DOI:**10.33099/2311-7249/2019-36-3-59-64**

УДК 355.43

Микола Олександрович Гульков
Віталій Станіславович Толкачов

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, У КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ УКРАЇНИ

У сучасному світі дедалі більшого значення набуває поняття інформаційної безпеки. Разом з поширенням загального доступу до інформації, слідуючи за розвитком комунікаційних систем, розширюється коло можливих інформаційних загроз, з якими стикається держава.

Саме тому інформаційна безпека перетворюється на одну з ключових складових національної безпеки. Деякі дослідники вважають, що забезпечення інформаційної безпеки необхідно не тільки для того, щоб зберегти недоторканість національного інформаційного простору, але й наполягають на тому, що вірно сформульована національна інформаційна стратегія сприяла б більш успішному вирішенню задач у політичній, економічній, соціальній та інших сферах життя. Припускається також можливий вплив відповідної інформаційної політики на позитивний хід розв'язання як внутріполітичних так і зовнішніх конфліктів.

В статті здійснюється порівняльний аналіз організації захисту інформації в країнах - членах НАТО та організації технічного захисту інформації в Україні. Запропонований метод зіставлення наявних результатів оцінювання компонентів довіри до безпеки визначених ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99 надають можливість отримати більш об'єктивну та адекватну оцінку використання засобів та компонентів обчислювальної системи, що використовуються в Україні при побудові автоматизованих систем.

Ключові слова: *інформаційна безпека, технічний захист інформації, політика безпеки.*

Вступ

Постановка проблеми. Починаючи послідовну аргументацію необхідності підтримки заходів по забезпеченню інформаційної безпеки на теренах України, слід зазначити, що певні кроки в цьому напрямку вже було зроблено, починаючи з перших років незалежності. Так у статті 17 Конституції України зазначено: "Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу". Чи означає це, що інформаційну безпеку поставлено на один рівень з такими важливими компонентами системи національних інтересів, як суверенітет та територіальна цілісність, і цей статус питання інформаційної безпеки є законодавчо закріпленим у найголовнішому нормативно-правовому акті? Саме так воно і є, адже інформаційна безпека, хоча і відрізняється за спрямуванням від інших складових цього твердження, тобто вона не належить до груп політичних та економічних національних інтересів, але не поступається ним за ступенем важливості.

Аналіз останніх досліджень і публікацій. В цілому співробітництво між НАТО та країнами-партнерами, одним з яких є і Україна, в рамках Ради євроатлантичного партнерства та Програми "Партнерство заради миру" (ПЗМ) передбачає певні зобов'язання сторін щодо обміну та захисту інформації [5]. Для збільшення транспарентності військового планування й оборонних бюджетів і забезпечення демократичного контролю над збройними силами сторони можуть брати участь у взаємному обміні інформацією про кроки, що вони почали або починають. Перед обміном будь-якою таємною інформацією між країною-учасницею ПЗМ і НАТО, органи по безпеці інформації повинні бути взаємно впевненими, що сторона, яка приймає інформацію, готова забезпечити захист інформації відповідно до вимог сторони, яка її передає.

Активізація інформаційного обміну потребує уніфікації термінів і понять у сфері технічного захисту та безпеки інформації, перегляду та вдосконалення нормативних документів та інструкцій у галузі інформаційних обмінів, їх гармонізації з міжнародними стандартами та створення сучасних механізмів моніторингу потоків інформації [2].

Метою статті є аналіз організації захисту інформації в країнах-членах НАТО та організації технічного захисту інформації в Україні.

Виклад основного матеріалу дослідження

Особливості організації технічного захисту інформації в країнах-членах НАТО

Однією з передумов тісної співпраці між Україною та країнами-членами НАТО є дотримання вимог стандартів та інших нормативних документів. Технічний захист інформації є дуже важливою компонентою під час взаємодії інформаційних систем різних країн. Особливо це стосується тих випадків, коли в системах циркулює інформація з обмеженим доступом, тому надзвичайно важливим є аналіз документів НАТО, в яких наведено рекомендації та вимоги щодо технічного захисту інформації.

Велику увагу захисту інформації приділяють у країнах-членах НАТО. Там створено розгалужену систему органів, які мають забезпечувати належний рівень захищеності інформації. Слід зауважити, що терміну "технічний захист", який використовується в Україні, документах НАТО та інших міжнародних нормативних документах, відповідає термін "security", у перекладі з англійської мови "безпека".

