УДК 004 (738.5+056.53)

ВІТАЛІЙ ЗУБОК

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ DNSSEC ДЛЯ ЗАХИСТУ ДОМЕННИХ ІМЕН В УКРАЇНСЬКОМУ СЕГМЕНТІ МЕРЕЖІ ІНТЕРНЕТ

Система доменних імен є невід'ємною частиною адресації в мережі Інтернет. Дефекти в реалізації протоколу DNS дозволяють використовувати його для зловмисних дій, підчас яких може бути порушено цілісність і доступність даних при обміні даними між DNS-клієнтом та DNS-сервером. Технологія DNSSEC, що призначена для захисту цілісності при обміні даними DNS, запобігає отриманню фальшивих даних DNS-клієнтами. Технологія полягає в тому, що кожна відповідь сервера DNS повинна мати електронний цифровий підпис, який можна перевірити через сервер DNS більш високого рівня. Хоча DNSSEC активно впроваджується протягом 10 років, повному переходу на DNSSEC заважають відносна складність налаштування доменних зон та відсутність готових рішень рівня Інтернет-користувача. В статті подано сучасний стан, порівняльний аналіз, проблеми та перспективи впровадження цієї технології для захисту інформаційних ресурсів, адреси яких знаходяться в доменному просторі домену UA. Результати аналізу свідчать, що в домені верхнього рівня UA підтримується валідація, trust anchor домену UA внесено в кореневу доменну зону, а отже, для доменів другого рівня в домені UA не існує адміністративних чи технічних перепон для впровадження технології DNSSEC. Її використання дозволить забезпечити виконання автентифікації DNS-серверів та валідації DNS-відповідей. Однак, відносна складність технології та відсутність готових рішень на рівні інтернет-користувачів стримують темпи впровадження DNSSEC. Водночас це обумовлено додатковими витрати операторів телекомунікацій та провайдерів послуг на адміністрування, а також відсутністю підтримки DNSSEC в обладнанні операторського рівня.

Ключові слова: безпека інформаційних ресурсів, система доменних імен, валідація доменів, DNSSEC, захист DNS-транзакцій.

Постановка проблеми. Система доменних є невід'ємною частиною адресації в мережі Інтернет та протягом багатьох років має ознаки постійного зростання [1], [5] - [8]. Дефекти в реалізації протоколу DNS дозволяють використовувати його для зловмисних дій. Проблема захисту клієнтів від отримання фальшивих даних DNS є важливою і актуальною [2], [3]. Для захисту цих даних існує та активно впроваджується механізм DNSSEC, згідно доктрини якого кожна відповідь серверу повинна мати цифровий підпис [3], [4].

Аналіз останніх досліджень і публікацій. Впровадження DNSSEC в світі триває з досить постійним темпом. Так, за даними SecSpider [6] щороку кількість "підписаних" доменів збільшується на порядок. Але Україна в цьому питанні не має лідерських позицій [8]. При цьому здебільшого досліджуються окремі аспекти використання цієї технології і, як наслідок, не приділяється уваги перспективам напрямам провадження для захисту українських інформаційних ресурсів.

Метою статті є дослідження сучасного стану, аналіз та оцінка перспектив впровадження технології DNSSEC для захисту українських інформаційних ресурсів.

Організація глобальної системи доменних імен. Система доменних імен (Domain Name System, DNS) – це розподілена база даних (див. табл. 1), що підтримує ієрархічну систему імен, основним (але не єдиним) призначенням якої є автоматичний пошук IP-адреси за відомим символьним. Протокол DNS є службовим протоколом прикладного рівня. Служба DNS побудована, як і більшість Інтернет-сервісів, за клієнт-серверною архітектурою. Кожен сервер доменних імен (name server) зберігає частку розподіленої бази імен в своїх таблицях, які мають назву доменних зон. Ієрархія серверів починається з системи кореневих серверів (root-servers), IP-адреси яких статично визначені для кожного домену верхнього рівня (top-level domain, TLD).

