УДК 004.236.13
DOI: 10.31673/2409-7292.2018.030610

Ліпінський В.В., Братков О.І.

ПИТАННЯ ВДОСКОНАЛЕННЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ СТВОРЕННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ТА ЗАСТОСУВАННЯ ДОСВІДУ КРАЇН НАТО

У статті розглянуто питання необхідності вдосконалення нормативно-правового регулювання при створенні та впровадженні комплексних систем захисту інформації в інформаційних системах з використанням положень стандартів НАТО. Акцентована увага га процесах створення, впровадження та подальшої підтримки систем захисту інформації, пошуку стандартизованих вимог відповідно до потреб у кожній окремій ситуації.

Ключові слова: Стандарти НАТО, Комплексні системи захисту інформації, Технічний захист інформації, Інформаційні системи, Центральний галузевий нормативний документ.

Вступ. На основі проведеного аналізу 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, виявилась суттєва різниця яка існує у положеннях нормативних актів України та НАТО, зокрема щодо особливостей створення КСЗІ в інформаційних системах та необхідності нормативного врегулювання сфери інформаційної безпеки.

В українському національному законодавстві використовується різні назви основного об'єкта вивчення (зокрема Інформаційна система – ІС, Автоматизована система – АС, тощо). У якості прикладу: НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»:

- інформаційна система – організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;
- телекомунікаційна система – організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином;
- інтегрована система - сукупність двох або кількох взаємопов'язаних інформаційних та (або) телекомунікаційних систем, в якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Під інформаційно-телекомунікаційною системою в цьому НД ТЗІ розуміється будь-яка система, яка відповідає одному з трьох наведених вище видів автоматизованих систем.

НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»:

Обчислювальна система; ОС (computer system) — сукупність програмних-апаратних засобів, призначених для обробки інформації.

Автоматизована система; АС (automated system) — організаційно-технічна система, що реалізує інформаційну технологію і об'єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється.

Комп'ютерна система; КС (computer system, target of evaluation) —сукупність програмно-апаратних засобів, яка подана для оцінки.

В усіх стандартах як НАТО, так і міжнародних, є тільки визначення інформаційної системи, іноді трапляється інформаційно-комунікаційна система.

Законодавством України визначається вимога до обов'язкового захисту абсолютно усієї інформації що відноситься до державних інформаційних ресурсів, а також програмного забезпечення, які знаходяться в інформаційних системах, шляхом створення комплексних

систем захисту інформації. Законодавчо визначається вимога до побудови комплексних систем захисту інформації в інформаційних системах 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. Нормативні акти в сфері технічного захисту інформації переважним чином висувають вимоги до розробників та Власників інформаційних систем щодо побудови комплексних систем захисту інформації, а не практичним рекомендаціям та методикам по захисту інформації в інформаційних системах та орієнтовані в першу чергу на захист інформації з обмеженим доступом.

Слід зауважити, що існує різне правове регулювання щодо процедур здійснення технічного захисту інформації та комплексів захисту інформації з окремими процедурами отримання експертних висновків. Існує вимога Держспецзв'язку щодо застосування Переліку, що містить номенклатуру засобів ТЗІ (технічних засобів, основним функціональним призначенням яких є захист інформації від загроз витоку, порушення цілісності та блокування; технічних засобів, в яких додатково до основного призначення передбачено функції захисту інформації; засобів, які призначені, спеціально розроблені або пристосовані для пошуку закладних пристроїв і які створюють загрозу для інформації; засобів, які спеціально розроблені або пристосовані для оцінювання захищеності інформації), відповідність яких вимогам нормативних документів з питань ТЗІ засвідчено позитивним експертним висновком, одержаними у порядку, який встановлено нормативно-правовими актами.

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.

Основна частина. Існує різниця у положеннях нормативних актів України та НАТО щодо визначення інформаційної безпеки. 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, для них забезпечення доступності системи та безпеки зв'язку та комунікацій якраз і є найголовнішими. Використання окремих положень встановлених стандартами НАТО при розробці та впровадженні нормативних документів, які стосуються саме підвищених вимог до доступності систем та захищеного зв'язку, допомогло б звузити фокус нормативного регулювання щодо підвищених вимог до інформаційних систем.

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, а можливо імплементувати в національне законодавство. 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.

Пропонується розробити прийняти нові або внести зміни до нормативно –правових актів у сфері технічного захисту інформації, а саме:

1. Необхідно розглянути можливість імплементації окремих положень стандартів НАТО, які стосуються з'єднання мереж оперативного застосування при різних варіантах їх поєднання. Для встановлення додаткових вимог пропонується прийняти STANAG 5067 C3B (Standard For Interconnection Of Ipv4 Networks At Mission Secret And Unclassified Security Levels) у якості стандарту використання мереж IPv4 [1].

2. Необхідно налагодити систему взаємодії різних комунікаційних мереж, які б могли використовуватися усіма державними 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, що належить до інформаційних ресурсів держави та інформації з обмеженим доступом. Пропонується прийняти стандарт для оцінки відповідності даної системи вимогам безпеки, за основу для якого взяти документ - AC/322-D(2014)0008-FINAL Consultation, Command And Control (C3) Board 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) [2]. Окремим пунктом у стандарті вказати, що оцінка відповідності системи на рівні мережі здійснюється за стандартом, прийнятим згідно попереднього пункту.

3. Якщо поєднувати регулювання абсолютно усіх моментів, що стосуються інформаційної безпеки, у рамках одного чи навіть групи документів, це погіршить зручність їх застосування. Тому, пропонується створити фреймворк, на зразок NIST Cybersecurity Framework. Для цього необхідно:

- 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); також, розробити нормативні документи, які б визначали правила користування технікою, яка належить системі, але виноситься за межі організації (корпоративні ноутбуки, при роботі з дому, PDA, засоби GSM та стільникового зв'язку із функціональними можливостями PDA);
- Створити центральний галузевий нормативний документ, узгодивши його з положеннями передбаченими в НД ТЗІ 3.7-003) та передбачити у ньому 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.

