личности, что значительно повышает эффективность кибербезопасности информационных систем сектора критической инфраструктуры.

Ключевые слова: несанкционированный доступ, информационные системы, биометрическая аутентификация, инженерия закономерностей, нечеткая логика.

FUZZY AUTHENTICATION MODEL FOR USERS OF SPECIAL PURPOSE INFORMATION SYSTEMS BASED ON BEHAVIORAL BIOMETRICS

The article deals with the urgent scientific problem of protecting information systems of the critical infrastructure sector from unauthorized access. The author proposes a model for the authentication of users of information systems based on the use of behavioral biometrics and the mathematical apparatus of the theory of fuzzy logic. The essence of the proposed approach is, first of all, to construct a user profile of the system based on the engineering of behavioral patterns (frequent dependencies) from a set of investigated parameters, which quite fully reflect its inherent subconscious characteristics during the reproduction of the process to be authenticated. Secondly, the problem of fuzzy authentication of system users is reduced to determining the level of compliance of their behavioral characteristics with the existing profile based on the analysis of a set of investigated parameters in conditions of some fuzziness and inaccuracy of control information. The presented model makes it possible to identify subconscious behavioral traits inherent in a particular user that are present in different psychoemotional states, in turn, it allows you to get rid of many descriptions of the states of each account and reduce the number of false positives in the process of identity authentication, which significantly increases the efficiency of cybersecurity of information systems in the critical infrastructure sector.

Keywords: unauthorized access, information systems, biometric authentication, engineering of laws, fuzzy logic.

Фесьоха Віталій Вікторович – доктор філософії у галузі Інформаційні технології, старший викладач кафедри Комп'ютерних інформаційних технологій Військового інституту телекомунікацій та інформатизації імені Героїв Крут.
E-mail: vitaliifesokha@gmail.com.
Orcid ID: 0000-0001-6612-1970.

Фесёха Виталий Викторович – доктор философии в области Информационные технологии, старший преподаватель кафедры Компьютерных информационных технологий Военного института телекоммуникаций и информатизации имени Героев Крут.

Vitalii Fesokha – PhD in Information Technologies, Senior lecturer of the Department of Computer Information Technologies of the Military Institute of Telecommunications and Information Technologies named after the Heroes of Kruty.

Фесьоха Надія Олександрівна – викладач кафедри Комп'ютерних інформаційних технологій Військового інституту телекомунікацій та інформатизації імені Героїв Крут.
E-mail: nadya_viti@i.ua.
Orcid ID: 0000-0002-9797-5589.

Фесёха Надежда Александровна – преподаватель кафедры Компьютерных информационных технологий Военного института телекоммуникаций и информатизации имени Героев Крут.

Nadiia Fesokha – lecturer of the Department of Computer Information Technologies of the Military Institute of Telecommunications and Information Technologies named after the Heroes of Kruty.

DOI: 10.18372/2410-7840.23.15431
УДК 004.056.53

АНАЛІЗ ДОСЛІДЖЕНЬ З РОЗГОРТАННЯ DNSSEC В ІНТЕРНЕТІ

Тетяна Приходько

Система доменних імен є невід'ємною частиною адресації в мережі Інтернет. Недоліки 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. Для захисту цілісності при обміні даними DNS призначена технологія DNSSEC, яка запобігає отриманню фальшивих даних DNS-клієнтами. В статті досліджується сучасний стан використання технології розширення безпеки системи доменних імен DNSSEC та розглядаються питання попиту на вивчення показників з розгортання протоколу DNSSEC і проблеми, що наразі існують з отриманням максимально повного уявлення про масштаби розгортання даного протоколу в Інтернеті. DNSSEC дозволяє власникам доменних імен використовувати метод цифрового підпису інформації, яку вони вносять в систему доменних імен DNS. Це забезпечує захист споживачів, так як дані DNS, які піддалися спотворенню, випадково або зі злим умислом, до них не доходять. Питання, яке вирішує DNSSEC: Чи можна довірятися відповіді DNS? З 2010 року була забезпечена можливість використання підпису DNSSEC на самому верхньому рівні DNS,

який називається кореневим, що істотно полегшує глобальне розгортання DNSSEC. Однак навіть десять років по тому темпи впровадження DNSSEC як і раніше залишаються низькими. В статті подано сучасний стан, порівняльний аналіз, проблеми та перспективи впровадження цієї технології для захисту інформаційних ресурсів. 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 та в реєстраторів доменних імен. Безпека DNS повинна бути невід'ємною частиною плану по забезпеченню безпеки усіх користувачів Інтернет, оскільки система, основним завданням якої є перетворення імен мережевих вузлів в IP-адреси, використовуються буквально всіма додатками і службами в мережі.

