ЗАХИСТ ІНФОРМАЦІЇ ТА ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

УДК 004.934:681.391

Юдін О. К., Весельська О.М.
Національний авіаційний університет

СУЧАСНІ ІНТЕГРАЦІЙНІ МОДЕЛІ МЕРЕЖЕВОЇ БЕЗПЕКИ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Проаналізовано традиційні підходи захисту інформаційних ресурсів і існуючі засоби для забезпечення інформаційної безпеки. Наведено класифікацію методів захисту інформаційної безпеки. Запропоновано новий підхід підключення засобів системи безпеки до інформаційних та телекомунікаційних мереж. Досліджено особливості і умови для впровадження нового підходу для підключення системи захисту і контролю трафіку.

Проанализированы традиционные подходы защиты информационных ресурсов и существующие средства для обеспечения информационной безопасности. Приведена классификация методов защиты информационной безопасности. Предложенновый поход подключения средств системы безопасности в информационных и телекоммуникационных сетей. Исследованы особенности и условия для внедрения нового подхода для подключения системы защиты и контроля трафика.

The traditional approaches two the protection or information resources and existing means or ensuringin formation security are analyzed. The classification or methods or information security protection is given. A new approach two connecting security systems two information and telecommunication networks is proposed. The features and conditions or implementing a new approach or connection or the system or protection and traffic control are explored.

Ключові слова: *інформаційна безпека, засоби захисту та контролю трафіка, методи захисту інформації, державні інформаційні ресурси, система безпеки інформаційних та телекомунікаційних мереж.*

Вступ

Стрімкий розвиток сучасних інформаційні технології на сьогоднішній деньдає можливість мати доступ до все більших об’ємів інформації. В таких умовахпотреба у інформаційній безпеці (ІБ) зростає в рази, в наслідок чого, з кожним роком збільшується фінансуваннясаме на засоби захисту та контролютрафіка в інформаційних та телекомунікаційних мережах.

За статистичними даними поданими компанією Gartner, світові витрати на інформаційну безпеку в 2016 році досягли $ 81,6 млрд., що на 7,9% більше в порівнянні з 2015 році. Основні витрати відбуваються в таких сферах, як консалтинг і IT-аутсорсинг. До кінця 2020 року найбільш високі темпи зростання будуть демонструвати напрямки тестування безпеки, IT-аутсорсингу і рішень для захисту від витоків інформації (DataLossPrevention - DLP) [1].

Аналіз та постановка задачі

25 лютого 2017 року президент України підписав Указ, яким увів в дію рішення Ради національної безпеки і оборони «Про Доктрину інформаційної безпеки України» [2]. Як зазначається у документі, необхідність прийняття Доктрини інформаційної безпеки України зумовлена виникненням актуальних загроз національній безпеці в інформаційній

сфері, а також потребою визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації і вільного обігу інформації. «Одним з життєво важливих національних інтересів виділено забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України».На теперішній час для забезпечення захисту інформації в інформаційних мережах використовують ефективні системи засобів різних розробників. Система засобів– це комплекс апаратних і програмних засобів, що забезпечують побудову систем захисту IP-трафіка в повній відповідності із законами України.Існуючі засоби досить ефективні, але для окремих вузлів і блоків. Кожний засіб відповідає за моніторинг і захист окремого вузла інформаційних та телекомунікаційних мереж. Що приводить до великих часових, матеріальних затрат, та ускладнює процес швидкого реагування на потенціальні загрози та шляхи їх попередження та знешкодження.

Мета даної статті – запропонувати новий підхід у розробцісучасних інтеграційних моделей мережевої безпеки, які в порівняння з існуючими, підвищують рівень захисту системи безпеки державних інформаційних ресурсів (ДІР) та оптимізують витрати.Розробитиструктурно-логічну схему нового запропонованого підключення моделі мережевою безпекидо інформаційних та телекомунікаційних мереж.

