УДК: 044.056:004.93'1 DOI: 10.46972/2076-1546.2020.18.10

І. В. Гуменюк, М. С. Басараба, О. В. Некрилов

МЕТОДИКА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КРИТИЧНИХ КОМПОНЕНТІВ МЕРЕЖ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Встановлено, що ефективність та надійність функціонування інформаційно-телекомунікаційних систем, зокрема мереж, які входять до їх складу, суттєво залежить від високого рівня захищеності критичних компонентів. Разом з тим постійне удосконалення технічного оснащення даних систем вимагає створення нового та покращення наявного методичного забезпечення кібернетичної безпеки. Одним із перспективних підходів вважається розроблення універсальної методики забезпечення кібербезпеки в умовах здійснення кібернетичних атак (впливів, загроз тощо) та несанкціонованого доступу неавторизованими користувачами до критичних вузлів (компонентів) мереж інформаційно-телекомунікаційної системи.

Своєчасне виявлення, оперативна протидія кібернетичним загрозам та несанкціонованому доступу до критичних компонентів мереж є необхідною складовою забезпечення високого рівня кібербезпеки інформаційно-телекомунікаційної системи в цілому, особливо в умовах ведення гібридної війни та збройної агресії з боку Російської Федерації, що обумовлює необхідність розроблення відповідного методичного забезпечення. З цією метою у статті запропоновано методику забезпечення кібербезпеки критичних компонентів мереж інформаційно-телекомунікаційної системи, в основу якої покладено: комплексне застосування контролю стану мережевих вузлів та доступу користувачів до них; фіксування фактів здійснення кібернетичних атак на підставі аналізу вхідного (вихідного) трафіка; своєчасне виявлення кібернетичних загроз та скоєння несанкціонованого доступу; оперативну протидію цим спробам.

У роботі наведено результати верифікації запропонованої методики. Показано, що її застосування дозволяє оперативно виявляти факти здійснення кібернетичних загроз та несанкціонованого доступу до критичних компонентів мереж інформаційно-телекомунікаційних систем, а також ефективно протидіяти цим спробам.

Ключові слова: *критичний компонент; мережа; інформаційно-телекомунікаційна система; кібербезпека; кібернетична атака; несанкціонований доступ; система виявлення вторгнень.*

Постановка проблеми в загальному вигляді. Інформаційний сектор завжди викликав великий інтерес у кіберзлочинних угруповань. За останніх п’ять років кібератаки здійснювалися на держустанови, сферу науки (освіти), фінансову, промислову та військову галузі [1]. Прикладом тому є значна кількість проведених атак у світі: кібератака хакерського угруповання Angels_Of_Truth (квітень – травень 2016 року, Канада); кібератака типу “credential stuffing” (початок 2019 року, США та Японія); кібератака типу “blackout” (березень 2019 року, Венесуела); серія нетиповий кібератак на банківський та енергетичний сектор (лютий 2020 року, Російська Федерація). В Україні в умовах складної та недостатньо стабільної політико-економічної ситуації такі випадки також мають місце.

Наприклад, кібератака на інфраструктурні об'єкти держави (грудень 2015 року, Прикарпаття, Київська, Чернівецька області); кібератака на внутрішні телекомунікаційні мережі (грудень 2016 року, Міністерство фінансів України); масштабна кібернетична атака російських хакерів (червень 2018 року); понад 10 тисяч різних видів кібератак виявлено та заблоковано (травень – червень 2020 року). Отже, в умовах, що склалися, актуальним є завдання розроблення нових ефективних та удосконалення відомих методів протидії кібернетичним атакам та несанкціонованому доступу (НСД).

Виходячи з даних передумов, сформульовано **мету** статті, яка полягає в розробленні методики забезпечення кібербезпеки критичних компонентів мережі інформаційно-телекомунікаційної системи (ІТС).