***Ключові слова**: безпека інформаційних ресурсів, кібербезпека, DNS, DNSSEC, TLD, gTLD, домен, доменна зона, ICANN.*

ВСТУП

Система доменних імен (англ. Domain Name System, далі DNS) щодня використовується всіма, від приватних користувачів до державних органів влади, які підключаються до Інтернету, і майже всіма пристроями в Інтернеті. Технологія була створена задовго до того, як хто-небудь взагалі почав думати про мережеву безпеку. DNS працює без автентифікації і шифрування, тобто наосліп обробляє запити будь-якого користувача.

З моменту її створення в 1983 році технологія все ще залишається вкрай вразливою до атак. Зокрема, на здатність зловмисників фальсифікувати відповіді на запити до DNS, тим самим дозволяючи перенаправляти кінцевих користувачів на веб-сайти під своїм контролем.

Для розв'язання проблеми зовнішніх атак використовується розширення системи безпеки доменних імен для протоколу DNS (англ. Domain Name System Security Extensions, далі DNSSEC).

Метою роботи є дослідження сучасного стану використання технології DNSSEC та попиту на дослідження масштабів розгортання даної технології в Інтернеті.

Існує так звана стратегія «глибокого захисту» (defense in depth), яка може поліпшити безпеку всієї системи, тому що організована таким чином, щоб у разі збою одного рівня захисту можна було використовувати інший рівень захисту, так як вона передбачає кілька незалежних рівнів. Розширення системи безпеки доменних імен DNSSEC може бути одним з цих рівнів глибокого захисту Інтернету. Поліпшення безпеки інтернету вимагає розгортання DNSSEC у всіх доменах верхнього рівня (англ. top-level domain, далі TLD) [1].

Ще на конференції Nordunet 2012 у презентації щодо DNSSEC було твердження, що понад 80% доменів можуть використовувати DNSSEC, якщо їх власники так вважатимуть за потрібне [2,9]. Це швидке зростання розгортання DNSSEC вже на вересень 2012 року, порушило багато питань щодо загального стану розгортання DNSSEC в Інтернеті і супутніх проблем, пов'язаних з розгортанням.

На кінець 2020 року Інтернет-корпорація з присвоєння імен і номерів (англ. Internet Corporation for Assigned Names and Numbers, далі ICANN) повідомила, що розширення безпеки системи доменних імен DNSSEC тепер розгорнуте у всіх 1195 існуючих доменах загального користування (англ. generic Top-Level Domain, gTLD).

Не дивлячись на широке розповсюдження DNSSEC на рівні Адміністраторів публічних доменів (особа, що здійснює заходи з адміністративного супроводу публічного домену та забезпечення його працездатності) доменних зон, впровадження в Інтернеті вимагає великих зусиль.

У міру того як Адміністратори публічних доменів починають підтримувати DNSSEC, Реєстратори доменів (особа, що надає послуги з реєстрації та супроводу доменного імені) також мають докладати зусилля в цьому напрямку для доменних імен, зареєстрованих через них, як і провайдери Інтернет повинні включити DNSSEC-валідацію на тих своїх Резолверах (DNS-сервери провайдерів), які обробляють запити до DNS.

Хоча застосування DNSSEC не вирішує всі проблеми захисту мережі Інтернет, технологія допомагає інтернет-користувачам добиратися до необхідного ресурсу і запобігає так званій «атаці посередника», де користувача, без його відома, направляють на потенційно шкідливий сайт. DNSSEC застосовується на додаток до інших технологій, таких як TLS (захист транспортного рівня, метод, зазвичай використовується в HTTPS), які захищають зв'язок між кінцевим користувачем і доменом [3].

