КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1(17), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.17.5764
УДК 004

Олексенко Віталій Петрович
Заступник командира частини
Військова частина А0106, Київ, Україна
ORCID ID:0000-0003-2757-498X
oleksenko.v.p.77@gmail.com

Штонда Роман Михайлович
Начальник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID:0000-0001-5986-0847
shtonda1982@ukr.net

Черниш Юлія Олександрівна
Старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID:0000-0002-6626-5656
kobernikoi@ukr.net

Мальцева Ірина Робертівна
Старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID:0000-0001-6073-4637
irenagold2402@gmail.com

СУЧАСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В РАДІОРЕЛЕЙНИХ ЛІНІЯХ ЗВ'ЯЗКУ

Анотація. У даній статті розглянуто вплив шкідливого програмного забезпечення AcidRain, що було застосовано по відношенню до України під час вторгнення рф. Тому після порушення роботи супутникового інтернет-сервісу Viasat велика частка передачі даних лягла на інші види зв'язку одним з яких є радіорелейний зв'язок. На сьогоднішній час радіорелейний зв'язок залишається одним із пріоритетних видів зв'язку. Основні умови, що визначають розвиток радіорелейного зв'язку та збереження його досить високої питомої ваги на ринку надання телекомунікаційних послуг, умовно можна розділити на організаційні, технічні і технологічні. Для забезпечення розвитку радіорелейного зв'язку та збереження його досить високої питомої ваги на ринку надання телекомунікаційних послуг, необхідно приділяти увагу кібербезпеці під час побудови радіорелейних ліній зв'язку. Для цього кожній посадовій особі на відповідному рівні необхідно звернути увагу на дані точки контролю для забезпечення надійного кіберзахисту в радіорелейних лініях зв'язку, а саме мати відповідні теоретичні знання адміністраторами та користувачами в інформаційно-комунікаційних системах, комунікаційних мережах, а також належно практично діяти під час забезпечення кібербезпеки при розгортанні радіорелейних ліній зв'язку. Кібератаки росії перед вторгненням в Україну довели, що кібератаки на сьогоднішній день відіграють важливу та стратегічну роль в сучасному світі та ведені бойових дій, незважаючи на те, чи відомо про це електорату. Ця загроза для нас була та є постійною і вона не стоїть на місці, а тільки розвивається. Кібератаки завдають нищівних проблем нашим інформаційно-комунікаційним системам, комунікаційним мережам та інфраструктурі з парадоксальними, подекуди плачевними наслідками. Надійна робота радіорелейних ліній зв'язку залежить від забезпечення кібербезпеки. На цьому варто акцентувати увагу, а разом із тим докласти максимальних зусиль. З кожним днем технічний прогрес буде все тільки більше зростати, як не парадоксально війна є «двигуном прогресу», а за зростанням технічного прогресу буде зростання залежності в кіберпросторі.

Ключові слова: кібератаки, кібербезпека, кіберзагрози, радіорелейний звязок

ISSN 2663 - 4023

ВСТУП

Протягом останніх років в науковому середовищі ведеться дискусія про роль та місце радіорелейних ліній зв’язку в системі передачі даних. Особливого загострення вона набула з початком широкого впровадження волоконно-оптичних ліній зв'язку з їх величезними можливостями забезпечення пропускної здатності на значні відстані та терміналів супутникового зв’язку, які мають можливість забезпечувати передачу даних на величезні відстані при мінімальних витратах сил та засобів зв’язку та мінімальному впливі на них зовнішніх впливів навколишнього середовища [1].

Разом з тим, як показує практика, застосування радіорелейних ліній зв’язку не втратило своєї актуальності на сьогоднішній час. Проте поруч із розвитком прогресуючих складових, технологічний прогрес стимулює появу нових викликів та окремих загроз, зокрема і щодо захисту радіорелейних ліній зв’язку від кібератак. Тож протистояння поширенню кібератак під час застосування радіорелейних ліній зв’язку стає пріоритетним завданням на національному рівні.

