УДК 004.236.13 DOI: 10.31673/ 2412-4338.2018.038893

Ліпінський В. В. *Державний університет телекомунікацій, Київ*

ЗАСТОСУВАННЯ СТАНДАРТІВ НАТО ПРИ СТВОРЕННІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Проведено аналіз стандартів НАТО, розглянуті питання можливого їх застосування при створенні та впровадженні комплексних систем захисту інформації на стадіях життєвого циклу інформаційних систем в сфері національної безпеки. Використання окремих положень стандартів НАТО допомогло б звузити фокус національного законодавства щодо підвищених вимог до інформаційних систем.

Ключові слова: *комплексна система захисту інформації, інформаційна безпека, стандарти НАТО, інформаційна система, національна безпека.*

Lipinskyi V. V. *State University of Telecommunications, Kyiv*

APPLICATION OF NATO STANDARDS FOR THE CREATION OF INFORMATION PROTECTION SYSTEMS IN THE AREA OF A NATIONAL SECURITY

The article analyzes the NATO standards, discusses the possible application of NATO standards in the creation and implementation of integrated information security systems at the stages of the life cycle of information systems in the area of national security. There is a difference in the provisions of the normative acts of Ukraine and NATO regarding the definition of information security. NATO – multi-element education, respectively, all regulatory regulation of information security is aimed at ensuring the interoperability of member countries systems while maintaining significant autonomy. NATO's regulations emphasize that the national regulatory framework remains the responsibility of each NATO member state, but does not require the transition to NATO regulations. Only minimal requirements are available, but they are identical to those adopted globally and specified in international standards and in Ukraine.

When it comes to information systems for defense purposes, for them ensuring the availability of the system and the security of communications and communications during tactical operations are just the most important. We have defense information systems in the legislation, as well as any information systems, with only increased protection requirements. The use of separate provisions set by NATO standards, which specifically addresses the increased requirements for system availability and secure communication, would help to narrow the focus of national legislation on the increased requirements for information systems. Since the provisions of NATO standards are directed, first of all, to uniting a large number of legal rules of the Alliance member countries, some principles may be applied for the unification (establishment of information exchange) between the information systems of different structures of our state.

Keywords: *integrated information security systems, information security, NATO standards, information systems, national security.*

Липинский В. В. *Государственный университет телекоммуникаций, Киев*

ПРИМЕНЕНИЕ СТАНДАРТОВ НАТО ПРИ СОЗДАНИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАСТИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Проведен анализ стандартов НАТО, рассмотрены вопросы возможного их применения при создании и внедрении комплексных систем защиты информации на стадиях жизненного цикла информационных систем в области национальной безопасности. Использование отдельных положений стандартов НАТО помогло бы сузить фокус национального законодательства относительно повышенных требований к информационным системам.

Ключевые слова: *комплексная система защиты информации, информационная безопасность, стандарты НАТО, информационная система, национальная безопасность.*

© Ліпінський В. В., 2018

Вступ. Постановка задачі дослідження

Інформаційні системи є невід'ємною частиною будь-якої галузі життєдіяльності держави, зокрема сфери національної безпеки.

Згідно із Законом України «Про національну безпеку України» від 21.06.2018 №2469-VIII *"Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, ... інформаційної безпеки, ... кібербезпеки України тощо. Загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони визначаються у ... Стратегії воєнної безпеки України, Стратегії кібербезпеки України..."*.

Воєнна доктрина України (затверджено Указом Президента України від 24.09.2015 №555/2015) визначає, що "*Головними тенденціями, що впливають на воєнно-політичну обстановку ... є: модернізація та вдосконалення спеціальними службами іноземних держав систем і комплексів технічної розвідки, нарощування їх можливостей, спроби несанкціонованого доступу до об'єктів інформаційної інфраструктури України; ... Забезпечення інформаційної складової національної безпеки здійснюватиметься шляхом запровадження ефективної системи заходів стратегічних комунікацій у діяльність органів сектору безпеки"*, а Державну службу спеціального зв'язку та захисту інформації України віднесено до сил оборони, як одного із центральних державних органів у частині виконання завдань з оборони держави.

У Законі України "Про оборону України" від 06.12.1991 №1932-XII вказано, що підготовка держави до оборони в мирний час включає захист інформаційного простору України та її входження у світовий інформаційний простір, створення розвинутої інфраструктури в інформаційній сфері.