Основна частина

Аналіз темпів розвитку інформаційних технологій показує стрімкийріст обсягів шифрованого трафікаSSL (SecureSocketsLayer), що займає 25-35% корпоративного трафіка. На його дешифрування витрачаються значні ресурси ІБ. Більш 50% мережевих атак у 2017 році проходиликрізь шифрований трафік. З кожним днем збільшується мобільність додатків та пристроїв, порушується безпека з вини принесених з собою пристроїв. Виходячи з цього, принцип захищеного периметра потребує сучасного підходу до структури використання засобів інформаційного захисту та перехід до моделі «Zero-Trust»[3]. Модель нульової довіри (Zero-Trust Model, ZTM) – агресивний підхід до забезпечення мережевої безпеки, що передбачає встановлення контролю за всіма наявними даними, виходячи з припущення, що кожен файл містить у собі потенційну загрозу. Тобто стає актуальним, як ніколи, питання що до зміни моделі захисту інформаційних ресурсів, яка б давала можливість контролювати трафік віртуального та фізичного середовища, використовувати всі існуючі засоби інформаційних технологій для інформаційного захисту.При внесенні змін у структуру інформаційних та телекомунікаційних мереж з метою покращення контролю трафіка треба врахувати, що віртуалізація елементів мережі потребує зберегти її захищеність, великі об’єми трафіка не проходять крізь фізичну мережу і стають сліпою зоною, міграція серверів, додатків всередині віртуального середовища ускладнює їх моніторинг.

Виходячи з особливостей використання, усі засоби інформаційного захисту можна поділити на дві великі групи: *активні засоби інформаційного захисту* (превентивні); *пасивні засоби інформаційного захисту* (реактивні)[4]. Активні засоби інформаційного захисту спрямовані на виявлення та повну або часткову нейтралізацію інформаційних загроз. Пасивні засоби спрямовані на протидію та локалізацію загроз. Багато засобів інформаційного захисту можуть виконувати обидві групи функцій,в залежності від умов використання, тому на практиці дуже складно зробити чітку категоризацію. Функціональна структура засобів інформаційного захисту, яка включає: програмно-технічні засоби; організаційно-економічні засоби; адміністративно-правові засоби; соціально-психологічні засоби наведена у табл.1.

Таблиця 1

Основні підходи та методи захисту інформації

Методи захисту	Підходи до захисту	
	Активний підхід	Пасивний підхід
Програмні методи	Антивірусні програми Дезінформація Розвідка (datamining) Прогнозування загроз	Віртуалізація Спам-фільтри Фаєрволи Моніторинг

	Проактивний захист	Протоколювання Криптографічний захист
Апаратні методи	Відеонагляд Радіоконтроль Біометрична ідентифікація Екранування	Смарт-карти Системи сигналізації Засоби енергазахисту
Організаційні методи	Управління доступом Патентування Перевірка, контроль та навчання персоналу	Резервне копіювання Управління інцидентами Договір про нерозголошення Фізичний захист обладнання та приміщень

Виходячи з цих міркувань,для оптимального захисту інформаційних і телекомунікаційних мереж потрібно:

- використовувати у тісній взаємодії активні та пасивні засоби інформаційного захисту в системі інформаційної безпеки підприємства;
- збільшити кількість точок моніторингу;
- збільшити кількість активних засобів контролю трафіку;
- забезпечити доступність віртуального середовища контролю для засобів ІБ;
- отримувати з мережі дешифровану копію трафіку;
- не впливати на відмовостійкість мережі.

На даний час для захисту інформаційних та телекомунікаційних мереж використовується традиційна схема підключення систем безпеки, яка не відповідає цим вимогам [4]. На рис.1 показана традиційна система захисту та контролютрафіка в інформаційних та телекомунікаційних мережах. Традиційно в системі інформаційної безпеки використовують засоби, наведені в табл.2.

Таблиця 2

Засоби захисту системи інформаційної безпеки

Назва засобу		Область використання
Скорочення	Повна назва	
Volpmonitor		Монітор що обладнаний мережевими модулями, камерою, мікрофоном і динаміками, які дають можливість входити в мережу і здійснювати відеодзвінки при підключенні кабелю до автоматизованих систем першого та другого класів.
Mallmonitor		Центральний монітор
WAF	WebApplicationFirewall	Програма, яка проводить автоматичну компіляцію і установку інших програм і бібліотек з метою знизити існуючі загрози з боку атак, спрямованих на експлуатацію вразливостей в веб-додатках.
SIEM	SecurityInformation&EventManagement	Система управління подіями і безпекою інформації або система управління подіями інформаційної безпеки. Дані рішення являють собою апаратно-програмні комплекси, які при інтеграції вже мають величезну кількість вбудованих правил безпеки і звітів.
DLP	DataLossPrevention	Системи захисту конфіденційних даних від внутрішніх загроз. При цьому під внутрішніми загрозами розуміються зловживання (навмисні або випадкові) з боку співробітників організації, мають легальні права доступу до відповідних даних, своїми повноваженнями.
IDS	IntrusionDetectionSystem	Система виявлення вторгнень. Програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в компьютерную систему або мережу, або несанкціонованого керування ними в основному через Інтернет.
APT	AdvancedPer	Атака, і люди, які стоять за нею. З одного боку, складна постійна