У нормативних документах НАТО вживається термін "ADP system" (automated data processing system), який у нашій державі тлумачать як автоматизована система (АС), відповідно до його поширення в нормативно-правових документах із технічного захисту інформації в Україні.

Завданням технічного захисту інформації є протидія загрозам безпеці АС.

Загрозами безпеці АС, згідно зі стандартом ISO 74982, є:

порушення інформації і (або) інших ресурсів;

спотворення і модифікація інформації;

викрадення, вилучення або втрата інформації і (або) інших ресурсів;

розкриття інформації;

порушення послуги.

Загрози класифікують як:

випадкові – загрози, які існують без чиїхось намірів (наприклад, помилки функціонування технічних засобів, помилки оператора і помилки в програмному забезпеченні);

навмисні – загрози, які можуть змінюватися від непідготовлених атак маніпулюванням легкодоступними засобами моніторингу до добре продуманих і підготовлених атак з використанням спеціального системного знання; спробу реалізації навмисної загрози називають атакою;

пасивні – загрози, які в результаті реалізації не модифікують інформацію в системі, не порушують операцій, що провадяться системою, і не змінюють стану системи (наприклад, пасивне списування інформації в процесі комунікації систем);

активні – загрози, які в результаті реалізації спричиняють модифікацію інформації, зміну стану системи і (або) операції, які провадить система. Приклад реалізації активної загрози - навмисна несанкціонована зміна таблиці маршрутизації.

Внутрішні атаки виникають, коли легальні користувачі діють недозволеним або неавторизованим способом. Найбільш відомі комп'ютерні злочини містять внутрішні атаки, які компрометують систему безпеки.

До методів захисту, які використовуються проти внутрішніх атак, належать:

ретельна комплектація персоналу;

створення довірчої комп'ютерної бази;

посилення служби аудиту проти означених атак.

Зовнішні атаки створюють за допомогою таких методів:

фізичний доступ до ліній зв'язку (активний чи пасивний);

перехоплення повідомлень;

маскування під легального користувача або під компоненту системи;

шунтування механізмів автентифікації або керування доступом.

Заходи і засоби безпеки завжди підвищують вартість системи і можуть робити її складною для використання. Тому ще до початку розроблення заходів і засобів безпеки треба чітко визначити ті загрози, проти яких система має бути захищеною. Цей процес називають оцінюванням загроз. Система є вразливою до різних загроз, але використовують тільки деякі з них, тому що атакуючий не має змоги це зробити або результат атаки не компенсує його зусиль і ризику розкриття його особи. Детальне дослідження загроз не є сферою застосування вищезазначеного стандарту, в загальному плані воно передбачає:

ідентифікацію вразливостей системи;

аналіз імовірності використання цих вразливостей;

оцінювання наслідків успішного проведення кожного з видів атаки;

оцінювання вартості кожного з видів атаки;

визначення потенційної вартості кожного з видів контрзаходів;

визначення множини механізмів безпеки, які себе виправдовують (можливо, на основі аналізу відповідних коштів).

Нетехнічні заходи безпеки, такі як страхове прикриття, можуть бути ефективнішими стосовно коштів, ніж технічні. Повної технічної безпеки, а також повної фізичної безпеки не може бути досягнуто. Доцільно встановити ціну атак достатньо високою, щоб знизити ризик до допустимого рівня.

Чільне місце в системі нормативних документів займає NATO security policy (C-M(55)15(Final)), в якому сформульовано основні принципи побудови системи забезпечення безпеки інформації, включаючи інформацію, що циркулює в АС. Між існуючими нормативними документами НАТО та різними стадіями життєвого циклу АС існує взаємозв'язок (див. рис. 1).