Нормативно-правові акти України в сфері кібербезпеки

Державною політикою України визначається, що кібербезпека є однією із провідних складових національної безпеки України, частиною оборонного сектору, а інформація, яка циркулює в інформаційних системах державних органів, підлягає захисту на найвищому рівні. Законодавством України визначається вимога до обов'язкового захисту абсолютно всієї інформації, а також програмного забезпечення, які знаходяться в інформаційних системах сфери національної безпеки, шляхом створення комплексних систем захисту інформації. Варто також наголосити на тому, що значну частину інформації, що належить до сектору національної безпеки, віднесено до державної таємниці України.

Розподіл повноважень у сфері захисту інформації, наведено у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах». Регулюючу функцію Державної служби спеціального зв'язку та захисту інформації, незалежно від сфери застосування інформації та інформаційних систем, визначено у Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 №3475-VI, а також те, що *"Державна служба спеціального зв'язку та захисту інформації України спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України"*.

Усе вищенаведене законодавчо визначає вимогу до побудови комплексних систем захисту інформації в інформаційних системах сфери безпеки і оборони для забезпечення безпеки даних, що є критично важливими для національної безпеки держави, а також для підтримки можливості оперативного обміну цими даними у процесі провадження діяльності у цій сфері.

Нормативно-правові акти України в сфері захисту інформації

Україна довгий час намагається стати повноправним членом Північноатлантичного альянсу. Кожна держава, яка наважилася на вступ до НАТО, має пройти певний процес приєднання до Альянсу.

Північноатлантичний альянс (далі – НАТО) – у першу чергу військове об'єднання, що створює особливі потреби та вимоги до захисту, характерні для оборонної сфери. Налагоджений зв'язок та ефективна підтримка прийняття рішень є критичними для військових формувань, оскільки необхідно безперервно забезпечувати спільне управління збройними силами та озброєнням, а також швидку та точну оцінку ситуації на основі якомога більшої кількості зібраної інформації високої якості.

Ці вимоги присутні й у інших сферах (управління бізнес-процесами, наприклад), тому більшість стандартів, окремих механізмів захисту та розробок запозичується з цивільного сектору.

Альянс – багатоелементне об'єднання, і це ставить питання ефективної взаємодії. Зовнішнє регулювання стає у часткову чи повну невідповідність із внутрішнім, а також з'являється проблема масштабування і сумісного керування елементами зі збереженням певного рівня автономності.

Таким чином, нормативно-правові акти, прийняті НАТО у сфері захисту інформації, можна умовно розподілити на дві групи:

- Міжнародні стандарти, які на державному рівні визнаються усіма країнами, що входять до Північно-Атлантичного Альянсу, і використання яких спрямоване на забезпечення сумісності (інтероперабельності).
- Власне документація НАТО – стандарти, положення та правила, які встановлюють мінімальні вимоги щодо забезпечення захисту інформації на встановленому рівні.

Задачі щодо гармонізації нормативно-правової бази України із стандартами НАТО

Якщо провести аналіз нормативно-правової бази України з питань створення КСЗІ на кожному етапі життєвого циклу інформаційних систем та аналізу стандартів НАТО щодо використання КСЗІ на стадіях життєвого циклу інформаційних систем, особливостей створення КСЗІ в інформаційних системах та застосування досвіду країн НАТО, виявиться наступне:

По-перше, існує різниця у положеннях нормативних актів України та НАТО щодо визначення інформаційної безпеки , а саме: НАТО – багатоелементне утворення, відповідно, усе нормативне регулювання сфери інформаційної безпеки направлено на забезпечення інтероперабельності систем країн-членів при збереженні значної автономії.

Через це, крізь усю документацію НАТО прослідковується акцент на забезпеченні захисту даних при їх передаванні каналами зв'язку. Українське законодавство таке питання розподілу та об'єднання не визначає, транспортна складова є важливим моментом, але не головним. Власне, в нормативних документах НАТО підкреслюється, що національна нормативна база залишається у кожної країни-члена НАТО своя, та не має вимоги переходити на нормативні документи НАТО.

Наявні лише мінімальні вимоги, але вони ідентичні прийнятим в усьому світі та зазначеним у міжнародних стандартах та в Україні, це – ISO 27001 та 27002 прийняті у вигляді СУІБ 1.0 та 2.0 (щоправда, у банківській системі).

