**DOI: 10.18372/2225-5036.29.17547**

# КЛАСТЕРНИЙ ПІДХІД ПОБУДОВИ МЕРЕЖ ЯК СПОСІБ ЗАБЕЗПЕЧЕННЯ ВІДПОВІДНОГО РІВНЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

**Кирило Сметанін**

*Житомирський військовий інститут імені С.П. Корольова*

**СМЕТАНІН Кирило Володимирович, к. т. н.**
*Рік та місце народження:* 1982 рік, м. Житомир, Україна.
*Освіта:* Житомирський військовий інститут імені С.П. Корольова, 2005 рік.
*Посада:* старший викладач кафедри захисту інформації та кібербезпеки з 2021 року.
*Наукові інтереси:* кібербезпека, комп'ютерні мережі , програмування.
*Публікації:* понад 20 друкованих публікацій, серед яких, конспект лекцій, авторські права на твір, наукові статті та патенти на винаходи.
*E-mail:* kiry221982@gmail.com.
*ORCID ID:* 0000-0002-6062-550X.

***Анотація.*** *Взаємодія між суб'єктами сучасного суспільства невід'ємно пов'язана з надійним функціонуванням комп'ютерних інформаційних систем і мереж. Безпека та якість обслуговування (англ. Quality of service, QoS) є двома ключовими мережевими послугами для забезпечення безпеки зв'язку (відповідно до українського національного стандарту ДСТУ ISO/IEC 27000:2017). Якість є ключовою вимогою, і з подальшим розвитком комп'ютеризованих інформаційних систем і мереж швидко зростають додаткові вимоги до безпеки. Характеристики безпеки, рівні обслуговування та вимоги до керування всіма мережевими службами мають бути визначені та включені до будь-якої угоди про надання послуг мережі. Інтенсивний розвиток комп'ютерних інформаційних систем і мереж підвищив уразливість системи та в рази збільшив можливість кібернетичних атак. Тому управління мережевою безпекою є ключовим елементом функціонування комп'ютерних систем і мереж. Вразливості безпеки в маршрутизаторах, балансувальниках і операційних системах міжмережевого екрану, такі атаки як «відмова в доступі» і «відмова в обслуговуванні» на ключові мережеві вузли і сервери, зміна параметрів і вторгнення в маршрутизатори тощо, впливають на доступність ресурсів і якість обслуговування. Такі питання, як забезпечення ключових параметрів QoS, захист пакетів даних, запобігання атакам вторгнень і атакам на відмову в обслуговуванні, – це лише деякі з питань, які необхідно вирішити, щоб забезпечити безпечний розподіл ресурсів, доступ і безпечні шляхи передачі, захист вмісту та кінцеві - завершення надання QoS. Механізми безпеки та QoS не є незалежними. Вибір механізму безпеки впливатиме на продуктивність QoS і навпаки. Задоволення вимог щодо якості обслуговування вимагає використання механізмів безпеки для забезпечення належного рівня обслуговування та виставлення рахунків. Неправильний вибір механізмів безпеки знизить продуктивність ретельно побудованої мережі, або інформаційно-комунікаційної системи(далі ІТС), а неправильний вибір рівнів обслуговування призведе до витоку інформації. Тобто оптимальний баланс параметрів QoS допомагає зменшити витік інформації. Таким чином в даній статті запропоновано кластерний підхід побудови мережі для своєчасного виявлення та реагування на кіберзагрози, а також несанкціонований доступ до критичних компонентів мережі який в свою чергу є необхідною складовою для забезпечення високого рівня кібербезпеки всієї ІТС.*

***Ключові слова:*** *кластер, мережа, інформаційно-комунікаційна система, кібербезпека, кібернетична атака, несанкціонований доступ, захищена система.*

**Постановка проблеми**

Захист національних інтересів в інформаційній сфері [1] будь-якої розвиненої в технологічному та економічному плані держави безпосередньо пов'язаний із кіберзахистом [2] електронних інформаційних ресурсів її громадян, суспільства і державних інститутів [3]. Насамперед захист державних ІТС від кібернетичних атак зловмисників. За останні декілька років кібернетичних атаки здійснювались на енергетичні системи, державні установи, об'єкти інфраструктури, державні фінансові організації та інші. Прикладами таких

