонено). Звіт користувача про інцидент КБ повинен містити його детальний опис, перелік співробітників, залучених до інциденту, прізвище співробітника, який виявив інцидент, дату виникнення та реєстрації інциденту КБ. Таким чином, кожен співробітник отримує інструкцію, що визначає, як діяти, наприклад, у випадку, якщо він продовжив роботу з документом і помітив, що з минулого разу в його документ були внесені зміни, які не відповідають дійсності, при цьому автору зміни невідомі. Також необхідно розробити інструкцію для фахівця, обов'язком якого є реєстрація інцидентів. Співробітник, який виявив інцидент, зв'язується зі співробітником, відповідальним за реєстрацію інцидентів КБ і виконання подальших дій. У невеликих компаніях співробітники звертаються безпосередньо до фахівця, який може усунути наслідки і причини інциденту (наприклад, до системного адміністратора або адміністратора безпеки). У досить великих компаніях, як правило, виокремлюють співробітника, який реєструє інцидент і передає інформацію про інцидент відповідним фахівцям. Така інструкція може містити, наприклад, правила і термін реєстрації інциденту, перелік необхідних первинних інструкцій для співробітника, що виявив інцидент, крім того, опис порядку передачі інформації про інцидент відповідному фахівцю, порядок контролю над усуненням наслідків і причин інциденту.

2. Усунення причин, наслідків інциденту КБ і його розслідування

Інструкція щодо усунення причин та наслідків інциденту включає загальний опис заходів, які необхідно вжити (конкретні дії для кожного виду інциденту визначати складно і не завжди доцільно), а також терміни, протягом яких слід усунути наслідки і причини інциденту. Терміни усунення наслідків і причин інциденту залежать від рівня інциденту. Доцільно розробити класифікацію інцидентів, визначити кількість рівнів

критичності інцидентів, описати інциденти кожного рівня і терміни їх усунення. Документ, що визначає, які події в компанії слід вважати інцидентом, також може описувати рівні інцидентів. Таким чином, інструкція з усунення наслідків і причин інциденту може містити: опис заходів, які вживаються для усунення наслідків і причин інциденту, терміни усунення і відомості про відповідальність за недотримання інструкції.

3. Розслідування інциденту

Цей етап передбачає визначення винних у його виникненні, збір доказів інциденту, накладення відповідних дисциплінарних стягнень. У великих компаніях, як правило, виділяють комісію з розслідування інцидентів КБ (до складу якої може входити співробітник, який реєструє інциденти). Інструкція з розслідування інцидентів повинна описувати: заходи щодо розслідування інциденту (у тому числі визначення винних), правила збору і зберігання доказів (особливо у випадку, якщо ситуація потребує використання доказів у судових органах) і правила накладення дисциплінарних стягнень.

4. Корегувальні та запобіжні заходи

Після усунення наслідків інциденту і відновлення нормального функціонування бізнес-процесів компанії, доцільним є проведення заходів щодо запобігання повторного виникнення інциденту. Для визначення необхідності реалізації таких заходів слід провести аналіз ризиків, в рамках якого визначається доцільність корегувальних і превентивних дій. У деяких випадках наслідки інциденту будуть незначними у порівнянні з корегувальними і запобіжними заходами, і тоді доцільно не здійснювати подальших кроків після усунення наслідків інциденту.

Для того, щоб процедура управління інцидентами КБ була ефективною, всі ці етапи моделі PDCA повинні безперервно і послідовно повторюватися. Через певний час (як правило, через півроку або рік) необхідно знову переглянути перелік подій, названих інцидентами, форму звіту та ін., впровадити оновлену процедуру, перевірити її функціонування і ефективність, реалізувати запобіжні заходи. Таким чином, цикл моделі PDCA буде безперервно повторюватися і гарантувати чітке функціонування процедури управління інцидентами і, головне, її постійне удосконалення.

3. ОТРИМАНІ РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Мережево-центричний підхід до моніторингу. Протидія виникненню та ліквідації наслідків інцидентів КБ за допомогою засобів, об'єднаних інформаційними мережами в єдину систему включає в себе:

1) постійний комп'ютерний моніторинг потенційно небезпечних місць та об'єктів для визначення необхідних заходів щодо ліквідації наслідків кожного виду можливих інцидентів;

2) здійснення необхідних заходів з підготовки до боротьби з наслідками можливих груп інцидентів;

3) формування цілей паралельної ліквідації можливих видів інцидентів, їх синхронізацію, узгодження і ранжування;

4) реалізація паралельних стратегій цілей, їх синхронізацію і взаємодію використовуваних ресурсів;

5) формування можливого набору паралельних оперативних впливів, їх диспетчеризацію, синхронізацію і маневрування ресурсами в динаміці управління.

