promote the development of young people in achieving their physical, intellectual, emotional, social and spiritual potential as individuals, responsible citizens and members of local, national and international communities. The definition of non-formal education in the documents of the first World Forum on Non-Formal Education, initiated by the 'Big Six' , is summarized as deeply diversified in terms of context, duration, provider, methods of provision and the result process carried out with the aim of acquiring life skills, values and principles, and as well as the development of attitudes based on an integrated system of values within planned, structured programs and processes of personal and social education of young people.

The evolution of WOSM's environmental activities within the implementation of the World Scout Environmental Program, the Scouts for SDG program and the Earth Tribe initiative was followed. The goals, criteria, actions and planned results of environmental activities in the European Scout Region have been identified. It is shown that this activity is an expediently organized system that includes an educational component aimed at the formation of environmental sustainability competences, an organizational component that involves establishing strategic partnerships with educational and resesrch institutions for the formation of environmental sustainability competences, and a practical component aimed at applying acquired competences in the transformation of Europe into an ecologically sustainable region.

Key words: *non-formal environmental education, World Organization of the Scout Movement, Scout Method, Ukraine, History*.

УДК 378(438)

Ян Фуззі
Інститут соціальних наук Академії Пьотрковської
(м. Пьотркув-Трибунальський, Польща)
ORCID ID 0009-0002-7449-9943
DOI 10.24139/2312-5993/2024.04/446-456

РОЗВИТОК СУЧАСНИХ ТЕХНОЛОГІЙ: ВИКЛИКИ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ПОЛЬЩІ

Основною метою статті є аналіз викликів національній безпеці, пов'язаних з розвитком сучасних технологій. Представлено вплив цього явища на багато аспектів безпеки в кіберпросторі. Також представлено взаємозв'язок розвитку сучасних технологій з військовою безпекою держави. Також представлено перехресне обговорення питань боротьби державних суб'єктів з терористичними загрозами, безпосередньо пов'язаними з динамічним технологічним прогресом. Проаналізовано можливості отримання освіти з кібербезпеки в університетах, у межах післядипломної освіти, на курсах і тренінгах. Доведено, що сучасні інформаційні технології пропонують передові засоби та можливості кібербезпеки. Однак, це також збільшує потенціал для кібератак, що вимагає постійного вдосконалення та адаптації політики кібербезпеки.

Ключові слова*: технологія, військова безпека, тероризм, кіберпростір, кібербезпека, вища освіта, Польща.*

Постановка проблеми. Стрімкий технологічний розвиток становить серйозну загрозу національній безпеці будь-якій країні, у тому числі й Польщі. Вони безпосередньо впливають на такі аспекти національної безпеки, як боротьба з тероризмом, забезпечення безпеки державних інституцій у кіберпросторі та гарантування постійного військового розвитку, необхідного для протидії як звичайним, так і гібридним загрозам. Функціонування державних утворень та їх громадян потребує постійної адаптації до середовища, що динамічно змінюється на міжнародній арені. Польща, як і будь-яка інша країна, для відстоювання власних національних інтересів, має бути в постійній готовності протистояти вищезгаданим викликам. Для цього необхідно якнайкраще використовувати можливості та пом'якшувати загрози, пов'язані з постійним міжгалузевим розвитком технологій.

Аналіз актуальних досліджень. На сучасному етапі розвитку Республіки Польща проблематика системи національної безпеки країни все частіше опиняється в колі інтересів значної кількості польських дослідників, серед яких цінними для даної наукової розвідки є роботи таких авторів, як А. Давідчук та П. Свобода (Dawidczyk, Swoboda, 2023), А. Місюк (Misiuk, 2017), Ж. Плачек (Płaczek, 2023) та ін. Науковці у своїх дослідженнях вивчали проблеми в законодавчому аспекті.

Різні аспекти проблеми кібербезпеки в Польщі стали предметом вивчення таких науковців, як Дж. Василевський (Wasilewski, 2016), С. Гвожьджєвіч (Gwoździewicz, 2018), Ф. Радонєвич (Radoniewicz, 2016), М. Савицький (Sawicki, 2013) та ін.

Метою статті є ідентифікація та діагностика технологічного розвитку в контексті національної безпеки Польщі та з'ясування провідних засад підготовки фахівців кібербезпеки в закладах вищої освіти країни.