атак є: 13 червня 2018 року німецька контррозвідка (Федеральне управління з інформаційної безпеки, BSI) оприлюднила інформацію про масштабну кібератаку на енергетичні компанії в країні з боку російських хакерів. Атака отримала назву англ. Berserk Bear. Зловмисники намагались здобути несанкціонований доступ до інформаційних систем компаній енергетичного сектора, але їм вдалось проникнути лише до офісних комп'ютерних мереж декількох компаній; 22 березня 2018 року муніципальні інформаційні системи міста Атланта була вражена здирницьким хробаком SamSam, який атакує уразливість в десеріалізації деяких серверах застосунків на Java. Зловмисники вимагали сплати викупу в біткоїн на суму еквівалентну близько $55 тисяч. Натомість місто звернулось по допомогу до фахівців з комп'ютерної безпеки й планує витратити близько $2 667 328 на усунення наслідків атаки та поліпшення захисту інформаційних систем; 15 лютого 2022 року DDoS-атака на 15 банківських сайтів, сайтів зо доменом gov.ua, також сайтів Міноборони, Збройних сил та Міністерства з питань реінтеграції тимчасово окупованих територій, що тривала близько 5 годин. За даними Ради національної безпеки США, кібератака була влаштована ГРУ Росії. Пізніше, 23 лютого, перед початком російського вторгнення в Україну було повторно атаковано низку державних сайтів та банківських сайтів. Компанія ESET виявила на зламаних сайтах шкідливі програмні засоби HermeticWiper, що були скомпільовані ще 28 грудня 2021 року [4].

Тому в сучасних умовах актуальною є задача розробки нових ефективних та вдосконалення відомих методів боротьби з мережевими атаками та несанкціонованим доступом (далі НСД). Виходячи з цих передумов, мета цієї роботи була сформульована для розробки кластерного підходу побудови мереж як спосіб забезпечення відповідного рівня кібербезпеки інформаційно-комунікаційної системи.

**Аналіз останніх досліджень і публікацій**

Інтеграція України у світовий інформаційний простір, розвиток суспільства нашої країни, як суспільства знань, призвели до появи нових загроз її національним інтересам, пов'язаних з кібербезпекою. За даними РНБО України тільки в першому півріччі 2020 року за злочини в кіберпросторі проти державності було засуджено більш ніж 20 чоловік. Згідно з дослідження "Глобальний індекс кібербезпеки" (Global Cybersecurity Index), яке щорічно проводить Міжнародний союз електрозв'язку (ITU), у 2022 році Україна зайняла 24 місце у рейтингу з 163 можливих. При цьому тільки дві пострадянських країн — Латвія (3) та Естонія (4) суттєво випередили нас у рейтингу, а ось країна агресор росія (29 місце), інші пострадянські країни Грузія (50 місце) Азербайджан (52 місце) та Білорусь (68 місце). Це свідчить про те, що України значну увагу приділяє кібернетичному захисту інформації, усвідомлюючи те що країна агресор росія достатньо близька розташована в даному рейтингу. В останнє десятиліття істотно зросла кількість досліджень, присвячених проблемам кіберпростору та його безпеки. На особливу увагу заслуговують праці К. Александера, Г. Раттрея, Д. Шелдона, К. Демчака, П. Домбро-вського, Дж. Наямол., С. Старра, Лі Джанга, А. Клімбурга. Дослідженню сутності кіберпростору як нового явища глобального безпекового середовища та термінологічні дослідження з кібербезпекової проблематики знайшли належне відображення у працях Дж. Ліпмана, Д. Фахренкурга, Ф. Крамера, Л. Вентца, Дж. Льюїса, Дж. Ліпмана, М. Лібіцкі, Д. Куела, С. Бейделмана, Л. Жанчевскі, А. Коларіка, М. Каветлі. Різні аспекти забезпечення кібернетичної безпеки досліджувалися у працях вітчизняних науковців, зокрема С. Бондаренка, О. Довганя, О. Дзьобаня, Д. Дубова, О. Климчука, О. Корченка, О. Мандзюка, О. Манжая, В. Панченко, М. Присяжнюка, В. Фурашева, В. Шеломенцева, В. Хорошка, В. Бурячка, Р. Грищука, С. Гнатюка, І. Храбана [5-7] та інші.

