УДК 004.056.5

А.С. Шевченко,
кандидат технічних наук

КОМПЛЕКСНИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМИ КІБЕРНЕТИЧНОГО ЗАХИСТУ ЗБРОЙНИХ СИЛ УКРАЇНИ

У статті розглядаються питання аналізу побудови та захисту кіберпростору Збройних Сил України на основі комплексного застосування наявних систем захисту інформації та кібернетичної безпеки.

Ключові слова: *кіберпростір, рівні кіберпростору, кібернетичний захист, системи захисту інформації, міжмережні екрани, системи виявлення та запобігання вторгненням, DLP, SIEM, VPN, антивірусний захист, розмежування доступу, системи аналізу захищеності.*

В статье рассматриваются вопросы анализа построения и защиты киберпространства Вооруженных Сил Украины на основе комплексного применения существующих систем защиты информации и кибернетической безопасности.

Ключевые слова: *киберпространство, уровни киберпространства, кибернетическая защита, системы защиты информации, межсетевые экраны, системы обнаружения и предотвращения вторжений, DLP, SIEM, VPN, антивирусная защита, разграничение доступа, системы анализа защищенности.*

Paper deals with the analysis of the construction and protection of cyberspace of the Armed Forces of Ukraine on the basis of an integrated application of existing systems of information protection and cybersecurity are considered.

Keywords: *cyberspace, levels of cyberspace, cyberprotection, systems of information protection, firewalls, systems of dection and prevention of attacks, DLP, SIEM, antivirus protection, access isolation, systems of an analysis of protection.*

Вступ

Кібербезпека – найбільш актуальний напрям захисту інформації на фоні глобальної інформатизації сучасного суспільства, включаючи і збройні сили держави. На сьогодні розвиток інформаційних технологій значно розширив можливості військового управління та збільшив можливості противника в реалізації атак на критичні елементи інформаційної інфраструктури.

У період із 2014 та до нині, під час анексії Автономної республіки Крим та в ході бойових дій на Сході України з боку Російської Федерації здійснюються масовані кібернетичні атаки на елементи критичної інформаційної інфраструктури як держави, так і Збройних Сил України.

Під час бойових дій реалізуються концепції інформаційних та кібернетичних операцій, які направленні на особовий склад та систему управління ЗС України. Система управління ЗС спирається на інформаційно-телекомунікаційні системи (далі – ІТС) при передачі команд бойового управління та здійснення повсякденної життєдіяльності.

Реалізація атак у кібернетичному просторі ЗС України призводить до витоку інформації, несанкціонованого доступу та порушення керованості елементами ІТС, відмови в доступі до ресурсів та систем, дезінформації особового складу ЗС. Наявність вразливостей ІТС, систем захисту інформації та низька підготовленість особового складу ЗС призводить до суттєвих ризиків інформаційної безпеки, а успішна реалізація кібернетичних атак – до значних збитків. З огляду на це, актуальним та невідкладним є захист кіберпростору ЗС України.

Аналіз останніх досліджень та публікацій показав, що на сьогодні значно актуалізувались питання забезпечення захисту інформації та кібербезпеки. Основні напрями наукових досліджень направлені на розвиток методологічної бази, формування концептуальних підходів, правових засад та термінології в галузі кібернетичної безпеки [1–5].

Мета

Стан інформаційної та кібернетичної безпеки у ЗС України вимагає негайного впровадження систем захисту інформації та кібернетичної безпеки. На сьогодні відсутні системи, які б дозволяли забезпечити захист інформації та кібернетичну безпеку ЗС в цілому. Тому для побудови системи кібернетичного захисту пропонується використання комплексного підходу, який дозволить поєднати існуючі системи та механізми захисту інформації для більш ефективного захисту кіберпростору ЗС України.

Метою роботи є підвищення безпеки кіберпростору ЗС України за рахунок комплексного використання наявних систем захисту інформації та кібернетичної безпеки.

Постановка завдання

Завданням дослідження є аналіз структури стану безпеки кіберпростору ЗС України та розробка рекомендацій щодо комплексного застосування систем захисту інформації та кібернетичної безпеки для його захисту.

Обмеження. В роботі розглядаються питання реалізації захисту кібернетичного простору технічними засобами.

