DOI https: //doi.org/10.?6486/mst2411-?816
DOI (Issue): https: //doi.org/10.?6486/mst2411-?816.2022.2(69)

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

№ 2(69), 2022

ВИДАЄТЬСЯ ЩОКВАРТАЛЬНО

ЗАСНОВНИК

Державний науково-дослідний інститут МВС України; Національний авіаційний університет; Національна академія внутрішніх справ

НАКАЗОМ

МОН України від 17.03.2020 № 409 науково-практичний журнал "Сучасна спеціальна техніка" включено до Переліку наукових фахових видань України відповідно до списку згідно з додатком 1 (категорія "Б")

ЗАРЕЄСТРОВАНО

Міністерством юстиції України 13 лютого 2015 року

Свідоцтво – серія КВ № 21221-11021Р

Науково-практичний журнал "Сучасна спеціальна техніка" внесено до переліку міжнародної науковометричної бази

Index Copernicus International Journal Master List

Рекомендовано до друку рішенням Вченої ради ДНДІ МВС України
(протокол від 29.06.2022 № 3)

Науково-практичний журнал посів ІІІ місце в конкурсі на краще наукове періодичне видання в системі МВС України у 2017 році та І місце у 2020 році

Київ 2022

ISSN 2411-3816 (Print)
СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS
DOI (Issue): https: //doi.org/10.36486/mst2411-3816.2022.2(69)
Issue 2(69)2022

УДК 004.056.5

Трофименко Олена Григорівна, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету "Одеська юридична академія", м. Одеса, Україна, ORCID ID 0000-0001-7626-0886
Логінова Наталія Іванівна, кандидат педагогічних наук, доцент, завідувачка кафедри інформаційних технологій Національного університету "Одеська юридична академія", м. Одеса, Україна, ORCID ID 0000-0002-9475-6188
Манаков Сергій Юрійович, кандидат технічних наук, доцент кафедри інформаційних технологій Національного університету "Одеська юридична академія", м. Одеса, Україна, ORCID ID 0000-0001-5930-4592
Янковський Олег Георгійович, кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету "Одеська юридична академія", м. Одеса, Україна, ORCID ID 0000-0001-8041-1843

КІБЕРРИЗИКИ В ОСВІТНЬОМУ СЕКТОРІ

У статті розглядаються питання кіберзахищеності закладів вищої освіти на тлі зростаючих кіберзагроз. Обґрунтовано актуальність пошуків комплексного й виваженого підходу до вирішення питань кібербезпеки закладів освіти як всеосяжної стратегії, що залучатиме дієві практики й передові технології. Проведено аналіз вразливостей та кіберризиків в освітньому секторі. З'ясовано, що повсюдне використання освітніх мереж і дистанційних технологій, а також величезна кількість людей, які отримують доступ до цих мереж через часто незахищені домашні інтернет-з'єднання та пристрої, суттєво збільшили й ускладнили і так карколомний ландшафт кіберзагроз в освітньому секторі.

***Ключові слова**: кіберризики, кібервразливості, кіберзагроза, кібератака, кіберзахист, кібербезпека, освітній сектор.*

Останнім часом кількість кіберзагроз стрімко зростає, і сама по собі кібер-злочинність нікуди не зникне. Тому організації та компанії вимушені вживати заходів щодо своєї кібербезпеки, яка є нині пріоритетом в їхніх IT бюджетах. За прогнозами Gartner [1], світовий ринок інформаційної безпеки 2022 року досягне $170,4 млрд. А за розрахунками Statista [2] до 2026 року обсяг глобального ринку кібербезпеки зросте до $345,4 млрд.

DOI (Article): https: //doi.org/10.36486/mst2411-3816.2022.2(69).10

Не в останню чергу зростання цих показників зумовлене спалахом пандемії COVID-19, через яку за умов карантину організації по всьому світу відправляли своїх співробітників на віддалену роботу з дому. Це порушило архітектуру мережі бізнесу, зробило її набагато більш відкритою, чим створило нові вразливі місця для використання зловмисниками і, відповідно, операційні та фінансові ризики. Переважно кібератаки спрямовані на дані й активи фінансових установ, урядів, корпорацій, різних підприємств і компаній. Проте не стали винятком у цьому переліку університети та академічні установи. Ризик атак на освітні мережі зростає, оскільки вони стають дедалі більш залежними від відкритого середовища і використання мобільних технологій та IoT.