Методологічне та організаційне забезпечення створення Національної системи кібернетичної безпеки досліджено в працях В. Горбуліна, В. Бутузова, М. Ожевана, В. Пилипчука, В. Петрова [8-9] та інших. У працях зазначених авторів недостатня увага приділялася вирішенню теоретичних, організаційних, технічних та практичних проблем забезпечення безпеки саме кіберпростору в ІТС державного сектору, зокрема питанням:

-вирішення проблем, пов'язаних із розбудови національного сегменту кіберпростору та його безпеки, централізованій координації зусиль щодо ефективної взаємодії усіх учасників процесу забезпечення кібербезпеки, у тому числі й приватного сектору;

-моніторингу ефективності захисту шляхом формування та використання чітких метрик оцінки станів кіберпростору, а саме конфіденційності інформації в ІТС, та його безпеки;

-вдосконаленню методів, механізмів і процедур кіберзахисту, управління змінами в реалізації політики безпеки, вдосконаленню операційної дисципліни підприємств за рахунок збільшення уваги інформаційним технологіям захисту (коригування існуючого й розробки нового програмного забезпечення відповідних інформаційних систем забезпечення кібербезпеки, точок контролю доступу для мережевих систем, застосунків, функцій, даних, веб-контенту, спільних мережевих інформаційних середовищ тощо);

-системному підходу до кіберзахисту, який забезпечує контроль, вдосконалює сумісність компонентів складових забезпечення кібербезпеки, підтримує точний реєстр апаратно-програмного обладнання складових кіберпростору;

-вдосконалення методів, механізмів і процедур скорочення часу, потрібного для запобігання кібератак (тобто часу, що витрачається на виявлення та припинення кібератак, та часу, що витрачається на знешкодження наслідків кібератак).

**Мета та постановка завдання**

Метою застосування кластерного підходу є створення максимально безпечної інформаційно-комунікаційної системи для забезпечення захисту інформації. Це досягається шляхом розбиття всієї системи на окремі кластери (канали зв'язку, вузлові комунікаційні з'єднання).

**Виклад основного матеріалу**

Інформаційно-комунікаційні системи на перший погляд абсолютно різні. Проте, порівнюючи їх, можна відзначити певні спільні риси. Для організації конкретного профілю (наприклад, профілю страхової компанії, виробничого об'єднання, органу державної влади тощо) є своя інформаційно-комунікаційна система. Кожна з ІКС має типові рівні, на яких вирішуються спільні для всіх систем задачі. Зазвичай розглядають чотири рівні (рис. 1).


Рис. 1. Рівні інформаційно-комунікаційної системи

1. Рівень мережі — відповідає за взаємодію вузлів ІКС. Елементами ІКС, що належать до цього рівня, є модулі, які реалізують стеки протоколів мережної взаємодії, наприклад TCP/IP. Також на цьому рівні функціонує специфічна апаратура — мережне обладнання.

2. Рівень операційних систем — відповідає за обслуговування програмного забезпечення, яке реалізує більш високі рівні, і його взаємодію з обладнанням. Серед типових представників цього рівня можна назвати такі поширені ОС, як Microsoft Windows, Sun Solaris і Linux.

3. Рівень систем керування базами даних (СКБД) — відповідає за зберігання та оброблення даних. Серед типових представників цього рівня можна назвати СКБД Oracle, а також MS SQL Server. Іноді СКБД є центральним елементом ІКС (наприклад, облік товарів на складі), а іноді виконує допоміжні функції, зокрема для зберігання технологічної інформації самої ІКС.

4. Рівень прикладного ПЗ — включає прикладний компонент і компонент подання. Прикладний компонент забезпечує виконання специфічних функцій ІКС. Компонент подання відповідає за взаємодію з користувачем і подання даних у необхідній формі. У різних варіантах архітектури ІКС прикладний компонент і компонент подання можуть міститися на одному або на різних комп'ютерах (компонент подання — на робочій станції клієнта, прикладний компонент — на сервері застосувань). На рівні прикладного ПЗ функціонують офісні застосування (наприклад, Microsoft Office, Star Office або Open Office), бухгалтерські програми, спеціально розроблені для кожної окремої ІКС програмні засоби, що реалізують специфічні для системи функції, та будь-які інші програми. Порушники можуть впливати на ІКС на будь-якому з цих рівнів. Кожному з них притаманні характерні вразливості, а відтак — різні засоби захисту [10].