Викладення основного матеріалу дослідження

Кібернетичний простір – це електронне інформаційне середовище, утворене організованою сукупністю взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [6].

Захист кіберпростору повинен здійснюватися безперервно на землі, в повітрі, морі та космосі [7; 8]. Реалізація захисту має враховувати середовища розповсюдження інформаційних потоків, включаючи і електромагнітний спектр (ЕМС).

Заходи захисту кіберпростору ЗС України повинні реалізовуватись на організаційному, технічному та правовому рівнях.

Організаційні заходи захисту кіберпростору у ЗС передбачають розробку правил доступу та роботи особового складу в ІТС, порядку обробки інформації та навчання основам інформаційної та кібернетичної безпеки. Крім того, особовий склад ЗС повинен бути навчений основам протистояння розвідці противника в інформаційному просторі – соціальній інженерії.

Більш детально розглянемо питання захисту кіберпростору ЗС України технічними засобами (програмними, апаратно-програмними).

Технічні заходи захисту кіберпростору передбачають захист електронного середовища ІТС Збройних Сил України.

Ураховуючи особливості побудови ІТС та сучасних систем захисту інформації, можна виділити такі функціональні рівні кіберпростору (рис. 1):

рівень інформаційних систем (програмного забезпечення);

рівень кінцевого телекомунікаційного обладнання;

рівень мережного телекомунікаційного обладнання;

рівень транспортної телекомунікаційної мережі [8].

Під час управління військами зазначені функціональні рівні кіберпростору взаємодіють з рівнями, які об'єднують особовий склад та фізичне середовище (стаціонарні та польові об'єкти). Впровадження захисту кіберпростору не повинно обмежуватись стаціонарною компонентою. Реалізація захисту польових елементів зумовлюється їх критичністю внаслідок функціонування за межами контрольованої зони впритул до засобів технічної розвідки противника, розвідки ліній зв'язку.

Для забезпечення безпеки кіберпростору ЗС України необхідне впровадження комплексу систем та механізмів захисту ІТС на різних функціональних рівнях кіберпростору. До таких систем та механізмів належать:

системи розмежування доступу користувачі до елементів ІТС;
системи міжмережного екранування на основі фаерволів (*Firewall*);
системи та механізми криптографічного захисту інформації;
віртуальні приватні мережі *VPN*;
системи антивірусного захисту елементів ІТС;
системи виявлення та запобігання вторгненням (*IDS/IPS*);
механізми автентифікації, авторизації та аудиту (*AAA*);
системи попередження втрати даних (*DLP – data loss prevention*);
системи управління інформаційною безпекою та подіями (*SIEM*);
системи аналізу захищеності (САЗ) [9–11].