Таблиця 1 – Список понять, скорочень і визначень

№ з/с	Поняття, скорочення	Визначення
1.	Доменна зона	база даних, яка містить інформацію про простір доменних імен, що зберігається на авторитетному сервері
2.	Авторитетний сервер	сервер DNS, призначений давати відповіді на DNS-запити, які стосуються виключно для окремих доменних зон, які сконфігуровано на сервері адміністратором
3.	Резолвер	DNS-клієнт, який посилає DNS-повідомлення, щоб отримати інформацію про запитуваній простору доменних імен
4.	Рекурсія	дія, що виконується, коли сервер DNS шукає відповідь на запит, що отриманий від іншого резолвера.
5.	Рекурсивний резолвер	DNS-сервер, який рекурсивно запитує за інформацію, запитувану в запиті DNS
6.	FQDN (fully-qualified domain name)	повне доменне ім'я пристрою в розподіленій базі даних DNS
7.	RR: resource record	формат, який використовується в DNS-повідомленях, та складається з наступних полів: ім'я, тип, клас, TTL, RDLENGTH і RDATA.
8.	TTL: час життя ресурсного запису	визначається в секундах та використовується кешуючими серверами для повторного використання відповіді.
9.	TCP, UDP	комунікаційні протоколи транспортного рівня
10.	SOA: start o authority	перший запис доменної зони, що містить службові параметри.

Корінь бази даних DNS керується Інтернет-корпорацією з адрес та імен – IANA [9]. Домени верхнього рівня поділяються на декілька видів:

– публічні домени загального призначення, за які відповідає IANA (наприклад: *com, net, org, info, biz*) – generic TLD, або gTLD;

– домени із спонсорською організацією, функціонування яких забезпечує якась організація, яка репрезентує спільноту, зацікавлену в існуванні цього домену (наприклад: *gov, edu, mil, travel, aero, mobi*) – sponsored TLD, або sTLD;

– домени, що складаються з двох літер та призначаються країнам і територіям у відповідності із міжнародним стандартом ISO 3166-1 (наприклад: *us, UA, uk, md, su*);

– інтернаціоналізовані домени країн, що складаються з символів національних алфавітів (наприклад: *укр*, السعودية, 中国) – internationalized domain names, або IDN ccTLD.

Особливості адміністрування домену UA. В домені UA делегуються приватні та публічні доменні імена [1]. Приватні призначаються для власного використання юридичними та фізичними особами, які мають відповідні зареєстровані знаки для товарів та послуг (згідно [1], таких доменів понад 19000). Публічні призначені для делегування в них піддоменів згідно з правилами, затвердженими адміністратором кожного публічного домену. Більшість публічних доменів є так званими регіональними доменами (наприклад: kiev.ua, kyiv.ua, ternopil.ua). Інші добре відомі – com.ua, net.ua, org.ua, in.ua.

Деякі публічні домени мають спеціальне призначення і особливі правила делегування. До таких належать:

– edu.ua: домени для державних та недержавних освітніх закладів України I-IV рівнів акредитації;

– gov.ua: домени для державних організацій та установ України.

Компоненти системи серверів імен. Технічно всі види TLD функціонують однаково, проте кожен вид має особливості делегування (так зветься процедура утворення доменного імені, нижчого за ієрархією) та адміністрування [9]. В кореневих серверах вказані декілька уповноважених (authoritative) серверів, на яких зберігається інформація про доменні зони вищіх доменів (TLD). Один з серверів DNS є основним (primary, master), інші – допоміжні (secondary, slave). Але цей розподіл ведеться на рівні конфігурації програмного забезпечення серверів. Для "зовнішнього світу" всі вони однаково уповноважені. Для функціонування доменної зони необхідний принаймні один уповноважений сервер.

Розрізняють дві головні функції DNS – зберігання доменних зон та виконання запитів стосовно IP-адрес та імен (резолвінг, resolving) [10], [11].

