УДК 681.3.96

АРТЮШИН Георгій Михайлович
ВОЛОЩЕНКО Андрій Сергійович

ШЛЯХИ ВДОСКОНАЛЕННЯ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СБ УКРАЇНИ

Постановка проблеми. На сучасному етапі перед Службою безпеки України постають численні виклики у сфері захисту інформації, що обробляється в її інформаційно-телекомунікаційних системах (далі – ІТС). Масове створення, впровадження й експлуатація цих систем разом із великими перевагами та зручностями породжують і значні небезпеки. Виток інформації технічними каналами, а також несанкціоноване проникнення у відомчі інформаційні системи можуть спричинити важкі наслідки для безпеки країни, протидія яким є особливо актуальною в умовах російської агресії проти нашої держави.

Ця проблематика відображена зокрема у переліку ризиків в «Антикорупційній програмі СБУ на 2021–2024 роки», де зазначено, що існують такі чинники, як: недосконаліть нормативно-правової бази з порушеного питання, недостатнє матеріально-технічне забезпечення, відсутній електронний документообіг, недостатня обізнаність співробітників СБУ з вимогами законодавства у сфері документообігу та захисту інформації з обмеженим доступом, недостатній рівень контролю за організацією модернізації ІТС та побудови їхніх комплексних систем захисту інформації (далі – КСЗІ) [1].

На сьогодні визначено низку причин, що викликають ці проблеми:

– ігнорування системного підходу до методології аналізу системи захисту інформації;

– недосконаліть механізмів повного й достовірного підтвердження якості системи захисту інформації;

– недоліки нормативно-правового та методичного забезпечення системи захисту інформації;

– недоліки організаційного забезпечення системи захисту інформації;

– недоліки матеріально-технічного забезпечення системи захисту інформації;

– недоліки фінансового забезпечення системи захисту інформації;

– недоліки кадрового забезпечення системи захисту інформації [2].

Аналіз останніх досліджень і публікацій. Захист критично важливих масивів даних повинен відповідати міжнародним і національним нормативно-методичним документам і стандартам. На теперішній час засто-

совуються високовартісні технічні засоби та впроваджуються суворо регламентовані організаційні заходи. Однак досі немає відповіді на найважливіше питання – наскільки рішення, що пропонується або реалізується, дійсно якісне та достатнє, яка його запланована й реальна ефективність, наскільки воно відповідає вимогам сучасності. Актуальність вирішення вказаної проблеми спонукала до розвитку теоретичних досліджень у цій сфері. Зокрема слід зазначити вагомий внесок таких учених-дослідників, як М. Вертузаєв, Д. Мялковський, Л. Скрипник, В. Хорошко. У Національній академії СБ України значних наукових результатів у галузі захисту інформації, що обробляється в інформаційно-телекомунікаційних та автоматизованих системах, досягли Г. Гулак, І. Касперський, В. Настрадін, О. Хмельницький.

Мета статті – на основі проведеного аналізу недоліків, розгляду та систематизації теоретико-практичних рекомендацій щодо вдосконалення механізмів забезпечення системи захисту інформації в інформаційно-телекомунікаційних системах СБ України обґрунтувати теоретико-методологічні засади оптимізації їхньої побудови.

Виклад основного матеріалу. Основу системи українського законодавства у сфері захисту інформації становлять: закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», Указ Президента «Про Положення про технічний захист інформації в Україні», інші нормативно-правові акти та нормативні документи системи ТЗІ. Вони визначають базову термінологію й положення про те, що захист інформації є одним із основних видів інформаційної діяльності у сфері державної політики і регулювання [3–9].

Слід також зазначити, що вибудована на основі Закону України «Про основні засади забезпечення кібербезпеки України» національна система кібербезпеки не забезпечує належним чином виконання завдань із забезпечення не тільки внутрішньої, а й міжнародної співпраці у сфері кібербезпеки. Цей закон на хвилі популярності тематики впроваджений на противагу законодавству у сфері захисту інформації, а не як його доповнення та розвиток. Його положення не поширюються на:

– відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) у комунікаційних та/або технологічних системах;

– діяльність, пов’язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

– комунікаційні системи, які не взаємодіють із публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем) [10].