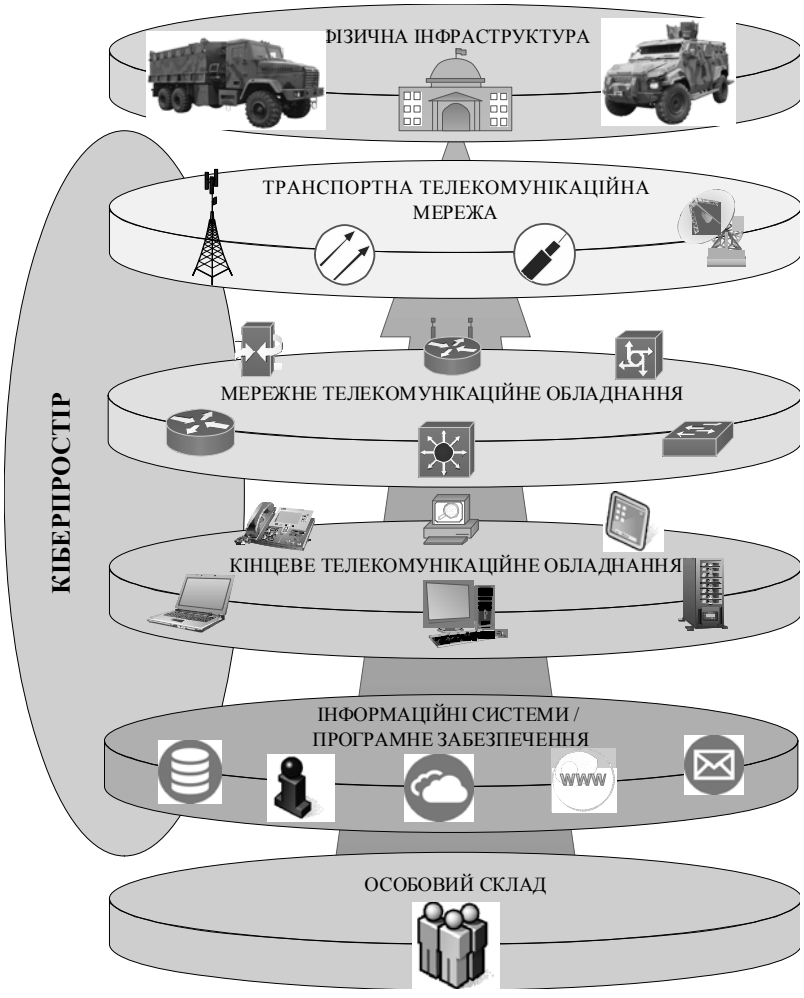

Рис. 1. Функціональні рівні кіберпростору Збройних Сил України

Представимо основні місця розташування програмних та апаратно-програмних засобів захисту інформації та кібернетичної безпеки відповідно до функціональних рівнів кіберпростору (рис. 1).

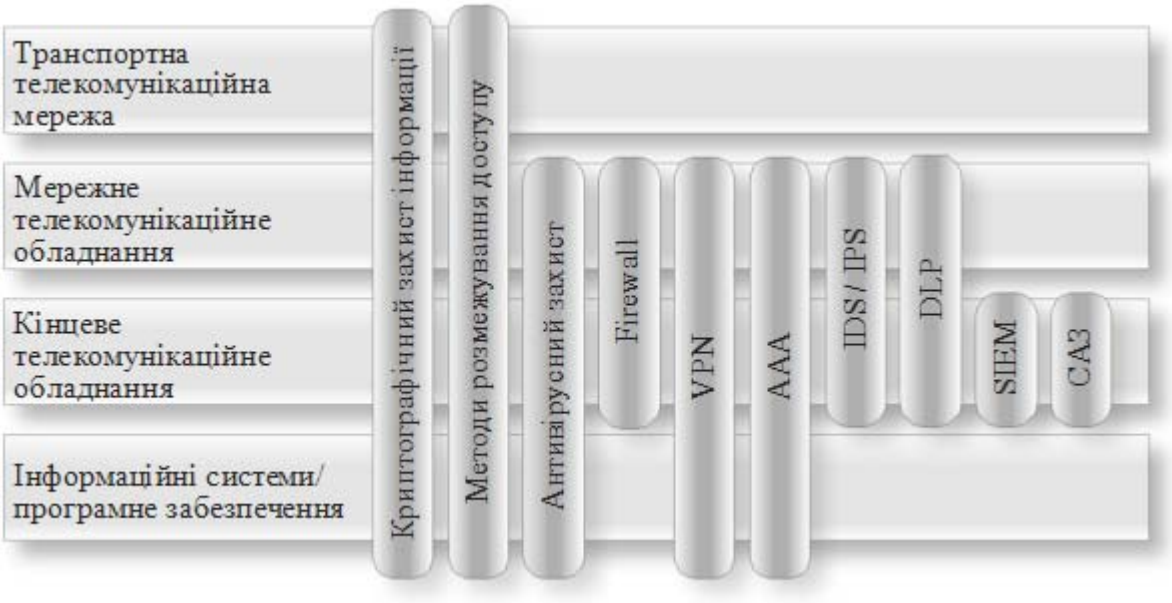

Рис. 2. Системи і механізми захисту інформації інформаційно-телекомунікаційних систем спеціального призначення

Розглянемо більш детально функціонування деяких систем та механізмів захисту інформації при захисті кібернетичного простору ЗС України.

Криптографічний захист інформації один з основних інструментів, що реалізує функції на кожному з функціональних рівнів кіберпростору, включаючи і реалізацію криптографічних функцій в інших системах захисту інформації: *VPN*, міжмережних екранах (механізм *deep packet inspection*), автентифікації тощо. Криптографічний захист інформації забезпечує конфіденційність та цілісність інформації.

