УДК 004.7:004.056 (045)

АРХІТЕКТУРА СУЧАСНОЇ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ АЕРОПОРТУ

Олег Ткаліч, Роман Одарченко, Сергій Гнатюк

Сучасний аеропорт має надавати своїм клієнтам своєчасні якісні та захищені інформаційні послуги. Постійне зростання кількості таких послуг (відповідно до розвитку інформаційно-комунікаційних технологій) та самих пасажирів стимулює до пошуку і впровадження нових концепцій та підходів до інтегрованого надання інформаційних послуг в аеропортах. Безумовно важливим є створення уніфікованої інформаційно-комунікаційної мережі, яка забезпечить високий рівень надання інформаційних послуг абонентам мережі, буде захищеною та безпечною для користування, також зможе інтегрувати у собі засоби безпеки, інформаційно-довідкові служби, розважальний контент, системи відеоспостереження, системи реєстрації пасажирів, інформацію експлуатаційних служб аеропорту, сенсорні мережі для інтелектуального управління системами життєзабезпечення аеропорту, операторів стільникового зв'язку, сучасних концепцій SDN, SDR, BYOD та IoT. З огляду на це, у статті запропоновано інтегрування зазначених сучасних і перспективних концепцій та технологій для оптимізації архітектури і топології корпоративної мережі аеропорту. Отримані результати дозволять підвищити економічну ефективність використання корпоративної мережі аеропорту, збільшити її захищеність, кількість та якість інформаційних послуг, дозволять спростити управління мережею та системами забезпечення життєдіяльності аеропорту.

***Ключові слова**: захист інформації, захищені інформаційні послуги, аеропорт, архітектура мережі, безпроводові мережі, сенсорні мережі, система моніторингу, інформаційно-комунікаційна мережа, SDN, SDR, BYOD, IoT.*

Вступ. На сьогодні кількість пасажиропотоків, які обслуговуються авіаперевізниками в аеропортах України постійно збільшується [1], тому на аеропорт, як місце очікування та обслуговування пасажирів, покладається відповідальність за надання якісних інформаційних послуг. Кожен пасажир та супроводжуюча особа хочуть отримувати оперативну інформацію стовно вильоту та прибування повітряних суден, скоротити час на реєстрацію, отримання багажу, орієнтуватися в приміщеннях аеропорту, комфортно проводити час в місцях очікування, мати «під рукою» карти, інформаційні довідники таксі, громадського транспорту тощо, а також отримувати багато інших корисних інформаційних послуг [2]. Слід відзначити, що кожен аеропорт має корпоративну мережу, розраховану на обслуговування як персоналу аеропорту, експлуатаційних служб, служби безпеки, так і пасажирів.

Зростання мобільних «розумних пристроїв» призводить до збільшення завантаженості каналів корпоративної мережі за рахунок великої кількості користувачів мережі та об'ємів трафіку, особливо це стосується трафіку від пасажирів. Також необхідно зважати на надзвичайно складну, з точки зору безпеки як аеропорту так і інформації самих пасажирів, ситуацію в Україні, а саме підвищені заходи безпеки щодо запобігання тероризму та інформаційної пропаганди. Усі ці чинники свідчать про необхідність створення уніфікованої інформаційно-комунікаційної мережі, яка забезпечить високий рівень надання інформаційних послуг абонентам мережі, буде захищеною та безпечною для користування, також зможе інтегрувати в собі засоби безпеки, інформаційно-довідкові служби, розважальний контент, системи відеоспостереження, системи реєстрації пасажирів, інформацію експлуатаційних служб аеропорту, сенсорні мережі для інтелектуального управління системами життєзабезпечення аеропорту, операторів стільникового зв'язку, сучасних концепцій SDN (Software-Defined Networking), SDR (Software-Defined Radio), BYOD (Bring Your Own Device) та IoT (Internet of Things).

Аналіз існуючих досліджень та постановка завдання. Технології, які розглядатимуться у статті, є предметом великої кількості наукових та практичних праць. У статті використано багато матеріалів з форумів та виставок, які проводили провідні розробники та інтегратори в IT сфері [2-6]. У роботах [8, 10] проведено аналіз застосування сучасних концепцій та архітектур інформаційно- комунікаційних мереж та систем, інтеграцію проводових та безпроводових мереж, інтеграцію систем відео спостереження до інформаційно-комунікаційної мережі підприємства та розрахунок кількості камер та пропускних спроможностей мережі. Розглянуто можливості застосування сенсорних мереж для забезпечення життєдіяльності аеропорту, проведено аналіз протоколів маршрутизації та можливість інтеграції до корпоративної мережі. У роботах [7, 9] проведено аналіз сучасних безпроводових технологій стандарту 802.11, розглянуто характеристики