База даних системи містить конфіденційні дані, які становлять інтерес для кіберзлочинця. Об'єкти, що містять дані, пов'язані з об'єктами служби, які містять властивості доступу, які визначають, які користувачі або групи користувачів мають дозвіл читати або змінювати об'єкт. Законні користувачі системи отримують доступ до бази даних за допомогою інтерфейсу прикладного програмування, який використовує визначені процедури для перетворення дій користувача в певні SQL-запити, зокрема для перевірки прав доступу. Для забезпечення нормальної роботи користувача гарантує коректність введеного запиту. Для доступу до інтерфейсу користувач повинен ввести ідентифікатор і пароль. Права користувача визначаються його приналежністю до заздалегідь визначених груп, управління правами користувача та властивостями доступу до об'єктів здійснюють спеціально авторизовані користувачі, так звані адміністратори безпеки.

Кіберзлочинець має можливість здійснити доступ до захищених даних на рівні прикладного ПЗ (рис. 2). Для цього він може спробувати підібрати пароль іншого користувача, якому доступ до цієї інформації дозволено, або отримати доступ із правами адміністратора і змінити права доступу до захищених об'єктів чи власні повноваження. Зрештою, він може спробувати знайти вразливість у прикладній програмі або скористатися відомою вразливістю. З цією метою порушнику доведеться створити певний специфічний запит, не передбачений розробниками програмного забезпечення, у відповідь на який система наддасть йому несанкціонований доступ.

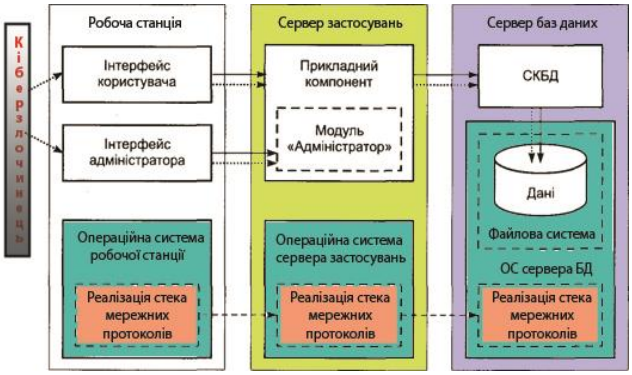


Рис. 2. Несанкціонований доступ на рівні прикладного ПЗ

Інший шлях: доступ на рівні СКБД. Такий доступ порушник здійснює в обхід прикладного ПЗ безпосередньо до бази даних (рис. 3).

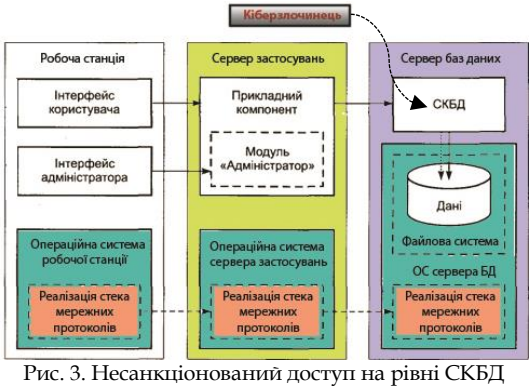


Рис. 3. Несанкціонований доступ на рівні СКБД

Для цього він може згенерувати специфічний SQL-запит або скористатися засобами самої СКБД для перегляду таблиць даних.

Нарешті, кіберзлочинець може спробувати здійснити доступ на рівні ОС. Зокрема, такий доступ може

полягати у несанкціонованому копіюванні файлів бази даних засобами файлової системи сервера (рис. 4).

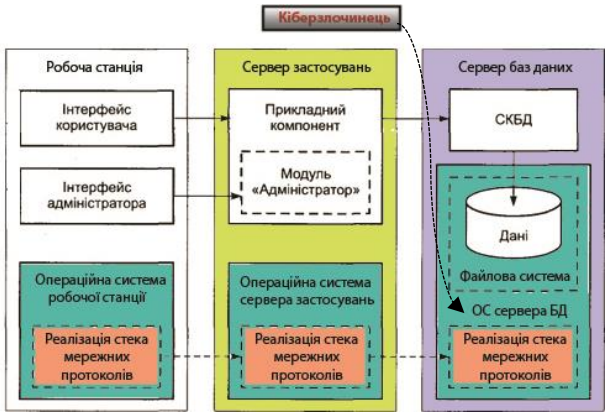


Рис. 4. Несанкціонований доступ на рівні ОС

Розглянуті рівні доступу передбачають наявність у користувача деяких повноважень у системі та доступу до її інтерфейсів. Останній рівень доступу — рівень мережі — потенційно може надати доступ користувачу, який не лише не має повноважень у системі, а й знаходиться поза її межами. На цьому рівні можлива атака на дані, які передаються у мережі, а також вплив через мережні засоби на вузли системи — сервери і робочі станції, внаслідок чого може бути створено передумови для доступу на вищих рівнях, наприклад, створено обліковий запис користувача-кіберзлочинця з правами адміністратора (рис. 5).