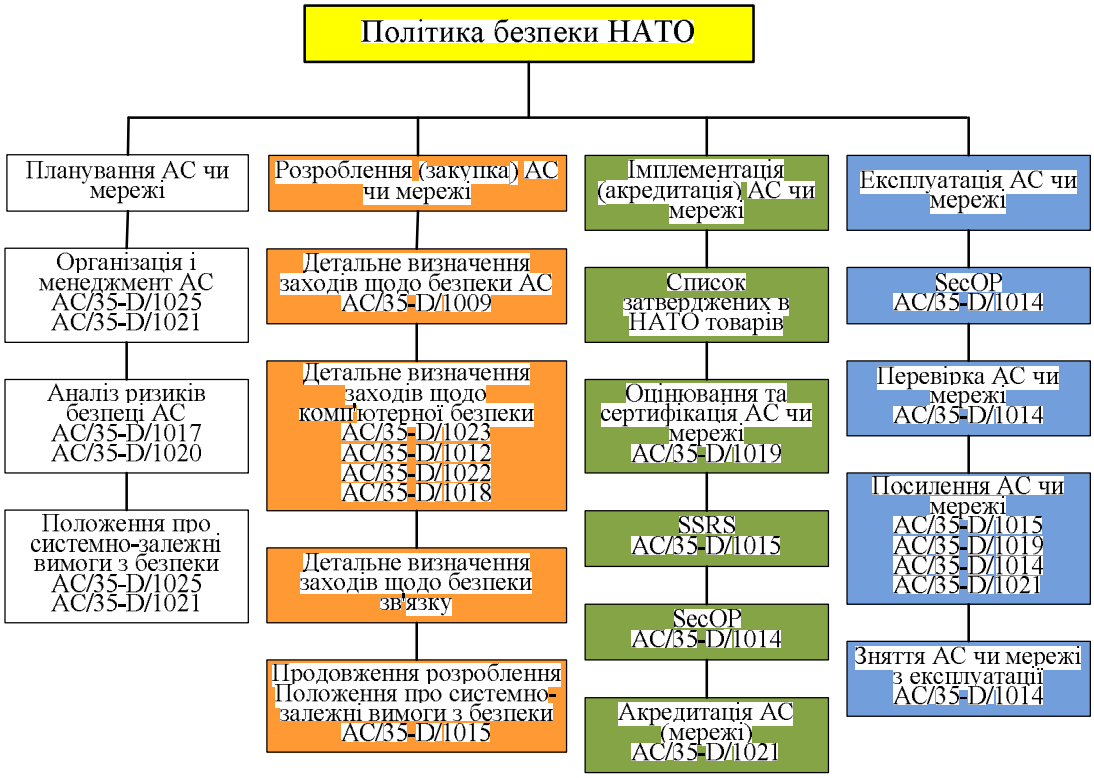

Рис. 1 Нормативно-технічні документи НАТО з безпеки АС, які використовуються протягом її життєвого циклу

Згідно з документом (C-M(55)15(Final)) необхідно створити Орган з безпеки, який відповідав би за утримання належного рівня безпеки і, зокрема, надати чинності визначеним у НАТО стандартам з безпеки та пов'язаній з ними настановній документації. Для кожної країни-члена НАТО, згідно з документом (C-M(55)15(Final)), необхідно створити національний орган з безпеки (NSA), який відповідав би за безпеку класифікованої інформації, що є власністю НАТО.

Головнокомандувачі НАТО та керівники військових агенцій НАТО, які діють під егідою Військового комітету НАТО, відповідають за безпеку в рамках своїх команд та агенцій. На них покладено відповідальність за створення організаційної структури з безпеки, за розроблення та реалізацію програм з безпеки відповідно до прийнятої Політики безпеки НАТО, а також за періодичне інспектування стану впровадження необхідних заходів з безпеки та підтримання її належного рівня.

Цивільні агенції НАТО відповідають перед Радою НАТО за підтримання належного рівня безпеки в рамках своєї сфери діяльності. Вони повинні встановити відповідну організаційну структуру безпеки згідно з прийнятими у НАТО правилами та належною системою нагляду за станом безпеки.

Для захисту конфіденційної інформації НАТО, яка зберігається, обробляється або передається в АС і мережах, у розділі X документа (C-M(55)15(Final)) визначено обов'язки Головнокомандувачів, керівників військових і цивільних Агенцій та функції Органу Акредитації з безпеки (SAA), Органу з автоматизованої обробки даних, Органу, який відповідає за експлуатацію АС, офіцерів безпеки АС і мереж, офіцерів безпеки офісу.

У системі нормативних документів із забезпечення АС велику увагу приділено питанням менеджменту безпеки.

Завдання менеджменту тісно пов'язані з такими етапами життєвого циклу АС:

планування АС;

розроблення (закупівля) АС;

імплементація АС;

експлуатація АС (її посилення);

зняття з експлуатації АС.

До завдань з менеджменту безпеки на етапі планування АС належать:

установлення організаційних засад та визначення завдань з менеджменту безпеки;

проведення аналізу ризиків безпеки АС для запланованої АС чи мережі;

розроблення Положення про системно залежні і вимоги з безпеки (SSRS), якщо цього вимагає Політика безпеки НАТО.