802.11n/ac/ad, розраховано кількість точок доступу на периметр приміщення у залежності від завад та перешкод, проведено оцінку адекватності моделей розповсюдження радіохвиль для 802.11n, розглянуто питання аутентифікації та авторизації безпроводового сегменту, атак у кіберпросторі, а в праці [11] запропоновано й обґрунтовано метод удосконалення структури мережі LTE за рахунок використання концепції HotSpot 2.0, яка дає змогу забезпечити підтримку автоматичного входу мобільних пристроїв у мережу і захищений доступ до партнерських мереж Wi-Fi. У роботі [12] проведено аналіз існуючих та перспективних технологій. Проте, на сьогодні питання застосування зазначених технологій для підвищення ефективності надання інформаційних послуг в аеропортах залишається відкритим. З огляду на це, ***метою цієї роботи*** є створення оптимальної архітектури захищеної уніфікованої інформаційно-комунікаційної мережі аеропорту за рахунок інтеграції сучасних технологій, систем моніторингу та єдиного центру управління мережею.

Основна частина дослідження. Корпоративні мережі, у тому числі і авіапідприємств, побудовані за трирівневою ієрархічною моделлю та включають до свого складу рівень ядра (Core), рівень розподілу (Distribution/Aggregation) та рівень доступу (Access). На рис. 1 представлено приклад побудови трирівневих ієрархічних моделей. Рівень ядра може використовувати як комутатори 3-го рівня, так і маршрутизатори, рівень розподілу – комутатори 2-го або 3-го рівня та маршрутизатори.

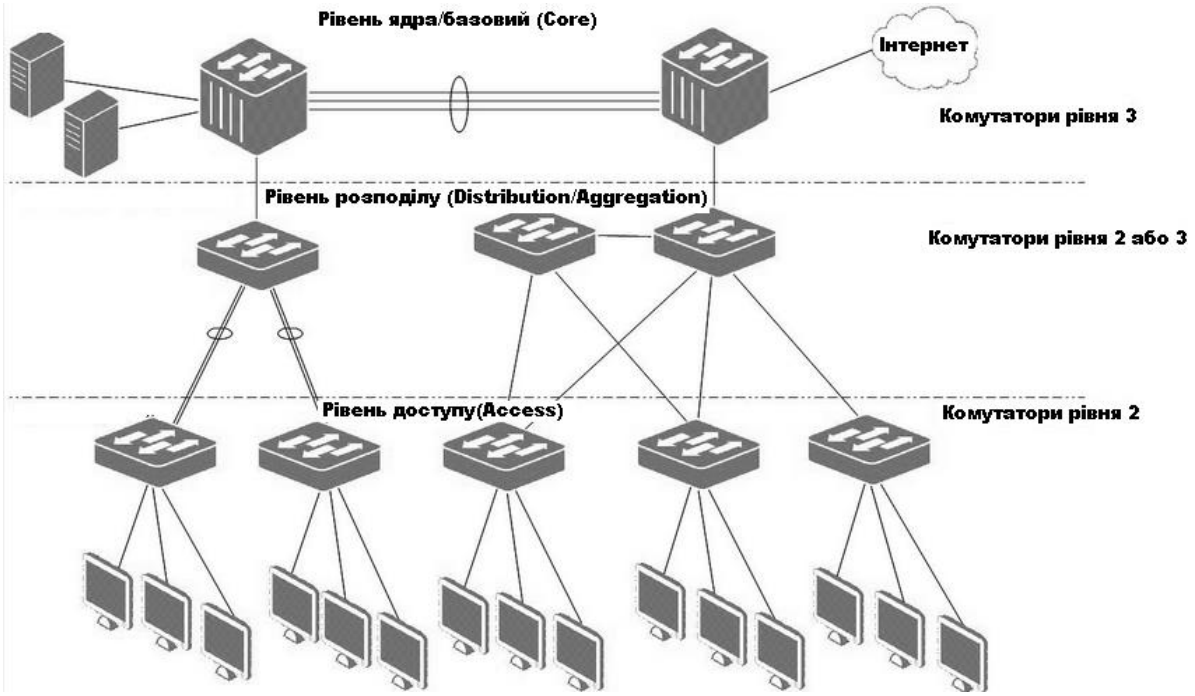
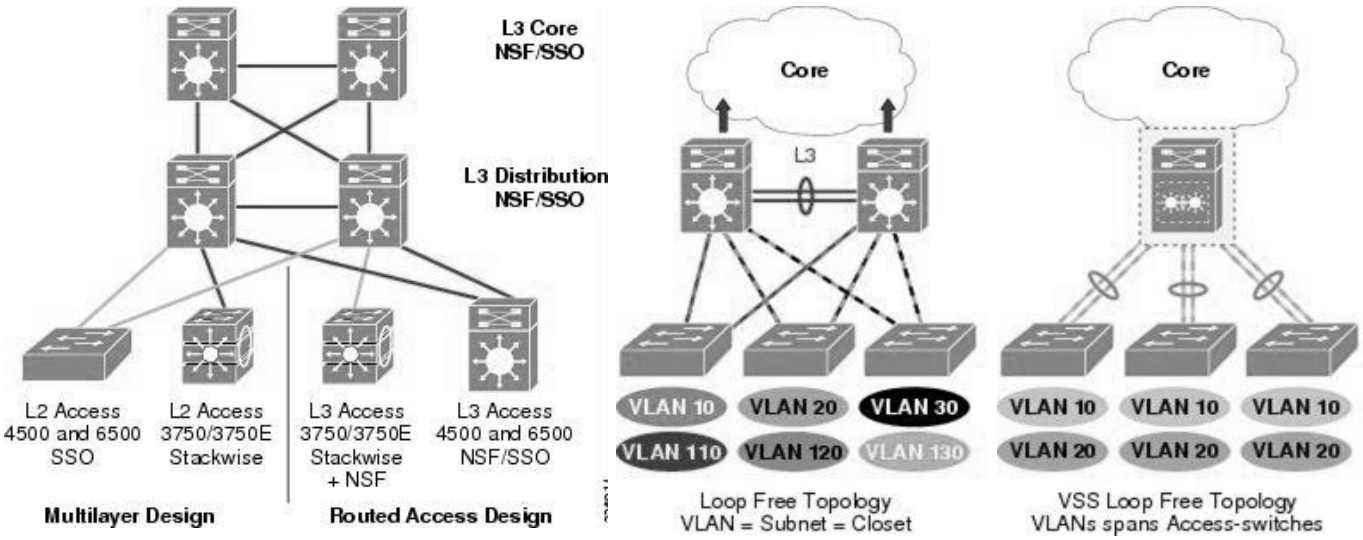