Аналіз останніх досліджень і публікацій. На сьогодні вже розроблено та реалізовано низку сучасних методів захисту інформації ІТС. Авторами у [2] розглянуто сучасні системи виявлення вторгнень у комп'ютерних системах; у [3] проаналізовано наявні протоколи та методи маршрутизації потоків даних; у [4] досліджено системи захисту інформації, які реалізовують аналіз, моніторинг, контроль мережевих потоків ІТС; у [5] розглянуто та проаналізовано основні можливості, принципи (механізми) функціонування систем виявлення атак; у [6] описано системи виявлення атак та їх технологічні особливості; у [7] подано теоретичний аналіз сучасних систем виявлення вторгнень, які забезпечують захист інформаційних систем та мереж.

Отже, результати аналізу науково-практичних джерел свідчать про те, що для вирішення завдань захисту ІТС розроблено достатню кількість науково-методичного та практичного забезпечення. Проте універсальній методиці захисту ІТС в умовах здійснення кібератак та НСД у науковій літературі не присвячено належної уваги.

Постановка завдання. Для мережі ІТС з N інформаційними вузлами необхідно розробити дієву методику, яка забезпечить відповідний рівень кібербезпеки її критичних компонентів. Топологію цієї мережі описує зв'язний граф $G=(V,E)$, де V – вузли (критичні компоненти), а E – ребра (канали зв'язку). Аналіз вхідного та вихідного трафіка мережі проводиться постійно. Рівень забезпечення кібербезпеки прийматимемо за нормований показник з межами $[0.1;0.9]$.

Виклад основного матеріалу. Забезпечення надійного захисту інформації, важливих компонентів ІТС є комплексним завданням, яке включає в себе сукупність взаємопов'язаних задач. Саме тому для досягнення мети завдання запропоновано методику, яка складається з таких кроків:

постійний контроль стану мережевих вузлів та каналів зв'язку мережі ІТС;

фіксування фактів здійснення кібернетичних атак із детальним описом рівня небезпеки загроз;

постійний контроль доступу користувачів до мереж ІТС;

своєчасне виявлення НСД до мережі ІТС та кіберзагроз, а також оперативна протидія їм.

Детально розглянемо кожен із кроків.

Етап 1. Постійний контроль стану мережевих вузлів та каналів зв'язку мережі ІТС. Оскільки важливим завданням управління мереж є підтримання функціональності та надійності кожного мережевого компонента, то для ІТС необхідно використовувати

ієрархічне управління, розподіливши мережу на окремі кластери (зони) з виділенням їх контролерів, вузлів-шлюзів і внутрішніх вузлів.

Множина N вузлів мережі ІТС розподіляється на k кластерів, які локально мінімізовані за відстанню між інформаційною точкою та центрами кластерів. Цільова функція алгоритму розраховується за формулою

$$J = \sum_{h=1}^{k} \sum_{v_i \in V_h} \left\| v_i - \mu_h \right\|^2 , \tag{1}$$

де μ_h – значення центрів кластера.

Цільова функція є локально мінімізованою для усіх кластерів (кожна точка з набору об'єктів знаходитися на мінімальній відстані від центра кластера, до якого вона належить). Вибір відповідного кластера для заданої точки в процесі роботи алгоритму обумовлений у такий спосіб:

$$\left\| v_i - \mu_h \right\|^2 = min \left\{ \left\| v_i - \mu_h \right\|^2 \right\}_{h=1}^{k} . \tag{2}$$

При цьому кожен кластер містить однакову кількість внутрішніх вузлів. Визначаємо опорну мережу контролерів кластерів та вузли-шлюзи, які формують віртуальну магістраль усієї мережі, що використовується як для передачі маршрутної інформації, так і для користувацького трафіка. Проаналізуємо процедуру формування основних елементів мережі.

