МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
Вибіркового освітнього компонента
КІБЕРТЕРОРИЗМ
Підготовки першого (бакалаврського) рівня вищої освіти

Луцьк – 2026

Силабус вибіркового освітнього компонента “Кібертероризм”. Підготовки першого (бакалаврського) рівня вищої освіти

Розробник:
Жигаревич О.К., старший викладач кафедри комп’ютерних наук та кібербезпеки

Погоджено
Гарант освітньо-професійної програми:
Гришанович Т. О.

Силабус освітнього компонента затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки
протокол № 6 від 15.01.2026 р.

Завідувач кафедри:

Гришанович Т. О.

І. Опис освітнього компонента

Найменування показників	Характеристика освітнього компонента
	Вибірковий
Денна форма навчання	Рік підготовки 2
150/5 кредитів	Семестр 3
	Лекції 10 год.
	Лабораторні 20 год.
	Самостійна робота 110 год.
ІНДЗ: є	Консультації 10 год.
	Форма контролю: залік

ІІ. Інформація про викладача

ПІП Жигаревич Оксана Костянтинівна
Науковий ступінь
Вчене звання -
Посада старший викладач
Контактна інформація Zhyharevych.Oksana@vnu.edu.ua
Дні занять http: http://194.44.187.20/cgi-bin/timetable.cgi?n=700

ІІІ. Опис освітнього компонента

1. Анотація курсу

Освітній компонент «Кібертероризм» розглядає такі питання, як формалізація понять "кібервійни", "кіберзахист", вивчає сучасні методи дослідження та аналізу кіберпростору; способи та механізми реалізації ефективних алгоритмів пошуку шкідливого програмного забезпечення у конкретних застосуваннях.

Стрімкий розвиток інформаційно-комунікаційної сфери та інформаційних технологій пришвидшив появу суспільно небезпечних дій – кіберзлочинності та кібертероризму. Кібертероризм – це багатогранний феномен, обумовлений багато в чому безконтрольним використанням глобальних мереж, а також недостатньою увагою з боку держави, громадянського суспільства і спецслужб до даного сегменту інформаційного простору. Кількість злочинів скоєних в кіберпросторі зростає пропорційно числу користувачів комп'ютерних мереж, є найшвидшими на планеті. Виходячи з того, що в даний час неможливо контролювати або обмежити доступ до інформаційних ресурсів Інтернету споживачів інформації, різко підвищується криміногенність даного інформаційно-комунікативного ресурсу. Таким чином, розвиток кібертероризму загрожує безпеці особистості, суспільства і держави. В умовах розвитку інформаційного суспільства кібертероризм вже давно переріс рамки регіонального і національного масштабу. Освітній компонент має на меті навчити здобувачів формулювати та ефективно вирішувати задачі із захисту інформації, виробити системний підхід до їх розв'язання, розглянути базові алгоритми обробки даних.

2. Мета і завдання освітнього компонента: Формування знання про захист персональних даних, структури даних, області їх використання, способи їх програмної реалізації; формування умінь і навичок програмно обробляти дані з використанням різних методів та алгоритмів шифрування інформації.

3. Результати навчання. Загальні компетентності:

Здатність до абстрактного мислення, аналізу та синтезу.
Здатність застосовувати знання у практичних ситуаціях.
Знання та розуміння предметної області та розуміння професійної діяльності.
Здатність бути критичним і самокритичним.
Здатність генерувати нові ідеї (креативність).
Здатність оцінювати та забезпечувати якість ІТ- проектів, інформаційних та комп'ютерних систем різного призначення, застосовувати міжнародні стандарти оцінки якості програмного забезпечення інформаційних та комп'ютерних систем, моделі оцінки зрілості процесів розробки інформаційних та комп'ютерних систем.
Здатність ініціювати, планувати та реалізовувати процеси розробки інформаційних та комп'ютерних систем та програмного забезпечення, включно з його розробкою, аналізом, тестуванням, системною інтеграцією, впровадженням і супроводом.
Оцінювати та забезпечувати якість інформаційних та комп'ютерних систем різного призначення.
Аналізувати сучасний стан і світові тенденції розвитку комп'ютерних наук та інформаційних технологій.

4. Soft Skills

Критичне та системне мислення – аналіз загроз, пошук рішень.
Комунікація і командна робота – виконання завдань в парах, підготовка звітів.
Етична відповідальність – усвідомлення важливості приватності й правил кібергігієни.
Прийняття рішень і розв'язання проблем – вибір оптимальних способів реагування на інциденти.
Адаптивність і самоорганізація – підтримка власної кібербезпеки, навчання новому.

5. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. ФЕНОМЕН КІБЕРТЕРОРИЗМУ У СВІТІ В УМОВАХ ГЛОБАЛІЗАЦІЇ ТА ЦИФРОВІЗАЦІЇ. НОВІ РИЗИКИ ДЛЯ МІЖНАРОДНОЇ БЕЗПЕКИ, ПОВ'ЯЗАНІ З КІБЕРТЕРОРИЗМОМ						
Тема 1. Генезис та еволюція кібертероризму: сутність, особливості, причини виникнення, історія розвитку, форми прояву.	28	2	4	20	2	РЗ
Тема 2. Цілі та об'єкти атак кібертерористів.	28	2	4	20	2	РЗ
Тема 3. Основні напрями та способи використання глобально інформаційно - телекомукаційної мережі інтернет та кіберпростору.	28	2	4	20	2	РЗ, РМГ
Разом за модулем 1	84	6	12	60	6	**14**
Змістовий модуль 2. КІБЕРТЕРОРИЗМ ЯК ЕЛЕМЕНТ ДЕСТАБІЛІЗАЦІЇ СУСПІЛЬНО-ПОЛІТИЧНОЇ ОБСТАНОВКИ ТА СИСТЕМИ СТРАТЕГІЧНИХ						

КОМУНІКАЦІЙ У СУСПІЛЬСТВІ						
Тема 1. Найвідоміші атаки кібертерористів на об'єкти критичної інфраструктури, електронний уряд, банківські системи та приватні компанії у світі та в УКРАЇНІ в історичній ретроперспективі та у сучасному часі.	38	2	4	30	2	РЗ
Тема 2. Хакерство, кібершпигунство, кібердеверсії, кіберрозвідка та кібертероризм: взаємозалежності.	28	2	4	20	2	РЗ
Разом за модулем 2	56	4	8	50	4	26
Види підсумкових робіт						Бал
Тестування						25
Модульна контрольна робота						10
ІНДЗ 1						15
ІНДЗ 2						10
Всього годин/Балів	150	10	20	110	10	100

Методи контролю*: ДС – дискусія, ДБ – дебати, Т – тести, ТР – тренінг, РЗ/К – розв'язування задач/кейсів, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота здобувача освіти, РМГ – робота в малих групах, МКР/КР – модульна контрольна робота/ контрольна робота, Р – реферат, а також аналітична записка, аналітичне есе, аналіз твору тощо.

6. Завдання для самостійного опрацювання.

Самостійна робота здобувачів включає в себе:

1. Опрацювання лекційного матеріалу.
2. Перевірка здійснюється під час практичних занять.
3. Підготовка до практичних занять, виконання домашніх завдань.
4. Перевірка здійснюється під час лабораторних занять.
5. Систематизація вивченого матеріалу перед заліком.
6. Перевірка здійснюється під час заліку.
7. Вивчення тем, що не розглядаються в курсі лекцій.
8. Підготовка ІНДЗ. Перевірка здійснюється під час здачі індивідуального завдання.

№ з/п	Тема	Кількість годин
1	Хакерство, кібершпигунство, кібердиверсії, кіберрозвідка та кібертероризм: взаємозалежності.	10
2	БПЛР, як загроза об'єктам критичної інфраструктури.	10
3	Критична інфраструктура у світі та в Україні як мішень кібертероризму.	10
4	Система суб'єктів національної системи кібербезпеки щодо протидії кібертероризму та забезпечення безпеки критично важливих об'єктів інфраструктури від загроз кібертероризму.	10

5	Кібертероризм як елемент та глобальна зброя гібридної війни – війни нового технологічного рівня в інформаційному просторі України.	10
6	Кібертерористи – на службі у держави як невидима складова кібервійськ.	10
7	Забезпечення кібербезпеки України від загроз кібертероризму: системний підхід до організації протидії.	10
8	Політичний та ідеологічний «хактивізм» в епоху інформатизації соціуму. Історія розвитку хактивізму на міжнародному рівні.	10
9	Інформаційна зброя в терористичних акціях та локальних конфліктах у кіберпросторі як інструмент силової політики.	5
10	Найвідоміші атаки кібертерористів на об'єкти критичної інфраструктури, електронний уряд, банківські системи та приватні компанії у світі та в Україні в історичній ретроперспективі та у сучасному економіко-політичному просторі.	5
11	Загроза міжнародного інформаційного тероризму: відомі дезінформаційні кампанії та війни у кіберпросторі.	10
12	Концептуальні засади кібернетичної могутності держави.	10

IV. Політика оцінювання

Політика щодо академічної доброчесності. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку визначеному викладачем. При цьому викладач залишає за собою право змінити завдання.