Рис. 1. Трирівнева ієрархічна модель корпоративних мереж

Сучасні вимоги до надання інформаційних послуг вимагають більшої функціональності, швидкості та надання нових послуг і сервісів, а також уніфікації та спільної роботи різних «розумних» пристроїв, за умов безпечного користування. Тому для аеропортів, як підприємств з величезною інфраструктурою, великою кількістю користувачів, як постійних так тимчасових, необхідно розробити модель уніфікованої архітектури та топологією мережі, що буде відповідати зазначеним вимогам. Необхідно розглянути інтеграцію проводових та безпроводових мереж, сенсорних мереж, систем відеоспостереження, охоронно-доглядових систем, систем спеціального зв'язку, моніторингових систем, інтеграції корпоративної мережі з системами стільникових операторів України, моніторингу всіх зазначених систем. Також необхідно забезпечити фронт та бек захист інформаційних ресурсів, втому числі і центрів обробки та збереження даних.

Для побудови такої архітектури необхідно використовувати технології віртуалізації, агрегації, резервування (каналів та інформації), безпроводових мостів, системи шлюзів з корпоративних мереж до мереж 2G, 3G, LTE, WSN. Використання зазначених технології дозволить збільшити продуктивність мережі та підвищити її захищеність. Для спрощення розуміння процесу зміни архітектури та топології розглянемо перехід до рішення за технологією Virtual Switching System (VSS) для кампусної мережі за рекомендаціями компанії Cisco (рис. 2) [13].



а) *б)* *в)*

Рис. 2. Топології VSS відповідно до рекомендацій Cisco:
а) Traditional Design Choices; б) Multilayer Design-Looped Topology; в) Multilayer Design-Loop Free Topology

Тобто, використовуючи сучасні комутаційні вузли, є можливість захисту інформації не лише за рахунок криптографічних алгоритмів та методів аутентифікації абонентів, а й шляхом використання віртуальних локальних мереж (VLAN), у які можливо об'єднувати різні сегменти мережі такі як сенсорні мережі (WSN), локальні безпроводові мережі (WLAN) тощо. Саме тому, у якості таких вузлів повинні бути пристрої, які підтримують концепції SDN та SDR, що зможуть самостійно переконфігуруватися та використати найбільш оптимальний алгоритм передачі даних між користувачем та послугою до якої направлено запит (рис. 3 [14]). Також це дозволить розмежувати доступ до мережі у відповідності до концепції BYOD.