Виконання запитів робить клієнт DNS – резолвер (resolver). Розподіл на сервери та резолвери досить умовний, бо для виконання деяких запитів сервер DNS може виступати в ролі резолвера, тобто клієнта.

Існують резолвери двох типів:

– stub resolver (клієнтський резолвер) – DNS-клієнт, вбудований в програмне забезпечення рівня застосувань (як правило він є частиною поштових агентів, браузерів і т.ін.); stub resolver формулює DNS-запити;

– recursive resolver (рекурсивний резолвер) – DNS сервер/клієнт, що приймає запити від клієнтських резолверів, та може на виконання цих запитів звертатися до інших серверів DNS (рекурсивна поведінка) або лише повертати посилання – referral – на авторитетні сервери (ітеративна поведінка).

Клієнтський резолвер має адміністративно задану IP-адресу рекурсивного резолвера своєї мережі або провайдера, та надсилає DNS-запити виключно до них. Натомість рекурсивний резолвер завжди виконує кешуючу функцію, тобто запам'ятовує дані, отримані за запитами клієнтів, та тримає їх в спеціальній структурі – кешу – протягом часу, визначеного або в параметрах кожного ресурсного запису (параметр TTL), або для зони в цілому. Кешуються також і негативні результати запитів (наприклад «ресурсний запис не знайдено»). Негативним результатам також присвоюється мінімальний термін кешування. Таким чином, дані, отримані клієнтом, в певний момент часу можуть відрізнятись від справжнього змісту файлу зони. Але ця різниця існуватиме лише протягом часу, визначеного в TTL. Тому керування часом кешування (шляхом встановлення TTL) надається адміністраторові доменної зони, а не адміністраторові рекурсивного резолвера.

Відповідно до протоколу DNS, резолвери взаємодіють між собою за допомогою 4 видів транзакцій.

DNS Query/Response – повідомлення від клієнтського резолверу на адресу авторитетного або рекурсивного резолвера. Він стосується ресурсних записів (RR) певного типу, що мають відношення до певного імені, наприклад стосовно IP-адреси, яка відповідає цьому імені.

Існують рекурсивні та нерекурсивні запити. Рекурсивні запити адресуються рекурсивним резолверам. Від останніх вимагається самостійно визначити авторитетні сервери та виконати пошук відповіді за допомогою нерекурсивних (ітеративних) запитів. Використовується транспортний протокол UDP. Якщо відповідь отримана не повністю, повторний запит має бути надісланий транспортним протоколом TCP, тобто з повноцінним встановленням сесії між клієнтом та сервером.

DNS Notify – звернення від master до всіх slave, що визначені для певного zone file в конфігурації DNS, після змін в цьому zone file. Вторинні сервери повинні ініціювати zone transfer.

Zone Transfer – засіб для вторинного сервера для отримання повного zone file (тобто всіх ресурсних записів водночас) від первинного (master) сервера. Запит ініціюється відповідно до параметра Refresh в SOA, чи за командою DNS Notify.

Dynamic update – засіб для DNS-клієнтів певного виду додавати та вилучати ресурсні записи з zone file. Механізм описаний в [10] та реалізований в Berkeley Internet Name Daemon (BIND) починаючи з версії 8. Зокрема, цей механізм може використовувати DHCP-сервер.

Проблеми безпеки транзакцій DNS. Дефекти в реалізації протоколу DNS дозволяють використовувати його для зловмисних дій [3]. Кожна окрема проблема ускладнюється через велику кількість операційних систем, бібліотек, окремих програмних застосувань, де реалізовано протокол DNS. Ось деякі з них.

DNS Amplification and reflection (підсилення та віддзеркалювання) – це використання відкритого резолвера для збільшення обсягу атак і приховування її справжнього джерела, які зазвичай є інструментами і методами атаки DoS або DDoS. Зловмисники бомбардують револьвер DNS-повідомленнями з використанням підробленого IP-адреса джерела, який є мішенню для атаки. Атаки цих типів використовують кілька DNS револьверів, тому вплив на цільові пристрої збільшуються.