Як зазначає Д. Мялковський, вітчизняна модель законодавства у сфері захисту інформації не застосовує сучасного ризик-орієнтованого підходу, є нединамічною щодо реагування на появу нових загроз та потребує

зміни своєї парадигми: від контролю за процесами захисту інформації до оцінки безпеки інформації, що повністю відповідає моделі ЄС. Це передбачатиме ревізію та осучаснення законів України про захист інформації в інформаційно-телекомунікаційних системах, державну таємницю, електронні довірчі послуги, а також тих, що визначають основні засади забезпечення кібербезпеки, ліцензування господарської діяльності в цій сфері.

Крім того, необхідним є внесення змін до низки указів Президента України та постанов Кабінету Міністрів України з урахуванням положень законодавства ЄС та НАТО, розвитку інформаційно-комп'ютерних технологій (далі – ІКТ) і постійного збільшення попиту на безпечні й надійні продукти забезпечення захисту інформації та довіри до електронних послуг.

Реалізація таких підходів надасть можливість провести ребрендинг та осучаснити сутність поняття «комплексна система захисту інформації», запровадивши ризик-орієнтований підхід до безпеки інформації, «акредитацію з безпеки» як механізм підтвердження за результатами комплексної оцінки заходів із запровадження як механізмів безпеки, так і обов'язкових для виконання в установах правил безпеки всіма співробітниками, які мають відношення до застосування ІКТ, надаючи можливість для широкого застосування міжнародних і галузевих стандартів (вимог) із захисту та безпеки інформації [11].

Отже, у зв'язку з розвитком стандартизації у сфері інформаційної безпеки (безпеки інформації), систем управління безпекою інформації, які ґрунтуються на ризик-орієнтованому підході, особливої актуальності для України набувають:

– розроблення системи безпеки інформації в автоматизованих системах (далі – АС), кібербезпеки на основі узагальнення та систематизації вітчизняного законодавства і його гармонізації з міжнародним;

– подальший перегляд чинних норм із метою модернізації (трансформації) механізмів побудови систем захисту інформації та їхнього функціонування відповідно до стандартів ISO/IEC серії 27, оцінювання відповідності їм з урахуванням кращих практик українського законодавства;

– поступовий перехід від регулювання створення комплексних систем захисту інформації систем із підтвердженою відповідністю до державного регулювання забезпечення безпеки критичної / чутливої інформації з урахуванням міжнародних стандартів ISO/IEC серії 27 і галузевих стандартів (правил) з організації та управління безпекою інформації (інформаційною безпекою), передових світових практик, їх імплементації, зокрема запровадження систем управління ризиками для інформаційних активів державних органів, підприємств, установ і організацій [12; 13];

– удосконалення законопроєкту «Про безпеку інформації та інформаційно-комунікаційних систем», який би доповнив та осучаснив існуючу систему захисту інформації, урахував положення інших законів України як у сфері національної безпеки, так і регулювання суспільних відносин у сфері кібербезпеки [14].

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, установленому законодавством.

Необхідно зазначити, що в дослідників та експертів є певна недовіра до впроваджених або таких, що впроваджуються в ІТС, КСЗІ з підтвердженою відповідністю, вказується на їхню деяку неспроможність протистояти сучасним загрозам безпеці інформації [2; 11–13].

Поясненням цього є часткова застарілість законодавства у сфері захисту інформації, зосередженість його норм на організаційно-технічних питаннях експлуатації відповідним чином оціненої та зафіксованої в атестаті відповідності КСЗІ, зайва кількість документів, велика тривалість розробки та погодження як технічних завдань на створення, так і документів із підтвердження відповідності КСЗІ, незадовільна робота служб захисту інформації, які повинні забезпечувати його модернізацію та розвиток, а також хронічна нестача коштів на виконання цих завдань.