Методи дослідження. У проведеному дослідженні використовувалися такі методи дослідження, як аналіз і критика літератури, порівняння, узагальнення.

Виклад основного матеріалу. Технологічний розвиток значною мірою відповідає за стан міжнародної безпеки держав в аспекті кіберпростору. Кіберпростір Республіки Польща включає, зокрема, ІКТ-системи, мережі та послуги, що мають особливе значення для внутрішньої безпеки держави, банківську систему, а також системи, що забезпечують функціонування транспорту, зв'язку, енергетики,

водної і газові інфраструктури та ІТ-системи охорони здоров'я (Przestrzelska, 2022, с. 11-24).

Кібербезпека є однією з найбільш часто обговорюваних тем безпеки. Украй важливо усвідомити як організаціям, так і державним установам, що розвиток інформованого суспільства безпосередньо залежить від відкритого та широкодоступного, але, насамперед, безпечного кіберпростору. Польща також зазнає кібератак. На думку З. Чмілевські, для забезпечення подальшого безперебійного розвитку держави потрібна адаптація національного законодавства, а також організаційні зміни, необхідні для забезпечення належного рівня безпеки в кіберпросторі (Chmielewski, 2016, с. 103-128).

Польський дослідник В. Смольський стверджує, що мотивацією для більшості кіберзлочинців зазвичай є прибуток, прикладом є так звані «хактивісти», які, переслідуючи ідеологічні цілі, здійснюють такі дії, як крадіжка та знищення конфіденційних даних або перешкоджання доступу до них. Кіберпростір також використовується терористами як інструмент для політично мотивованої діяльності (Smolski, 2015, с. 2).

Через суперечки та проблеми військова безпека Польщі значною мірою залежить від технологічного розвитку. Приклад тому – використання штучного інтелекту у військовій сфері. Експерименти з використання штучного інтелекту в автономних системах зброї проводяться в усьому світі вже кілька років і незабаром, безсумнівно, приведуть до нового покоління зброї.

У разі одночасного використання кількох систем озброєння в динамічно змінюваному оперативному середовищі раптова взаємодія між системами може призвести до непередбачуваних наслідків. Небажані політичні та стратегічні наслідки також можуть виникнути, якщо особи, які ухвалюють рішення, не встигають за темпами змін на майбутньому полі бою. За таких умов і з високим ступенем оцифрованих командних процесів і автономності бойових систем відкритий збройний конфлікт може виникнути швидко (Kopczewski, Krawczyk, 2019, с. 101-113).

Слід також розглянути потенційне використання нанотехнологій для військових цілей. Композиційні матеріали мають високі термічні, механічні та електричні властивості. З них можна виготовляти розумну уніформу, яка у разі поранення та втрати свідомості солдата визначає наявність альбуміну та автоматично надсилає радіосигнал про

допомогу. Композитні матеріали завдяки своїй легкості, гнучкості та хорошим властивостям поглинання енергії пропонують великий потенціал для виготовлення броні, яка захищає все тіло солдата. Легкі, пористі поверхні нановолокон мають мембранні властивості, які можуть сприймати, розщеплювати та фільтрувати токсини, що з'являються на полі бою, і таким чином забезпечують ефективний захист від хімічних і біологічних агентів. Домішки наночастинок срібла, магнію, нікелю та титану значно покращують дезактиваційні властивості нановолокон (Banasik, 2019, с. 125-139).

У боротьбі з тероризмом можна використовувати передові сучасні технології. Кризові ситуації вимагають складних заходів. Одним із таких заходів є система PROTEUS, як інтегрована мобільна система. Проєкт PROTEUS був започаткований у 2009 році з метою покращення роботи силових служб під час аварійно-рятувальних та пожежних операцій, стихійних лих та антитерористичної діяльності. Система PROTEUS у цілому створює вдосконалений інтегрований центр кризового менеджменту. Багаторічна інженерна робота створила систему, яка дозволяє діяти в надзвичайних ситуаціях, наслідки яких можна передбачити, а також у подіях, які змушують використовувати нетрадиційні методи. З цієї причини система PROTEUS була забезпечена низкою технологій для виконання поставленого завдання. Конструкція включає:

- Мобільний командний центр (МКД);
- Операторський центр мобільних роботів;
- Маленький мобільний робот;
- Мобільний інтервенційний робот;
- Мобільний робот з розширеним функціоналом;
- Безпілотний літальний апарат (БПЛА).