Якщо говорити саме про інформаційні системи оборонного призначення, для них забезпечення доступності системи та безпеки зв'язку та комунікацій під час тактичних операцій якраз і є найголовнішими. У нас інформаційні системи оборонного призначення в законодавстві розглядаються, як і будь-які інформаційні системи, тільки із підвищеними вимогами до захисту.

Використання окремих положень встановлених стандартами НАТО, які стосуються саме підвищених вимог до доступності систем та захищеного зв'язку, допомогло б звузити фокус національного законодавства щодо підвищених вимог до інформаційних систем.

З огляду на вищевикладене, доцільно здійснити наступне:

1) Необхідно розглянути можливість імплементації окремих положень стандартів НАТО, які стосуються з'єднання мереж оперативного застосування (стратегічного та тактичного призначення) при різних варіантах їх поєднання (наприклад, STANAG 5067 C3B [1] – «Стандарт взаємозв'язку мереж IPv4 на рівнях безпеки Mission Secret та Unclassified» (Standard For Interconnection Of Ipv4 Networks At Mission Secret And Unclassified Security Levels)).

2) Встановити додаткові вимоги (оскільки вони носять специфічний характер відносно цивільних інформаційних систем) окремо для інформаційних системи оборонного призначення.

По-друге, оскільки положення стандартів НАТО направлені, в першу чергу, на об'єднання великої кількості правових норм країн – членів альянсу, деякі принципи можливо застосувати для об'єднання (налагодження обміну інформацією) між інформаційними системами різних структур нашої держави. Інформація, необхідна для забезпечення оборони, неоднорідна і не походить з одного джерела. Комплексну картину можна скласти, лише об'єднавши розвідувальну, тактичну, стратегічну інформацію, оперативну інформацію військових підрозділів різних родів військ та правоохоронних органів, МНС, метеорологічних служб тощо – необхідний механізм захищеного зв'язку між ними усіма.

Тому, можливо:

1) Налагодити систему різних комунікаційних мереж, які б могли використовуватися усіма структурами, що забезпечують захист національних інтересів і для цього використовують інформаційні системи. Це стосується, звичайно, і органів державного управління, які повинні у реальному часі здійснювати обмін інформацією із сектором оборони.

2) Для оцінки відповідності даної системи застосувати STANAG 5067 C3B [1] – «Стандарт взаємозв'язку мереж IPv4 на рівнях безпеки Mission Secret та Unclassified» (Standard For Interconnection Of Ipv4 Networks At Mission Secret And Unclassified Security Levels) та AC/322-D(2014)0008-FINAL: Consultation, Command And Control (C3) Board [2] – «Мінімальні вимоги безпеки ІТС (включаючи кіберзахист) для національних ІТС, критичних для реалізації основних завдань НАТО» (Minimum Requirements Of CIS Security (including Cyber Defence) For National CIS Critical For Nato Core Tasks).

По-третє, у стандартах НАТО не існує поняття «комплексна система захисту інформації». Інформаційна безпека сама по собі розглядається як комплекс, що поєднує у собі не тільки безпеку даних, програмного та апаратного забезпечення, а й безпеку персоналу, фізичну безпеку, безпеку навколишнього середовища тощо. При побудові систем забезпечення безпеки, документація НАТО розглядає усі типи носіїв інформації, як паперові, так і електронні. Не часто всередині організації (військової, в тому числі) обробляється лише інформація на якомусь одному типі носіїв.

В національному ж законодавстві усі вищевказані поняття рознесені, підкреслюється, що вимоги стосуються систем, в яких інформація оброблюється електронними засобами обчислювальної техніки тощо. З точки зору застосування даних норм на практиці, така ситуація не є правильною.

У якості прикладу комплексного підходу, визначеного у стандартах НАТО, можна навести:

- AC/35-D/1014-REV3 SECURITY COMMITTEE [3] – «Положення про структуру та зміст Порядку проведення робіт із забезпечення безпеки інформаційних та комунікаційних систем (ІКС)» (Guidelines for the Structure and Content of Security Operating Procedures (SecOPs) for Communication And Information Systems (CIS)): *"Під час проведення робіт повинні бути розглянуті:*
  - *Адміністрування та організація безпеки;*
  - *Фізична безпека;*
  - *Безпека персоналу;*
  - *Безпека інформації;*
  - *INFOSEC - комп'ютерна, криптографічна безпека, безпека передавання та приховання випромінювання;*
  - *План дій на випадок непередбачуваних обставин;*
  - *Управління конфігурацією;*
  - *Координація".*