Відповідно до [7] у широкому розумінні під *моніторингом* розуміють систематичне накопичення та обробку даних про стан і динаміку зміни параметрів

аналізованого об'єкта або процесу і представлення результатів у зручному для керівника або експерта вигляді. Завданням моніторингу при комплексному управлінні підготовкою до ліквідації наслідків різних категорій інцидентів є своєчасна оцінка виникнення загроз кожній категорії інцидентів КБ, аналіз динаміки їх розвитку та їх комплексна оцінка. У динаміці це збір та аналіз даних про втрати від інцидентів.

Мережево-центрична система моніторингу об'єднує засоби моніторингу всіх рівнів і напрямків управління в єдине ціле. Вона повинна забезпечувати доведення всієї необхідної інформації до адресатів в реальному часі або близькому до нього в міру її отримання та, що дуже важливо, використовуючи інформацію, отриману на всіх рівнях і напрямках управління. Такий підхід дозволяє різко поліпшити розуміння сформованої ситуації керівниками усіх ступенів, підвищити рівень взаємодії і здійснювати синхронізацію зусиль по горизонталі і вертикалі управління. Необхідно зазначити, що порушення хоча б одного з перерахованих принципів може привести до серйозних ускладнень. Мережево-центрична концепція орієнтована не тільки на ефективне управління наявними технічними, фінансовими та іншими засобами, а й на досягнення інформаційної переваги в економіці, політиці, соціальній сфері і т.д., забезпечуючи здатність системи оперативно адаптуватися до швидкоплинної обстановки і переносити функції стратегічного та оперативного управління по вертикалі і горизонталі відповідно до потреб сформованої обстановки. Для цього мережево-центричний моніторинг повинен забезпечувати в реальному часі комплексний багаторівневий аналіз потоків окремих малоінформативних, а часто і суперечливих, первинних відомостей про появу нових об'єктів або процесів, а також динаміку зміни параметрів. Система повинна вміти змінювати логіку аналізу сформованої обстановки в міру зміни джерел інформації та отриманих нових даних про ситуацію. Вихід з ладу однієї або кількох локальних підсистем моніторингу не повинен призвести до колапсу всього мережево-центричного моніторингу.

При роботі команд реагування на інциденти КБ типу CSIRT (Computer Security Incident Response Team) [10] (вживатимемо європейський варіант назви, оскільки на американський аналог CERT сьогодні захищено авторські права згідно законодавства США) відповідно до запропонованої концепції встановлено таку послідовність (рис. 5): в середовищі ІКТ відбувається певна *подія КБ* $E_1, E_2 \dots E_n$ (відповідно до [2] подією КБ будемо розуміти ідентифіковану поведінку системи, сервісу чи мережі, яка вказує на можливе порушення КБ, політики, вихід з ладу засобів контролю чи раніше невідома ситуація, яка може мати відношення до КБ).

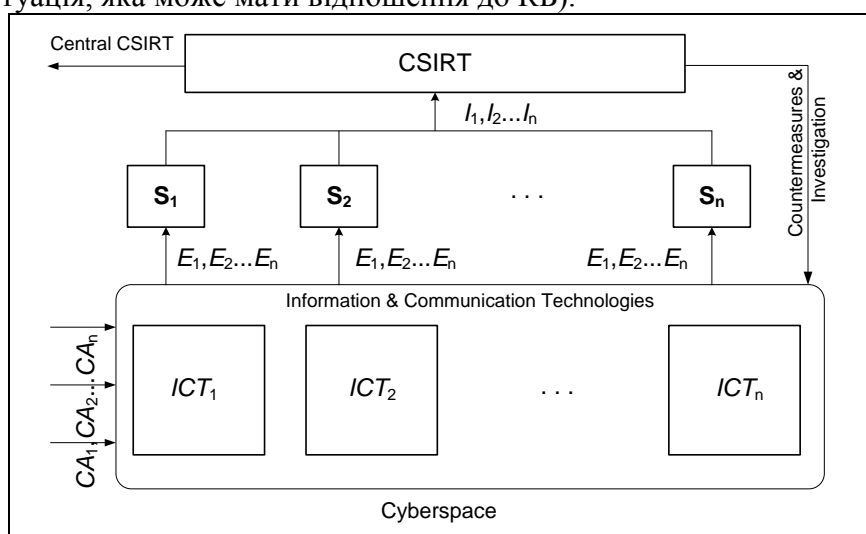


Рис. 5. Схема реалізації концепції мережево-центричного моніторингу інцидентів КБ