Комунікаційна політика. Здобувачі вищої освіти повинні мати активовану університетську пошту. Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту, можливе інше (додаткове) джерело комунікації, визначене викладачем для більш оперативного зв'язку зі студентами.

Політика щодо перескладання. Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).

Політика щодо оскарження оцінювання. Політика щодо оскарження оцінки. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку згідно «Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки»

Політика щодо відвідування занять. Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, академічна мобільність, які необхідно підтверджувати відповідними документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин навчання може проводитися у дистанційній формі за погодженням з керівником курсу та деканом факультету. Декан факультету видає розпорядження про дистанційне навчання на основі заяви здобувача. Під час дистанційного навчання лабораторні роботи виконуються відповідно до розкладу занять. На початку заняття викладач повідомляє варіант завдання, який здобувач повинен виконати. Звіт про

виконання лабораторної роботи необхідно завантажити в Moodle до завершення заняття. Вимоги до звітів наведені в описах лабораторних робіт у системі Moodle. Після закінчення заняття можливість здачі буде припинено. Роботи, подані несвоєчасно, не підлягають оцінюванню.

Навчання може здійснюватися за індивідуальним графіком відповідно до Положення про організацію освітнього процесу здобувачів освіти за індивідуальним графіком навчання у Волинському національному університеті імені Лесі Українки. Для цього здобувач подає заяву на ім'я декана, який, враховуючи успішність та підстави, погоджує або відхиляє подану заяву. У разі погодження здобувач освіти погоджує із викладачем план роботи, форми та терміни контролю. Індивідуальний графік затверджується на один семестр, а під час академічної мобільності – не більше ніж на рік.

Усі умови навчання в дистанційній формі та за індивідуальним графіком також подані у дистанційному курсі цього освітнього компоненту системи Moodle.

Бонуси. Після завершення вивчення курсу та перед початком екзаменаційної сесії здобувачам вищої освіти можуть бути нараховані додаткові бали за наукову діяльність. Такі бали надаються за участь у наукових конференціях, підготовку публікацій, здобуті результати в олімпіадах чи конкурсах студентських наукових робіт та інші досягнення у предметній галузі освітнього компонента. Порядок і систему нарахування бонусних балів визначає та затверджує науково-методична комісія факультету.

Визнання результатів навчання, отриманих у формальній, неформальній освіті. Під час вивчення освітнього компонента можливе визнання результатів навчання отриманих у формальній, неформальній та/або інформальній освіті. Порядок визнання результатів навчання для здобувачів вищої освіти, набутих у: формальній освіті (академічна мобільність студентів на території України чи поза її межами, для студентів, які переводяться, поновлюються з інших ЗВО (вітчизняних чи іноземних); неформальній та/або інформальній освіті здійснюється згідно «ПОЛОЖЕННЯ про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

Підсумковий контроль

Форма контролю – семестровий залік. Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе оцінювання всіх видів запланованої навчальної роботи протягом семестру: нараховується за якісне виконання лабораторних, контрольних, тестових контрольних робіт та виконання індивідуального завдання. Максимальна кількість балів, яку може отримати здобувач під час поточного оцінювання за семестр – 100 балів. Залік виставляється за результатами поточної роботи за умови, що здобувач освіти виконав ті види навчальної роботи, які визначено силабусом освітнього компонента.

У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та добрати ту кількість балів, яку було визначено на пропущені теми. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи.

У випадку, якщо здобувач освіти протягом поточної роботи набрав менше як 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання анульовуються. Максимальна кількість балів на залік під час ліквідації академічної заборгованості, становить 100. На заліку, під час ліквідації академічної заборгованості, здобувач отримує комплексне завдання, яке охоплює всі теми і всі форми контролю, які пропонувалися при вивченні освітнього компонета.