Методи розмежування доступу використовуються для забезпечення розділення доступу суб'єктів чи груп суб'єктів до множини об'єктів ІТС. Як правило, розмежування доступу ґрунтується на впровадженні матриці доступу відповідно до існуючої політики безпеки. Розмежування доступу реалізується шляхом упровадження облікових записів користувачів різних рівнів згідно з повноваженнями та застосування політик безпеки (групових, локальних). Останні реалізуються, як правило, в операційних системах.

Методи розмежування доступу напряму не належать до механізмів захисту інформації, але значною мірою дозволяють забезпечити виконання політик безпеки інформації.

Розмежування доступу реалізовується на всіх функціональних рівнях кіберпростору.

Міжмережне екранування здійснюється за допомогою фаерволів (міжмережних екранів, анг. *Firewall*, нім. *Brandmauer*). Міжмережні екрани (МЕ) − комплекс апаратно-програмних чи програмних засобів, що здійснює контроль та фільтрацію інформаційних потоків відповідно до заданих правил політики безпеки.

На сьогодні міжмережні екрани реалізуються в таких виконаннях.

1. *Апаратно-програмні МЕ* реалізуються як окремі мережні пристрої. На цей час упроваджена концепція *Next Generation Firewall* (*NGFW*) − сучасні міжмережні екрани, крім функцій фільтрації трафіку, здійснюють антивірусний захист, створення каналів *VPN*, виявлення та захист від вторгнень та інші.

2. *Програмні МЕ* реалізуються у вигляді інтегрованого програмного забезпечення операційних систем, фаерволів, антивірусного програмного забезпечення, окремого спеціалізованого програмного забезпечення.

Сучасні міжмережні екрани (*NGFW*) дозволяються реалізувати фільтрацію трафіку за IP-адресами, портами відправника та отримувача, протоколами, здійснювати перевірку трафіку за вмістом (*App Control, Web Control, Email proxy*), блокування підозрілого трафіку (*Spam Blocker*, *APT Blocker*) та інші функції.

Для ефективного захисту інформації в ІТС Збройних Сил України доцільно використовувати МЕ для захисту мереж (критичних сегментів мережі − *DMZ*), критичних елементів ІТС та автоматизованих робочих місць. У першому та другому випадках використовуються апаратно-програмні МЕ, у третьому − програмні МЕ.

Віртуальні приватні мережі VPN використовуються для забезпечення захищеного обміну інформацією між мережами (*site-to-site*) та захищеного доступу віддалених користувачів. Суть *VPN* полягає в створенні криптографічно захищеного віртуального тунелю, що забезпечує конфіденційність та цілісність при обміні інформацією.

Як правило, використовуються схеми організації каналів *VPN*: мережа-мережа, клієнт-сервер. До основних протоколів віртуальних приватних мереж належать протоколи *IPsec, L2TP, PPTP, TLS* (*SSL*).

Серверні програмні модулі протоколів *VPN* реалізуються в серверних операційних системах, маршрутизаторах, *NGFW* та інших засобах.

Функції *VPN* інтегровані майже в усі сучасні маршрутизатори, що знижує затрати на організацію захищених каналів зв'язку.

Системи антивірусного захисту є невід'ємною складовою будь-якого елементу ІТС. Антивірусне програмне забезпечення, разом з існуючими методами (сигнатурним, евристичним, виявлення аномалій), впроваджує нові технології та механізми захисту − "пісочниця", емуляція, реалізація декількох антивірусних модулів тощо.

На сьогодні реалізовані основні підходи щодо антивірусного захисту: системи антивірусного захист шлюзів (*gateway antivirus*) та захист кінцевих точок (*end point security*). Для ефективного антивірусного захисту доцільне провадження обох підходів.

Аналогічно до інших програмних засобів існують як комерційні, так і умовно безкоштовні антивірусні засоби: ці засоби мають обмежені функціональні можливості.

Системи виявлення та запобігання вторгненням (*IDS/IPS*) − це програмно-апаратні чи програмні засоби, які призначені для виявлення фактів несанкціонованого доступу (НСД) до ІТС чи підозрілої активності. Системи виявлення вторгнення *IDS* дозволяють виявляти кібернетичні атаки, системи запобігання вторгненнями *IPS* реалізують функції захисту, що дозволяють блокувати НСД чи несанкціоновані дії.