У закладах вищої освіти циркулюють великі обсяги персональних даних і фінансової інформації про студентів, викладачів та співробітників, а також інформації про наукові дослідження, що робить їх привабливою мішенню для кібер- злочинців. За даними Microsoft [3] сектор освіти найбільше потерпає від корпоративних зіткнень зі шкідливим програмним забезпеченням і посідає перше місце (82,6 %) за кількістю випадків виявлення зловмисного програмного забезпечення, порівняно з галузями торгівлі (8,41 %), медицини (3,93 %), телекомунікацій (2,39 %), фінансів (1,52 %) та інших.

Нині будь-який освітній заклад має оцінити свій профіль кіберризиків, зважаючи на те, які його активи і процеси піддаються впливу ззовні. І, відповідно, варто обирати програмне забезпечення, інструменти та методології безпеки, які якнайкраще контролюватимуть доступ до цих даних, щоб захистити їх. Кіберризики означають ризики фінансових втрат (прямих і непрямих), повної або часткової зупинки діяльності, а також шкоди репутації закладу або приватної особи [4].

Управління кіберризиками є базовим процесом щодо ідентифікації вразливостей, оцінки небезпек, грамотної підготовки до атак і загроз, мінімізації тяжкості можливих наслідків у разі реалізації ризиків. За сучасних умов управління кіберризиками пов'язане зі здатністю забезпечення працездатності організації і безпеки її даних. Управління ризиками кібербезпеки складається з моделювання ризику несприятливих наслідків через загрози кібербезпеці, оцінки того, чи ризик несприятливих наслідків відповідає критеріям прийнятності ризику, зниження ризику до прийнятних рівнів за допомогою відповідних заходів.

Питанням аналізу кіберризиків присвячені численні наукові дослідження. Так, стаття [5] пояснює, чому кібератаки стали особливо проблематичними під час COVID-19. Робота [6] спрямована на побудову формальної онтологічної моделі для оцінки ризиків кібербезпеки, яка враховує цифрові характеристики людини. Дослідження [7] ілюструє приклад багатонаціональної компанії, яка зазнає економічних втрат, спричинених проблемами кібербезпеки, разом із різноманітними системами кіберризиків, моделями та методами, які використовуються для захисту активів та аналізу інвестицій у безпеку. Автори статті [8] розглядають концепцію побудови ігрової моделі кібербезпеки як засобу кількісної ідентифікації кіберризиків. У статті [9] розглянуто загальну модель загроз та вразливостей кібербезпеки у закладах вищої освіти. Науковці продовжують пошуки вдалих моделей і методів для кібербезпеки, зокрема аналізуючи різноманітні системи кіберризиків.

DOI (Article): https: //doi.org/10.36486/mst2411-3816.2022.2(69).10
Issue 2(69)2022 http://suchasnaspetstehnika.com/

При цьому ефективність запропонованих залежить від специфіки сфери діяльності підприємства, організації чи компанії. Різні підходи і специфічні аспекти в пошуках рішення проблем, пов'язаних із питаннями аналізу кіберризиків та забезпеченням кібербезпеки, свідчать про актуальність цієї тематики й потребу подальших наукових досліджень, особливо щодо специфіки можливих кіберризиків закладів вищої освіти.

Мета дослідження полягає в аналізі вразливостей та кіберризиків у освітньому секторі.