Визначення контролерів кластерів. Територіально розподілені на непересічні кластери абоненти за відомими методами на максимальному енергетичному рівні (усі вузли знаходяться в зоні дії хоча б одного доступного вузла) розсилають HELLO-повідомлення з метою визначення доступності усіх вузлів з урахуванням метрики кожного кластера. За отриманими відповідями кожний вузол визначає максимально можливу кількість вузлів, які можуть бути підключені до нього, та формує таблицю зв'язності. Вузли один одному, зокрема через транзитні (HOP-повідомлення), відправляють Cluster-повідомлення. У такий спосіб визначається вузол як потенційно можливий контролер кластера із максимальним ступенем зв'язаності (кількістю підключених до нього вузлів). Контролер кластера, у свою чергу, розсилає повідомлення кожному вузлу кластера, формуючи нову таблицю маршрутизації.

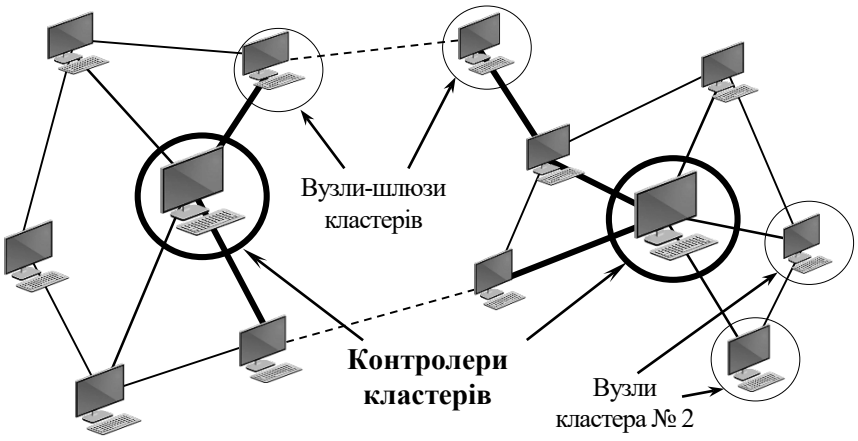

Рис. 1. Визначення контролерів кластерів та вузлів-шлюзів мережі

Визначення вузлів-шлюзів. Вузли різних кластерів з урахуванням однакової метрики мережі розсилають один одному, зокрема й через транзитні вузли, повідомлення для визначення відстаней між ними.

У такий спосіб вони формують тимчасову таблицю маршрутизації, у якій міститься інформація про відповідні відстані. Вузли різних кластерів з мінімальними значеннями відстаней визначаються як потенційно можливі вузли-шлюзи (див. рис. 1). Ці вузли формують власні таблиці маршрутизації до потенційних контролерів та шлюзів інших кластерів [8].

Для постійної підтримки актуальності таблиць маршрутизації та цілісності топології мережі контролери кластерів періодично розсилають вузлам інформацію про стан каналів. В умовах успішного проведення кібератаки на вузол кластера (він визначається як потенційно небезпечний) здійснюється його фізична ізоляція (рис. 2). Такий підхід ефективний для забезпечення кібербезпеки іншого кластера.