Resource utilization (атаки з використання ресурсів) спрямовані на виснаження програмно-апаратних ресурсів пристрою, на якому реалізовано резолвер: центральний процесор, пам’ять, буфери сокетів. Ці типи атак намагаються поглинути всі наявні ресурси, щоб негативно вплинути на операції резолвера.

DNS cache poisoning (отруєння кешу DNS) відбувається, коли зловмисник відправляє інформацію про фальсифіковану RR до DNS резолвера. Після того, як DNS резолвер отримує інформацію про фальсифіковану RR, вона зберігається в кеші DNS для часу життя (TTL) встановленого в RR. Зловмисники використовують цю техніку підміни RR, зокрема, для перенаправлення користувачів із законних сайтів на шкідливі сайти.

Дві перші атаки використовують відкриті резолвери, тобто такі, запити до яких може надіслати будь-який хост. Реалізація атак призводить до порушення доступності даних DNS. Останній тип атак спрямований на порушення цілісності і несе найбільшу загрозу для користувачів.

Застосування технології DNSSEC для захисту цілісності транзакцій. Для захисту клієнтів від отримання фальшивих даних, тобто для захисту транзакцій у напрямку сервер-клієнт, існує та активно впроваджується механізм DNSSEC (The Domain Name System Security Extensions) [4], [5], [6]. Згідно доктрини DNSSEC, кожна відповідь серверу повинна мати цифровий підпис. Верифікуючи цей підпис, резолвер з’ясовує, чи є отримана інформація ідентичною до тієї, що розташована на авторитетному сервері. Таким чином, DNSSEC забезпечує автентифікацію сервера, цілісність даних при передачі, але не їхню конфіденційність: відповіді DNS не шифруються. Для функціонування DNSSEC було застосовано нові типи ресурсних записів, серед яких запис типу RRSIG. Запис містить дані про підпис.

Резолвер, який здатний перевіряти підписи, називають validating resolver. Перш ніж перевіряти отриману дані за допомогою відкритого ключа, що знаходиться в цифровому підписі, резолвер має встановити довіру до цього ключа, тобто побудувати довірчий ланцюжок. Для цього резолвер розглядає список відомих йому довіренних ключів (trust anchors), та будує послідовність відомих йому ключів (ланцюжок довіри), за допомогою якої встановлює довіру до нового отриманого.

Для побудови ланцюжка використовується ієрархічний простір доменних серверів. Trust anchors отримуються не за допомогою транзакцій DNS, а постачаються безпосередньо в конфігурації програмного забезпечення DNSSEC і містять ключі кореневих серверів DNS.

Стан впровадження DNSSEC в світі та в домені UA. Широкому впровадженню DNSSEC, що почалось з підписання кореневої зони у 2010 році, передувала низка проблем, що мали бути вирішені. Основною зміною, пов'язаною з впровадженням DNSSEC в кореневій зоні, є істотне збільшення розміру відповіді на запит клієнта. Великі DNS-відповіді очікують різні небезпеки: це і фрагментація пакетів на шляху їх слідування, неможливість їх складання клієнтом, або фільтрація пакетів, що перевищують по довжині історичні 512 байт. Іншими словами, при значному збільшенні розміру відповідей зростає ризик, що клієнт не зможе

отримати відповідь на запит до кореневого сервера. Тому впровадження DNSSEC на кореневих серверах відбувалось поступово, разом із спостереженнями, та тривало 6 місяців [1].

На березень 2017 р. за даними [7] в кореневій доменній зоні присутні 1530 TLD, з них 1376 підписані за технологією DNSSEC, тобто, їхні trust anchors опубліковано в кореневій зоні.

За даними VeriSign Labs [8] вже в понад 1600000 доменних зонах в світі впроваджено DNSSEC і вони підтримують валідацію. Більшість адміністраторів TLD та провідні реєстратори доменів за даними ICANN [9] підтримують валідацію.