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

4. При розробці нормативних документів в сфері технічного захисту інформації, пропонується звести усі терміни, що стосуються визначення систем, до двох конкретних понять, взявши за основу документ - ISO/IEC 27000 Information technology. Security techniques. Information security management systems. Overview and vocabulary та Dictionary of Military and Associated Terms. US Department of Defense 2005 [3]:

Відповідно до першого: information system – applications, services, information technology assets, or other information handling components;

Відповідно до другого: communications and information system – an assembly, which nclude personnel, equipment and procedures, organized to accomplish specific informationconveyance and processing functions.

5. Пропонується при розробці галузевих нормативних актів застосовувати додаткові визначення функціональних профілів захищеності. За рішенням експертів, необхідно обрати один з наступного переліку документів:

SP 800-53 “Рекомендовані контролі безпеки для федеральних інформаційних систем”[4];

The Information Technology Security Evaluation Criteria (ITSEC) [5];– додатково містить детально описані рівні безпеки;

“Загальні критерії оцінки захисту інформаційних технологій (ISO 15408: Common Criteria for Information Technology Security Evaluation [6]) – вважаються більш повними порівняно з ITSEC, проте в них менш детально описано вимоги до механізмів захисту організаційного рівня і вимоги з фізичного захисту; більшу увагу сконцентровано на технічному захисті інформації.

6. Пропонується нормативно встановити у відповідність функції та рівні гарантій безпеки з урахуванням положень НД ТЗІ 2.5-004 та обраного стандарту НАТО, за AC/322-D(2014)0008-FINAL Consultation, Command And Control (C3) Board [7] 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) скласти функціональний профіль (чи кілька, для різних систем) та прийняти його базовим для інформаційних систем оборонного призначення. Видати складений профіль окремим галузевим нормативним документом.

7. Створити галузевий нормативний документ з класифікації та категоріювання систем, у якому:

по-перше, звести разом положення ТПКО-95 та НД ТЗІ 1.6-005-2013, усунути положення, які дублюються;

по-друге, визначити класифікацію АС за архітектурою на класифікацію за користувачами й характером використання, вказати нові положення у даному стандарті, узгодивши їх з положеннями НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» розділу 5, а також в усі подальші розділи, пов’язані з даним питанням (або до нового стандарту згідно із попереднім пунктом);

8. Створити нормативний документ (регламент проведення робіт) з обстеження середовищ, у якому привести перелік середовищ у відповідність з AC/35-D/1021-REV3 SECURITY COMMITTEE [8]. Інакше, можливо в НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» у пунктах 6.1.2.4-6.1.2.7 вказати належність кожного підпункту зовнішньому, внутрішньому чи електронному середовищу згідно стандартів НАТО, основуючись на AC/35-D/1021-REV3, і таким чином забезпечуючи можливість сумісного використання без значної зміни національного стандарту.

У новому стандарті (регламенті) вказати, або внести до змінених пунктів НД ТЗІ 3.7-003-2005, відповідно до групування, вимоги щодо аналізу режиму безпечного функціонування, реалізації принципу найменших привілеїв та вимоги щодо обміну інформацією, а також вартості ресурсів та систем підтримки.

9. Створити нормативний документ – регламент проведення атестації інформаційно-телекомунікаційних систем, в якому передбачити варіанти результатів проведення атестації згідно пункту про результати проведення атестації AC/35-D/1021-REV3 SECURITY COMMITTEE Інструкція з атестації інформаційних та телекомунікаційних систем (ІТС). Посилання на даний документ вказати у:

НД ТЗІ 2.1-001-2001 «Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення» пунктах 4.1, 5.3 та 5.4;

«Положення про державну експертизу в сфері технічного захисту інформації», затвердженого Наказом Адміністрації ДССЗЗІ №93 від 16.05.2007, розділі ІІ пунктах 4, 27, 28, 29 (внести відповідні пункти до розділу ІІІ, Додатків 8 та 9);

НД ТЗІ 2.6-001-11 “Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах” пункті 2.3 Додатку А, Додатках Д та Ж.

Висновки. Імплементація в національне законодавство окремих норм нормативно-правових актів, прийняті в країнах НАТО у сфері захисту інформації, таких як Міжнародні стандарти, які на державному рівні визнаються усіма країнами, що входять до Північно-Атлантичного Альянсу і використання яких спрямоване на забезпечення сумісності (інтероперабельності) так і власне документація НАТО допомогло б звузити фокус нормативного регулювання щодо підвищених вимог до інформаційних систем.

Список використаних джерел:

1. STANAG 5067 C3B (Standard For Interconnection Of Ipv4 Networks At Mission Secret And Unclassified Security Levels).
2. стандарт для оцінки відповідності даної системи вимогам безпеки, за основу для якого взяти AC/322-D(2014)0008-FINAL Consultation, Command And Control (C3) Board.
3. ISO/IEC 27000 Information technology. Security techniques. Information security management systems. Overview and vocabulary та Dictionary of Military and Associated Terms. US Department of Defense 2005.
4. SP 800-53 “Рекомендовані контролі безпеки для федеральних інформаційних систем”;
5. The Information Technology Security Evaluation Criteria (ITSEC).
6. ISO 15408: Common Criteria for Information Technology Security Evaluation.
7. AC/322-D(2014)0008-FINAL Consultation, Command And Control (C3) Board.
8. AC/35-D/1021-REV3 SECURITY COMMITTEE

Надійшла: 2.05.2018 Рецензент: д.т.н. Вишнівський В.В.