Постановка проблеми. Однією із найактуальніших проблем є саме кібератаки на інформаційно-комунікаційні системи та комунікаційні мережі, пов’язані з вторгнення російської армії на територію нашої держави. Повномасштабне вторгнення постійно супроводжується агресією у кіберпросторі та постійними спробами заподіяти шкоду нашим об’єктам критичної інфраструки. Нашій країні доводиться постійно стикатися з новими кіберзагрозами.

Аналіз останніх досліджень і публікацій. На сьогоднішній час проведена велика робота щодо заміни застарілих аналогових радіорелейних станцій зв’язку сучасними цифровими магістральними радіорелейними станціями. Але питання щодо забезпечення кібербезпеки в радіорелейних лініях зв’язку майже не відображене в наукових праця за даним напрямком. Тому ми здійснили комплексне дослідження, даного питання, яке дозволить надійно протидіяти кіберзагрозам та кібератакам під час розгортання та застосування за призначенням радіорелейних ліній зв'язку.

Мета статті. Метою даної статті є можливість обговорення цих проблем, їх аналізу, пошуку рішень для забезпечення кібербезпеки радіорелейних ліній зв’язку.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Від самого початку війни стало відомо про величезну кількість кібератак на українські ресурси. Напад російських хакерів на Україну розпочався буквально за кілька хвилин до повномаштабного вторгнення військ. За даними агентства Reuters, США, Великобританія та Європейський Союз офіційно звинуватили рф у великомасштабному кібернападі, який порушив роботу супутникового інтернет-сервісу Viasat за годину до початку війни 24 лютого 2022 року. Це спричинило знищення «десятків тисяч» супутникових терміналів [2]. Активно зазначається що, дана атака торкнулася також європейських інтернет-користувачів та деяких вітрових електростанцій. А ще під хвилю потрапили українські військові та декілька сотень цивільних клієнтів.

Під час цієї кібератаки 24 лютого було запущено шкідливе програмне забезпечення AcidRain. AcidRain видалив усі дані на модемі та маршрутизаторі Viasat, через що всі вони перестали працювати. І саме так були знищені тисячі терміналів. Попереднє програмне забезпечення російських хакерів було дуже руйнівним і малонаціленим. Однак AcidRaid — це скоріше зброя загального призначення [3].

Тому після порушення в роботі супутникового інтернет-сервісу Viasat велика частка передачі даних лягла на інші види зв’язку одним з яких був радіорелейний зв’язок.

Протягом багатьох років більше «ставок» було зроблено на супутниковий зв'язок тоді, як радіорелейному приділялось менше уваги. Однак все змінилось після вторгнення російських військ, супутниковий зв'язок був подавлений шкідливим програмним забезпечення AcidRain тоді, як радіорелейні лінії зв'язку працювали на повну силу своїх можливостей.

А отже одним з найбільш стійких, економічних та швидкісних способів організації передачі інформаційно-транспортних потоків на великі відстані залишається радіорелейний зв'язок. Раніше, в основному, апаратура лінії такого зв'язку була аналоговою, зараз їй на зміну прийшли сучасні цифрові радіорелейні станції, що мають високу пропускну здатність [4]. Їх пропускна здатність складає 155 Мбіт/с і більш, а передача сигналів ведеться з використанням багатопозиційних видів модуляції. Сучасні цифрові радіорелейні станції характеризуються наявністю системи дистанційного обслуговування, яка програмно підтримує елементи мережі та рівень управління мережею, а також забезпечує контроль, управління та обслуговування обладнання [5].

Основні умови, що визначають розвиток радіорелейного зв'язку та збереження його досить високої питомої ваги на ринку надання телекомунікаційних послуг, умовно можна розділити на організаційні, технологічні та технічні [6].