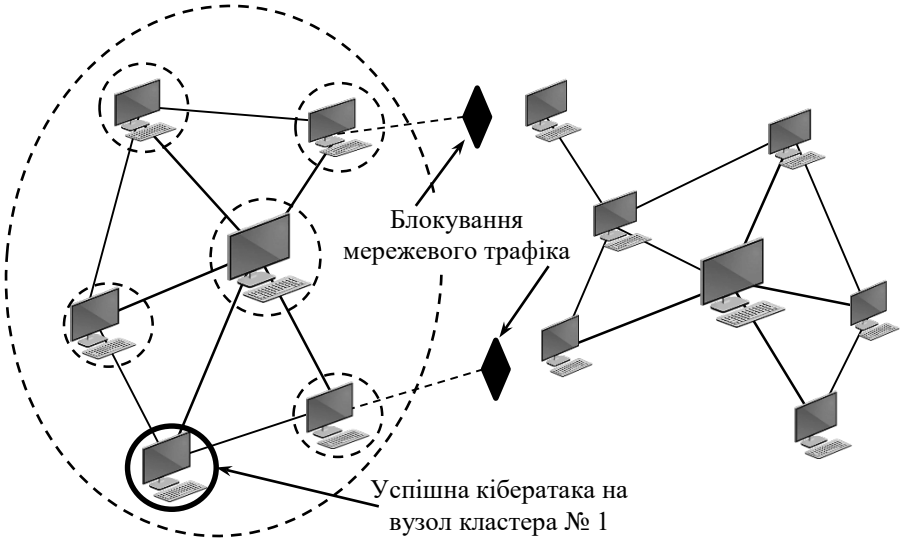

Рис. 2. Фізична ізоляція потенційно небезпечного кластера

Етап 2. Фіксування фактів здійснення кібернетичних атак із детальним описом рівня небезпеки загроз. На даному кроці проводиться аналіз вхідного (вихідного) трафіка кластерів мережі, зокрема з використанням наявної системи виявлення вторгнень Intrusion Detection System (IDS). У результаті виконання поточного кроку визначаються рівні безпеки мережі: допустимий (трафік містить певну загрозу, однак може фільтруватися) та небезпечний (вхідний трафік блокується для подальшого проходження в мережу). Свого пікового значення кібербезпека мережі ІТС набуватиме за умови застосування багаторівневого захисту.

Етап 3. Постійний контроль доступу користувачів до мереж ІТС. На даний момент розвитку інформаційних технологій парольні, які базуються на унікальній персональній інформації, та атрибутні методи ідентифікації втрачають свою актуальність, проте користуються великим попитом серед користувачів. Порівняно з цими методами біометричні характеристики користувача як спосіб автентифікації можуть гарантувати підвищений рівень безпеки, враховуючи особливості біометричних даних конкретної особи.

Для забезпечення перевірки автентичності користувачів на даному етапі реалізовують такі заходи.

Виявлення та локалізація геометрії обличчя користувача на зображенні відеопотоку. Для пошуку форми (геометрії) обличчя на зображенні систем відеоспостереження використано алгоритм Віоли – Джонса. Як правило, цей пошук відбувається швидко, проте інтелектуальне вивчення ознак класифікатором проводиться тривалий час.

У разі використання даного методу відеозображення подається в інтегральному вигляді (матриця значень сумарної яскравості) для підвищення оперативності аналітичних обчислень та розрахунків:

$$L(x,y)=\sum_{i=0}^{i\le x}\sum_{j=0}^{j\le y} I(i,j), \tag{3}$$

де $I(i,j)$ – значення яскравості пікселя на зображенні.

Кожен елемент $L(x,y)$ відповідає сумі пікселів, які знаходяться в певному прямокутнику. При цьому для вхідного відеопотоку проводиться нормалізація зображення за масштабом, яскравістю тощо.

Обчислення набору базових ознак (характеристик) зображення. Основними принципами, на яких ґрунтується метод Віоли – Джонса, є використання базових понять теорії розпізнавання об'єктів, зокрема ознак (примітивів) Хаара, застосування їх каскаду для аналізу результату ідентифікації. Усі ознаки надходять на вхід класифікатора та обробляються з деяким підсиленням, так званим "бустингом" (*від англ.* boost – вдосконалення, посилення) [9].

Ознаки (примітиви) Хаара – це відображення f:

$$\chi \Rightarrow D_f, \tag{4}$$

де D_f – множина допустимих значень ознаки.

За умови, що ознаку $f_1,...,f_n$ визначено, вираз (4) набуде такого вигляду:

$$\chi \Rightarrow \{f_1,...,f_n\}, \tag{5}$$

який називають ознакою опису об'єкта.

Порівняння обчислених ознак з еталонними, що містяться в базі даних.

Загальну структуру контролю доступу користувачів до мереж ІТС наведено на рис. 3.