Поєднання всіх частин обладнання створює додаткову систему, яка забезпечує інтеграцію між людиною та машиною. Завдяки цьому додатку антитерористичні та контртерористичні операції забезпечують високий рівень ліквідації кризової ситуації. Головним міркуванням проєктувальників була мобільність систем, включених у проєкт. Завдяки такому рішенню можна координувати дії безпосередньо на місці події, що економить час для передачі інформації та ухвалення рішень. Згодом можливість налаштування підсистем покращує, серед іншого, розвідку завдань у важкодоступних районах, а також зняття та знешкодження зарядів ВР.

Довговічність і стійкість до пошкоджень обладнання дозволяє виконувати операції в найекстремальніших умовах. У свою чергу, дистанційне керування мобільними роботами дозволяє підтримувати безпечну відстань від загрозливої зони, не створюючи загрози для операторів машини (Pniak, 2016, с. 161-175).

У зв'язку із зазначеним вище та підвищеним інтересом до досліджуваної проблеми звернемося до питання кібербезпеки в Республіці Польща. Так, 1 серпня 2018 року Президент Республіки Польща підписав «Акт про національну систему кібербезпеки», імплементувавши в польський правопорядок Директиву Європейського Парламенту та Ради (ЄС) про заходи для високого загального рівня безпеки мережевих та інформаційних систем на території Союзу (Директива 2016/1148), т.зв. Директива NIS.

Метою Акту про національну систему кібербезпеки, підготовленого Мінцифрою, була розробка правових норм, які дозволять імплементувати директиву NIS та створити ефективну систему безпеки ІКТ на національному рівні.

На підставі проведеного дослідження зазначимо, що система кібербезпеки Польщі спрямована на забезпечення кібербезпеки на національному рівні, зокрема:

- безперебійне надання основних і цифрових послуг;
- досягнення відповідного високого рівня безпеки ІТ-систем, які використовуються для надання цих послуг.

Система, що будується, включає операторів ключових послуг (у тому числі з енергетики, транспорту, охорони здоров'я та банківського сектору), постачальників цифрових послуг, команди CSIRT (група реагування на інциденти комп'ютерної безпеки) на національному рівні, секторальні команди кібербезпеки, організації, що надають послуги з кібербезпеки, компетентні органи з кібербезпеки та єдиний контактний пункт для зв'язку в межах співпраці в Європейському Союзі у сфері кібербезпеки. Оператори основних послуг зобов'язані впроваджувати ефективні заходи безпеки, оцінювати ризики кібербезпеки та повідомляти про серйозні інциденти та розглядати їх у співпраці з CSIRT національного рівня. Вищезазначені суб'єкти також зобов'язані призначити особу, відповідальну за кібербезпеку послуг, що надаються, обробку і звітність про інциденти, а також обмін знаннями з кібербезпеки. Органи державного управління, а також телекомунікаційні підприємці також включені до національної

системи кібербезпеки – у спосіб, гармонізований з існуючими нормами у цій сфері.

Вимоги щодо кібербезпеки також стосуються постачальників цифрових послуг, тобто платформ онлайн-торгівлі, послуг хмарних обчислень та пошукових систем в Інтернеті. Зважаючи на міжнародну специфіку цих суб'єктів, зобов'язання постачальників цифрових послуг охоплюються регулятивним режимом, гармонізованим на рівні ЄС. Тут Закон посилається на імплементаційне рішення Європейської Комісії.

22 жовтня 2019 року Радою міністрів була схвалена Стратегія кібербезпеки Республіки Польща на 2019-2024 роки. Стратегія замінила Національну рамкову політику кібербезпеки Республіки Польща на 2017-2022 роки.

Основною метою Стратегії стало підвищення рівня стійкості до кіберзагроз та рівня захисту інформації в державному, військовому та приватному секторах. Поширення знань і передового досвіду серед громадян також сприяє кращому захисту інформації.