Дані передумови можуть бути обумовлені наступними чинниками:

1. Організаційні передумови:

об'єктивною необхідністю підвищення пропускної здатності системи зв'язку, що пов'язана зі стійкою тенденцією зростання числа користувачів і все більшими можливостями розширення номенклатури та підвищення якості комунікаційних послуг [7];

все більш яскраво вираженим переходом до передачі даних та мультимедійної інформації, в тому числі й у русі;

зниженням питомої ваги передачі голосових повідомлень, появою стійкої тенденції до передачі різнорідної інформації (передача даних, відео, голос) в пакетованому вигляді [8];

можливостями реалізації сучасних схем об'єднання і поділу цифрових потоків, каналів, повідомлень й сполучення різнорідних ліній зв'язку з метою перерозподілу телекомунікаційного ресурсу на інформаційно важливих (пріоритетних) напрямках;

можливостями побудови розгалужених радіорелейних мереж з можливостями динамічної реконфігурації та адаптацією режимів роботи обумовлених потребами користувачів і впливом середовища розповсюдження.

2. Технологічні передумови:

можливостями щодо впровадження автоматизації в управлінні процесами встановлення і ведення зв'язку, адаптивного регулювання потужності, зміни режимів роботи, безперервного контролю якості зв'язку і його підтримку на заданому рівні, документування (ведення реєстру подій і т.д.), зручності користування обладнанням, реалізації дистанційного керування обладнанням і т.д.

3. Технічні передумови:

необхідністю пошуку і застосування простих недорогих технічних (в тому числі і інтерфейсних) рішень для доведення різнорідної інформації безпосередньо до споживача, в тому числі того, що знаходиться в русі (використання технологій пакетних радіорелейних систем, LTE і т.д.), при роботі в умовах міжсимвольної інтерференції і складної радіоелектронної обстановки (застосування сигнально-кодових конструкцій, багаточастотних сигналів OFDM, COFDM, ведення радіоелектронної боротьби і т.д.);

необхідністю забезпечення високої надійності функціонування обладнання і ліній зв'язку шляхом автоматизації управління ними, резервування елементів основного

обладнання, впровадженням тестування ліній (мереж), шляхом широкого використання шлейфів по трактах інтерфейсу, необхідністю швидкого пошуку несправностей;

використанням сучасної елементної бази, мініатюризацією надвисокочастотного обладнання, освоєнням більш високих ділянок діапазону надвисокочастотного обладнання (з метою можливості більш компактного розміщення обладнання в одному малогабаритному контейнері) і т.д.

Тому для забезпечення розвитку радіорелейного зв'язку та збереження його досить високої питомої ваги на ринку надання телекомунікаційних послуг, необхідно приділяти увагу кібербезпеці під час побудови радіорелейних ліній зв'язку.

Кожній посадовій особі на відповідному рівні необхідно звернути увагу на дані точки контролю для забезпечення надійного кіберзахисту в радіорелейних лініях звязку:

1. Теоретичні знання:

пройти Very Verified: онлайн-курс з медіаграмотності та отримати сертифікат із позитивним результатом [9];

пройти онлайн-курс Обережно! Кібершахраї та отримати сертифікат із позитивним результатом [10];

пройти онлайн-курс Основи кібергігієни та отримати сертифікат із позитивним результатом [11], для військовослужбовці курс Кібергігієни розроблений Військовим інститутом телекомунікацій та інформатизації імені Героїв Крут;

слідкувати за відповідними повідомленнями на різних офіційних ресурсах Держспецзв'язку та CERT-UA. Ці органи першими публікують офіційні попередження не лише про можливі кіберзагрози, а й про те, як мінімізувати їхні ризики [12];

старатися вивчати та активно аналізувати слабкі місця вашого кіберзахисту, щоб щоденно укріплювати їх.