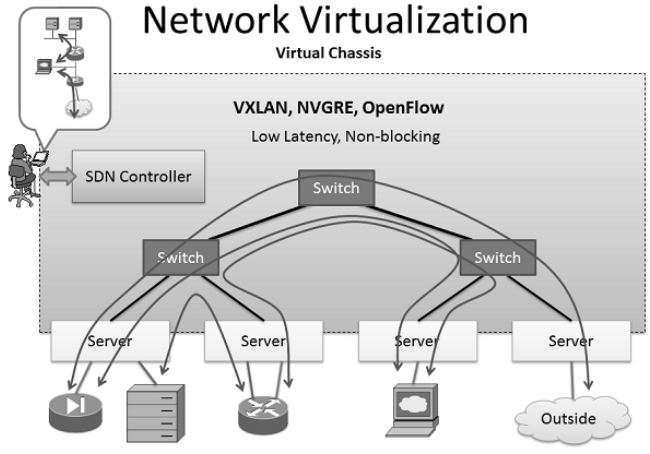


Рис. 3. Концепція SDN на практиці

Тепер, наклавши на цю архітектуру мережі розробки компанії Cisco Expressway або Collaboration Edge [3], можемо розробити архітектуру захищеної мережі для користувачів (рис. 4), які, як було зазначено, мають фронт та бек фаєрволи, підтримують концепцію уніфікованих комунікацій (UC) та хмарні сервіси.

Для повноти картини залишилось розглянути внутрішню архітектуру мережі аеропорту та центри інтеграції мереж і послуг, у залежності від фізичних параметрів (проводові, безпроводові) та стандартів передачі (WSN, WLAN, 3G, LTE, Ethernet, FTTH, xDSL, систем рухомого радіозв'язку (CPP)) (рис. 5). Зрозуміло, що всі інформаційні центри розділені на захищені сегменти мережі за допомогою фізичних та програмних засобів. Контент співробітників та тимчасових користувачів також рознесений у різні VLAN. Враховано можливість рознесених контентосховищ для підрозділів аеропорту, користувачів (пасажирів та супроводжуючих осіб), підприємств, що орендують робочі площі.

Для забезпечення необхідних швидкостей і використання концепції BYOD та IoT слід використовувати на рівні доступу точки доступу Wi-Fi різних стандартів 802.11n та 802.11ac, працюючих у режимі мосту. Це можливо за рахунок різних радіусів дії та швидкостей, на яких працюють зазначені стандарти. Тобто у місцях найбільшого скупчення абонентів потрібно використовувати точки доступу 802.11ac, в інших – 802.11n, які в свою чергу можуть збирати та ретранслювати дані сенсорних мереж.