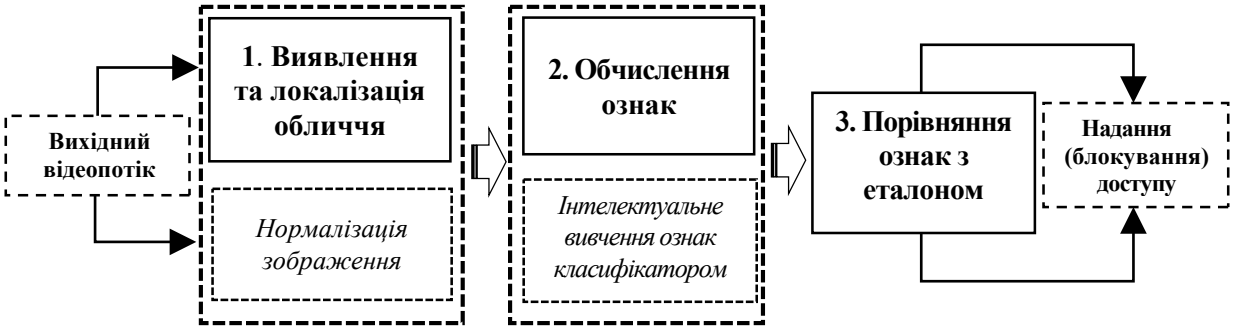

Рис. 3. Структура контролю доступу користувачів до мереж ІТС

За умови скоєння кібератак та/або НСД до мереж ІТС виконується ***своєчасне їх виявлення й оперативна протидія цим спробам та кіберзагрозам.*** Останній етап методики ґрунтується на узагальненні інформації про кіберзагрози або скоєння НСД, зокрема: власне сам факт здійснення кібернетичних атак (час, "компонент-жертва", нова або повторна загроза тощо); деталізований опис рівня небезпеки загрози.

Верифікацію запропонованої методики проведено на мережі ІТС, яка складається з 12 кластеризованих вузлів, кожен із яких умовно приймається за критичний компонент. Топологію вихідної мережі наведено на рис. 4, її характеристику – у табл. 1. Тестовими типами атак обрано user-to-root (U2R) та PROBE.