	sistentThreat	загроза (APT) є високоточною кібератакою. З іншого боку, APT можна назвати групу, що оплачують цільову атаку.
IPS	IntrusionPrev entionSystem	Програмна або апаратна система мережевої та комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки і автоматично захищає від них.
Anti-malware		Програма використовує технологію швидкого сканування системи для виявлення та знищення різного роду шкідливих програм. В першу чергу програма орієнтована на боротьбу зі шпигунськими модулями.
Forensics		Пкомплекс для проведення комп'ютерних експертиз та дослідження носіїв інформації фахівцями з інформаційної безпеки.
Analitics		Сервіси, що надаються пошуковими системати для створення детальної статистики відвідувачів веб-сайтів.
SPAN		Апаратний пристрій, що приєднується безпосередньо до кабелю комп'ютерної мережі і передає копію мережевого трафіку іншому пристрою.

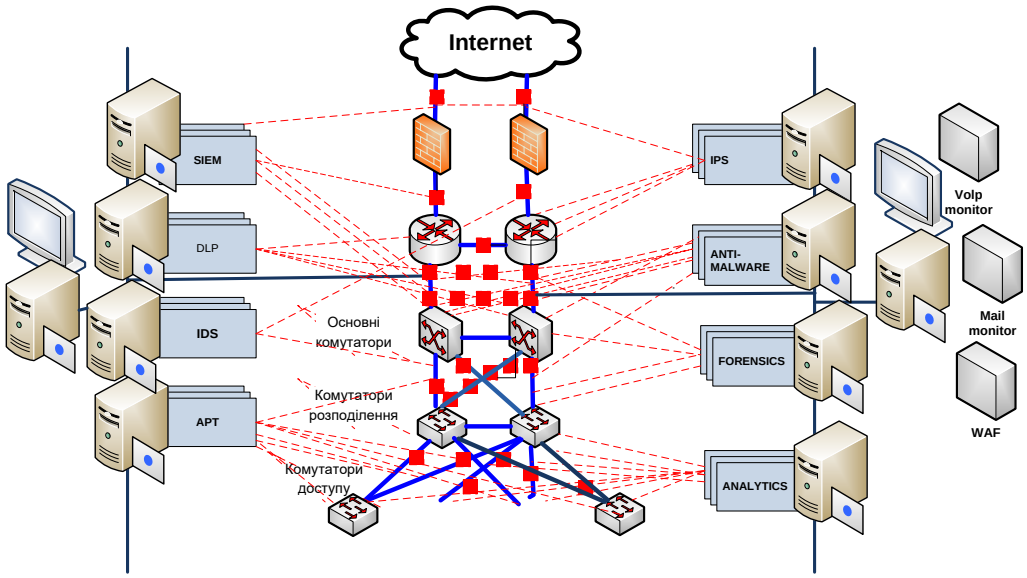


Рис.1 Структурно-логічна схема підключення систем інформаційної безпеки традиційним способом.

На наведеній на рис. 1 схемі видно, що кожен засіб виконує свої конкретні задачі захисту, вони працюють автономно, незалежно один від одного, і кожному блоку потрібно мати свій окремий доступ до ресурсів зовнішнього трафіку.

В зв'язку з цим виникають проблеми, а саме:

- проблема отримання зовнішнього трафіку кожним засобом;
- конкуренція за SPAN;
- децентралізація управління;
- висока вартість впровадження нових систем;
- зниження відмово стійкості інформаційних та телекомунікаційних мереж.