Створення новітньої системи кіберзахисту закладу вищої освіти (ЗВО) неможливе без всебічного аналізу можливих ризиків. Ризик кібербезпеки визначається ймовірністю втрати критичних активів, конфіденційної інформації або репутації внаслідок кібератаки чи-то злому в мережі організації. Ризик кібербезпеки зазвичай визначається шляхом вивчення суб'єкта загрози, на зразок вразливостей та наслідків, пов'язаних із порушенням IT-інфраструктури. Вразливості - це слабкі місця, недоліки або помилки, які можуть використовуватися зловмисниками для отримання несанкціонованого доступу під час атак соціальної інженерії, DDoS-атак і розширених постійних загроз (Advanced persistent threat, APT). Залежно від типу та наслідків атаки, прямі та непрямі наслідки можуть впливати на діяльність, фінанси, репутацію та стан відповідної організації.

Інтерес кіберзлочинності до освітнього сектора зумовлений наявністю значної кількості персональних даних як студентів, так і штату працівників. Крім того, багато навчальних закладів мають інформацію про передові дослідження, технологічні інновації та інтелектуальну власність, яку також цінують потенційні хакери. При цьому традиційно освітні установи вищої школи дотримуються академічної відкритості та сприяють вільному обміну інформацією під час співпраці з іншими дослідниками як всередині, так і поза межами університету. І з часом такі взаємозв'язки в університетах продовжують зростати, а відтак пропорційно зростає поле доступу для кібератак. Усе це становить виклики для кібербезпеки, які не спостерігаються в інших галузях. Іронія ситуації полягає в тому, що численні науковці вишів досліджують сучасні проблеми кібербезпеки і публікують свої дослідницькі статті щодо її забезпечення, тоді як сам сектор вищої освіти часто має проблеми з кіберзахистом і потребує втручання відповідних технічних спеціалістів. Проте через обмежені бюджети таких штатних фахівців може собі дозволити далеко не кожен університет чи то академія.

Спектр кіберзагроз для сектора вищої освіти доволі широкий: від крадіїв персональних даних та комерційних таємниць до програм-вимагачів, від несегменто- ваних мереж віддалених працівників та студентів до взаємовідносин між структурними підрозділами, філіалами та комерційними партнерами. Наявність численних комп'ютерних лабораторій у різних структурних підрозділах цих закладів, де для великої кількості студентів і викладачів з різним ступенем технічних знань розміщені комп'ютери та системні пристрої з вільним доступом, ніяк не сприяє забезпеченню інформаційної безпеки університетів. Як наслідок, заходи кібербезпеки часто послаблюються на користь зручності та функціональності. Крім того, вільний потік робочої сили та щорічна ротація нових студентів і співробітників також додають вразливості освітньому сектору.

Істотний вплив на послаблення рівня кібербезпеки університетів відбувся внаслідок швидкого переходу до віддаленої роботи, електронного навчання та он-лайн-викладання на початку пандемії COVID-19, що порушило архітектуру мереж освітніх організацій, зробивши дані всередині мереж набагато більш відкритими. Адже вдома студенти і працівники можуть використовувати незахищені чи застарілі пристрої, які більш уразливі для атак, що ненавмисно створюють додаткові вразливості.

Суттєвим є те, що багато викладачів університетів для онлайн-викладання обрали платформу Zoom, оскільки вважають її економічно ефективною і зручною як для себе, так і для студентів. Нині Zoom продовжує покращувати захист від зовнішнього втручання і навіть пропонує наскрізне шифрування для забезпечення конфіденційності відеодзвінків, проте наявне зараз шифрування не є наскрізним у загальноприйнятому його розумінні, коли тільки користувачі мають доступ до криптографічних ключів, необхідних для розшифрування вмісту. Випадки масових "зумбомбінгів" та передачі даних користувачів Facebook і Google без їх згоди були визнані компанією та для задоволення претензій колективного позову виплачені відповідні, призначені судом багатомільйонні кошти [10]. Відтак варто зважати на те, що наразі платформа Zoom не надає надійного захисту для дзвінків і формує додаткові проблеми кібербезпеки.