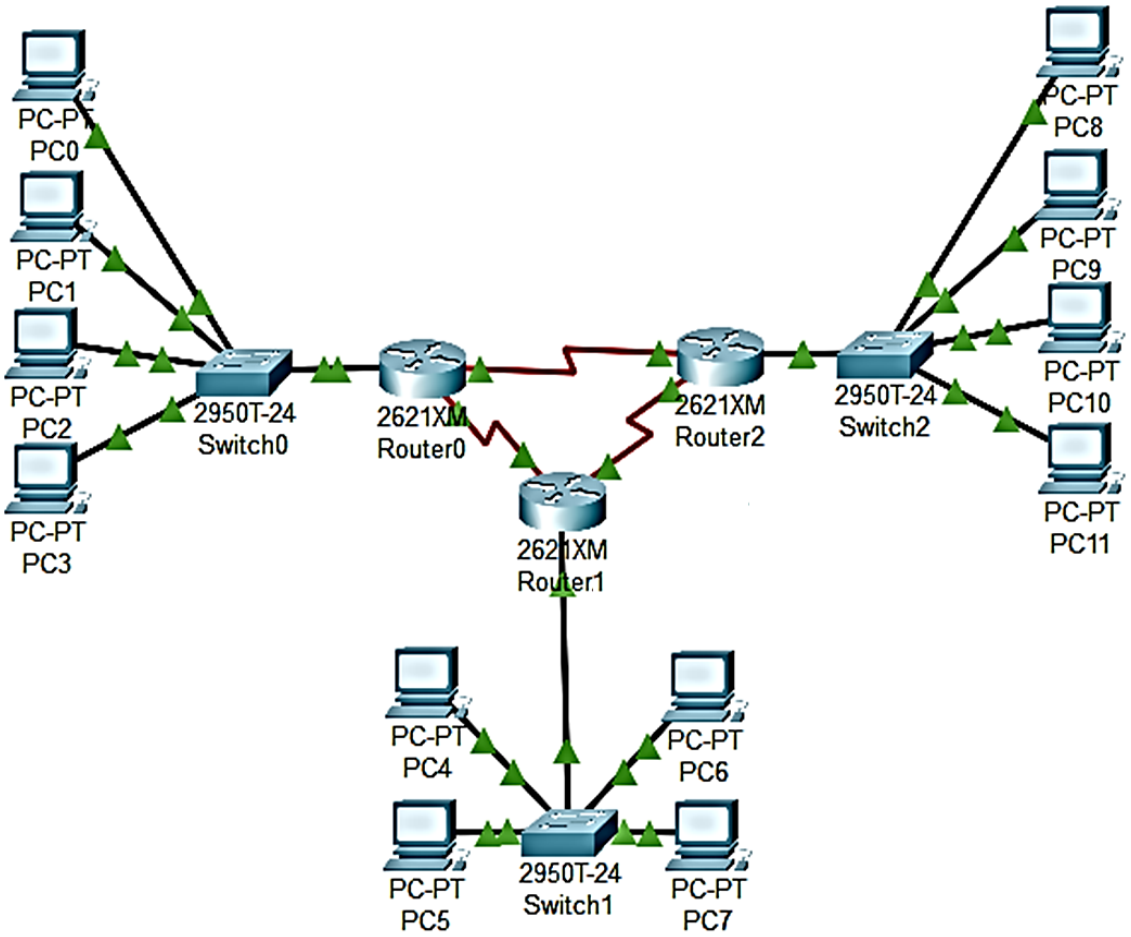

Рис. 4. Структура вихідної мережі ІТС

Таблиця 1

Характеристика досліджуваної мережі

Номер мережевого вузла	Наявність [+] та відсутність [-] компонентів забезпечення кібербезпеки		
	Контроль стану вузлів та каналів зв'язку	Система виявлення вторгнень	Контроль доступу користувачів
Кластер № 1 (Switch 0 – вузол-шлюз; Router 0 – контролер кластера)			
№ 1, PC 0	+	-	-
№ 2, PC 1	+	-	-
№ 3, PC 2	+	-	-
№ 4, PC 3	+	-	-

Продовження таблиці 1

Номер мережевого вузла	Наявність [+] та відсутність [-] компонентів забезпечення кібербезпеки		
	Контроль стану вузлів та каналів зв'язку	Система виявлення вторгнень	Контроль доступу користувачів
Кластер № 2 (Switch 1 – вузол-шлюз; Router 1 – контролер кластера)			
№ 5, PC 4	+	+	-
№ 6, PC 5	+	+	-
№ 7, PC 6	+	+	-
№ 8, PC 7	+	+	-
Кластер № 3 (Switch 2 – вузол-шлюз; Router 2 – контролер кластера)			
№ 9, PC 8	+	+	+
№ 10, PC 9	+	+	+
№ 11, PC 10	+	+	+
№ 12, PC 11	+	+	+

Результати проведення досліджень надано в табл. 2.

Таблиця 2

Результати верифікації запропонованої методики

Мережевий компонент	Рівень кібербезпеки ([0,5 і вище] – достатній; [менше 0,5] – недостатній)		
	Етап 1	Етап 2	Етап 3
Кластер № 1	0,9	0,1	0,1
Кластер № 2	0,9	0,8	0,1
Кластер № 3	0,9	0,9	0,9
Мережа ІТС	0,9	0,5	0,3

Аналіз отриманих результатів свідчить про те, що кожен етап методики (системи IDS, контроль доступу тощо) – один із технічних інструментів забезпечення кібербезпеки, він не повинен розглядатися окремо або як заміна для будь-якого іншого.

Висновки та перспективи подальших досліджень. У даній роботі наведено результати вирішення актуального науково-практичного завдання, яке полягало в удосконаленні наявних методів протидії кібернетичним атакам та НСД, а саме в розробленні методики забезпечення кібербезпеки критичних компонентів мережі ІТС.

В основу запропонованої методики покладено: комплексне застосування контролю стану мережевих вузлів та доступу користувачів до них; фіксування фактів здійснення кібернетичних атак на підставі аналізу вхідного (вихідного) трафіка; своєчасне виявлення кібернетичних загроз та скоєння НСД; оперативну протидію цим спробам.