Документ визначає п'ять конкретних завдань, як-от:

- розвиток національної системи кібербезпеки;
- розробку національних стандартів кібербезпеки;
- збільшення національного потенціалу у сфері технологій кібербезпеки;
- розвиток обізнаності та соціальних компетентностей у сфері кібербезпеки;
- побудову сильної міжнародної позиції Республіки Польща у сфері кібербезпеки.

Незаперечним є той факт, що кібербезпека є ключовою проблемою сучасного світу. Виклики, пов'язані з інформаційною безпекою та захистом, стали повсякденною реальністю не лише для підприємців, але й для приватних осіб, які наражаються на широкий спектр загроз. Це дуже широка мультидисциплінарна галузь знань, яка швидко і постійно розвивається.

Дослідження галузевих організацій чітко демонструють величезний дефіцит спеціалістів на ринку – цифри сягають сотень тисяч необхідних людей, що однозначно формує попит на ринку праці. Відтак, важливим стає питання про підготовку фахівців з кібербезпеки в Республіці Польща.

Щоб стати фахівцем з кібербезпеки в Польщі, зазвичай потрібен ступінь із комп'ютерних наук, комп'ютерних мереж або суміжної

галузі. Найпоширенішими напрямами навчання є інформатика або комп'ютерна інженерія. До того ж, існують також спеціальні магістерські або аспірантські програми, пов'язані з кібербезпекою, які дозволяють отримати спеціальні знання та навички в цій галузі.

Навчання фахівців з кібербезпеки зосереджене на аналізі й запобіганні загрозам, пов'язаним із комп'ютерними атаками, кіберзлочинністю та захистом даних. Здобувачі вищої освіти вчаться захищати мережі, комп'ютерні системи, бази даних, мобільні програми та інші цифрові ресурси.

Під час вивчення кібербезпеки здобувачі вищої освіти отримують практичні навички виявлення загроз, проникнення в системи, моніторингу та реагування на інциденти, а також розробки та впровадження захисних стратегій. Вони також дізнаються про останні тенденції та методи, які використовують хакери, і про те, як з ними боротися.

Здобувачі вищої освіти з кібербезпеки також мають можливість вивчати законодавство про кіберзлочинність та управління ризиками. Етика також є важливою частиною програми, оскільки фахівці з кібербезпеки повинні знати та дотримуватися етичних принципів у своїй роботі.

Після закінчення навчання випускники мають широкий вибір кар'єрних можливостей. Вони можуть працювати аналітиками загроз, проникати в системи з метою тестування, керувати інцидентами безпеки, розробляти захисні стратегії для організацій або працювати в секретних службах. Попит на фахівців з кібербезпеки високий, оскільки галузь стає все більш важливою в епоху цифрових технологій.

У Республіці Польща фахівців з кібербезпеки готують у різних типах університетів, наприклад:

1. Технічні університети. Багато фахівців із кібербезпеки отримують знання в таких технічних університетах, як політехнічні факультети, факультети IT або телекомунікацій. Навчання, спрямоване на вивчення технологій та комп'ютерних систем, можуть бути особливо корисними для розвитку навичок кібербезпеки.

2. Класичні університети. Є багато університетів, які пропонують навчання інформатиці. Вони пропонують курси, пов'язані з криптографією, аналізом загроз, захистом комп'ютерної мережі, аналізом даних або управлінням ризиками. Навчання в університеті

також може надає можливість отримати практичний досвід, беручи участь у дослідницьких проєктах або стажуваннях.

4. Військові заклади вищої освіти. Військові часто мають справу з аспектами кібербезпеки та пропонують спеціалізовані навчальні програми для майбутніх експертів у цій галузі. Військові університети зазвичай зосереджені на техніці захисту від кіберзагроз і національній безпеці в контексті ІТ-мереж.

Поширеними в закладах вищої освіти Республіки Польща є магістерські програми, які готують фахівців із кібербезпеки.

Навчання другого циклу для фахівця з кібербезпеки є розвитком знань і навичок, набутих під час навчання першого циклу в цій галузі. Так, пропонується низка варіантів:

1. Комп'ютерні науки – спеціалізація з кібербезпеки: ця програма зосереджена на питаннях, пов'язаних із безпекою комп'ютерів, мереж і систем баз даних.

2. Інформаційна безпека – спеціалізація з кібербезпеки: ця програма складається з курсів поглибленого рівня з інформаційної безпеки, захисту даних, аналізу ризиків та управління інцидентами.