V. Шкала оцінювання

Оцінка в балах за всі види навчальної діяльності	**Оцінка**
90 – 100	Відмінно
82 – 89	Дуже добре

75 - 81	Добре
67 -74	Задовільно
60 - 66	Достатньо
1 – 59	Незадовільно

VI. Рекомендована література та інтернет-ресурси.

Основна література

1. Гущин О.О. До питання правового регулювання кібероперацій. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.- практ. конф. (Київ, 30 березня 2018 р.). Київ: Нац. акад. СБУ, 2018. URL: http:// academy.ssu.gov.ua/upload/file/aktualn_problemi_upravl_nnya_nformac_ycnoyu_ bezpekoyu_derzhavi.pdf. С. 52–54.
2. Демедюк С. Кібербезпека у цифрову епоху: чи готова Україна до нових викликів? URL: https://www.pravda.com.ua/columns/2020/08/7/7262150/.
3. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. К.: НІСД, 2018. 84 с.
4. Деякі питання об’єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р., №943. URL: https://zakon.rada.gov.ua/ laws/show/943-2020-п#Text.
5. Діордіца І. В. Кібертероризм як елемент дестабілізації системи стратегічних комунікацій. URL: https://goal-int.org/kiberterorizm-yakelementi-destabilizacii-sistemi-strategichnix-komunikacij/.
6. Доценко О. М. Комплекс навчально-методичного забезпечення з дисципліни «Інформаційний тероризм». Харків: Харківський національний університет імені В. Н. Каразіна, 2020. URL: http://international-relations-tourism.karazin. ua/themes/irtb/resources/c531f6713680adb421918b059ea97f66.pdf.
7. Про внесення змін до Указів Президента України від 27 січня 2015 року №37 та від 7 червня 2016 року №242: Указ Президента України від 28.01.2020 р., №27. URL: https://www.president.gov.ua/documents/272020-32041; https:// zakon.rada.gov.ua/laws/show/27/2020#Text.
8. Реформуємо Держспецзв’язку України. URL: https://thedigital.gov.ua/ news/reformuemo-derzhspetszvyazok-ukraini.

Додаткова дітература та Інтернет-ресурси

9. Бугайчук К. Л., Шорохова Г. М. Забезпечення кібербезпеки як умова протидії терористичній діяльності: нормативно-правові аспекти. Протидія терористичній діяльності: міжнародний досвід і його актуальність для України: матер. ІІ Міжнар. наук.-практ. конф. (15 груд. 2017 р.) / Нац. акад. прокуратури України. Київ, 2018. С.135–138.

10. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. Комп'ютерні науки та кібербезпека. 2019. №1. С. 18–30. URL: https://periodicals.karazin.ua/cscs/article/view/13080/12378.
11. Вейтас М. В. Лукашенко М. І. Кібертероризм: тенденції розвитку та механізми протидії. Науковий огляд. 2018. № 4 (47). URL: https://naukajournal.org/index.php/naukajournal/article/viewFile/1545/1625.
12. Від WannaCry до Petya.A. Наймасштабніші хакерські атаки в Україні та світі. URL: https://tsn.ua/svit/vid-wannacry-do-petya-a-naymasshtabnishihakerski-ataki-v-ukrayini-ta-sviti-952558.html.
13. Вірус Petya і ще 4 великі хакерські атаки на Україну. URL: https://ua.112.ua/statji/virus-petya-i-shche-4-velyki-khakerski-ataky-na-ukrainu-398200.html.
14. Гуцалюк М. В. Актуальні питання забезпечення кібербезпеки України. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ: Нац. акад. СБУ, 2018. URL:
15. Єврокомісія пропонує науковий підхід у протидії гібридним загрозам. URL: https://www.ukrinform.ua/rubric-world/3144070-evrokomisia-proponuenaukovij-pidhid-u-protidii-gibridnim-zagrozam.html.
16. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.
17. Жайворонок О. І. Сучасні загрози інформаційного тероризму в умовах гібридної війни проти України. Державне управління: удосконалення та розвиток. 2018. №4.
18. Збитки від масштабної хакерської атаки з використанням вірусу WannaCry оцінили в 1 млрд доларів. URL: https://ua.112.ua/suspilstvo/zbytkyvid-masshtabnoi-khakerskoi-ataky-z-vykorystanniam-virusu-wannacry-otsinyly-v-1- mlrd-dolariv-391987.html.
19. Звоздецька О. Нові підходи Північноатлантичного Альянсу (НАТО) у сфері кібербезпеки в умовах загострення інформаційного протистояння. Медіафорум: аналітика, прогнози, інформаційний менеджмент: зб. наук. праць. Чернівці: Чернівецький нац. ун-т, 2018. Том 6. С. 71–93. 5
20. Історії найвідоміших хакерських атак. URL: http://www.volynpost.com/ news/69808-istorii-najvidomishyh-hakerskyh-atak.
21. Кіберзлочинність не спить – як не потрапити у тенета аферистів. URL: https://news.finance.ua/ua/news/-/395023/kiberzlochynnist-ne-spyt-yak-nepotrapyty-v-siti-aferystiv.
22. Кібертероризм як нова форма тероризму. URL: https://www.referat911.ru/Mejdunarodnye-otnosheniya/kberterorizm-yak-nova-forma-terorizmu/32661- 1277891-place1.html.
23. Корпоративна безпека для власників бізнесу в сучасних умовах / ТОВ «Консалтингова компанія «СІДКОН» / за наук. ред. Ю. І. Когута. К.: ТОВ «Підприємство «ВІ ЕН ЕЙ», Київ, 2018. 287 с.
24. Корсун К. Про новітню Стратегію кібербезпеки. URL: https://www.facebook.com/kostiantyn.korsun/posts/1109563899228710; https://www.ukrinform.ua/ rubric-technology/2738078-pro-novitnu-strategiu-kiberbezpeki.html.