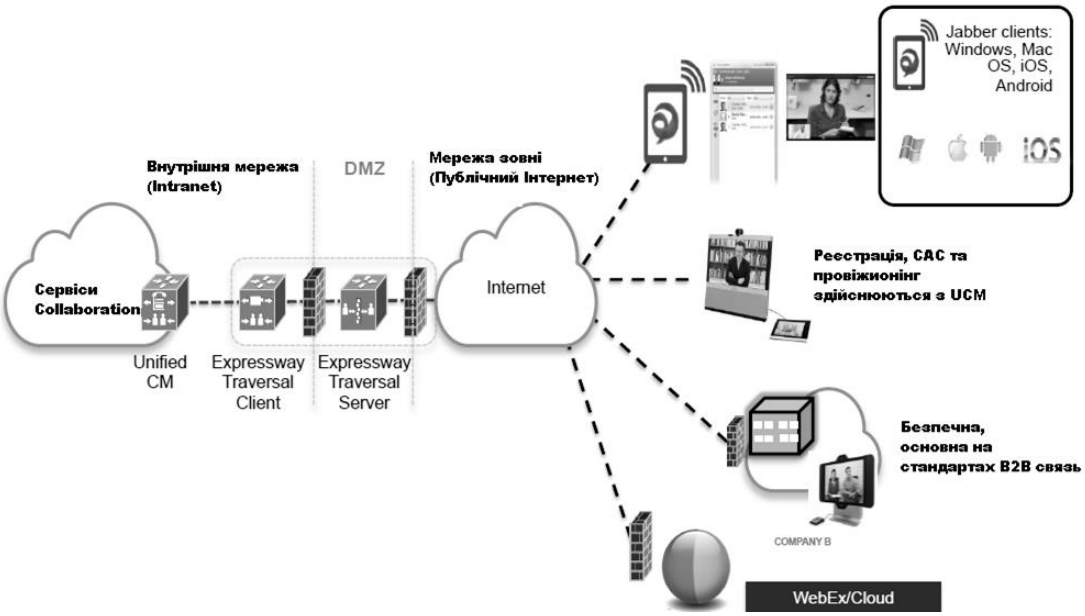


Рис. 4. Технології Expressway або Collaboration Edge

Використавши на рівні доступу технології Wi-Fi можливо забезпечити розв'язання декількох важливих задач (рис. 5): 1) оперативний доступ до інформації аеропорту як співробітниками, так і тимчасовими абонентами; 2) зменшення витрат на обладнання за рахунок використання пристроїв співробітників; 3) єдина захищена система управління мережею SDN, що також скорочує витрати на адміністрування мережі; 4) можливість надання абонентам розважального контенту, потокового відео, аудіо, послуг IP- телефонії; 5) моніторинг місцезнаходження пасажирів, персоналу, багажу; 6) зменшення навантаження на інформаційні центри аеропорту (єдина електронна інформаційна база); 7) можливість підвищення доходів аеропорту за рахунок реклами товарів та послуг для пасажирів.

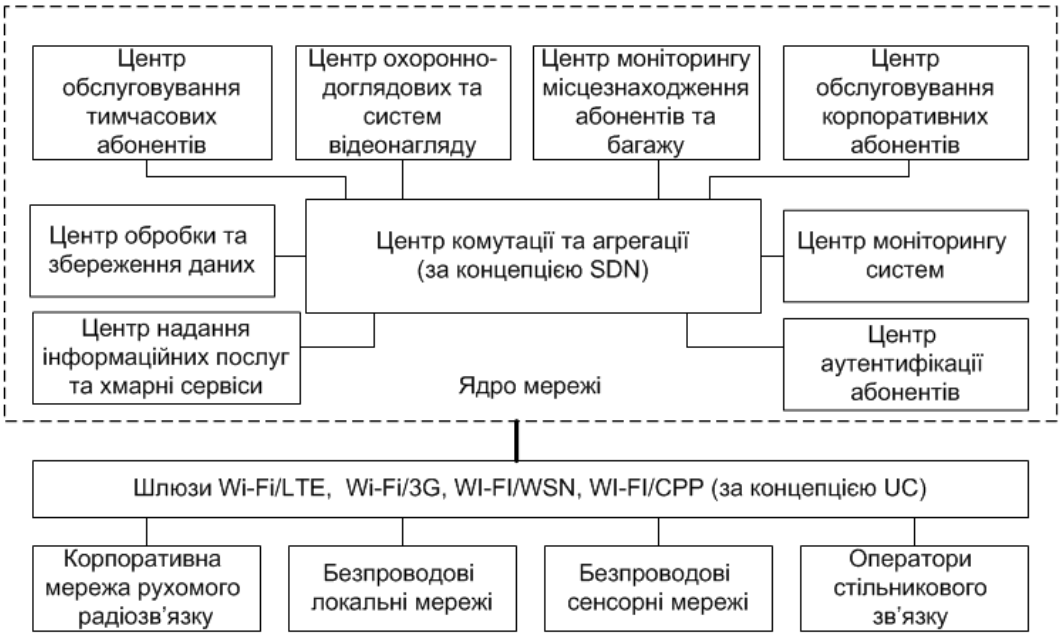


Рис. 5. Архітектура оптимізованої мережі аеропорту

Застосування такої архітектури дозволить проводити моніторинг не лише користувачів мережі, контролювати захист переданих даних але й проводити моніторинг систем життєзабезпечення аеропорту, оперативного інформування співробітників та пасажирів, щодо поточної інформації рейсів, багажу, розваг та розважального контенту. Також, це дозволить абонентам, не підключеним до операторів зв'язку України, отримати послуги зв'язку за допомогою WLAN, надати таку послугу терміналам, що не підтримують 2G, 3G а лише LTE. Для більш широкого застосу-

вання такої уніфікованої архітектури необхідно створити користувацьку програму, яка буде використовувати отримані від мережі підприємства вичерпну інформацію для користувача.

Висновки. Запропоновані у цій роботі архітектура та топологія мережі дозволять зменшити витрати на утримання корпоративної мережі, збільшити кількість та якість пропонованих абонентам послуг, уніфікувати корпоративну мережу в одному центрі управління, відповідатимуть сучасним вимогам до надання захищених інформаційних послуг абонентам. Також ця стаття дає поштовх для розвитку подальших наукових досліджень та впровадження практичних рішень – уніфікації системи, модернізації та удосконалення систем шлюзів, точності визначення місцеположення, дослідження використання мостових з'єднань, розробки програмного забезпечення для абонентів та управління мережею, створення нових методів захисту від кіберзагроз, а також політик безпеки при впровадженні сучасних та перспективних концепцій.