Здебільшого виділяють три основні класи *IDS*: мережні (*Network-based IDS, NIDS*), вузлові (*Host-based IDS, HIDS*) та гібридні.

Архітектура *IDS/IPS* ґрунтується на використанні консольних та сенсорних систем. У системі кібернетичного захисту сенсори збирають інформацію про небезпечну активність та надсилають до консолей, які систематизують, журналюють та здійснюють управління.

На сьогодні існує ряд реалізацій *IDS/IPS* передовими розробниками засобів захисту інформації та програмних засобів з відкритим кодом: *Snot, OSSEC, Prelude, Bro* та інші.

Разом із ефективністю виявлення кібернетичних атак та своєчасної їх нейтралізації досить важливими є реалізація систематизації несанкціонованих дій та їх візуалізація, що дозволяє адекватно оцінювати стан кібернетичної безпеки.

Механізми автентифікації, авторизації та аудиту (*AAA – authentication, authorization, accounting*) – невід'ємні механізми захисту програмного забезпечення (*web*, баз даних тощо), операційних систем, інформаційних систем, систем захисту тощо.

Механізми автентифікації та авторизації забезпечують санкціонований доступ користувачів до систем (засобів) та надання повноважень відповідно до політики безпеки.

Механізми аудиту дозволяють на основі журналів (логів) здійснювати запис подій та інцидентів порушення інформаційної безпеки. Аудит дозволяє проводити розслідування інцидентів та виявлення порушників, які діють усупереч політиці інформаційної безпеки.

Механізми AAA тією чи іншою мірою реалізуються на усіх функціональних рівнях кіберпростору.

Системи попередження втрати даних (*DLP – Data Loss Prevention*) – системи, які досить інтенсивно розвиваються останнім часом. В ІТС Збройних Сил України існує велика кількість інформації, яка не належить до інформації з обмеженим доступом, але в сукупності розкриває певні відомості. Це – поштові адреси, телефонні номери, особисті ідентифікаційні номери, банківські реквізити установ, технологічна інформація тощо. Окремі з цих відомостей не становлять відносної цінності але в сукупності втрата зазначених масивів інформації є суттєвим ризиком інформаційної безпеки ЗС України.

Системи *DLP* на основі застосування криптографічних методів захисту, розмежування доступу дозволяють забезпечити збереження даних користувачів та організацій, блокувати доступ до несанкціонованих каналів. Деякі модулі *DLP* на *NGFW* забезпечують перевірку вмісту трафіку на наявність конфіденційних даних.

Сукупність розрізнених систем та механізмів захисту, незважаючи на свою функціональність, не відображає цілісної картини стану інформаційної безпеки організації.

Системи SIEM. Для реалізації моніторингу і аудиту подій інформаційної безпеки мережі в цілому використовуються системи *SIEM* (*Security Information and Event Management*). Ці системи включають у себе засоби автоматизованого збору подій, їх формалізації та узагальнення, відображення у зручному для аналізу вигляді. *SIEM* дозволяють проводити моніторинг та аудит стану інформаційної безпеки одночасно від багатьох робочих станцій, мережних пристроїв з різними платформами.

Системи аналізу захищеності (сканери безпеки) призначені для проведення аналізу та дослідження власних систем на наявність вразливостей. САЗ забезпечують аудит інформаційної безпеки мереж, операційних систем, систем управління базами даних та іншого спеціалізованого програмного забезпечення. Використання САЗ дозволяє вчасно виявляти вразливості ІТС, елементів ІТС та систем захисту інформації на основі пасивного або активного сканування. На сьогодні САЗ здебільшого інтегруються з SIEM. У комплексі ці системи дозволяють більш ефективно проводити аудит стану інформаційної безпеки та вчасно перекривати вразливості систем.