Авжеж, спеціалістами в сфері мережевої безпеки були виявлені та наведені основні компоненти безпеки DNS, серед яких і посилення безпеки за рахунок захищеності серверів та створення шаблонів введення в експлуатацію; і аналітика та звітність за рахунок ведення журналів подій; і кіберрозвідка та виявлення загроз за рахунок вивчення та аналізу отриманих аналітичних даних про загрози з загальнодоступних джерел; і впровадження удосконалених протоколів DNSSEC, DoT та DoH. Але, чи можна виміряти, наскільки добре розповсюджене використання DNSSEC?

Яка кількість DNS-resolvers (комп'ютери / сервери, які провайдери використовують для пошуку конкретного вузла, запитуваного користувачем, коли дані отримані, користувач перенаправляється на відповідну IP-адресу) наразі виконує перевірку DNSSEC доменного імені? Яка кількість користувачів Інтернету користуються цими засобами? Ці питання дедалі стають вкрай важливими.

Тож безпека DNS повинна бути невід'ємною частиною плану по забезпеченню безпеки, оскільки система, основним завданням якої є перетворення імен мережевих вузлів в IP-адреси, використовуються буквально всіма додатками і службами в мережі.

Про актуальність проведення досліджень свідчить опублікований ICANN запит пропозицій, щодо пошуків підрядника, здатного досліджувати масштаби розгортання DNSSEC у Інтернеті [4], а саме, вивчати академічні та галузеві публікації, знаходити і фіксувати різні методології та показники, які використовуються для вимірювання всіх аспектів розгортання DNSSEC та готувати рекомендації за показниками, які дають максимально повне уявлення про масштаби розгортання DNSSEC.

Постає питання, чого варті системи захисту, що наразі використовуються багатьма державними та приватними організаціями або приватними особами, коли на рівні DNS захист відсутній?

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У відповідь на загрози, пов'язані з вразливістю DNS, міжнародна організація зі стандартизації (англ. Internet Engineering Task Force, далі IETF) розробила DNSSEC - засіб для перевірки цілісності DNS-запитів. Іншими словами, DNSSEC може дати впевненість в тому, що відповідь на ваш DNS-запит не підроблена. Впровадження DNSSEC є не тільки кращою галузевої практикою, але також ефективно допомагає уникнути більшості атак на DNS.

Короткий опис роботи DNS. Щоб зрозуміти як працюють DNS-атаки та протокол системи безпеки доменних імен DNSSEC важливо мати загальне розуміння як працює система доменних імен DNS.

Кожна відвідана веб-сторінка, кожен надісланий електронний лист, кожна картинка чи відео, що отримані із соціальних мереж: усі ці взаємодії використовують DNS для перетворення зручних для людини доменних імен на відповідні йому IP-адреси, що необхідні серверам, маршрутизаторам та іншим мережевим пристроям для перенаправлення трафіку через Інтернет до потрібного місця призначення.

Наведено відповідь на запит мережевою командою *host* до доменного імені *icann.org*, офіційний сайт корпорації ICANN, який ми можемо використати як приклад:

icann.org has address 192.0.43.7
icann.org has IPv6 address 2001:500:88:200::7
icann.org mail is handled by 10 pechora1.icann.org.
icann.org mail is handled by 10 pechora5.icann.org.
icann.org mail is handled by 10 pechora3.icann.org.
icann.org mail is handled by 10 pechora4.icann.org.

Бачимо відповідність назві сайту *icann.org* адрес серверу *192.0.43.7 та 2001:500:88:200::7*, де реально знаходиться цей сайт. Використання Інтернету на будь-якому пристрої починається з

DNS, коли користувач вводить ім'я веб-сайту у браузері на своєму телефоні або ноутбуці, браузер, в свою чергу, за допомогою DNS-client, який є частиною операційної системи пристрою, передає запит до DNS-resolver. DNS-resolver, в свою чергу, у відповідь на запит DNS-client, має надсилати власні запити DNS, як правило, на кілька різних авторитативних серверів імен. Коли DNS-resolver надсилає запит до авторитетного сервера імен, він не має можливості перевірити справжність відповіді. DNS-resolver може перевірити лише те, що відповідь надходить із тієї самої IP-адреси, куди DNS-resolver надіслав оригінальний запит. Але покладатися на IP-адресу джерела відповіді - це ненадійний механізм перевірки достовірності даних. Закладена структура DNS не дозволяє розпізнати підроблену відповідь на один зі своїх запитів. Інакше кажучи, зловмисник може направити користувача на потенційно шкідливий сайт, а користувач цього просто не помітить.