ЛІТЕРАТУРА

[1]. В аэропорту «Борисполь» впервые с начала года зафиксировано увеличение пассажиропотока [Електронний ресурс]. – Режим доступу: https://kbp.aero/ru/about/press-center/news/2015 /1023/.

[2]. Архив Expo [Електронний ресурс]. – Режим доступу: http://expo.muk.ua/archive/.

[3]. ЦОД и безопасность: на пороге перемен [Електронний ресурс]. – Режим доступу: http://www. cisco.com/web/UA/events/SecurityForum 2014/ index.html.

[4]. Международный Форум AC&ADMOB-2015 в Киеве [Електронний ресурс]. – Режим доступу: http://kyiv-ac-admob-2015.ciseventsgroup.com/.

[5]. Международный Гранд Форум ACAIP-2015 в Киеве [Електронний ресурс]. – Режим доступу: http://kyiv-acaip-2015.ciseventsgroup.com/.

[6]. Международный Форум ADCAC&AIPBIT-2015 в Днепропетровске [Електронний ресурс]. – Режим доступу: http://dnipropetrovsk-2015.cisevents group.com/.

[7]. Ткаліч О.П., Одарченко Р.С., Устинов О.Ю., Колодинський Д.О. Розрахунок зони покриття бездротової мережі Wi-Fi для визначення місцезнаходження абонентів в аеропорту / Проблеми інформатизації та управління. – № 2 (50). – 2015. – С. 88-96.

[8]. Тимошенко О.С., Ткаліч О.П. Інтеграція мереж передачі IP-трафіку з системами відеоспостереження об'єктів // Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», 2-5 червня 2014 р., НАУ. – Київ. – С. 33.

[9]. Шрамко М.О., Ткаліч О.П. Безпроводова мережа для доступу до баз даних // Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», 2-5 червня 2014 р., НАУ. – Київ. – С. 31.

[10]. Беспроводные сети для сервисов местоположения // Материалы Cisco Connect 2014.

[11]. Best Practices to Make BYOD, CYOD and COPE Simple and Secure [Електронний ресурс]. – Режим доступу: https://www.citrix.com/content/dam/ citrix/en_us/documents/oth/byod-best-practices.pdf.

[12]. Одарченко Р.С. Використання концепції мереж SDN для розподілу трафіку між мережами LTE та Wi-Fi / Р.С. Одарченко, О.П. Ткаліч // Наукоємні технології. – 2014. – Вип. 4(24). – С. 432-437.

[13]. Virtual Switching Systems Design Introduction [Електронний ресурс]. – Режим доступу: http://www.cisco.com/c/en/us/td/docs/solutions /Enterprise/Campus/VSS30dg/campusVSS_DG/V SS-dg_ch1.html.

[14]. Network Virtualization is like a big virtual chassis [Електронний ресурс]. – Режим доступу: http://bradhedlund.com/2011/10/12/network-virtualization-is-like-a-big-virtual-chassis/.

[15]. Ткаліч О.П. Підвищення ефективності використання корпоративної мережі за концепцією BYOD / О.П. Ткаліч, Р.С. Одарченко, Є.Ю. Шеремет, А.В. Марченко, Є.В. Рибальченко // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: збірник наукових праць. – Житомир: ЖВІ НАУ, 2013. – Вип. № 7. – С. 77-87.

REFERENCES

[1]. At the airport "Borispol" for the first time since the beginning of the year recorded an increase in passenger flow [Access Mode]: https://kbp. aero/ru/about/press-center/news/2015 /1023/.

[2]. Archive Expo [Access Mode]: http://expo. muk.ua/ archive/.

[3]. Data-center and security: on the verge of change [Access Mode]: http://www.cisco.com/web/UA/ events/ SecurityForum2014/index.html.

[4]. International Forum AC&ADMOB-2015 in Kiyv [Access Mode]: http://kyiv-ac-admob-2015.cisevents group.com/.

[5]. International Grand Forum ACAIP-2015 in Kiyv [Access Mode]: http://kyiv-acaip-2015.cisevents group.com/.

[6]. International Forum ADCAC&AIPBIT-2015 In Dnepropetrovsk [Access Mode]: http://dnipropetrovsk -2015.cisevents group.com/.