- AC/322-D(2014)0008-FINAL: Consultation, Command and Control (C3) Board [2] – «Мінімальні вимоги безпеки ІТС (включаючи кіберзахист) для національних ІТС, критичних для реалізації основних завдань НАТО» (Minimum Requirements Of CIS Security (including Cyber Defence) For National CIS Critical For Nato Core Tasks): (Додаток "F" до Політики безпеки НАТО) "безпека ІТС" є складовою ширшого поняття "Забезпечення безпеки інформації" разом з іншими галузями, включаючи безпеку персоналу та фізичну безпеку. Мінімальні вимоги, що стосуються персоналу та фізичної безпеки, розглядаються в спеціальних директивах, наведених у посиланнях у даному стандарті".

До того ж, невід'ємно від інших положень, приділено увагу функціям захисту, які у національному законодавстві у рамках КСЗІ не розглядаються, а негласно покладаються на DLP-системи. Наприклад, у Мінімальних вимогах [2] (AC/322-D(2014)0008-FINAL) наявні розділи, в яких містяться вимоги до дій, які необхідно вжити у випадку надзвичайної ситуації або виявлення інциденту, порядку використання мережі Інтернет та соціальних мереж, а також порядок координації дій із відповідними уповноваженими органами.

У AC/35-D/1014-REV3 увага приділяється користувачам портативних засобів обчислювальної техніки та зв'язку, які включають ноутбуки, електронні записники та кишенькові комп'ютери з можливістю зберігання, обробки та/або передавання даних (наприклад, "електронні помічники" PDA та BlackBerry), а також засоби GSM та стільникового зв'язку із функціональними можливостями PDA. Порядок повинен включати інструкції для користувачів, які беруть портативні засоби обчислювальної техніки та зв'язку на місії поза межами організації, чи використовують для роботи вдома. Регулювання таких моментів у національних стандартах відсутнє.

Якщо поєднувати регулювання усіх вищевказаних моментів у рамках одного чи навіть групи документів, це погіршить зручність їх застосування. Тому, варто розглянути можливість створення фреймворку, на зразок NIST Cybersecurity Framework. Для цього необхідно:

- Узгодити між собою існуючі нормативні документи (наприклад, положення ТПКО-95 та НД ТЗІ 1.6-005 майже ідентичні), усунути повторення;

- Створити (або якщо такі існують у інших сферах – модифікувати та застосувати їх) нормативні документи, які регулюють питання забезпечення фізичної безпеки, безпеки персоналу, навколишнього середовища (за основу можна взяти список, наведений у AC/35-D/1014-REV3) [3] ; також, переглянути, якщо існують (у тому числі у вигляді окремих пунктів НД ТЗІ), або в іншому випадку – розробити нормативні документи, які б визначали правила користування технікою, яка належить системі, але виноситься за межі організації (корпоративні ноутбуки при роботі з дому, PDA, BlackBerry, засоби GSM та стільникового зв'язку із функціональними можливостями PDA);
- Створити центральний документ або обрати його з існуючих (найкращим варіантом представляється НД ТЗІ 3.7-003); у ньому передбачити посилання на інші документи за етапами побудови системи забезпечення інформаційної безпеки так, щоб увесь фреймворк мав форму «дерева»; у цьому «дереві» на початку повинні бути наведені керівні принципи та вимоги, а далі слідують «розгалуження» за кожним логічним розділом.

Висновки. Такий підхід дозволить уніфікувати процеси створення, впровадження та подальшої підтримки систем захисту, швидко знаходити стандартизовані вимоги відповідно до потреб у кожній окремій ситуації.

Список використаної літератури:

1. STANAG 5067 C3B Standard For Interconnection Of Ipv4 Networks At Mission Secret And Unclassified Security Levels.

2. AC/322-D(2014)0008-FINAL. Consultation, Command And Control (C3) Board. Minimum Requirements Of CIS Security (including Cyber Defence) For National CIS Critical For NATO Core Tasks.

3. AC/35-D/1014-REV3 SECURITY COMMITTEE Guidelines For The Structure And Content Of Security Operating Procedures (SecOPs) For Communication And Information Systems (CIS).

Автор статті (Author of the article)

Ліпінський Вадим Володимирович – аспірант кафедри інформаційної та кібернетичної безпеки (Lipinskyi Vadym Volodymyrovych – post-graduate student of the Information and Cybernetic Security Department). Phone: +380 50 710 2239. E-mail: info@ics.org.ua.