Практичне значення одержаних результатів полягає в можливості інтеграції наукового результату в мережі ІТС для забезпечення відповідного рівня кібербезпеки.

СПИСОК ЛІТЕРАТУРИ

1. Гуменюк І. В., Басараба М. С., Некрилов О. В. Методика захисту інформації важливих компонентів мережі інформаційно-телекомунікаційної системи // ІІІ Всеукр. наук.-техн. конф. "Комп'ютерні технології: інновації, проблеми, рішення" : тези доповідей. Житомир : Житомирська політехніка, 2020. С. 27–28.

2. Казмірчук С., Корченко А., Паращук Т. Аналіз систем виявлення вторгнень // Захист інформації, 2018. Т. 20, № 4. С. 259–276.
3. Уманець Я. Л. Протоколи та методи маршрутизації потоків даних у перспективних мобільних радіомережах з динамічною топологією // Системи озброєння і військова техніка, 2013. № 2. С. 150–159.
4. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. Харків : Вид. ХНЕУ, 2013. 476 с.
5. Толюпа С. В., Штаненко С. С., Берестовенко Г. В. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови // Зб. наук. праць ВІТІ. 2018. № 3. С. 112–122.
6. Зоріна Т. І. Системи виявлення і запобігання атак в комп'ютерних мережах // Вісник Східноукраїнського нац. ун-ту ім. В. Даля. 2013. № 15 (1). С. 48–52.
7. Колодчак О. М. Сучасні методи виявлення аномалій в системах виявлення вторгнень // Computer Systems and Networks, 2012. № 745. 2012. С. 98–104.
8. Пількевич І. А., Бойченко О. С., Гуменюк І. В. Метод децентралізованого управління мережевими ресурсами інформаційно-комунікаційних мереж // Технічна інженерія. Житомир : ДУ "Житомирська політехніка", 2019. № 2 (84). С. 100–109.
9. Гуменюк І. В., Басараба М. С., Некрилов О. В. Біометрична ідентифікація у кіберпросторі на основі розпізнавання обличчя // Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн : тези доп. наук.-практ. конф. (24–25 жовтня 2019 р.). Житомир : ЖВІ, 2019. С. 205–207.

Подано 10.10.2020

REFERENCES

1. Humeniuk, I. V., Basaraba, M. S., & Nekrylov, O. V. (2020). Metodyka zakhystu informatsii vazhlyvykh komponentiv merezhi informatsiino-telekomunikatsiinoi systemy [Methods of information protection of important components of the information and telecommunication system network]. In *III Vseukr. nauk.-tekhn. konf. "Komp'iuterni tekhnolohii: innovatsii, problemy, rishennia": tezy dopovidei [III All-Ukrainian. scientific and technical conf. "Computer technology: innovations, problems, solutions": abstracts of Papers]*. (pp. 27–28). Zhytomyr: SU Zhytomyr polytechnic [in Ukrainian].
2. Kazmirchuk, S., Korchenko, A., & Parashchuk, T. (2018). Analiz system vyiavlennia vtorhnen [Analysis of intrusion detection systems]. *Zakhyst informatsii [Information security, Vol. 20,* № 4, 259–276 [in Ukrainian].
3. Umanets, Ya. L. (2013). Protokoly ta metody marshrutyzatsii potokiv danykh u perspektyvnykh mobilnykh radiomerezhakh z dynamichnoiu topolohiieiu [Protocols and methods of routing data streams in advanced mobile radio networks with dynamic topology]. *Systemy ozbroiennia i viiskova tekhnika [Weapons systems and military equipment], 2,* 150–159 [in Ukrainian].
4. Ostapov, S. E., Yevseiev, S. P., & Korol, O. H. (2013). *Tekhnolohii zakhystu informatsii [Information protection technologies]*. Kharkiv [in Ukrainian].