Серед підписаних TLD присутній і домен України – UA. Роботи з включення DNSSEC в домені було завершено ще в червні 2012 року [1], коли в кореневу зону було включено trust anchor домену UA (див. рис.1).

```
domain:   UA
ds-rdata: 56514 10 2
  bdd7a310534f76b2b6b25c94f816f9b9f260a2e35f526a9287e3307fb2cd16d8
```

Рисунок 1 – Trust anchor домену UA в кореневій доменній зоні

Факт наявності DS домену .UA в кореневій зоні означає, що всі записи доменної зони UA можуть бути валідовані, тобто захищено цілісність відповідей на DNS-запити та автентифіковано джерело відповідей. Однак, доменна зона UA містить в основному записи, які стосуються делегування приватних та публічних доменів 2-го рівня.

Згідно [1], станом на березень 2017 року лише незначна кількість доменів другого рівня в доменній зоні UA підписано з використанням DNSSEC – не більше двох десятків, тобто 0,1%. Серед 63 публічних доменів підписані лише наступні географічні домени:

chernovtsy.ua	khmelnitskiy.ua	rovno.ua
chernivtsi.ua	km.ua	rivne.ua
cv.ua		rv.ua

Не підписано також і домен для для державних організацій та установ України *gov.ua*.

Адміністратор домену UA підтримує внесення DNSSEC записів в зону в ручному режимі, та завершує модернізацію програмного комплексу взаємодії з реєстраторами для автоматизації ведення записів, пов’язаних з технологією DNSSEC.

Зауважимо, що Україні делеговано також IDN-домен верхнього рівня *укр*. На час написання даної роботи в кореневій доменній зоні відсутній trust anchor цього домену, отже він не був підписаний за технологією DNSSEC.

Розглянемо зворотну сторону – чи підтримують DNSSEC клієнтські резолвери, тобто, чи проводять вони валідацію відповідей DNS. Проект APNIC Labs [10] збирає та публікує дані, згідно яких 22% DNS-запитів з українських мереж – з валідацією. Для порівняння зведемо дані по сусідніх країнах у табл. 2.

Таблиця 2 – Відсоток валідованих DNS-запитів по деяких країнах Європи та Азії

№ з/с	Країна	% валідованих DNS запитів
1	Норвегія	81,2
2	Швеція	75,9
3	Чехія	35,9
4	Азербайджан	31,5
5	Польща	29,4
6	**Україна**	**22,2**
7	Росія	16,1
8	Словаччина	13,7
9	Угорщина	10,9
10	Казахстан	7,43

Причини повільного впровадження DNSSEC. Тотальне впровадження DNSSEC ”згори” вважається технологічно неприйнятним. Ініціатива має надходити від адміністраторів доменів нижчого рівня до верхнього.

Серед відомих проблем, що перешкоджають більш широкому впровадженню DNSSEC не лише в Україні, але й в світі, найчастіше згадуються наступні:

- відсутність масового розуміння технології DNSSEC через її відносну складність;
- додаткові витрати операторів телекомунікацій та провайдерів послуг на адміністрування;
- відсутність готових рішень валідуючого резолвера для інтернет-користувача, які б постачались разом з обладнанням, операційними системами, браузерами;
- відсутність підтримки DNSSEC в обладнанні операторського рівня.

Висновки. Технологія DNSSEC призначена для захисту цілісності DNS-відповідей та автентифікації їхніх джерел і на сьогодні є важливою складовою інформаційної безпеки. Відносна складність технології та відсутність готових рішень на рівні інтернет-користувачів стримують темпи впровадження DNSSEC.

В домені верхнього рівня UA підтримується валідація, trust anchor внесено в кореневу доменну зону, а для доменів другого рівня в домені UA нема адміністративних чи технічних перепон для впровадження технології DNSSEC, яка дозволить виконання автентифікації DNS-серверів та валідації DNS-відповідей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Доменна статистика .UA за підсумками січня 2017 року. [Електронний ресурс]. Доступно: https://hostmaster.ua/news/?stat201701. Дата звернення: Берез. 28, 2017.