Для вирішення цих проблем, запропоновановбудувати в систему захисту та контролю трафікамодуль, який забезпечує видимість у фізичних, віртуальних, віддалених сайтах, як єдиний модуль із загальним керівництвом і моделями політики, а не у вигляді набору непересічних вузлів. Така уніфікована модель управління дозволяє швидко та ефективно моніторititрафіку фізичному та віртуальному просторі. При внесенні змін у структуру захисту інформаційних та телекомунікаційних мереж з метою покращення контролю трафіка, треба врахувати наступні особливості: віртуалізація елементів мережі потребує зберегти її захищеність; великі об'єми трафіка, що не проходять крізь фізичну мережу, стають сліпою зоною; міграція серверів, додатків

всередині віртуального середовища ускладнює їх моніторинг. Виходячи з цих особливостей, підключення системи захисту і контролю трафіка виконується з урахуванням наступних умов: наданнятрафіку віртуальної та фізичної мережі одним і тим же отримувачам, оптимізація копійтрафіку для кожного отримувача, наданнявеликих можливості обробки трафіка, інтеграція з зовнішніми системами управління, універсальність, тобто можливість використання і для інших проектів (не тільки для ІБ). За поданими умовами, та з урахуванням перелічених особливостей, пропонується нова схема підключення системи безпеки сучасної модифікованоїсистеми, що наведена на рис.2.

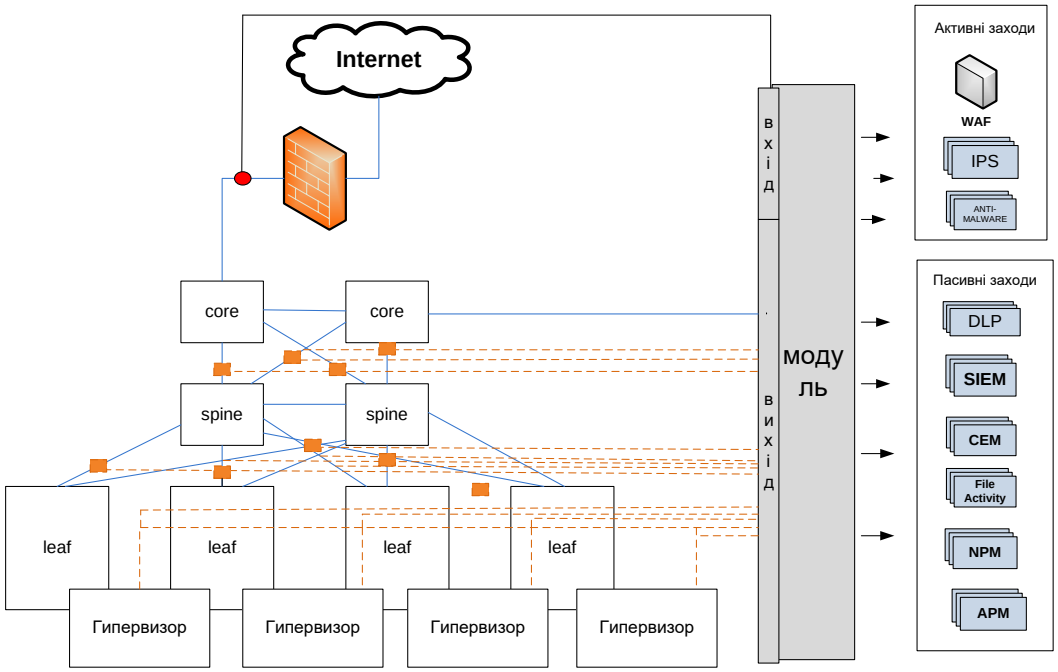
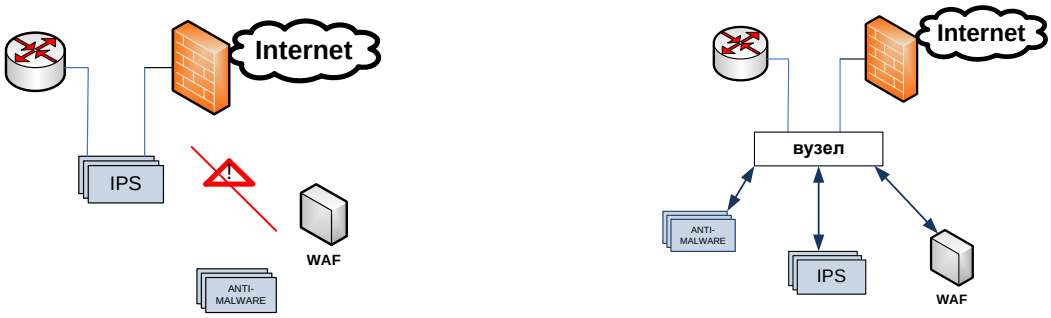