Для навчальних закладів від початку пандемії COVID-19 віртуальні технології стали важливим фактором у навчанні, і тому вкрай важливо вживати заходів для подолання ризиків. З іншого боку, дослідження [11] показало, що під час пандемії певна невизначеність і невпевненість у "завтрашньому дні", різної природи страхи підвищують емоційний стан людей, роблять їх більш сприйнятливими до шахрайства. Через це за даними Всесвітньої організації охорони здоров'я (ВООЗ) кількість кібератак під час пандемії COVID-19 зросла вп'ятеро [12]. Розуміючи фактори, які роблять людей більш вразливими до кібератак, можна краще підготуватися та навчитися реагувати на можливі кіберінциденти.

Кіберризики є динамічними, вони доволі часто і сильно змінюються. Грамотне визначення та управління кіберризиками дозволить розподілити раціонально бюджет на кібербезпеку і грамотно підготуватися до атак і загроз заздалегідь. Під час первинної оцінки ризиків варто, у першу чергу, визначити цілі управління кібербезпекою установи. Після цього треба визначити критично важливі елементи, які впливають на ключові процеси освітнього закладу. Кожен ризик, у класичному розумінні, оцінюється за двома параметрами: ймовірності й потенційного збитку. З огляду на кількісні показники, формується карта ризиків і їхній пріоритет. Таку оцінку необхідно проводити регулярно, розширюючи карту ризиків, щоб охопити якомога більше потенційних ризиків для організації. Робота з ризиками полягає в оцінці кожного з них та розробленні заходів (мінімізації, прийняття, ухилення, перекладання і диверсифікації) для вибору правильного інструмента та заходів управління відповідним ризиком. Згодом інструмент може бути переглянутий та змінений після перевірки його ефективності. Перегляд процесів і карти кібер- ризиків має відбуватися на регулярній основі. Саме такий циклічний підхід допомагає працювати з актуальною інформацією та актуальними погрозами.

DOI (Article): https://doi.org/10.36486/mst2411-3816.2022.2(69).10
Issue 2(69)2022 http://suchasnaspetstehnika.com/

Проведений аналіз вразливостей та кіберризиків у освітньому секторі дозволив з'ясувати, що повсюдне використання освітніх мереж і дистанційних технологій, а також величезна кількість людей, які отримують доступ до цих мереж через часто незахищені домашні інтернет-з'єднання та пристрої, суттєво збільшили й ускладнили і так карколомний ландшафт кіберзагроз в освітньому секторі. Нині освітній сектор наражається на більш широкий спектр проблем, ніж інші сектори, особливо внаслідок переходу до дистанційного та гібридного навчання. Адміністраторам університетських мереж самотужки важко їх захищати, враховуючи розміри і сегментованість, кількість внутрішніх і зовнішніх користувачів та обсяги обміну інформацією.

Активність кіберзагроз щодо сектора освіти зростає, а тому фахівці з кібербезпеки повинні діяти швидко й на випередження. З адміністративної точки зору, необхідно розробити та впровадити відповідну політику навчання та безпеки, а також провести тестування на проникнення, щоб визначити, чи правильно працюють заходи безпеки. ЗВО мають оцінити свій профіль кіберризиків, зважаючи на те, які саме бізнес-активи та процеси піддаються зовнішньому впливу, і відповідно до цього обирати програмне забезпечення, інструменти та методології безпеки, які контролюватимуть доступ до даних, наприклад, брандмауери або шифрування, щоб краще захистити великі обсяги цінних досліджень і персональних даних.

Розбудувати всеосяжну і надійну систему кіберзахисту за недовгий час й за обмеженого бюджету нереально. Саме тому освітні академічні установи для забезпечення своєї діяльності повинні робити більше за менші кошти, тобто засоби й підходи до зменшення поверхні атаки та її складності мають обиратися й реалізуватися саме з точки зору їх ефективності. А вже надалі робити все можливе щодо розширення й посилення захисту своїх програм, мереж та систем, поглибленого моніторингу кіберризиків та забезпечення безпеки для кожного пристрою своєї IT-інфраструктури від несанкціонованого доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Forecast Analysis: Information Security, Worldwide. URL: https://www.gartner.com/en/documents/3889055 (дата звернення: 04.03.2022).