Слід також звернути увагу і на те, що для прискорення роботи DNS-resolvers в своєму в кеші зберігають дані DNS, які вони отримують від авторитативних DNS-серверів. Час, протягом якого DNS-resolver зберігає запис, називається TTL (time to live). Якщо DNS-client надсилає запит на отримання даних DNS, що знаходяться в кеші DNS-resolver, то останній може відповісти негайно, без затримки, пов'язаної з необхідністю спочатку відправити запит одному або декільком авторитативним серверам. Однак у використання можливостей кешування є і зворотна сторона: якщо зловмисник відправляє підроблену відповідь DNS, яку попередньо було прийнято DNS-resolver, то це призводить до отруєння кеша. Після цього DNS-resolver починає повертати шахрайські дані DNS іншим, хто робить запит до вже скомпрометованої адреси.

Робота над пошуком рішення проблеми недостатньої надійності механізмів перевірки автентичності в DNS почалася в далеких 1990-х роках, її результатом став протокол DNSSEC, який дозволяє підвищити надійність перевірки автентичності в DNS за допомогою цифрових підписів, заснованих на криптографії відкритого ключа. При використанні DNSSEC не запити і відповіді DNS підписуються ключем, а самі дані DNS підписуються власником цих даних.

Застосування DNSSEC дозволяє забезпечити дві важливі функції в DNS:

- Перевірка справжності джерела даних дозволяє DNS-resolver перевірити, чи дійсно отримані дані надійшли з тієї зони, звідки, як він вважає, вони мають бути.
- Перевірка цілісності даних дозволяє DNS-resolver перевірити, чи не були ці дані змінені під час передачі, після того як власник зони підписав їх закритим ключем цієї зони.

Як привести DNSSEC в дію? Для правильної роботи протоколу DNSSEC повинні бути задіяні обидві його сторони: публікація, яка виконується власниками доменів, і пошук, який зазвичай виконується мережевими операторами, такими як інтернет-провайдери. Щоб від DNSSEC була користь, їх повинні використовувати обидві сторони [5].

Власники доменів, відповідальні за публікацію даних DNS, повинні забезпечити підписання своїх даних DNS за допомогою DNSSEC, для цього необхідно включити DNSSEC-підпис на своїх DNS-серверах (або у своїх реєстраторів) і передати реєстратору інформацію, що називається DS-записом.

Мережевим операторам потрібно всього лише включити перевірку DNSSEC на Резолверах, які обробляють DNS-запити для користувачів. Програмне забезпечення Резолверів все частіше включає перевірку DNSSEC за замовчуванням.

Тож здається, що для повноцінного розгортання DNSSEC потрібно виконати досить чіткі і на перший погляд прості завдання, оператори мережі мають здійснити включення перевірки DNSSEC, а власники доменів мають додати цифровий підпис до використовуваних ними імен.

То чому ж загальносвітовий рівень впровадження DNSSEC, який був розроблений понад 20 років назад, ледь досяг 25%, згідно статистичного аналізу регіонального інтернет-реєстратора APNIC (Азіатсько-Тихоокеанський мережевий інформаційний центр).

Відповісти на це питання можливо, попередньо дослідивши масштаби розгортання DNSSEC у Інтернеті, починаючи з моменту запуску до сьогодення, проаналізувавши причини гальмування, що пов'язані з тими чи іншими технічними, економічними та адміністративними аспектами, як на рівні держав так і світовому рівні. Щодо держав, як приклад державного регулювання питань розповсюдження DNSSEC в Україні, слід згадати Постанову Кабміну від 12 червня 2019 р. № 493 «Про внесення змін до деяких постанов Кабінету Міністрів України щодо функціонування офіційних веб-сайтів органів виконавчої влади», в загальних положеннях якої наведено наступне: «Офіційний веб-сайт (веб-портал) органу виконавчої влади та офіційні веб-ресурси, що пов'язані з діяльністю органу виконавчої влади (далі - офіційний веб-сайт), повинні бути розміщеними в домені GOV.UA та у разі потреби у домені .УКР.