25. Лінія кібернетичної оборони України: перші подробиці про новий кібер-центр (відео). URL: https://defence-ua.com/weapon_and_tech/v_ukrajini_rozgornutij_kiber_tsentr_navischo_ta_jaki_zavdannja_virishuje_video-1328.html.
26. Мельник Д. С. Щодо актуальних потреб захисту національної критичної інформаційної інфраструктури України. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ: Нац. акад. СБУ, 2018. URL: http://academy.ssu.gov.ua/upload/file/aktualn_problemi_upravl_nnya_nformac_ycnoyu_bezpekoyu_derzhavi. pdf. С. 112–115.
27. Національний координаційний центр кібербезпеки посилює співпрацю із міжнародними виробниками кібер-технологій. URL: https://www.rnbo.gov.ua/ua/Diialnist/4658.html.
28. Нікітюк В. А. Атака на ланцюг постачання. URL: https://ela.kpi.ua/bitstream/123456789/31304/1/Nikitiuk_bakalavr.pdf.
29. Пелещак О. Р. Деякі аспекти кримінально-правової характеристики кібердиверсій. Соціально-правові студії. 2020. Вип. 3 (9). С. 26–33.
30. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: між народний досвід та українські реалії. Young Scientist. 2019. №12.1 (76.1). С. 55–59.
31. Україну атакували кіберзброєю з арсеналу розвідки США – NYT. URL: https://m.tyzhden.ua/news/195645.
32. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 р., №242/2016. URL: https://zakon.rada.gov. ua/laws/show/242/2016#Text.
33. Службу безпеки Twitter очолив відомий хакер. URL: https://www. dw.com/uk/sluzhbu-bezpeky-twitter-ocholyv-vidomyi-khaker/a-55623118.
34. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері: Центр глобалістики «Стратегія XXI». К., 2019. 27 с.
35. Ткачук Н. А. Актуальні кіберзагрози сучасного безпекового середовища. Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2018. №7. URL: https://www.inter-nauka.com/uploads/public/15381330973208.pdf.
36. ТОП-10 найбільших хакерських атак. URL: https://ilounge.ua/ua/review/ top-10-bolshih-hakerskih-atak.
37. Турчак А. В. Механізми забезпечення інформаційної безпеки як складової державної безпеки України: дис. …канд. наук з держ. управл. Київ, 2020. 229 с.
38. У Держспецзв'язку створено Державний центр кіберзахисту та протидії кіберзагрозам. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=156473.
39. У РНБО планують створити Центр протидії гібридним загрозам – Данілов. URL: https://www.ukrinform.ua/rubric-polytics/3127252-u-rnbo-planuutstvoriti-centr-protidii-gibridnim-zagrozam-danilov.html.
40. Хакерські атаки, які увійшли в історію. URL: https://magneticone. academy/khakerski-ataky-iaki-uviishly-v-istoriiu/.
41. Шуневич В., Драч Т. Специфічні засоби ведення інформаційної війни. URL: http://www.vtei.com.ua/doc/2020/28_02_2020/6/23.pdf.

42. Як захиститися у світі, де головна зброя – одиниці та нулі? Холодна війна 2.0. URL: https://defence-ua.com/army_and_war/jak_zahistitisja_u_sviti_de_golovna_zbroja_odinitsi_ta_nuli-2437.html.
43. Україну атакували кіберзброєю з арсеналу розвідки США – NYT. URL: https://m.tyzhden.ua/news/195645.
44. Україну атакує новий вірус-здирник XData. URL: https://ua.112.ua/ suspilstvo/ukrainu-atakuie-novyi-virus-vymahach-xdata-391325.html.