2. Size of the cybersecurity market worldwide from 2021 to 2026. URL: https://www.statista.com/ statistics/595182/worldwide-security-as-a-service-market-size/ (дата звернення: 04.03.2022).

3. Most affected industries. URL: https://www.microsoft.com/en-us/wdsi/threats (дата звернення: 04.03.2022).

4. Кіберризики: як розуміти та управляти. https://10guards.com/ua/articles/cyber-risks/ (дата звернення: 04.03.2022).

5. *Williams Ch., Chaturvedi R., Chakravarthy K.* Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research.* 2020. Vol 22. DOI: 10.2196/23692. URL: https://wwwjmir.org/2020/9/ e23692/ (дата звернення: 04.03.2022).

6. *Jureviciene A., Brilingaite A., Bukauskas L.* Digital Human in Cybersecurity Risk Assessment. *HCII 2021. Lecture Notes in Computer Science.* 2021. Vol 12776. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-78114-9_29. URL: https://link.springer.com/chapter/10.1007%2F978-3-030-78114-9_29#citeas (дата звернення: 04.03.2022).

7.*Domingues V.* Finance and Cybersecurity Risk Management: Dissertation. 2018. 51 p. URL: https://www.researchgate.net/publication/344711134_Finance_and_ Cybersecurity_Risk_Management (дата звернення: 04.03.2022).

8. Savchenko V., Matsko O. Cybersecurity risk management on the basis of game-theoretic approach. *Modern information security.* 2019. Vol. 2(38). P. 6-16. DOI: 10.31673/2409-7292. 2019.020616.

9. *UlvenJ., Wangen G.* A Systematic Review of CybersecurityRisks in Higher Education. *Future Internet.* 2021. Vol. 13. 39 p. DOI: 10.3390/fi13020039. URL: https://www.researchgate.net/publication/348975661_A_Systematic_Review_of_Cybersecurity_Risks_in_Higher_Education (дата звернення: 04.03.2022).

10. Zoom to pay $85M for lying about encryption and sending data to Facebook and Google. URL: https://arstechnica.com/tech-policy/2021/08/zoom-to-pay-85m-for-lying-about-encryption-and-sending-data-to-facebook-and-google/ (дата звернення: 04.03.2022).

11. *Naidoo R.* A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems.* 2020. Vol. 29(3). P. 306-321. DOI: 10.1080/0960085x.2020.1771222.

12. WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. URL: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (дата звернення: 04.03.2022).

REFERENCES

1. Forecast Analysis: Information Security, Worldwide. URL: https://www.gartner.com/en/documents/3889055 (Date of Application: 04.03.2022) [in English].

2. Size of the cybersecurity market worldwide from 2021 to 2026. URL: https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/ (Date of Application: 04.03.2022) [in English].

3. Most affected industries. URL: https://www.microsoft.com/en-us/wdsi/threats (Date of Application: 04.03.2022) [in English].

4. Кіберризики: як розуміти та управляти. Cyber risks management. URL: https://10guards.com/ ua/articles/cyber-risks/ (Date of Application: 04.03.2022) [in Ukrainian].

5. *Williams, Ch., Chaturvedi, R., Chakravarthy, K.* (2020) Cybersecurity Risks in a Pandemic. Journal of Medical Internet Research. Vol 22, No 9. DOI: 10.2196/23692. URL: https://www.jmir.org/ 2020/9/e23692/ (Date of Application: 04.03.2022) [in English].

6. *Jureviciene, A., Brilingaite, A., Bukauskas, L.* (2021) Digital Human in Cybersecurity Risk Assessment. In: HCII 2021. Lecture Notes in Computer Science, vol 12776. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-78114-9_29. URL: https://link.springer.com/chapter/10.1007%2F978-3-030-78114-9_29#citeas (Date of Application: 04.03.2022) [in English].

7. *Domingues, V.* (2018). Finance and Cybersecurity Risk Management: Dissertation. 51 p. URL: https://www.researchgate.net/publication/344711134_Finance_and_Cybersecurity_ Risk_Management (Date of Application: 04.03.2022) [in English].