2. Практичні дії:

потрібно завжди пам'ятати про безпеку системи, яка залежить конкретно та абсолютно точно від кожного працівника. Хакери здатні напасти на компанію або ж установу і через робітників різних фірм та установ, викравши їхні дані. В особливій небезпеці знаходяться – військові, а також всі державні діячі. Ці категорії людей мають абсолютно точно звикнути до кібергігієни та прийняти її за норму повсякденного життя, щоб не боротися з важкими наслідками в разі атак;

постійно під час роботи на автоматизованих робочих місцях застосовувати двофакторну автентифікацію. Що таке двофакторна автентифікація? Автентифікація – це процес підтвердження особи для доступу до комп'ютерної системи або онлайн-обліковки. Виділяють три основні фактори автентифікації: фактор знання (те, що ми знаємо, наприклад пароль або PIN-код), фактор володіння (те, що ми маємо, як-от мобільний пристрій або посвідчення особи) і фактор властивості (те, що є частиною нас, наприклад відбиток пальця або голос). Існують також фактори розташування й часу, але вони зустрічаються набагато рідше. Двофакторна автентифікація лише означає, що ваша система безпеки використовує два фактори. Інакше кажучи, двофакторна автентифікація – це додатковий рівень безпеки, окрім вашого пароля або PIN-коду;

застосовувати відповідні логіни та паролі. Логін, як за правилом повинен містити прізвище та ініціали користувача. Пароль має містити не менше ніж 10 символів без натяку на певну річ або дату (символи це великі та малі літери, цифри а також знаки !@#$%&* тощо, приклад vRs!6$3wNk);

постійно оновлювати антивірусне програмне забезпечення, не менше ніж раз на сім днів. Антивірусне програмне забезпечення, яке дозволено для використання в державних та інших установах має відповідний сертифікат та опубліковано на офіційному сайті Держспецзв'язку;

застосовувати програмно-апаратні та програмні міжмережеві екрани, їх також називають firewall, брандмауери. Найліпше віддавати перевагу програмно-апаратним міжмережевим екранам наступного покоління Next-Generation Firewall (NGFW), які включають в себе традиційні міжмережеві екрани з додатковими функціями фільтрації міжмережевих пристроїв, що забезпечують безпеку активним захистом від кіберзагроз, під час та після проведення кібератаки на радіорелейну лінію зв'язку. Слід мати також і резервний міжмережевий екран, який повинен бути розгорнутий в мережі як дублюючий та забезпечувати безперебійну роботу в разі виходу з ладу основного міжмережевого екрану. Система централізованого керування міжмережевими екранами повинна здійснюватися із застосуванням програмно-апаратного комплексу кібербезпеки. Також слід пам'ятати про оновлення, налаштування та підтримання в робочому стані програмних міжмережевих екранів. Не рекомендується використовувати міжмережеві екрани, які є на різноманітних сайтах в безкоштовному вигляді для завантаження;

для управління міжмережевими екранами необхідно створити центр управління міжмережевими екранами він також буде одиним з елементів кібербезпеки інтегрований в мережеві екрани, який в системі Програмно-апаратного комплексу кібербезпеки узагальнений в централізовану консоль для виконання завдань адміністрування, управління, аналізу та звітності. Центр управління міжмережевими екранами дає змогу налаштовувати, керувати роботою, оновлювати сигнатури та програмні засоби, здійснювати моніторинг подій, знімати індикатори кіберзагроз і тощо;

для належної роботи програмно-апаратного комплексу кібербезпеки та центру управління міжмережевими екранами слід встановлювати однакове мережеве обладнання та технології, які забезпечують надійність мережевого з'єднання, а також однаковий рівень керованості від одного виробника. Вказане дасть змогу один і той самий пристрій у разі необхідності використовувати будь-де, лише змінивши інтерфейс, що в свою чергу підвищує стабільність, надійність мережі та зменшує вартість у керуванні міжмережевими екранами.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Радіорелейний зв'язок відносно не новий вид зв'язку але на сьогоднішній час своєї актуальності не втратив. Питома частка передачі даних лягає в повній мірі на радіорелейний зв'язок. Тому для забезпечення розвитку радіорелейного зв'язку та збереження його досить високої питомої ваги на ринку надання телекомунікаційних послуг, необхідно постійно приділяти увагу кібербезпеці під час побудови радіорелейних ліній зв'язку. Додержання правил та вимог, які наведенні в нашій статті, дозволить будувати радіорелейні лінії зв'язку з додержанням правил кібербезпеки та можливістю протидіяти витоку інформації.