5. Toliupa, S. V., Shtanenko, S. S., & Berestovenko, H. V. (2018). Klasyfikatsiini oznaky system vyiavlennia atak ta napriamky yikh pobudovy [Classification features of attack detection systems and directions of their construction]. *Zb. nauk. prats VITI [Collection of scientific works of the Military Institute of Telecommunications and Information Technologies named after Heroiv Krut], 3,* 112–122 [in Ukrainian].
6. Zorina, T. I. (2013). Systemy vyiavlennia i zapobihannia atak v komp'iuternykh merezhakh [Systems of detection and prevention of attacks in computer networks]. *Visnyk Skhidnoukrainskoho nats. un-tu im. V. Dalia [Bulletin of the Volodymyr Dahl East Ukrainian National University], 15* (1), 48–52 [in Ukrainian].
7. Kolodchak, O. M. (2012). Suchasni metody vyiavlennia anomalii v systemakh vyiavlennia vtorhnen [Modern methods of detecting anomalies in intrusion detection systems]. *Computer Systems and Networks, 745,* 98–104 [in Ukrainian].
8. Pilkevych, I. A., Boichenko, O. S., & Humeniuk, I. V. (2019). Metod detsentralizovanoho upravlinnia merezhevymy resursamy informatsiino-komunikatsiinykh merezh [Method of decentralized management of network resources of information and communication networks]. *Tekhnichna inzheneriia [Technical Engineering],* 2 (84), 100–109. Zhytomyr: SU Zhytomyr polytechnic [in Ukrainian].
9. Humeniuk, I. V., Basaraba, M. S., Nekrylov, O. V. (2019). Biometrychna identyfikatsiia u kiberprostori na osnovi rozpiznavannia oblychchia [Biometric identification in cyberspace based on face recognition]. In *Problemy teorii ta praktyky informatsiinoho protyborstva v umovakh vedennia hibrydnykh viin : tezy dop. nauk.-prakt. konf. [Problems of theory and practice of information confrontation in the conditions of hybrid wars: abstracts of reports of the scientific-practical conference of the Korolov Zhytomyr Military Institute]*. Zhytomyr, October 24–25, 2019. (pp. 205–207). Zhytomyr: ZhMI [in Ukrainian].

I. V. Humeniuk, M. S. Basaraba, O. V. Nekrilov

METHODS OF ENSURING CYBER SECURITY OF CRITICAL COMPONENTSNETWORKS OF INFORMATION AND TELECOMMUNICATION SYSTEM

It is established that the efficiency and reliability of information and telecommunication systems, in particular the networks that are part of them, significantly depends on the high level of protection of critical components. However, the constant improvement of the technical equipment of these systems requires the creation of new and improvement of existing methodological support for cyber security. One of the promising approaches is the development of a universal method of cybersecurity in the context of cyberattacks (influences, threats, etc.) and unauthorized access by unauthorized users to critical nodes (components) of information and telecommunications systems.

Timely detection, prompt counteraction to cyber threats and unauthorized access to critical network components is a necessary component of ensuring a high level of cybersecurity of the information and telecommunications system as a whole, especially in the context of hybrid warfare and armed aggression by the Russian Federation. To this end, the article proposes a method of cybersecurity of critical components of information and telecommunications systems, which is based on the integrated application of monitoring the state of network nodes

and user access to them, recording the facts of cyberattacks based on analysis of incoming (outgoing) traffic, timely detection of unauthorized access to and commission of cyber threats, as well as operational response to these attempts. The paper presents the results of verification of the proposed methods.

To this end, the article proposes a method of cybersecurity of critical components of information and telecommunications systems, which is based on the integrated application of monitoring the state of network nodes and user access to them, recording the facts of cyberattacks based on analysis of incoming (outgoing) traffic, timely detection of unauthorized access to and commission of cyber threats, as well as operational response to these attempts. The paper presents the results of verification of the proposed method. It is shown that its application allows to quickly detect the facts of cyber threats and unauthorized access to critical components of information and telecommunication systems networks and effectively counteract these attempts.

Keywords: *critical component; chain; information and telecommunication system; cybersecurity; cyberattack; unauthorized access; intrusion detection system.*