8. *Savchenko, V., Matsko, O.* (2019). Cybersecurity risk management on the basis of game- theoretic approach. *Modern information security.* Vol. 2(38). P. 6-16. DOI: 10.31673/24097292.2019.020616 [in English].

9. *Ulven, J., Wangen, G.* (2021) A Systematic Review of CybersecurityRisks in Higher Education. *Future Internet.* Vol. 13, 39 p. DOI: 10.3390/fi13020039. URL: https://www.researchgate.net/publication/348975661_A_Systematic_Review_of_Cybersecurity_Risks_in_Higher_Education (Date of Application: 04.03.2022) [in English].

10. Zoom to pay $85M for lying about encryption and sending data to Facebook and Google. URL: https://arstechnica.com/tech-policy/2021/08/zoom-to-pay-85m-for-lying-about-encryption-and-sending-data-to-facebook-and-google/ (Date of Application: 04.03.2022) [in English].

11. *Naidoo, R.* (2020) A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems.* Vol. 29(3). P. 306-321. DOI: 10.1080/0960085x.2020.1771222 [in English].

12. WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. URL: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (Date of Application: 04.03.2022) [in English].

DOI (Issue): https: //doi.org/10.36486/mst2411-3816.2022.2(69)
Issue 2(69)2022
UDC 004.056.5

Trofymenko Olena,
PhD, Docent, Associate Professor of the Department of Information Technologies of the National University "Odessa Law Academy", Odesa, Ukraine, ORCID ID 0000-0001-7626-0886

Lohinova Nataliia,
PhD, Docent, Head of the Department of Information Technologies of the National University "Odessa Law Academy", Odesa, Ukraine, ORCID ID 0000-0002-9475-6188

Manakov Serhii,
PhD, Associate Professor of the Department of Information Technologies of the National University "Odessa Law Academy", Odesa, Ukraine, ORCID ID 0000-0001-5930-4592

Yankovskyi Oleh,
PhD, Docent, Associate Professor of the Department of Information Technologies of the National University "Odessa Law Academy", Odesa, Ukraine, ORCID ID 0000-0001-8041-1843

CYBER RISKS IN THE EDUCATION SYSTEM

Research article considers issues of cyber security of higher educational institutions against the background of growing cyber threats. The relevance of the search for an integrated and balanced approach to solving cybersecurity issues of higher educational institutions is justified, considering the strategy that attracts effective practices and advanced technologies. It has been noted that circulation of large amounts of personal data and financial information about students, teachers and employees, as well as information about scientific research in higher educational institutions makes them an attractive target for cybercriminals. An analysis of vulnerabilities and cyber risks in the education sector was carried out. The creation of the latest cyber protection system of higher education is impossible without a comprehensive analysis of possible risks. It has been found that the widespread use of educational networks and remote technologies, as well as the huge number of people accessing these networks through often unprotected home Internet connections and devices, have significantly increased and complicated the already complex landscape of cyber threats in the education sector. The education sector now faces a wider range of challenges than other sectors, particularly as a result of the shift to distance and hybrid learning. The activity of cyber threats in the education sector is growing rapidly. Therefore, universities must assess their cyber risk profile and determine which business assets and processes are exposed to external influences. In accordance with this, the software has been chosen, tools and security methodologies that will control access to data. For example, firewalls have been used or encryption to better protection of large amounts of valuable research and personal data has been realized.

Keywords: cyber risk, cyber vulnerability, cyber threat, cyber-attack, cybersecurity, education system.

Отримано 12.05.2022

DOI (Article): https: //doi.org/10.36486/mst2411-3816.2022.2(69).10

DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2022.2(69) Issue 2(69)2022

З М І С Т

СИСТЕМИ ТА МЕТОДИ ОБРОБКИ ІНФОРМАЦІЇ

ІНФОРМАЦІЙНЕ ТА НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ НАУКОВОЇ ДІЯЛЬНОСТІ

ТЕХНІКА, ЗБРОЯ, ТРАНСПОРТ ТА ОБМУНДИРУВАННЯ