До завдань з менеджменту безпеки на етапі розроблення (закупівлі) АС належать:

розроблення детального визначення загальних заходів з безпеки, які покривають фізичну безпеку, безпеку персоналу, безпеку документів і процедурну безпеку;

розроблення детального визначення заходів щодо комп'ютерної безпеки, а саме:

1) визначення класів функціональних послуг і рівнів гарантій;

2) визначення аспектів безпеки, пов'язаних з об'єднанням АС;

3) визначення характеристик безпеки в документах на закупівлю обладнання;

4) розроблення детального визначення заходів з безпеки зв'язку стосовно безпеки передавання, захисту від витоку конфіденційної інформації через технічні канали, криптографічного захисту;

5) продовження розроблення Положення про системно залежні вимоги з безпеки (SSRS), якщо цього вимагає Політика безпеки НАТО.

До завдань з менеджменту безпеки на етапі імплементації АС належать:

звернення до списку НАТО щодо продуктів з комп'ютерної безпеки та списку НАТО з комп'ютерної безпеки "Продукти, що знаходяться в стадії оцінювання" як основного джерела інформації стосовно комп'ютерної безпеки;

звернення до списку НАТО рекомендованих продуктів як основного джерела інформації стосовно продуктів, що захищають інформацію від витоків через технічні канали;

проведення оцінювання та сертифікації АС, якщо цього вимагає Політика безпеки НАТО;

завершення Положення про системно залежні вимоги з безпеки (SSRS), якщо цього вимагає Політика безпеки НАТО;

формулювання Процедур безпечної експлуатації (SecOP) АС;

акредитація АС, що уможливлює зберігання, оброблення або передавання секретної інформації НАТО в цьому середовищі.

До завдань з менеджменту безпеки на етапі експлуатації АС належать:

зберігання, оброблення та передавання секретної інформації НАТО в експлуатаційному середовищі відповідно до затверджених Процедур безпечної експлуатації (SecOP);

проведення, згідно з Політикою безпеки НАТО, періодичних перевірок стану безпеки АС.

До завдань з менеджменту безпеки на етапі посилення АС належать:

перегляд Положення про системно залежні вимоги з безпеки (SSRS), якщо цього вимагає Політика безпеки НАТО;

проведення в разі виникнення потреби повторного оцінювання та повторної сертифікації АС;

перегляд Процедур безпечної експлуатації (SecOP) АС;

повторна акредитація АС, яка підтверджує можливість зберігання, оброблення та передавання секретної інформації НАТО в цьому експлуатаційному середовищі.

До завдань з менеджменту безпеки на стадії зняття з експлуатації АС належать:

проведення належної архівації або розсекречування (знищення) постійних чи змінних носіїв зберігання комп'ютерної інформації;

проведення належної архівації або знищення паперової документації.

У нормативному документі НАТО C-M(2000)54 - NATO Policy for Standardization наведено механізми, за допомогою яких НАТО досягає взаємодії, використовуючи стандарти. Визнаючи важливість стандартизації для НАТО, Північноатлантична Рада заснувала Організацію НАТО зі стандартизації (NS0) з тим, щоб гармонізувати і координувати діяльність у галузі стандартизації. NSO охоплює:

комітет НАТО зі стандартизації (NCS);

представників країн-членів НАТО у NCS;

штатну групу НАТО зі стандартизації (NSSG);

агенцію НАТО зі стандартизації (NSA).

Кожен із цих органів відповідає за процес розроблення і перегляд стандартів, забезпечення механізмів, які сприяють обміну інформацією, необхідною для національних експертів у справі узгодження положень стандартів.

NCS наглядає за діяльністю NSO, яка відповідає за надання підтримки комітетам, призначеним перевіряти вимоги стандартів, затверджувати завдання стандартизації і розробляти та затверджувати стандарти. Ці комітети можуть передавати функції розроблення та затвердження стандартів підлеглим групам. Стандарти НАТО оформлюють у вигляді:

угод зі стандартизації (STANAGs);

публікацій Альянсу (APs);

міждержавних публікацій (MPs).

У рамках цих документів досягається взаємодія національних військових структур.

Вищезазначені документи розробляють згідно з правилами, сформульованими в AAP-03 - Directive for the Development and Production of STANAGs та APs. Як тільки STANAGs ,APs або MPs прийнято, члени Альянсу повинні як найшвидше їх реалізувати, щоб побудувати та підтримувати основні елементи у взаємодії військових структур з метою оптимізації використання ресурсів.