[7]. Tkalich O., Odarchenko R., Ustunov O., Kolodunskyy D. *Calculating coverage of wireless Wi-Fi network for*

locating subscribers in the airport Problems of informatization and management, № 2 (50), 2015, P. 88-96.
[8]. Tumochenko O., Tkalich O. *The integration of IP networks traffic with CCTV facilities* Scientific conference "Problems of exploitation and security of information and communication systems", 2-5 june 2014, NAU, Kiyv, P. 33.
[9]. Sramko M, Tkalich O. *Wireless network for access to databases* Scientific conference "Problems of exploitation and security of information and communication systems", 2-5 june 2014, NAU, Kiyv, P. 31.
[10]. Wireless networks for location services // Cisco Connect 2014 materials.
[11]. Best Practices to Make BYOD, CYOD and COPE Simple and Secure, [Access Mode]: https://www. citrix.com/content/dam/citrix/en_us/documents / oth / byod-best-practices.pdf.
[12]. Odarchenko R., Tkalich O. *Using the concept of SDN networks for the distribution of traffic between LTE networks and Wi-Fi* Science-Based Technologies, 2014, Num. 4(24), P. 432-437.
[13]. Virtual Switching Systems Design Introduction, [Access Mode]: http://www.cisco.com/c/en/us/td/ docs/solutions/Enterprise/Campus/VSS30dg/ cam pusVSS_DG/VSS-dg_ch1.html.
[14]. Network Virtualization is like a big virtual chassis. [Access Mode]: http://bradhedlund.com/2011/10 /12/network-virtualization-is-like-a-big-virtual-chassis/.
[15]. Tkalich O, Odarchenko R., Sheremet E., Marchenko A., Rybalchenko E. *More efficient use of corporate network by BYOD concept* The problems of creating, testing, application and maintenance of complex information systems, Zhitomir: ZHVI NAU, 2013, № 7, P. 77-87.

АРХИТЕКТУРА СОВРЕМЕННОЙ ЗАЩИЩЕННОЙ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СЕТИ АЭРОПОРТА

Современный аэропорт должен предоставлять своим клиентам своевременные качественные и защищенные информационные услуги. Постоянный рост количества таких услуг (в соответствии с развитием информационно-коммуникационных технологий) и самих пассажиров стимулируют к поиску и внедрению новых концепций и подходов к интегрированному предоставлению информационных услуг в аэропортах. Безусловно важным является создание унифици-рованной информационно-коммуникационной сети, которая обеспечит высокий уровень предоставления информационных услуг абонентам сети, будет защищенной и безопасной для использования, также сможет интегрировать в себя средства безопасности, информационно-справочные службы, развлекатель-ный контент, системы видеонаблюдения, системы регистрации пассажиров, информацию эксплуатаци-онных служб аэропорта, сенсорные сети для интеллек-туального управления системами жизнеобеспечения аэропорта, операторов сотовой связи, современных концепций SDN, SDR, BYOD и IoT. Учитывая это, в статье предложено интегрирование указанных совре-менных и перспективных концепций и технологий для оптимизации архитектуры и топологии корпора-тивной сети аэропорта. Полученные результаты позволят повысить экономическую эффективность использования корпоративной сети аэропорта, увеличить ее защищенность, количество и качество информационных услуг, позволят упростить управление сетью и системами обеспечения жизнедеятельности аэропорта.

Ключевые слова: защита информации, защищенные информационные услуги, аэропорт, архитектура сети, беспроводные сети, сенсорные сети, система мониторинга, информационно-коммуникационная сеть, SDN, SDR, BYOD, IoT.

ARCHITECTURE OF MODERN SECURED INFORMATION & COMMUNICATION AIRPORT NETWORK

Modern airport should provide on-time quality and secured services to their customers. The increasing of these services (according to information and communication technology develop ent) and number of passengers impetus to searching and implementation new concepts and approaches to integrated information services providing in airports. Certainly the unified information & communication network creation is very important. This can provide a high level of information services to network subscribers. Also this network will be secured for users and can integrate security means, call centers, entertainment content, video monitoring systems, passengers registration systems, information of airport operating agency, sensor networks for intellectual management of life sustaining airport systems, cellular communication operators, modern concepts like SDN, SDR, BYOD and IoT. In this context this paper presents integration of mentioned modern and prospective concepts and technologies for airport corporate network`s architecture and topology optimization. Given results give possibility to increase the economic efficiency of airport corporate network using. Also it enables high security of the network, information services quantity and quality increasing, simplify the management of network and life sustaining airport systems.

Index terms: information security, secured information services, airport, network architecture, wireless networks, sensor networks, monitoring system, information & commubication network, SDN, SDR, BYOD, IoT.