3. Кібербезпека та управління ризиками: ця програма поєднує в собі технічні та управлінські аспекти кібербезпеки, зосереджуючись на управлінні ризиками, пов'язаними з кібератаками.

4. Системна інженерія – спеціалізація з кібербезпеки: ця програма охоплює питання, пов'язані з проєктуванням, упровадженням та обслуговуванням ІТ-систем високого рівня безпеки.

5. Право в кібербезпеці: ця програма зосереджена на правових і нормативних аспектах, пов'язаних з кібербезпекою, як-от: захист персональних даних, кіберзлочинність і юридична відповідальність.

6. Кібербезпека та управління інцидентами: ця програма зосереджена на аналізі кіберінцидентів, управлінні та відновленні після атак.

До того ж, в Республіці Польща заклади вищої освіти пропонують післядипломну освіту з кібербезпеки. Так, популярними й поширеними є такі післядипломні освітні програми:

1. Кібербезпека та управління ризиками – ця програма зосереджена на розумінні та управлінні ризиками інформаційної безпеки. Здобувачі вищої освіти отримують знання про ідентифікацію та оцінку загроз, управління інцидентами безпеки, захист даних, а також правові та етичні аспекти кібербезпеки.

2. Комп'ютерні мережі та IT-безпека – ця програма охоплює питання, пов'язані з проєктуванням, керуванням та безпекою комп'ютерних мереж. Здобувачі вищої освіти дізнаються про основні мережеві технології, протоколи зв'язку, аналіз загроз і методи захисту мереж від кібератак.

3. Безпека IT-систем – ця програма фокусується на захисті IT-систем від загроз. Студенти отримають знання про архітектуру IT-систем, основні загрози системам, аудит безпеки, аналіз ризиків та методи захисту систем.

4. Післядипломне навчання з кібербезпеки в технічних університетах і коледжах. Ці програми зосереджені на передових темах кібербезпеки, таких як безпека веб-додатків, зворотне проєктування, проникнення в систему, криптографія тощо.

Це лише кілька прикладів, існує багато інших програм післядипломної освіти, доступних для фахівців з кібербезпеки. Вибір навчання залежить від індивідуальних уподобань і кар'єрних цілей.

До того ж, у Польщі поширеними є різноманітні курси та тренінги, які допоможуть отримати знання та навички у сфері кібербезпеки, наприклад:

1. Сертифікований спеціаліст із безпеки інформаційних систем (CISSP). Це міжнародний сертифікат, що підтверджує знання та навички управління загрозами IT-безпеці.

2. Сертифікований етичний хакер (CEH). Цей курс зосереджений на методах навчання, які використовують хакери, щоб підвищити обізнаність спеціалістів із кібербезпеки та допомогти виявити вразливі місця безпеки.

3. Сертифікований менеджер з інформаційної безпеки (CISM). Цей сертифікат підтверджує здатність керувати, проєктувати та проводити аудит інформаційної безпеки.

4. CompTIA Security+. Цей курс призначений для початківців у сфері кібербезпеки. Пропонує базові знання про захист мереж і систем.

5. Сертифікований професіонал з наступальної безпеки (OSCP). Цей сертифікат є поглибленим курсом, який вивчає методи проникнення та тестування на проникнення. Він призначений для фахівців з кібербезпеки, які хочуть розширити свої навички практичного виявлення вразливостей безпеки.

6. Інститут SANS. SANS пропонує широкий спектр курсів і тренінгів з кібербезпеки, таких як управління інцидентами, тестування на проникнення, аналіз зловмисного програмного забезпечення тощо.

Висновки та перспективи подальших наукових розвідок. Дослідження показує, що сучасні технології мають значний вплив на національну безпеку Польщі. Сучасні інформаційні технології пропонують передові засоби та можливості кібербезпеки. Однак, це також збільшує потенціал для кібератак, що вимагає постійного вдосконалення та адаптації політики кібербезпеки. Розвиток військових технологій, включаючи штучний інтелект, нанотехнології чи кіберзброю, змінює обличчя національної оборони. Польщі необхідно ефективно інвестувати в сучасні оборонні технології, щоб підтримувати свою обороноздатність на належному рівні. Сучасні технології впливають на захист критичної інфраструктури від потенційних терористичних атак. Інтегровані IT-системи можуть підвищити ефективність, але водночас збільшують ризик кібератак, які можуть мати серйозні наслідки для функціонування країни. Також необхідно посилити міжнародне співробітництво для обміну передовим досвідом і спільної роботи для захисту від сучасних технологічних загроз.