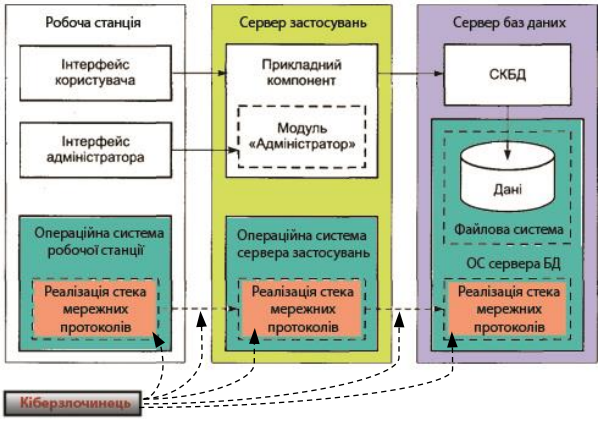


Рис. 5. Несанкціонований доступ на рівні мережі

Саме на цьому рівні інформаційно-комунікаційної системи хакери та кіберзлочинці намагаються створити найбільшу небезпеку до системи. Метою функціонування будь-якої системи кіберзахисту є, в першу чергу, мінімізація проміжку часу $T_{\text{компр}}$ від початку атаки на кіберпростір $t_{\text{атаки}}$ до моменту виявлення та блокування атаки $t_{\text{блок}}$. Крім того, важливим параметром є також фінансові витрати на відновлення працездатності функціонування інфраструктури кіберпростору $S$ та втрати від їх простою $V$, які, звісно, бажано теж мінімізувати. У більшості випадків така мінімізація досягається за рахунок введення певної обчислювальної надмірності у інфраструктуру діагностування кіберпростору $D$, що дозволяє одночасно покращити якість сервісу на час атаки шляхом забезпечення доступності, цілісності та конфіденційності інформації. Тому у загальному вигляді цільову функцію мети функціонування системи кіберзахисту можна представити у вигляді (1):

$$Z = \min F(T_{\text{компр}}, S, V, D) = \min F(t_{\text{блок}} - t_{\text{атаки}}, S, V, D) \quad (1).$$

Найбільш адекватними критеріями для оцінювання виявлення системою кібератак можуть бути такі показники як точність та повнота. Точність (*Precision*) – це міра того, наскільки точним є робота системи з виявлення кібератак: більша точність відповідає меншій кількості помилкових виявлених атак $FP$ (*False Positives*). У той же час, повнота (*Recall*) показує скільки фактично атак виявила система. Більш високе значення повноти відповідає меншій кількості пропущених атак $FN$ (*False Negative*). В ідеалі ми хочемо мати класифікатор з високою точністю і повнотою, оскільки це відповідає низьким значенням $FP$ і $FN$. Точність та повнота обчислюються за формулами (2) [11]:

$$Precision = \frac{TP}{(TP + FP)}, \qquad Recall = \frac{TN}{(TN + FN)}, \quad (2)$$

де $TP$ – кількість кібератак, що вірно виявлені системою; $TN$ – кількість подій, яких система правильно не визнала кібератакою; $FP$ – кількість подій помилково виявлених системою, як кібератака; $FN$ – кількість невиявлених системою кібератак.

Якщо система кіберзахисту функціонує по багатокластерному сценарії, то точність і повнота розраховуються окремо для кожного кластеру. Щоб розрахувати ці метрики для певного кластеру, інші кластери розглядаються як один (такий підхід називається “одним проти всіх”). Нарешті, точність і повнота для всіх кластерів об'єднуються разом з використанням середньозваженої величини [12].

Для виявлення пошкодженого або атакованого кластера системи необхідно постійний контроль стану мережевих вузлів та каналів зв’язку мережі ІТС. Тому визначення контролерів кластерів та визначення вузлів-шлюзів , які формують віртуальну магістраль усієї мережі, що використовується як для передачі маршрутної інформації, так і для користувацького трафіка [13], є необхідною та достатньою умовою надійного функціонування інформаційно-комунікаційної системи в цілому.

**Висновки.** Розглянувши відповідні рівні інформаційно-комунікаційної системи та проаналізувавши можливі вразливості кожного з них, необхідно звернути максимальну увагу на рівень, який пов'язаний з мережними послугами. Саме кластерний підхід дає можливість визначити частину мережі, яка атакована кіберзлочинцями та в найкоротший час прийняти рішення про унеможливлення цієї кібератаки.