Ткаліч Олег Петрович, кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем, Національний авіаційний університет.
E-mail: tkalich@nau.edu.ua.
Ткалич Олег Петрович, кандидат технических наук, доцент, доцент кафедры телекоммуникационных систем, Национальный авиационный университет.
Tkalich Oleg, PhD, Associate Professor of Telecommunications systems Academic Department, National Aviation University.

Одарченко Роман Сергійович, кандидат технічних наук, доцент кафедри телекомунікаційних систем, Національний авіаційний університет.
E-mail: odarchenko.r.s@mail.ru.
Одарченко Роман Сергеевич, кандидат технических наук, доцент, доцент кафедры телекоммуникационных систем, Национальный авиационный университет.
Odarchenko Roman, PhD, Associate Professor of Telecommunications systems Academic Department, National Aviation University.
Гнатюк Сергій Олександрович, кандидат технічних наук, доцень, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет.
E-mail: s.gnatyuk@nau.edu.ua.
Гнатюк Сергей Александрович, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий, Национальный авиационный университет.
Gnatyuk Sergiy, PhD, Associate Professor of IT-Security Academic Department, National Aviation University.

УДК 621.391:519.2

ОБОБЩЕННАЯ СТАТИСТИЧЕСКАЯ АТАКА НА СИНХРОННЫЕ ПОТОЧНЫЕ ШИФРЫ

Антон Алексейчук, Сергей Конюшок, Артем Сторожук

В настоящее время наиболее мощными атаками на синхронные поточные шифры являются атаки на основе подобранных векторов инициализации. К ним относятся кубическая атака Динура-Шамира, статистическая атака Фишера-Хазаи-Майера (FKM), а также их различные модификации и усовершенствования. Атака FKM строится на основе статистических приближений булевых функций, связанных с алгоритмами шифрования, функциями, зависящими лишь от некоторых разрядов ключа. Разработчиками атаки предложен способ нахождения указанных приближений, однако не дано теоретического обоснования эффективности этого способа. Кроме того, остается открытым вопрос о том, можно ли повысить эффективность атаки FKM, выбирая приближения из более широкого класса булевых функций. В настоящей статье предлагается атака на синхронные поточные шифры, обобщающая как кубическую атаку, так и атаку FKM. Эта атака базируется на алгебраически вырожденных приближениях булевых функций, что предоставляет больше возможностей для реализации основной идеи атаки FKM. Предложен полиномиальный вероятностный алгоритм построения указанных приближений по известным подпространствам, допустимым для заданной булевой функции. Показано, что, выбирая определенным образом параметры этого алгоритма, можно строить атаки на синхронные поточные шифры, заметно более эффективные по сравнению с полным перебором ключей.

Ключевые слова: *поточный шифр, нелинейный криптоанализ, атака на основе подобранных векторов инициализации, алгебраически вырожденная булева функция, нахождение приближений булевых функций.*

Введение. В настоящее время наиболее мощными атаками на синхронные поточные шифры (СПШ) являются атаки на основе подобранных векторов инциализации (ВИ). К ним относятся кубическая атака [10], статистическая атака FKM [13], а также их различные модификации и усовершенствования [6–9, 11, 12]. В принципе, подобные атаки применимы к любому криптографическому алгоритму, который может быть описан с помощью булевой функции $F:\{0,1\}^{l_0}\times\{0,1\}^{l_1}\to\{0,1\}$, один из аргументов которой является секретным, а другой – общедоступным параметром. В случае СПШ в качестве F можно взять (рассматриваемый как функция ключа $k\in\{0,1\}^{l_0}$ и вектора инициализации $c\in\{0,1\}^{l_1}$) знак выходной последовательности генератора гаммы шифра в некотором такте. Предполагается, что функция F доступна противнику в виде оракула («черного ящика»), в частности, алгоритм, реализующий эту функцию, может быть не известен.

На этапе предвычислений противник может подавать на вход оракула любые пары векторов $(x,y)\in\{0,1\}^{l_0}\times\{0,1\}^{l_1}$, вычисляя значения $F(x,y)$, чтобы собрать нужную информацию о свойствах функциии F. Затем противник получает доступ к оракулу $F_k(c)=F(k,c)$, $c\in\{0,1\}^{l_1}$, где значение ключа $k\in\{0,1\}^{l_0}$ не известно. Противник может выбирать любые векторы $c\in\{0,1\}^{l_1}$ и вычислять значения $F_k(c)$ при фиксированном ключе k, стремясь восстановить этот ключ (или получить о нем некоторую информацию). Другой возможной стратегией противника является построение различающей атаки, направленной на то, чтобы статистически отличить (за приемлемое время с достаточно