Тож постає потреба осучаснити сутність поняття КСЗІ, запровадивши ризик-орієнтований підхід до безпеки інформації, спростивши процеси створення КСЗІ, та оптимізувати пакет документів, зменшивши їхню кількість до мінімально необхідної.

На основі власного досвіду та галузевих досліджень визначено такі проблеми, що ускладнюють швидке, якісне та доступне створення КСЗІ:

– надто формалізований підхід до документації (велика кількість документів, надлишковість і дублювання інформації в них, «паперовий» захист). Як приклад, із метою контролю за правомірністю зареєстрованих подій у ІТС має вестися журнал реєстрації подій у паперовому вигляді, що ніяк не відповідає викликам сучасності;

– великі терміни проведення державної експертизи (протягом двох місяців (для АС класу «1») та протягом шести місяців (для АС класу «2»), як передбачено нормативною базою) та інструментального контролю (один раз на 20 місяців, як передбачено календарними планами) [1];

– недостатня актуалізація вимог і рекомендацій, відсутність централізованої та суворо типізованої системи конкретних моделей побудови АС відповідно до різних класів;

– відсутність ефективної системи ринкового нагляду у сфері захисту інформації, як наслідок, монополізація цієї сфери окремими підприємствами та відповідно висока вартість послуг;

– застаріла матеріально-технічна база в регіональних органах СБУ;

– недостатнє фінансування на закупівлю апаратних засобів, ліцензійного програмного забезпечення для повсякденної діяльності, спеціалізованого програмного забезпечення для

протидії несанкціонованому доступу та задля захисту даних для подальшого створення КСЗІ в АС класу «1» та «2» для потреб регіональних органів;

– обмеження кількості АС, призначених для обробки інформації, що становить державну таємницю, у регіональних органах, яке встановлене відомчими документами, не відповідає викликам сучасності та не сприяє ефективній роботі підрозділів цих органів;

– відсутність у регіональних органах СБУ спеціалізованого обладнання для проведення робіт із ТЗІ в повному обсязі своїми силами.

Ще одна серйозна проблема – питання кадрового забезпечення створення КСЗІ.

Фахівці зазначають, що профільна освіта з кібербезпеки, інформаційної безпеки, технічного та криптографічного захисту інформації в Україні потребує вдосконалення, як і курси підвищення кваліфікації. Нестачу профільних знань фахівці компенсують зазвичай підготовкою й отриманням міжнародних професійних сертифікатів (наприклад, CISSP, CISM, 0SCP, GSEC 320 та інших), що дає хороший базовий рівень. Однак на державному рівні такі сертифікати визнання не отримали. Ситуацію варто було б змінити [12; 13].

Для трансформації галузі захисту інформації необхідне розроблення ефективної політики у сфері підготовки кадрів, виокремлення причин низького фахового забезпечення впровадження та експлуатації ІТС, нових систем надання електронних послуг. Стислий аналіз стану справ із підготовки фахівців у цій сфері вказує на наявність системних проблем, які потребують негайного вирішення.

Слід зазначити, що спеціальності «Безпека інформаційно-телекомунікаційних систем», «Криптологія», «Технічний захист інформації» та «Управління інформаційною безпекою» самі по собі є базовими і не входять до спеціальності «Кібербезпека», оскільки остання згідно з міжнародним стандартом ISO/IEC 27032:2012 є лише окремим доменом безпеки та забезпечує конфіденційність, цілісність і доступність інформації в кіберпросторі, що проявляється лише у взаємодії людей та організацій в інтернеті [12; 13; 15].

Системи технічного захисту інформації (зокрема захисту від витоку технічними каналами), управління інформаційною безпекою, безпека інформаційно-комунікаційних систем (зокрема АС класу «1» та «2»), що є вкрай важливими для безпеки нашої держави саме сьогодні, коли відбувається загострення протистояння в інформаційній сфері у зв’язку з російською агресією, не охоплюються лише напрямом підготовки «Кібербезпека».