Подальшими дослідженнями в даному напрямку є відпрацювання вимог, що висуваються до міжмережевих екранів, які заплановані для використання в радіорелейних лініях зв'язку, розрахунок потреби в міжмережевих екранах, відпрацювання схем підключення міжмережевих екранів тощо.

Боремося з кібертерором разом! Разом до перемоги! Слава Україні!

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Женжера, С. та ін. (2015). Історія розвитку електрозв'язку. Невідомі сторінки. *Системи обробки інформації, 5*(130), 6–10.

2 Нечет Т. Війна росії проти України почалася з кібернападу на супутники. За годину до вторгнення були знищені «десятки тисяч» терміналів Viasat. ITC.ua. https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/ (дата звернення: 01.09.2022).

3 Мальцева, І., Черниш, Ю., Штонда, Р. (2022). Аналіз деяких кіберзагроз в умовах війни. : *Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка, 4*(16), 37-44. https://csecurity.kubg.edu.ua/index.php/journal/article/view/362

4 Якимчук, Ю. (2022). Проблеми проектування цифрових радіорелейних ліній. *Збірник тез: сучасні інфокомунікаційні технології.* https://dut.edu.ua/uploads/n_10254_58714921.pdf.

5 Современная радиорелейная связь. (2017). https://lantorg.com/article/sovremennaya-radiorelejnaya-svyaz

6 Кушнір, О., Васюта, К., Озеров, С., Литвин, А., Северілов, А. (2017). Основні тенденції та перспективи розвитку військового радіорелейного зв'язку. *Збірник наукових праць Харківського університету Повітряних Сил*, *4*, 7–11. http://irbis-nbuv.gov.ua

7 Musavian, L., Aissa, S., Lambotharan, S. (2010). Effective capacity for interference and delay constrained cognitive radio relay channels. *IEEE transactions on wireless communications*, *9*(5), 1698–1707. https://doi.org/10.1109/tcomm.2010.05.090600

8 Sakarellos, V. K., Skraparlis, D., Panagopoulos, A. D., Kanellopoulos, J. D. (2010). Outage Performance Analysis of a Dual-Hop Radio Relay System Operating at Frequencies above 10GHz. *IEEE Transactions on Communications*, *58*(11), 3104–3109. https://doi.org/10.1109/tcomm.2010.091310.0900692

9 Very Verified: онлайн-курс з медіа грамотності. Дія. Цифрова Освіта. (2021). https://osvita.diia.gov.ua/courses/very-verified.

10 Обережно! Кібершахраї. Дія. Цифрова Освіта. (2021). https://osvita.diia.gov.ua/courses/attention-cyber-fraudsters.

11 Основи кібергігієни. Дія. Цифрова Освіта. (2021). https://osvita.diia.gov.ua/courses/cyber-hygiene

12 Комітет з питань цифрової трансформації інформує як посилити кіберзахист підприємствам та установам. *Офіційний портал Верховної Ради України*. https://www.rada.gov.ua/news/razom/221800.html

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023

Vitalii P. Oleksenko
Deputy commander of the unit
Military unit A0106 Kyiv, Ukraine
ORCID ID:0000-0003-2757-498X
oleksenko.v.p.77@gmail.com

Roman M. Shtonda
Head of Research Department
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID:0000-0001-5986-0847
shtonda1982@ukr.net

Yuliya O. Chernish
Senior Researcher
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID:0000-0002-6626-5656
kobernikoi@ukr.net

Irina R. Maltseva
Senior Researcher
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID:0000-0001-6073-4637
irenagold2402@gmail.com