Домен, на якому розміщений офіційний вебсайт, повинен бути підписаний із застосуванням технології захисту доменних імен DNSSEC».[6]. Провести вимірювання для отримання відповіді, яка ж кількість офіційних веб-ресурсів використовує технологію, цілком можливо, просто порахувавши кількість підписаних доменних імен в доменній зоні.

Таку інформацію може відслідкувати Реєстр відповідної доменної зони. Тобто окремі Реєстри зони можуть зробити висновок про кількість використання DNSSEC у своїй локальній зоні, шляхом реєстрації записів DS (RR). Але складання загальної картини розповсюдження DNSSEC в усьому Інтернеті є більш складним завданням.

Проблематика пов'язана в знаходженні кількісного показника, в основі якого є питання кількості підписаних зон, кількості перевірених запитів, кількості DNS-resolvers з підтримкою DNSSEC, кількості користувачів.

Кожне з наведених кількісних питань не має простої відповіді, це залежить як від технічних факторів, так і від фінансових та адміністративних, як на рівні державному так і на рівні приватних підприємств, уповноважених на запровадження DNSSEC на своїх рівнях.

Якщо ж звернутись до пропорції, а не до абсолютної кількісті, то, можливо розглянути способи отримання відповідей. Таким чином перейдемо від питання «яка кількість?» до «яка частка?», і переформулюємо:

- Яка частка DNS-resolver підтримує DNSSEC?

- Яка частка користувачів використовує DNSSEC і де ці користувачі?

Ці питання стосуються кінцевих користувачів та цілісності служби, що надається кінцевим користувачам, а не про доменні зони як такі. Іншими словами, це питання щодо використання DNSSEC на відміну від питань про те, скільки доменів підписані DNSSEC. В економічному плані можна сказати, що це погляд в сторону попиту, а не на пропозицію DNSSEC [2]. Проаналізувати частку та місцезнаходження наразі можемо завдяки статистиці, яку збирає APNIC. З другого кварталу 2019 року кількість validating користувачів зросла з 12% до 22%, майже до подвоєння. В цілому близько 68% користувачів не виконують жодної перевірки DNSSEC в даний час, порівняно з 86%, коли це вимірювання розпочалось у 2013 році [7].

Якщо в цифрах, то рівень перевірки DNSSEC загальносвітовий наведено на рис.2, та огляд у процентному співвідношенні країн Східної Європи наведено на рис.3, де Україна має третю позицію по розповсюдженню DNSSEC.

З наведеного, кількість користувачів DNSSEC зростає, але цього недостатньо, щоб уникнути атак, таких як серія міжнародних кампаній по захопленню DNS в 2018 і 2019 роках, що привела до появі першої в світі Директиви з надзвичайних ситуацій Агентства США з кібербезпеки і безпеки інфраструктури (US-CERT) і підштовхнула ICANN до повторного призову до всіх зацікавлених сторін повністю розгорнути DNSSEC [5].

Вже в травні 2021 року Інтернет-корпорація ICANN опублікувала запит пропозицій (RFP), щоб знайти підрядника, здатного досліджувати масштаби розгортання DNSSEC в Інтернеті [8].