До складу робочих груп, які розробляють стандарти, включають представників країн-членів НАТО, а також країн Партнерства заради миру, якщо це не суперечить Доктрині НАТО з безпеки. Діяльність робочих груп підтримує Агенція НАТО зі стандартизації, яка відповідає також за супроводження баз даних, що містять STANAGs, APs та MPs.

Оцінювання рівня захищеності АС і виконання робіт з сертифікації засобів технічного захисту інформації

Як відомо, у системі технічного захисту інформації України велике значення має проведення державної експертизи як комплексної системи захисту інформації (КСЗІ), яка є невід'ємною складовою частиною АС (коли планується оброблення інформації, порядок захисту якої регламентується законами України

або іншими нормативно-правовими актами), так і засобів технічного захисту інформації від несанкціонованого доступу (Положення про державну експертизу в сфері технічного захисту інформації, введено в дію наказом Адміністрації Держспецзв'язку України № 93 від 16.05.2007 р. (зі змінами)) та оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, введений в дію наказом Адміністрації Держспецзв'язку України № 112 від 04.07.2008 р.).

При проведенні експертних робіт із державної експертизи експерти керуються вимогами НД ТЗІ 2.5-004 - 99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", введеного в дію наказом ДСТСЗІ СБУ № 22 від 28. 04. 1999 р.

У країнах-членах НАТО цим заходам також надають значну роль. Серед нормативних документів, які стосуються цього напряму, слід відзначити AC/35-D/1019 Guidelines for the evaluation and certification of ADP systems and networks and computer security (COMPUSEC) products. Крім того оцінювання (сертифікація) засобів технічного захисту інформації та компонентів обчислюваної системи АС здійснюється відповідно до вимог Єдиних критеріїв оцінки безпеки інформаційних технологій, встановлених міжнародним стандартом ISO/IEC 15408 Information technology. Security techniques. Evaluation criteria for IT security, більш відомий під назвою Common Criteria (CC).

Засоби та компоненти обчислювальної системи, які оцінені на відповідність стандарту ISO/IEC 15408, також широко використовуються в Україні при побудові АС різного призначення. З метою спрощення процесу аналізу та прийняття рішення щодо можливого використання певного засобу (компонента обчислювальної системи) у складі комплексу засобу захисту КСЗІ було введено в дію ряд документів, а саме: НД ТЗІ 2.6-002-2015 "Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99", введений в дію наказом Адміністрації Держспецзв'язку України від 27.04.2016 р. № 293, НД ТЗІ 2.6-003-2015 "Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99", введений в дію наказом Адміністрації Держспецзв'язку України від 27.04.2016 р. № 294 та НД ТЗІ 2.7-013-2016 "Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99", введений в дію наказом Адміністрації Держспецзв'язку України від 27.04.2016 р. № 295.

Зазначені нормативні документи спрощують завдання експертам щодо проведення експертних робіт, шляхом зіставлення наявних результатів оцінювання компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99.

Висновки й перспективи подальших досліджень

Формування і реалізація єдиної державної політики по забезпеченню захисту національних інтересів від загроз в інформаційній сфері, прийняття відповідних законодавчих актів, координація діяльності органів державної влади по забезпеченню інформаційної безпеки послідовно сприятимуть приведенню української національної системи інформаційної безпеки у відповідність зі світовими стандартами у даній сфері.

Література

1. Закон України Про національну безпеку України від 21 червня 2018 року № 2469-VIII (Відомості Верховної Ради (ВВР), 2018, № 31). **2.** Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. *Офіц. вид.* Київ. КМ України, 2006. 8с. **3. Заячук Я.І.** Аналіз та оцінка ризиків інформаційної безпеки локально-обчислювальної мережі. *Восточно-Европейский журнал передовых технологий.* 2012. № 58. С 40-43. **4. Василенко В.С.** Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах. URL: http://www.rusnauka.com/11_EISN_2010/Informatica/64-068.doc/htm **5.** Security within the North Atlantic Treaty Organisation (C-M(2002) 49). URL:http://arhives.nato.int/amendments-to-nato-c-m-55-15 final. **6. Анісімов А.В., Заславський В.А., Фаль О.М.** Основи інформаційної безпеки та захисту інформації у контексті євроатлантичної інтеграції України. *Науково-методологічний посібник*. Київ, ДП "НВЦ "Євроатлантикінформ". 2006.