**Список літератури**

[1] Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія. Житомир: ЖВІ, 2020. 180 с.

[2] Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: Монографія / за заг. ред. проф. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.

[3] Про основні засади забезпечення кібербез-

пеки України: Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017, № 45, 403 с.

[4] Дописувачі Вікіпедії, "Перелік кібератак" Українська Вікіпедія, https: // uk. wikipedia. org/ wiki/ Перелік_кібератак (переглянуто 23 лютого, 2023).

[5] В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. К.: ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.

[6] Ткаченко О.А., Ткаченко К.О. Кіберпростір і кібербезпека: проблеми, перспективи, технології // Цифрова платформа: інформаційні технології в соціокультурній сфері 2018. №177. С. 75-84.

[7] Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. 2 (42). С. 54-62.

[8] Петров В.В. Щодо формування національної системи кібербезпеки України // Стратегічні пріоритети. №4 (29). 2013 р. С. 12-130.

[9] Петров В.В. Співробітництво України з НАТО щодо забезпечення кібербезпеки // Міжнародні відносини. Серія" Політичні науки". 2018. Вип. 18-19.

[10] М.В. Грайворонський, О.М. Новіков. Безпека інформаційно-комунікаційних систем 2009. 608 с.

[11] Powers David MW. Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation. Journal of Machine Learning Technologies. 2 (1), P. 37–63, 2011.

[12] K.N. Junejo, J. Goh, Behaviour-Based Attack Detection and Classification in Cyber Physical Systems Using Machine Learning, CPSS '16: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, May 2016.

[13] Гуменюк І.В., Басараба М.С., & Некрилов О.В. (2021). Методика забезпечення кібербезпеки критичних компонентів мереж інформаційно-комунікаційної системи. // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем, (18), С. 101–110. https://doi.org/10.46972/2076-1546.2020.18.10.

**УДК 004.056**

***Smetanin K. Cluster approach of building networks as a way of ensuring the appropriate level of cyber security of the information and telecommunication system***

***Abstract.*** *Interaction between the subjects of modern society is inextricably linked to the reliable functioning of computer information systems and networks. Security and quality of service (Quality of service, QoS) are two key network services to ensure communication security (according to the Ukrainian national standard DSTU ISO/IEC 27000:2017). Quality is a key requirement, and with the further development of computerized information systems and networks, additional security requirements are rapidly increasing. Security features, service levels, and management requirements for all network services must be defined and included in any network service agreement. The intensive development of computer information systems and networks has increased the vulnerability of the system and multiplied the possibility of cyber-attacks. Therefore, network security management is a key element in the functioning of computer systems and networks. Security vulnerabilities in routers, balancers and firewall operating systems, denial-of-access and denial-of-service attacks on key network nodes and servers, changing parameters and hacking routers, etc., affect resource availability and quality of service. Issues such as ensuring key QoS parameters, protecting data packets, preventing intrusion attacks and denial-of-service attacks are just some of the issues that need to be addressed to ensure secure resource allocation, access and secure transmission paths, content protection, and end-to-end - completion of QoS provisioning. Security mechanisms and QoS are not independent. The choice of security mechanism will affect QoS performance and vice versa. Meeting quality of service requirements requires the use of security mechanisms to ensure appropriate levels of service and billing. The wrong choice of security mechanisms will reduce the performance of a carefully constructed network, or information and telecommunications system (hereinafter ITS), and the wrong choice of service levels will lead to information leakage. That is, the optimal balance of QoS parameters helps to reduce information leakage. Thus, this article proposes a cluster approach to building a network for timely detection and response to cyber threats, as well as unauthorized access to critical network components, which in turn is a necessary component to ensure a high level of cyber security of the entire ITS.*

***Key words****: cluster, network, information and telecommunication system, cyber security, cyber-attack, unauthorized access, secure system.*

**Сметанін Кирило Володимирович,** к. т. н., старший викладач кафедри захисту інформації та кібербезпеки Житомирського військового інституту ім. С.П. Корольова.

**Kyrylo Smetanin,** candidate of technical sciences (PhD), senior lecturer of the department of information protection and cyber security of the Zhytomyr Military Institute named after S.P. Korolev.

Отримано *15 січня 2023 року*, затверджено редколегією *27 березня 2023 року*