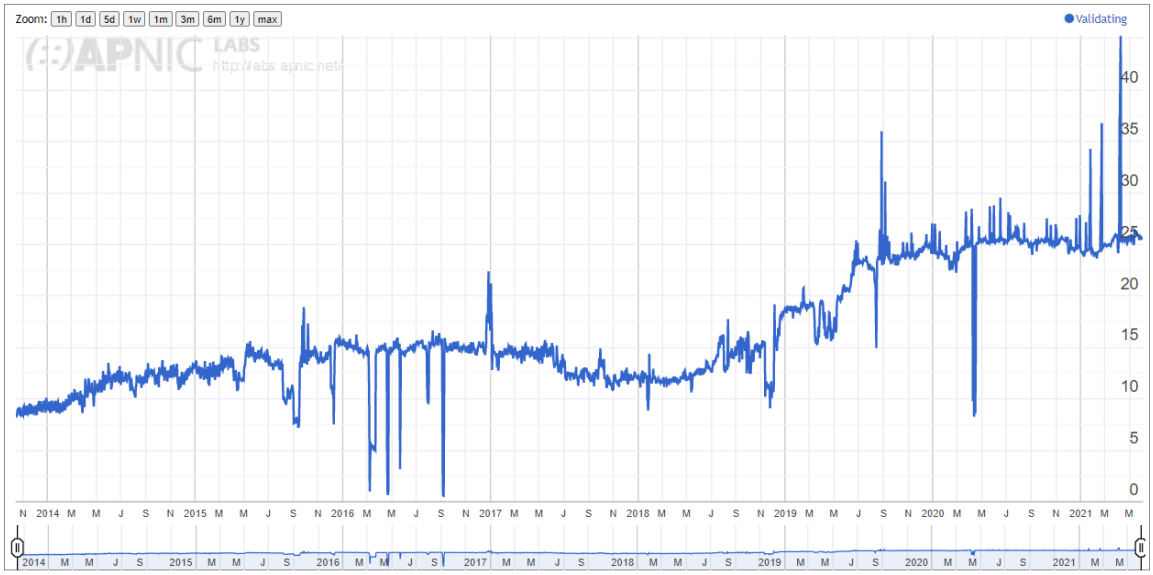

Рис.1 Швидкість перевірки DNSSEC до травня 2021 року. Графік отримано з офіційного ресурсу регіонального інтернет-реєстратора APNIC (Азіатсько-Тихоокеанський мережевий інформаційний центр).

Робота охоплює такі завдання:

1. Вивчення академічної та галузевої літератури, пов'язаної з розгортання розширень безпеки DNS (DNSSEC).

2. Пошук і документування різних технік та показників, що використовуються для вимірювання DNSSEC розгортання, включаючи підписання, перевірку та будь-які інші відповідні заходи. Як метрику можна вказувати абсолютне значення, коефіцієнт або інший відповідний параметр.

3. Проаналізувати задокументовані метрики та рекомендувати, які метрики повинна мати організація ICANN, щоб отримати найбільш повне уявлення про стан розгортання DNSSEC.

4. Підготувати вичерпний звіт, в якому деталізувати висновки, включаючи детальну бібліографію усіх джерел, до яких звертались.

Code	Region	DNSSEC Validates
XA	World	25.43%
XE	Europe	34.52%
XC	Americas	30.20%
XF	Oceania	30.09%
XD	Asia	22.19%
XB	Africa	21.67%
XG	Unclassified	1.13%

Рис.2 Рівень перевірки DNSSEC по світу та регіонах. Вибірку отримано з офіційного ресурсу регіонального інтернет-реєстратора APNIC (Азіатсько-Тихоокеанський мережевий інформаційний центр).

Повний текст запиту до світової спільноти, зацікавленої в забезпеченні стабільної, безпечної та відмовостійкої екосистеми DNS було опубліковано в документі Project Overview for the DNSSEC Deployment Metrics Research RFP [8].

CC	Country	DNSSEC Validates
CZ	Czech Republic, Eastern Europe, Europe	71.03%
PL	Poland, Eastern Europe, Europe	53.00%
UA	Ukraine, Eastern Europe, Europe	36.38%
RU	Russian Federation, Eastern Europe, Europe	30.10%
BG	Bulgaria, Eastern Europe, Europe	27.89%
SK	Slovakia, Eastern Europe, Europe	18.77%
MD	Republic of Moldova, Eastern Europe, Europe	10.57%
HU	Hungary, Eastern Europe, Europe	10.46%
BY	Belarus, Eastern Europe, Europe	10.39%
RO	Romania, Eastern Europe, Europe	5.41%

Рис.3 Рівень перевірки DNSSEC країн Східної Європи. Вибірку отримано з офіційного ресурсу регіонального інтернет-реєстратора APNIC (Азіатсько-Тихоокеанський мережевий інформаційний центр)

Після всебічного аналізу згідно завдань, що опубліковані ICANN, можливо буде виявити місця гальмування в розгортанні DNSSEC і вибудувати стратегії щодо подальших дій, для прискорення впровадження DNSSEC в Інтернеті.