Зазначена подія пов'язана з певними ІКТ-складовими критичної інформаційної інфраструктури $ICT_1, ICT_2 \dots ICT_n$, спричинена як кібератаками $CA_1, CA_2 \dots CA_n$, так і ненавмисними діями, що надходить на сенсори $S_1, S_2 \dots S_n$. Сенсорами у мережево-центричній системі управління можуть бути джерела надходження інформації, зокрема:

- системи виявлення / попередження вторгнень IDS/IPS;
- системи контролю цілісності;
- міжмережеві екрани;
- honeypot системи;
- системи аналізу уразливостей;
- експлойти;
- операційні системи;
- спеціалізовані системи виявлення інцидентів типу SIEM;
- антивірусні та антиспамові системи;
- звернення користувачів у системах типу Service Desk чи Help Desk тощо).

Зазначені сенсори ідентифікують та фіксують інциденти $I_1, I_2 \dots I_n$ за певним набором їх параметрів, порівнюючи з відповідними шаблонами. Мережево-центричний моніторинг визначається тим, що для кожної системи управління інцидентами КБ формується мережа агентів (сенсорів). Загальну систему управління інцидентами сектору (галузі), регіону чи держави можна відобразити як складну мережу взаємопов'язаних центрів CSIRT кампусного типу (рис. 6) [3], кожен з яких має можливість (саме така модель побудови центрів CSIRT є найбільш вдалою для секторів критичної інфраструктури держави):

- мати чітко сформульовану мету функціонування;
- діяти відповідно до закладених при його створенні правил і алгоритмів;
- керувати базою даних, що містить необхідну йому інформацію;
- вміти використовувати результати моніторингу, реагуючи на них своїми діями;
- проявляти власну ініціативу;
- посилати і отримувати повідомлення від інших систем і вступати з ними у взаємодію.

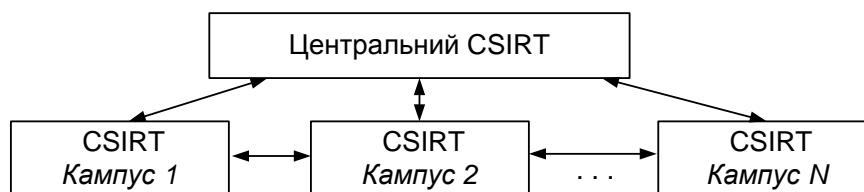


Рис. 6. Схема реалізації CSIRT кампусного типу

Побудована таким чином мережево-центрична система дозволяє зв'язати в єдиний інтерфейс управління, моніторингу і вироблення управляючих рішень всіх абонентів (посадових осіб), що входять до її складу структурних підрозділів, програмні продукти, Web сторінки, мультимедіа, а також необхідні персональні дані для їх використання різними програмними застосунками незалежно від місцезнаходження абонентів мережі.

При цьому обов'язковим є дотримання основних принципів мережево-центричного управління [7]:

1) усі елементи системи прив'язані до єдиного координатно-тимчасового поля, тобто діють в єдиному просторі станів;



2) дані для спільного використання надаються своєчасно і безперебійно; постійна підтримка систематичності спостережень за станом системи та потенційно-небезпечними об'єктами;

3) забезпечення своєчасності отримання, комплексності оброблення та використання поточної інформації, що надходить і зберігається;

4) система повинна бути самоорганізуючою, тобто здатна підтримувати, відновлюватись і адаптувати до нових умов свою структуру і поведінку, зокрема бути стійкою до часткових відмов вузлів мережі і ліній зв'язку;