ЛІТЕРАТУРА

Banasik, M. (2019). Znaczenie nowoczesnych technologii dla bezpieczeństwa. *Rocznik Bezpieczeństwa Międzynarodowego, 12(2),* 125–139.

Chmielewski, Z. (2016). Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich. *Studia Z Polityki Publicznej, 3(2(10),* 103–128.

Dawidczyk, A., Swoboda, P. (2023). Designing security policy objectives for the use of the national security strategy. *Bezpieczeństwo Narodowe, 42 (1),* 33-61.

Hybrid Threats: 2007 cyber attacks on Estonia (2019). In Aday S., Andžāns M., Bērziņa-Čerenkova U., Granelli F., Gravelines J., Hills M., Holmstrom M., Klus A., Martinez-Sanchez I., Mattiisen M., Molder H., Morakabati Y., Pamment J., Sari A., Sazonov V., Simons G., Terra J. (2019). Hybrid Threats. A Strategic Communications Perspective. Riga: NATO Strategic Communications Centre of Excellence.

Kopczewski, M., Krawczyk, J. M. (2019). Wybrane elementy bezpieczeństwa wewnętrznego państwa na podstawie założeń „Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej". *Doctrina. Studia społeczno-Polityczne, 8(8),* 101–113.

Misiuk, A. (2017). Role of public administration in the field of state defense. *Przegląd Nauk o Obronności, 3,* 31-52.

Płaczek, J. (2023). Propozycja nowej strategii bezpieczeństwa narodowego RP. *Przegląd Geopolityczny, 44,* 54-70.

Pniak, S. (2016). Wybrane techniki wykorzystywane przez terrorystów. *Studia Bezpieczeństwa Narodowego, 10(2),* 161-175.

Przestrzelska, K. (2022). Security In Cyberspace. *National Security Studies, 25(3),* 11-24.

Smolski, W. (2015). *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa* [online]. Wrocław: E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2. [dostęp: 23 marzec 2024].

Zawisza, J. (2015). Cyberprzestrzeń jako zagrożenie bezpieczeństwa państwa. *Journal of Modern Science, 27(4),* 403-416.

SUMMARY

Jan Fussy. Development of modern technologies: challenges for national security of Poland.

The main purpose of the article is to analyze national security challenges related to the development of modern technologies. The impact of this phenomenon on many aspects of safety in cyberspace is presented. The relationship between modern technologies with the military security of the state is also presented. There is also a cross-discussion of the struggle of state entities with terrorist threats directly related to dynamic technological progress. The possibilities of cybersecurity education at universities, within the framework of postgraduate education, courses and trainings are analyzed. The study shows that modern technologies have a significant impact on Poland's national security. Rapid technological development poses a serious threat to national security for any country, including Poland. They directly influence national security aspects as the fight against terrorism, ensuring the security of state institutions in cyberspace and guaranteeing permanent military development necessary to counteract both common and hybrid threats. The functioning of state entities and their citizens requires constant adaptation to an environment that changes dynamically in the international arena. Poland, like any other country, should be in constant readiness to resist the above mentioned challenges to defend their own national interests. To do this, you need to use the opportunities and soften the threats associated with the constant inter -sectoral development of technology. Modern information technologies offer advanced means and capabilities of cybersecurity. However, it also increases the potential for cyberattacks, which requires constant improvement and adaptation of cybersecurity policy. The development of military technologies, including artificial intelligence, nanotechnology, or cybercribe, changes the face of national defense. Poland needs to be effectively investing in modern defense technologies in order to maintain their defense capability at a proper level. Modern technologies influence the protection of critical infrastructure from potential terrorist attacks. Integrated IT systems can increase efficiency, but at the same time increase the risk of cyberattacks that can have serious consequences for the country's functioning. It is also necessary to strengthen international cooperation to exchange advanced experiences and work together to protect against modern technological threats.

***Key words**: technology, military safety, terrorism, cyberspace, cybersecurity, higher education, Poland.*