ВИСНОВКИ

За результатами дослідження сучасного стану використання технології DNSSEC можна зробити висновок, що впровадження даної техноло-

гії в Інтернеті вимагає великих зусиль і витрат (часто значних) в усьому світі.

Впровадження цього досить старого нововведення неухильно просувається вперед, але наведений аналіз показує, що цього недостатньо для повного розгортання. Загальна картина безпеки в Інтернеті досить жалюгідна. Шлях між URL-адресою в адресний рядок браузера і сторінкою сайту, яку ми отримуємо, вимагає неабиякої кількості сліпої довіри. Як на світовому рівні, так і на рівні держав окремо потрібно покращити стійкість інфраструктури адресації та маршрутизації, потрібно зміцнити DNS і зробити її більш стійкою до спроб її скомпрометувати. Для правильної роботи протоколу DNSSEC повинні бути задіяні власники доменів, які відповідають за публікацію інформації в DNS, і повинні простежити за тим, щоб їх дані DNS були підписані DNSSEC, та мережеві оператори повинні включити DNSSEC-валідацію на тих своїх Резолвер, які обробляють запити до DNS.

Регулювання роботи задіяних сторін має відбуватись як на державному рівні, так і на рівні міжнародних організацій, діяльність яких має відношення до DNS.

ЛІТЕРАТУРА

[1] Протокол DNSSEC развернут во всех доменах общего пользования. [Електронний ресурс]. – Режим доступу: https://www.icann.org/ru/ announcements/details/domain-name-system-security -extensions-now-deployed-in-all-generic-top-level-domains-23-12-2020-ru.

[2] Counting DNSSEC. [Електронний ресурс]. – Режим доступу: https://labs.ripe.net/author/gih/ counting-dnssec/.

[3] ICANN призывает к полному развертыванию DNSSEC и сотрудничеству в рядах сообщества для защиты интернета. [Електронний ресурс]. – Режим доступу: https://www.icann.org/ru/anno uncements/details/icann-calls-for-full-dnssec-deplo yment-promotes-community-collaboration-to-pro tect-the-internet-22-2-2019-ru.

[4] Запрос предложений: исследование показателей развертывания DNSSEC. [Електронний ресурс]. – Режим доступу: https://www.icann.org/ru/ announcements/details/request-for-proposal - resear ching-dnssec-deployment-metrics-17-5-2021-ru.

[5] DNSSEC: Защита DNS. [Електронний ресурс]. – Режим доступу: https://www.icann.org/en/ system/files/files/octo-006-24jul20-ru.pdf.

[6] ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ "Про внесення змін до деяких постанов Кабінету Міністрів України щодо функціонування офіційних веб-сайтів органів виконавчої влади". [Електронний ресурс]. – Режим доступу: https:// zakon.rada.gov.ua/laws/show/493-2019-%D0% BF# Text.

[7] DNSSEC validation revisited By Geoff Huston on 2 Mar 2020. [Електронний ресурс]. – Режим доступу: https://blog.apnic.net/2020/03/02/dnssec-validation-revisited/.

[8] Project Overview for the DNSSEC Deployment Metrics Research RFP 17 May 2021. [Електронний ресурс]. – Режим доступу: https://www.icann.org /en/system/files/files/rfp-dnssec-deployment-metrics-research-17may21-en.pdf.

[9] NORDUnet conference. [Електронний ресурс]. – Режим доступу: https://events.nordu.net/display /ndn2012web/Programme.

АНАЛИЗ ИССЛЕДОВАНИЙ ПО РАЗВЕРТЫВАНИЮ DNSSEC В ИНТЕРНЕТЕ

Система доменных имен является неотъемлемой частью адресации в сети Интернет. Недостатки 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. Для защиты целостности при обмене данными DNS предназначена технология DNSSEC, которая предотвращает получение фальшивых данных DNS-клиентами. В статье исследуется современное состояние использования технологии расширения безопасности системы доменных имен DNSSEC и рассматриваются вопросы спроса на изучение показателей по развертыванию протокола DNSSEC и проблемы, которые существуют с получением максимально полного представления о масштабах развертывания данного протокола в Интернете. DNSSEC позволяет владельцам доменных имен использовать метод цифровой подписи информации, которую они вносят в систему доменных имен DNS. Это обеспечивает защиту потребителей, так как данные DNS, подвергшихся искажению, случайно или со злым умыслом, до них не доходят. Вопрос, который решает DNSSEC: Можно ли доверять ответу DNS? С 2010 года была обеспечена возможность использования подписи DNSSEC на самом верхнем уровне DNS, который называется корневым, что су-