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ, КАК СОСТАВЛЯЮЩАЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, В КОНТЕКСТЕ ЕВРОАТЛАНТИЧЕСКОЙ ИНТЕГРАЦИИ УКРАИНЫ

Николай Александрович Гульков
Виталий Станиславович Толкачев

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В современном мире все большее значение приобретает понятие информационной безопасности. Вместе с распространением общего доступа к информации, следуя за развитием коммуникационных систем, расширяется круг возможных информационных угроз, с которыми сталкивается государство.

Именно поэтому информационная безопасность превращается в одну из ключевых составляющих национальной безопасности. Некоторые исследователи считают, что обеспечение информационной безопасности необходимо не только для того, чтобы сохранить неприкосновенность национального информационного пространства, но и настаивают на том, что верно сформулирована национальная информационная стратегия способствовала бы более успешному решению задач в политической, экономической, социальной и других сферах жизни. Предполагается также возможное влияние соответствующей информационной политики на положительный ход решения как внутриполитических так и внешних конфликтов.

В статье осуществляется сравнительный анализ организации защиты информации в странах - членах НАТО и организации технической защиты информации в Украине. Предложенный метод сопоставления имеющихся результатов оценки компонентов доверия к безопасности определенных ISO/IEC 15408 требованиям НД ТЗИ 2.5-004-99 предоставляют возможность получить более объективную и адекватную оценку использования средств и компонентов вычислительной системы, используемые в Украину при построении автоматизированных систем.

Ключевые слова: *информационная безопасность, техническая защита информации, политика безопасности*

TECHNICAL PROTECTION OF INFORMATION AS A COMPONENT OF INFORMATION SECURITY, IN THE CONTEXT EURO-ATLANTIC INTEGRATION OF UKRAINE

Mykola Hulkov
Vitalii Tolkachov

National Defense University of Ukraine named by Ivan Cherniakhovsky, Kyiv, Ukraine

In today's world, the notion of information security is becoming increasingly important. Together with the dissemination of universal access to information, following the development of communication systems, the range of possible information threats facing the state is expanding.

This is why information security becomes one of the key components of national security. Some researchers believe that ensuring information security is necessary not only to preserve the integrity of the national information space, but also to insist that a properly formulated national information strategy would contribute to a more successful solution to the political, economic, social and other spheres of life. It is also possible to influence the relevant information policy on the positive course of resolving both internal and external conflicts.

The article provides a comparative analysis of the organization of information security in NATO member countries and the organization of technical protection of information in Ukraine. The proposed method of comparing the available results of the assessment of security components of the ISO / IEC 15408 defined with the requirements of ND TZI 2.5-004-99 provides an opportunity to obtain a more objective and adequate assessment of the use of the tools and components of the computer system used in Ukraine for the construction of automated systems.

Keywords: *information security, technical protection of information, security policy.*

References

1. Zakon Ukrajiny Pro nacionaljnu bezpeku Ukrajiny vid 21 chervnja 2018 roku № 2469-VIII (Vidomosti Verkhovnoji Rady (VVR), 2018, № 31). **2.** Pravyla zabezpechennja zakhystu informaciji v informacijnykh, telekomunikacijnykh ta informacijno-telekomunikacijnykh systemakh. Ofic. vyd. Kyjiv. KM Ukrajiny, 2006. 8s. **3. Zajachuk Ja.I**. Analiz ta ocinka ryzykiv informacijnoji bezpeky lokaljno-obchysljuvaljnoji merezhi. Vostochno-Evropejskyj zhurnal peredovыkh tekhnologhyj. 2012. № 58. S 40-43. **4. Vasylenko V.S.** Ocinjuvannja ryzykiv bezpeci informaciji v lokaljnykh obchysljuvaljnykh merezhakh. URL: http://www.rusnauka.com/11_EISN_2010/Informatica/64-068.doc/htm **5.** Security within the North Atlantic Treaty Organisation (S-M(2002) 49). URL:http://arhives. nato.int/amendments-to-nato-c-m-55-15final. **6. Anisimov A.V., Zaslavsjkyj V.A., Falj O.M.** Osnovy informacijnoji bezpeky ta zakhystu informaciji u konteksti jevroatlantychnoji integhraciji Ukrajiny. Naukovo-metodologhichnyj posibnyk. Kyjiv, DP "NVC “Jevroatlantykinform”. 2006.