[2] DNS Best Practices, Network Protections, and Attack Identification. [Online]. Available: http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html. Accessed on: Mar. 20, 2017.

[3] R. Arends, R. Austein, M. Larson, D. Massie and S. Rose, “DNS Security Introduction and Requirements”. [Online]. Available: https://www.ietf.org/rfc/rfc4033.txt. Accessed on: Mar. 20, 2017.

[4] R. Arends, R. Austein, M. Larson, D. Massie and S. Rose, “Resource Records for the DNS Security Extensions”. [Online]. Available: https://www.ietf.org/rfc/rfc4034.txt. Accessed on: Mar. 21, 2017.

[5] ICANN Research. TLD DNSSEC Report. [Online]. Available: http://stats.research.icann.org/dns/tld_report/. Accessed on: Mar. 20, 2017.

[6] SecSpider Global DNSSEC deployment tracking. [Online]. Available: http://secspider.verisignlabs.com/stats.html. Accessed on: Mar. 18, 2017.

[7] Deploying DNSSEC. [Online]. Available: https://www.icann.org/resources/pages/deployment-2012-02-25-en. Accessed on: Mar. 20, 2017.

[8] DNSSEC Validation Rate by country. [Online]. Available: http://gronggrong.rand.apnic.net/cgi-bin/worldmap. Accessed on: Mar. 20, 2017.

[9] Internet Assigned Numbers Authority. Domain Name Services. [Online]. Available: https://www.iana.org/domains. Accessed on: Mar. 24, 2017.

[10] P. Vixie, S. Thomson, Y. Rekhter and J. Bound, “Dynamic Updates in the Domain Name System (DNS UPDATE)”. [Online]. Available: https://www.ietf.org/rfc/rfc2136.txt. Accessed on: Mar. 20, 2017.

[11] R. Arends, R. Austein, M. Larson, D. Massie and S. Rose, “*Protocol Modifications for the DNS Security Extensions”*. [Online]. Available: https://www.ietf.org/rfc/rfc4035.txt. Accessed on: Mar. 26, 2017.

Стаття надійшла до редакції 30 березня 2017 року.

REFERENCE

[1] .UA Domain Statistics by January 2017 summary. [Online]. Available: https://hostmaster.ua/news/?stat201701. Accessed on: Mar. 28, 2017.
[2] DNS Best Practices, Network Protections, and Attack Identification. [Online]. Available: http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html. Accessed on: Mar. 20, 2017.
[3] R. Arends, R. Austein, M. Larson, D. Massie and S. Rose, "DNS Security Introduction and Requirements". [Online]. Available: https://www.ietf.org/rfc/rfc4033.txt. Accessed on: Mar. 20, 2017.
[4] ICANN Research. TLD DNSSEC Report. [Online]. Available: http://stats.research.icann.org/dns/tld_report/. Accessed on: Mar. 20, 2017.
[5] SecSpider Global DNSSEC deployment tracking. [Online]. Available: http://secspider.verisignlabs.com/stats.html. Accessed on: Mar. 18, 2017.
[6] SecSpider Global DNSSEC deployment tracking. [Online]. Available: http://secspider.verisignlabs.com/stats.html. Accessed on: March 18, 2017.
[7] Deploying DNSSEC [Online]. Available: https://www.icann.org/resources/pages/deployment-2012-02-25-en. Accessed on: Mar. 20, 2017.
[8] DNSSEC Validation Rate by country. [Online]. Available: http://gronggrong.rand.apnic.net/cgi-bin/worldmap. Accessed on: Mar. 20, 2017.
[9] Internet Assigned Numbers Authority. Domain Name Services. [Online]. Available: https://www.iana.org/domains. Accessed on: Mar. 24, 2017.
[10] P. Vixie, S. Thomson, Y. Rekhter and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)". [Online]. Available: https://www.ietf.org/rfc/rfc2136.txt. Accessed on: Mar. 20, 2017.
[11] R. Arends, R. Austein, M. Larson, D. Massie and S. Rose, "*Protocol Modifications for the DNS Security Extensions"*. [Online]. Available: https://www.ietf.org/rfc/rfc4035.txt. Accessed on: Mar. 26, 2017.