Крім того, через відсутність системного поповнення молодими спеціалістами, брак ефективної системи заохочень для фахівців профілів підготовки у сфері безпеки інформації та безпеки телекомунікаційних систем (мереж), загалом гостру нестачу фахівців захистом інформації часто опікуються співробітники, які не мають відповідної компетенції, знань і навичок. Це твердження стосується навіть особового складу підрозділів ТЗІ, до якого висуваються обов’язкові вимоги щодо відповідної освіти. Водночас

комплектування служби захисту такими фахівцями здійснюється за залишковим принципом.

Система служби захисту інформації не є ефективною та не відповідає реальним потребам забезпечення захисту інформації через недостатню кваліфікацію співробітників підрозділів, що входять до її складу, щодо експлуатації ІТС та впровадження КСЗІ з підтвердженою відповідністю, що становить серйозну загрозу та потребує перегляду функціонування системи.

Також необхідні розширення та забезпечення комплектування штату підрозділів ТЗІ в повному обсязі через значне навантаження, що не сприяє якісному контролю над захистом інформації, підвищення кваліфікації та забезпечення спеціалізованим обладнанням для проведення робіт із ТЗІ в повному обсязі своїми силами.

Відповідно до Рекомендацій парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» було б доцільним:

– організувати ефективну співпрацю бізнес-структур, вищих навчальних закладів, зокрема й Національної академії СБУ, та студентів щодо укладення тристоронніх договорів цільової підготовки фахівців у галузі інформаційно-комп'ютерних технологій та захисту інформації;

– забезпечити створення депозитаріїв цифрових навчальних матеріалів;

– забезпечити оновлення матеріальної бази вищих навчальних закладів і наукових установ, що проводять дослідження та готують фахівців у галузі інформаційної безпеки [15].

Висновки. Проведений аналіз недоліків у сучасних підходах до побудови комплексних систем захисту інформації, огляд та систематизація теоретико-практичних рекомендацій щодо вдосконалення механізмів забезпечення системи захисту інформації доводять, що процедура створення КСЗІ на сьогодні є доволі заплутаною. Немає єдиного нормативно-методичного документа, у якому було б повною мірою, послідовно викладено описаний процес. Це створює певні обмеження та незручності для осіб, які не мають профільної освіти або відповідного досвіду роботи.

Термінологічна та нормативно-правова база у сфері захисту інформації (КСЗІ в АС класу «1» та «2» зокрема) потребує подальшого вдосконалення з урахуванням досвіду розроблення національних стандартів, гармонізованих із стандартами ISO/IEC та ETSI, приведення у відповідність до регламентів і директив у сфері безпеки інформаційних систем, сертифікації з кібербезпеки.

Вирішення зазначених проблем у системі СБ України можливе шляхом ужиття таких заходів:

1. Запровадження оцінювання апаратно-програмних засобів на предмет їхньої кібер- і технічної захищеності з урахуванням міжнародних стандартів.

2. Розвиток державно-приватного партнерства у сфері безпеки інформації шляхом створення сприятливих умов для залучення бізнес-структур та широкого кола фахівців для діалогу й опрацювання найбільш значущих для

суспільства питань безпеки інформації, налагодження ділових стосунків із постачальниками апаратних засобів обробки й передачі даних та розробниками спеціалізованого програмного забезпечення у сфері протидії НСД і захисту даних.

3. Спрощення процедури запровадження КСЗІ в державних органах, підвищення прозорості процедури отримання сертифікатів відповідності вимогам КСЗІ та зниження вартості її впровадження.

4. Забезпечення розробки й обов'язкового впровадження програмного забезпечення власного виробництва з метою забезпечення кібербезпеки в Україні відповідно до міжнародних стандартів.

5. Розгляд питання щодо оптимізації кількості засобів електронно-обчислювальної техніки, призначеної для обробки інформації, що становить державну таємницю, з урахуванням реальних обсягів завдань.

6. Організація навчання з оволодіння основами ІКТ в обсягах, необхідних для їх використання в майбутній професійній діяльності випускниками вищих навчальних закладів, залучення фахівців інформаційної сфери до розроблення стандартів освіти, навчальних планів і навчальних програм.