Впровадження наведених систем та механізмів захисту інформації дозволить забезпечити безпеку кіберпростору ЗС України. Системи захисту реалізують свої основні функції на рівні програмного забезпечення та мережного обладнання. Впровадження складних технологічних систем захисту інформації на кінцеві пристрої – здебільшого автоматизовані робочі місця, спричинить значні труднощі, що викличе необхідність у висококваліфікованих кадрах з кіберзахисту. У зв'язку з цим, основний напрям забезпечення безпеки кіберпростору ЗС України повинен бути направлений на впровадження мережних засобів захисту – шлюзів безпеки (*security gateway*). На сьогодні шлюзи безпеки становлять такі засоби захисту, як *NGFW*, *UTM* (*Unified Threat Management*) та *NFIPS* (*Next-Generation Intrusion Prevention System*). Кожен із цих засобів захисту включає тією чи іншою мірою набір систем, які розглядались у статті. Відповідно до досліджень NSS labs до основних лідерів у галузі кібернетичної безпеки належать: *Cisco, WatchGuard, Check Point, Dell SonicWall, Fortinet, McAfee* та інші [12].

Вибір засобів захисту для потреб ЗС України питання досить складне. Окрім впровадження функцій захисту, слід враховувати можливість централізованого моніторингу стану інформаційної безпеки та кібернетичних атак, так як, наприклад, реалізують засоби *WatchGuard Dimension* [13] або *Cisco FirePower* [14].

Забезпечення кібербезпеки Збройних Сил України – завдання яке потребує значних фінансових затрат, тому до його вирішення потрібно підійти комплексно, враховуючи досвід країн НАТО та США. Впровадження систем та механізмів захисту інформації дозволять забезпечити комплексний захист кіберпростору ЗС України з урахуванням стаціонарної та польової компоненти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Шаховал О.А.* Рекомендації щодо розробки стратегії забезпечення кібербезпеки України / О.А. Шаховал, І.Л. Лозова, С.О. Гнатюк // Захист інформації, – 2016. – Т. 18, № 1. – С. 57–65.

2. *Головка А.А.* Захист кіберпростору як складова інформаційної безпеки України в умовах гібридної війни / А.А. Головка // Young Scientist. – 2016. – № 4 (31). – С. 333–336.

3. *Титаренко О.М.* Стратегія захисту національного кіберпростору: досвід Франції / О.М. Титаренко // Новітні інформаційно-комунікаційні технології (30 березня – 30 квітня 2015 р.) : ІІІ наук.-практ. семінар : тези доп. – Дніпропетровськ : ДРІДУ НАДУ, 2015 [Електронний ресурс]. – Режим доступу: http://www.dridu.dp.ua/ konf/konf_dridu/itis%20seminar %202015/s1.html#sec3.

4. Развитие киберпространства и информационная безопасность / В.И. Хаханов, С.В. Чумаченко, Е.И. Литвинова, А.С. Мищенко // Радіоелектроніка, інформатика, управління. – 2013. – № 1. – С. 151–157.

5. *Шеломенцев В.П.* Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 2 (28). – С. 299–309.

6. Військовий стандарт 01.004.004. (Видання 1). Воєнна політика, безпека та стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення. – К. : Міністерство оборони України, 2014 р. – 22 с.

7. Стратегія кібербезпеки України [Електроний ресурс]. – Режим доступу : http:// zakon5.rada.gov.ua/laws/show/96/2016.

8. Cyberspace operations : Air Force Doctrine Document 3-12. – DOD US. – Government Printing Office, 2010. – 60 p.

9. *Шевченко А.С.* Забезпечення захисту кіберпростору ЗСУ / А.С. Шевченко // Телеком. Телекоммуникации и сети. Военная связь. Технологии, решения, проекты. – 2016. – Специальный выпуск. – С. 68–71.

10. *Поповский В.В.* Защита информации в телекоммуникационных системах : учебник : в 2-х т. / В.В. Поповский, А.В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 1. – 238 с.

11. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М. : ДМК Пресс, 2012. – 592 с.

12. NSS Labs Announces 2016 NGFW Group Test Results [Електроний ресурс]. – Режим доступу : https://www.nsslabs.com/company/news/press-releases/nss-labs-announces-2016-ngfw-group-test-results/.

13. WatchGuard Dimension. Oceans of data instantly become security intelligence [Електроний ресурс]. – Режим доступу : http://www.watchguard.com/wgrd-products/dimension.

14. *Лукацкий А.* Контроль и мониторинг периметра сети / А. Лукацкий [Електроний ресурс]. – Режим доступу : https:// www.cisco.com/ c/dam/ m/ru _ru/ events/ 2016/ cisco-security-roadshow/ pdf/ 4_ Firepower. pdf.

Отримано 28.11.2016
Рецензент Рибальський О.В., д.т.н