5) система повинна бути відкритою, тобто обмінюватися ресурсами з середовищем тощо.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, розроблена у цій роботі концепція мережево-центричного моніторингу інцидентів КБ дозволяє визначити найбільш важливі об'єкти захисту критичної інформаційної інфраструктури, а також прогнозувати категорії інцидентів КБ, які виникнуть внаслідок реалізації певної кібератаки, та їх рівень небезпеки. У подальшому планується, на базі цієї концепції, розробити відповідні методи та інструментальні засоби, які будуть корисними для команд реагування на інциденти типу CSIRT в контексті ефективної обробки інцидентів у різних секторах критичної інфраструктури держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] С.О. Гнатюк, «Концепція мережево-центричного управління інцидентами кібербезпеки в критичній інформаційній інфраструктурі», *Інформаційна безпека*, №3 (23), С. 66-72, 2016.
- [2] В.О. Гнатюк, «Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі», *Безпека інформації*, №3 (19), С. 175-180, 2013.
- [3] ISO/IEC 27035-1:2016, *Information technology, Security techniques, Information security incident management, Principles of incident management*, 49 p., 2016.
- [4] С.О. Гнатюк, Ю.Є. Хохлачова, А.О. Охріменко, А.К. Гребенькова, «Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки», *Захист інформації*, №1 (54), С. 121-126, 2012.
- [5] «Парадигма сетецентрического управления и ее влияние на процессы управления войсками», 2015. [Online]. Available: <http://agat.by/pres/statia%20nayka-3.pdf> [Accessed: 21- Nov- 2018].
- [6] «Network centric warfare and wireless communications», 2015. [Online]. Available: <http://www.meshdynamics.com/military-mesh-networks.html> [Accessed: 21- Nov- 2018].
- [7] Э.А. Трахтенгерц, В.М. Шершаков, Д.А. Камаев, *Сетецентрические методы компьютерной поддержки управления ликвидацией последствий чрезвычайных ситуаций*, М.: ЛЕНАНД, 2015, 160 с.



Sergiy O. Gnatyuk

Doctor of Science (Engineering), Associate Professor, Lead Researcher
National Aviation University, Kyiv, Ukraine
OrcID 0000-0003-4992-0564

s.gnatyuk@nau.edu.ua

Vitaliy V. Kishchenko

Applicant for PhD degree
National Aviation University, Kyiv, Ukraine
OrcID 0000-0004-3652-1524

vitaliy.kyschenko@gmail.com

Vitaliy V. Kotelianets

Applicant for PhD degree
Central Ukrainian Technical University, Kropyvnytsky, Ukraine
OrcID 0000-0004-2152-3265

v.kotelianets@gmail.com

Madina Bauyrzhan

PhD Student
Kazakh National Research University named after K.I. Satpayev, Almaty, Republic of Kazakhstan
OrcID 0000-0003-2144-7845

madina890218@gmail.com

NETWORK-CENTRIC MONITORING FOR CYBERINCIDENTS IN SECTORS OF CRITICAL INFRASTRUCTURE OF THE STATE

Abstract. Information and communication technologies implementation in most areas of human life is aimed at improving the efficiency of business processes, but the emergence of new vulnerabilities and cyberthreats generates cybersecurity incidents. To localize and neutralize incidents effective management techniques are necessary. These processes are very actual for critical information infrastructure of the state, because destructive influences on objects of critical information infrastructure can cause big losses for the state (human life, material and status losses). Known methods for incidents management are not oriented on some special components and parameters of the cyberspace. It complicates implementation of these methods in real information and communication systems. From this viewpoint, in this paper the concept of network-centric incident management was developed. It allows to identify the most important (real) objects of critical information infrastructure protection and cybersecurity incidents to predict the categories that arise as a result of specific cyberattacks and their risk level. Further research study consists in instrumental tools based on mentioned concept. These tools can be useful for incidents prediction (character and level of losses) in information and communication systems of state critical infrastructure objects.

Keywords: incident; cybersecurity; network-centric monitoring; concept; critical infrastructure, CSIRT.

REFERENCES

- [1] S.O. Gnatyuk, «Concept of network-centric management of cybersecurity incidents in critical information infrastructure», *Informatsiyna bezpeka*, №3 (23), P. 66-72, 2016. (in Ukrainian)
- [2] V.O. Gnatyuk, «Analyze of definitions “incident” and its interpretation in cyberspace», *Bezpeka informatsii*, №3 (19), P. 175-180, 2013. (in Ukrainian)
- [3] ISO/IEC 27035-1:2016, *Information technology, Security techniques, Information security incident management, Principles of incident management*, 49 p., 2016.
- [4] S.O. Gnatyuk, Yu.Ye. Khokhlachova, A.O. Okhrimenko, A.K. Grebenkova, «Theoretical bases of information security incidents management systems construction and functioning», *Zakhyst informatsii*, №1 (54), P. 121-126, 2012. (in Ukrainian)



- [5] «Paradigm of network centric management and its influence on army forces management», 2015. [Online]. Available: <http://agat.by/pres/statia%20nayka-3.pdf> [Accessed: 21- Nov- 2018]. (in Russian)
- [6] «Network centric warfare and wireless communications», 2015. [Online]. Available: <http://www.meshdynamics.com/military-mesh-networks.html> [Accessed: 21- Nov- 2018]. (in English)
- [7] E.A. Trakhtengerts, V.M. Shershakov, D.A. Kamaev, Network-centric methods for computer support of disaster recovery management, M.: LENAND. 2015, 160 P. (in Russian)