Рис. 2. Структурно-логічна схема підключення засобів системи безпеки до інформаційних та телекомунікаційних мереж запропонованим новим способом

До активних заходів системи захисту належать WAF, IPS, Antimalware. Інтеграція декількох активних систем ІБ в один інтерфейс практично неможлива через зниження відмовостійкості мережі. Що в такому випадку робити? Якщо вибрати точку інтеграції, втрачається ефективність засобу ІБ. Можна ускладнити топологію мережі, та що робити, якщо в систему треба буде впровадити ще одну активну систему? Відповіді на ці питання дає новий підхід до підключення системи захисту, шляхом встановлення єдиного вузла для декількох активних систем ІБ, як неведено на рис.3.



а) б)

Рис. 3. Традиційний підхід(а), та сучасний підхід (б) підключення активних засобів захисту у систему безпеки державних інформаційних ресурсів

Переваги сучасного підходу підключення активних засобів з єдиним вузлом дає наступні: простота інтеграції і надійність, можливість пропускання різнихтрафіків через активні пристрої, постійна перевірка доступності кожного пристрою ІБ, різні сценарії реагування на аварії, можливість підключення пасивних засобів ІБ.

Завдяки такому підключенню та введенню у схему нового комутатора та вузла з'являється можливість значно підвищити рівень захисту системи безпеки державних інформаційних ресурсів та мати доступ до трафіку у будь якому сегменті мережі. Крім того такий спосіб підключення надає нові можливості, а саме: підключення будь-яких засобів ІБ/моніторингу/аналітики, зменшити кількість точок підключення, зменшити вплив на робочу мережу, збільшити продуктивності засобів ІБ/моніторингу, продовжити строки експлуатації рішень, оптимізувати витрати.

Висновки

Виходячи з вищесказаного, в умовах стрімкого розвитку інформаційних технологійзапропоновано шляхивдосконалення існуючих систем захисту ДІР,та перехід до нових моделеймережевої безпеки, що відповідають потребам сьогодення і забезпечують захищеність великих об'ємівтрафікуу реальному часі, як у фізичному так і віртуальному просторі. Це стає можливим при умові використання спеціально розроблених модулів, які будуть забезпечувати видимість у фізичних, віртуальних, віддалених сайтах та нових інфраструктурах, як єдиний модуль із загальним управлінням і єдиною моделлю політики безпеки, а не у вигляді набору непересічних вузлів.

Список використаних джерел

1. Гордиенко Д. В. Возможный подход к сравнительной оценке экономической мощи ведучих развитых и развивающихся стран мира // Национальные интересы: приоритеты и безопасность. – 2016. – №. 2 – С. 332-335.

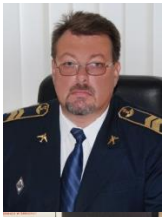
2. Вісник України. Указ Президента «Про доктрину інформаційної безпеки України» – 2017. – Т. 514. – С. 1783.

3. Юдін О. К., Бучик С. С. Класифікація загроз державним інформаційним ресурсам інженерно-технічного спрямування. Методологія побудови класифікатора // Наукоємні технології. – 2015. – Т. 25. – №. 1. – С. 188-195.

4. Gallatin T. et al. Packet switch methods and systems : пат. 9391925 США. – 2016.

5. Юдін О.К. Інформаційна безпека держави. – К.: Консум, 2005. – 576 с.

Інформація про авторів:



Юдін Олександр Костянтинович – доктор технічних наук, професор, директор Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету; наукові інтереси: інформаційні технології, кібербезпека.

E-mail: kszi@ukr.net

Весельська Ольга Михайлівна – асистент кафедри комп'ютеризованих систем захисту інформації Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету; наукові інтереси: інформаційні технології, кібербезпека.

E-mail: olga_veselskaya@ukr.net