MODERN APPROACHES TO PROVIDING CYBER SECURITY IN RADIO RELAY COMMUNICATION LINES

Abstract. This article examines the impact of the AcidRain malware, which was used against Ukraine during the Russian invasion. Therefore, after the disruption of the Viasat satellite Internet service, a large share of data transmission fell on other types of communication, one of which is radio relay communication. Today, radio relay communication remains one of the priority types of communication. The main conditions that determine the development of radio relay communication and the preservation of its rather high specific weight in the market for the provision of telecommunication services can be conventionally divided into organizational, technical and technological ones. In order to ensure the development of radio relay communication and to preserve its rather high specific weight in the market for the provision of telecommunication services, it is necessary to pay attention to cyber security during the construction of radio relay communication lines. To do this, each official at the appropriate level must pay attention to these points of control to ensure reliable cyber protection in radio relay communication lines, namely, have the appropriate theoretical knowledge of administrators and users in information and communication systems, communication networks, as well as properly act in practice under time to ensure cyber security when deploying radio relay communication lines. Russia's cyberattacks before the invasion of Ukraine proved that cyberattacks today play an important and strategic role in the modern world and are being waged, regardless of whether the electorate knows about it. This threat to us was and is constant and it does not stand still, but only develops. Cyberattacks cause devastating problems to our information and communication systems, communication networks and infrastructure with paradoxical, sometimes deplorable consequences. The reliable operation of radio relay communication lines depends on ensuring cyber security. You should focus on this, and at the same time make maximum efforts. Every day, technological progress will only grow more and more, paradoxically, war is the "engine of progress", and behind the growth of technical progress will be the growth of dependence in cyberspace.

Key words: cyber attacks, cyber security, cyber threats, radio relay communication

REFERENCES

1 Zhenzhera, S. and others. (2015). The history of the development of telecommunications. Unknown pages. Information Processing Systems, 5(130), 6–10.

2 Nechet T. Russia's war against Ukraine began with a cyberattack on satellites. An hour before the invasion, "tens of thousands" of Viasat terminals were destroyed. ITC.ua. https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/ (date of application: 01.09.2022).

3 Maltseva, I., Chernysh, Yu., Shtonda, R. (2022). Analysis of some cyber threats in the conditions of war. : Electronic specialized scientific publication Cybersecurity: education, science, technology, 4(16), 37-44. https://csecurity.kubg.edu.ua/index.php/journal/article/view/362

4 Yakymchuk, Yu. (2022). Design problems of digital radio relay lines. Collection of theses: modern information and communication technologies. https://dut.edu.ua/uploads/n_10254_58714921.pdf.

5 Modern radio relay communication. (2017). https://lantorg.com/article/sovremennaya-radiorelejnaya-svyaz

6 Kushnir, O., Vasyuta, K., Ozerov, S., Lytvyn, A., Severilov, A. (2017). The main trends and prospects for the development of military radio relay communication. Collection of scientific works of Kharkiv Air Force University, 4, 7–11. http://irbis-nbuv.gov.ua

7 Musavian, L., Aissa, S., Lambotharan, S. (2010). Effective capacity for interference and delay constrained cognitive radio relay channels. IEEE transactions on wireless communications, 9(5), 1698–1707. https://doi.org/10.1109/tcomm.2010.05.090600

8 Sakarellos, V.K., Skraparlis, D., Panagopoulos, A.D., Kanellopoulos, J.D. (2010). Outage Performance Analysis of a Dual-Hop Radio Relay System Operating at Frequencies above 10GHz. IEEE Transactions on Communications, 58(11), 3104–3109. https://doi.org/10.1109/tcomm.2010.091310.0900692

9 Very Verified: an online course on media literacy. Action. Digital Education. (2021). https://osvita.diia.gov.ua/courses/very-verified.

10 Be careful! Cyber fraudsters. Action. Digital Education. (2021). https://osvita.diia.gov.ua/courses/attention-cyber-fraudsters.

11 Basics of cyber hygiene. Action. Digital Education. (2021). https://osvita.diia.gov.ua/courses/cyber-hygiene

12 The Committee on Digital Transformation informs enterprises and institutions how to strengthen cyber protection. The official portal of the Verkhovna Rada of Ukraine. https://www.rada.gov.ua/news/razom/221800.html