Список використаних джерел

1. Антикорупційна програма Служби безпеки України на 2021–2024 роки. URL: https://ssu.gov.ua/antylcoruptsiina-prohrama-2021-2024 (дата звернення: 05.05.2022).

2. Актуальні проблеми управління інформаційною безпекою держави : збірник тез наукових доповідей, (Київ, 4 квіт. 2019 р.). Київ : Національна академія Служби безпеки України, 2019. 384 с.

3. Перелік актів законодавства у сфері технічного захисту інформації. URL: https://cip.gov.ua/ua/news/perelik-aktiv-zakonodavstva-u-sferi-tekhnichnogo-zakhistu-informaciyi (дата звернення: 05.05.2022).

4. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» : нормативний документ системи ТЗІ. URL: https://tzi.ua/assets/files/Ll_003_99.pdf (дата звернення: 25.05.2022).

5. ДСТУ 3396.2 «Захист інформації. Технічний захист інформації. Терміни та визначення» : Державний стандарт України від 01.01.1998. URL:https://tzi.com.ua/478.html (дата звернення: 15.05.2022).

6. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.Ua/laws/show/2657-12#Text (дата звернення: 15.05.2022).

7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94%D0%B2%D (дата звернення: 23.05.2022).

8. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.Ua/laws/show/3855-12#Text (дата звернення: 23.05.2022).

9. Про Положення про технічний захист інформації в Україні : Указ Президента від 27.09.1999 № 1229/99. URL: https://zalcon.rada.gov.ua/ (дата звернення: 21.05.2022).

10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.

rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.06.2022).

11. Мялковський Д. В. Державне регулювання забезпеченням безпеки надання електронних довірчих послуг : дис. … канд. наук з держ. упр. Київ, 2020. 297 с.

12. Актуальні проблеми управління інформаційною безпекою держави : збірник тез наукових доповідей, (Київ, 15 трав. 2020 р.). Київ : Національна академія Служби безпеки України, 2020. 363 с.

13. Кібергігієна. Кібербезпека. Безпека держави : матеріали наукових семінарів, (Київ, 27 листоп. 2020 р.). Київ : Київський національний торговельно-економічний університет, 2020. 100 с.

14. Про безпеку інформації та інформаційно-комунікаційних систем : проєкт Закону України. URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-rozrobila-proekt-zakonu-ukrayini-pro-bezpeku-informaciyi-ta-informaciino-komunikaciinikh-sistem (дата звернення: 05.06.2022).

15. Про Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні» : Постанова Верховної Ради України від 03.07.2014 № 1565-VII. URL: https://zakon.rada.gov.ua/laws/show/1565-18#Text (дата звернення: 25.05.2022).

Анотація. У статті в межах обґрунтування теоретико-методологічних засад оптимізації побудови захищених інформаційно-телекомунікаційних систем проведено аналіз недоліків у сучасних підходах до побудови комплексних систем захисту інформації, огляд і систематизацію теоретико-практичних рекомендацій щодо вдосконалення механізмів забезпечення системи захисту інформації. Проаналізовано механізми взаємодії складових системи захисту інформації. Запропоновано підходи щодо вдосконалення нормативно-правових та організаційних механізмів захисту інформації з обмеженим доступом у відомчих інформаційно-телекомунікаційних системах.

Ключові слова: захист інформації, інформаційно-телекомунікаційні системи, автоматизовані системи, інформаційна безпека, комплексна система захисту інформації, інформаційно-комп'ютерні технології, кібербезпека, інформаційна діяльність.

Abstract. An analysis of shortfalls in short-term approaches to the development of complex systems to protect information, overview and organization of theoretical and applied foundations to optimize mechanisms to insure the information security and telecommunication systems are carried out in the research. Mechanisms of interaction between information components of security systems are analyzed. Approaches concerning the improvement of regulatory and organizational mechanisms for the protection of information with restricted access in the information and telecommunication systems of the Security Service of Ukraine are highlighted.

Key words: information protection, information and telecommunication systems, automated systems, information security, comprehensive system of information protection, information and computer technologies, cyber security, information activity.