щественно облегчает глобальное развертывание DNSSEC. Однако даже десять лет спустя темпы внедрения DNSSEC по-прежнему остаются низкими. В статье представлены современное состояние, сравнительный анализ, проблемы и перспективы внедрения этой технологии для защиты информационных ресурсов. Относительная сложность технологии и отсутствие готовых решений на уровне интернет-пользователей сдерживают темпы внедрения DNSSEC. В то же время это обусловлено дополнительными затратами операторов телекоммуникаций и провайдеров услуг на администрирование, а также отсутствием поддержки DNSSEC в оборудовании операторского уровня и у регистраторов доменных имен. Безопасность DNS должна быть неотъемлемой частью плана по обеспечению безопасности всех пользователей Интернет, поскольку система, основной задачей которой является превращение имен сетевых узлов в IP-адреса используются буквально всеми приложениями и службами в сети.

Ключевые слова: безопасность информационных ресурсов, кибербезопасность, DNS, DNSSEC, TLD, gTLD, домен, доменная зона, ICANN.

ANALYSIS OF RESEARCH ON DEVELOPMENT OF DNSSEC ON THE INTERNET

The domain name system is an integral part of addressing on the Internet. Disadvantages in the implementation of the DNS protocol allow it to be used for malicious actions, during which the integrity and availability of data may be violated when exchanging data between the DNS client and the DNS server. DNSSEC technology is designed to protect the integrity of DNS data exchange, which prevents DNS clients from receiving false data. The article examines the current state of use of DNSSEC domain name enhancement technology and discusses the demand for DNSSEC deployment indicators and the problems that currently exist with obtaining the fullest possible understanding of the scale of deployment of this protocol on the Internet. DNSSEC allows domain name owners to use the method of digitally signing the information they enter into the DNS domain name system. This provides consumer protection, as DNS data that has been corrupted, accidentally or with malicious intent, does not reach them. Question addressed by DNSSEC: Can DNS answers be trusted? Since 2010, it has been possible to use the DNSSEC signature at the top level of the DNS, called the root, which greatly facilitates the global deployment of DNSSEC. However, even ten years later, the pace of DNSSEC implementation remains low. The article presents the current state, comparative analysis, problems and prospects of implementation of this technology for the protection of information resources. The relative complexity of the technology and the lack of ready-made solutions at the level of Internet users constrain the pace of DNSSEC implementation. 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 DNSSEC support for operator-level equipment and domain name registrars. DNS security should be an integral part of the plan to ensure the security of all Internet users, because the system, whose main task is to convert the names of network nodes into IP addresses, are used by virtually all applications and services on the network.

Keywords: security of information resources, cybersecurity, DNS, DNSSEC, TLD, gTLD domain, domain zone, ICANN.

Приходько Тетяна Юріївна - керівник департаменту сервісної/технічної підтримки ТОВ «Інтернет Інвест».
E-mail: tata@mirohost.net.
Orcid ID: 0000-0001-6909-7697.
Приходько Татьяна Юрьевна - руководитель департамента сервисной/технической поддержки ООО «Интернет Инвест».
Tetiana Prykhodko - head of Support Department, Internet Invest, Ltd..

Козловський Валерій Валерійович - д.т.н., професор, завідувач кафедри засобів захисту інформації Національний авіаційний університет.
E-mail: vvkzeos@gmail.com.
Orcid ID:0000-0002-8301-5501.
Козловский Валерий Валериевич - д.т.н., профессор, заведующий кафедрой средств защиты информации Национального авиационного университета
Kozlovskyi Valeriy- Doctor of Technical Sciences, Professor, Head of the Department (Department of information security systems) National Aviation University.

Яковів Іван - аспірант, Національний авіаційний університет.
E-mail: vvkzeos@gmail.com.
Orcid ID:0000-0002-8301-5501.
Яковив Иван - аспирант, Национальный авиационный университет.
Jakoviv Ivan - postgraduate student, National Aviation University.