ВИТАЛИЙ ЗУБОК

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ DNSSEC ДЛЯ ЗАЩИТЫ ДОМЕННЫХ ИМЕН В УКРАИНСКОМ СЕГМЕНТЕ СЕТИ ИНТЕРНЕТ

Система доменных имен является неотъемлемой частью адресации в сети Интернет. Дефекты в реализации протокола DNS позволяют использовать его для злонамеренных действий, во время которых может быть нарушена целостность и доступность данных при обмене данными между DNS-клиентом и DNS-сервером. Технология DNSSEC, которая предназначена для защиты целостности при обмене данными DNS, предотвращает получение фальшивых данных DNS-клиентами. Технология заключается в том, что каждый ответ сервера DNS должна иметь электронную цифровую подпись, которую можно проверить через сервер DNS более высокого уровня. Хотя DNSSEC активно внедряется в течение 10 лет, полному переходу на DNSSEC мешают относительная сложность настройки доменных зон и отсутствие готовых решений уровня Интернет-пользователя. В статье представлены современное состояние, сравнительный анализ, проблемы и перспективы внедрения этой технологии для защиты информационных ресурсов, адреса которых находятся в доменном пространстве домена UA. Результаты анализа свидетельствуют, что в домене верхнего уровня UA поддерживается валидация, trust anchor домена UA внесены в корневую доменную зону, а следовательно, для доменов второго уровня в домене UA не существует административных или технических препятствий для внедрения технологии DNSSEC. Ее использование позволит обеспечить выполнение автентификации DNS-серверов и валидации DNS-ответво. Однако, относительная сложность технологии и отсутствие готовых решений на уровне интернет-пользователей сдерживают темпы внедрения DNSSEC. В тоже время это обусловлено

дополнительными расходами операторов телекоммуникаций и провайдеров услуг администрирования, а также отсутствием поддержки DNSSEC оборудованием операторского уровня.

Ключевые слова: безопасность информационных ресурсов, система доменных имен, валидация доменов, DNSSEC, защита DNS-тарнзакций.

VITALII ZUBOK

USE OF DNSSEC TECHNOLOGY FOR DOMAIN NAMES PROTECTION IN THE UKRAINIAN SEGMENT OF THE INTERNET

The domain names system is an integral part of addressing in the Internet. Defects in the implementation of the DNS protocol allow to use it for malicious actions, during which the integrity and availability of data when exchanging data between the DNS client and the DNS server may be affected. DNSSEC technology, designed to protect the integrity of the DNS data exchange, prevents DNS clients from receiving false data. The base of technology is that every DNS server response must have an electronic digital signature that can be verified through a higher level DNS server. Although DNSSEC has been actively deployed for 10 years, the complete transition to DNSSEC is hampered by the relative complexity of setting up domain zones and the lack of ready-made user-level decisions. The article presents the current state, comparative analysis, problems and prospects of the implementation of this technology for the protection of information resources, the addresses of which are in the UA domain. The analysis results indicate that the validation is supported in UA domain, the trust anchor of the UA domain is recorded into the root domain zone, and therefore, for second level domains in the UA domain there are no administrative or technical barriers for the implementation of the DNSSEC technology. Its use will allow performing DNS server authentication and validating DNS responses. However, the relative complexity of the technology and the lack of ready solutions at the level of Internet users hamper the pace of implementation of DNSSEC. At the same time, this is due to the additional costs of telecommunications operators and service providers for administration, as well as the lack of support for DNSSEC in carrier-grade equipment.

Keywords: security of information resources, domain name system, domain validation, DNSSEC, DNS transactions security.

Віталій Юрійович Зубок, кандидат технічних наук, доцент кафедри кібербезпеки та захистосування автоматизованих інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: vit@visti.net.

Виталий Юрьевич Зубок, кандидат технических наук, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Vitalii Zubok, candidate of technical sciences, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.