УДК 004.051:004.056.5-048.35 к.т.н., доц. **Стрельбіцький М.А.** (НАДПСУ)

ОБҐРУНТУВАННЯ ПОКАЗНИКА ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА СТАДІЇ МОДЕРНІЗАЦІЇ

У сучасних умовах кількість загроз інформації постійно зростає. Це впливає на ефективність функціонування правоохоронних органів. З метою запобігання реалізації зазначених загроз керівництво прикордонної служби адаптує всі складові відомства до вимог сьогодення. Це вимагає здійснювати модернізацію інформаційно-телекомунікаційних систем та їх систем захисту інформації. Зазначені системи являють собою складні організаційно-технологічні структури. Вищенаведене вимагає адаптації існуючих підходів до оцінювання ефективності систем захисту інформації в інтегрованій інформаційно-телекомунікаційній системі на стадії модернізації.

Проведений аналіз поняття захисту інформації показав, що в наведеному визначенні комплексна система захисту інформації розглядається ізольовано від зовнішнього середовища. В дослідженнях інших авторів поняття зовнішнього середовища розглядається тільки як джерело загроз. Такий підхід має раціональне підґрунтя, так як позитивний вплив не призводить до зниження якості функціонування інформаційно-телекомунікаційної системи. В статті пропонується розглядати зовнішнє середовище як складову яка здійснює неконтрольований вплив на функціонування системи. Крім того, наведено визначення поняття зовнішнього середовища як сукупність об'єктів, що не входять до системи захисту інформації та безпосередньо не приймають участь в процесі захисту інформації, але здійснюють вплив на досягнення мети захисту інформації.

Вищенаведені дослідження дозволили сформувати узагальнену структуру функціонування системи захисту інформації. Аналіз цієї структури показав, що вплив дестабілізуючих факторів на процес захисту інформації здійснюється опосередковано через умови застосування системи. Керуюча система з метою дотримання заданого (нормативного) рівня захисту має можливість визначати допустимі умови застосування. Під умовами застосування системи захисту інформації розуміється сукупність факторів організаційно-ситуаційного характеру, які впливають на ситуацію в якій система виконує свої завдання та визначає допустимі результати виконання завдань функціонального характеру.

Функціонування системи захисту інформації описується багатовимірним векторним показником. При оцінюванні якості системи необхідно визначити сукупність критеріїв які належать класу критеріїв придатності. Таким чином, якщо показники якості системи належать множині допустимих значень, то система захисту інформації придатна до використання за призначенням та виконує свої функції.

В результаті проведених досліджень показано, що вектор показників якості функціонування системи захисту інформації складається з чотирьох складових показників: цілісності, конфіденційності, доступності, спостереженості. Зазначимо, що компоненти зазначеного вектору являються кількісними характеристиками кількісних результатів самого процесу захисту інформації. Будемо вважати, що їх якісна характеристика завчасно забезпечується ще до початку експлуатації системи захисту інформації.

В загальному випадку на характеристики системи захисту інформації діє множина випадкових факторів, що визначає зазначені величини як випадкові. Разом із тим, апріорі випадковими є значення множини допустимих значень показника якості. Це пов'язано з тим, що завчасно невідомо, які повинні бути результати роботи системи захисту інформації, щоб забезпечити необхідний рівень захисту. Окремі дослідження при визначенні умов застосування та функціонування системи приймають припущення про найгірший їх варіант (з точки зору захисту інформації). Зазначене припущення призводить до неправомірно великих витрат ресурсів. В результаті проведених досліджень визначено, що показником ефективності системи захисту інформації є ймовірність належності значень випадкового вектору показників якості системи випадковій множині допустимих значень.

В статті сформульовані семантичні аспекти оцінювання ефективності системи захисту інформації, наведена узагальнена структура її функціонування в інформаційно-телекомунікаційних системах на стадії модернізації. Це дозволило обґрунтувати поняття ефективності захисту інформації, як властивості цілеспрямованого процесу, що

характеризується ступенем досягнення мети системи захисту. Дане поняття носить стохастичний характер та залежить від сукупності зовнішніх та внутрішніх чинників. Таким чином, значення ймовірності знаходження показників якості системи захисту інформації в допустимих межах є показником ефективності процесу захисту інформації. На підставі розробленого показника сформовано критерій придатності системи.

Ключові слова: показник ефективності, система захисту інформації, модернізація

Постановка проблеми. Забезпечення безпеки державних інформаційних ресурсів в умовах стрімкого розвитку інформаційних технологій вимагає наявності високоефективних систем захисту інформації. Зазначені системи являють собою складні організаційно-технологічні структури, створення яких вимагає вирішення комплексу системних задач. В процесі розвитку інформаційних технологій і зростанням значущості технічних засобів зв'язку інформація піддається все більшій кількості загроз, які за умови їх реалізації можуть призвести до збитків національного масштабу. У цих умовах ефективність функціонування правоохоронних органів в значній мірі залежить від можливості системи захисту інформації запобігти реалізації загроз. Це особливо актуально для прикордонного відомства, яке в значній мірі пов'язано з особливостями організації захисту державного кордону України, процесу пропуску через державний кордон осіб і транспортних засобів та вантажів, специфікою функціонування на адміністративній межі та на лінії розмежування в зоні проведення антитерористичної операції.

Функціонування Державної прикордонної служби України (ДПСУ) здійснюється в умовах складної та динамічної ситуації. З метою вирішення в цих умовах завдань керівництвом прикордонної служби здійснюється адаптація організаційно-штатної структури до викликів сьогодення, провадиться раціоналізація логістичних процесів, вдосконалення матеріально-технічного забезпечення, зокрема модернізація інформаційно-телекомунікаційних систем (ІТС). Вищенаведене вимагає адаптації існуючих підходів до оцінювання ефективності систем захисту інформації на стадії модернізації інтегрованої інформаційно-телекомунікаційної системи (ІІТС) прикордонного відомства.

Аналіз останніх досліджень та публікацій. Впровадження та обслуговування систем захисту інформації потребує значних витрат ресурсів. Як показали аналогічні дослідження, що були проведені в цивільних організаціях витрати коштів на захист інформації досягають 20-30 % усього бюджету на інформаційні технології [1]. Разом із тим, модернізація основних засобів інформаційно-телекомунікаційних системах вимагає також і модернізацію її системи захисту. У цих умовах актуальною є проблема аналізу ефективності функціонування систем спрямованих на забезпечення інформаційної безпеки.

Над розв’язанням зазначеної проблеми у сфері оцінювання ефективності СЗІ працюють Архипов О.Є., Архипова С. А., Бородавко І.Т., Ворожко В.П., Голубничий О.Г., Конахович Г.Ф., Корченко А.Г., Носок С.А., Потапов В.Г., Пузиренко О.Ю., Риндюк В.А. [2-7]. Разом із тим, на теперішній момент залишаються дискусійними методологічні підходи до оцінювання ефективності систем захисту інформації.

Метою статті є розробка семантичних аспектів оцінювання ефективності процесу захисту інформації та на їх основі обґрунтування показника ефективності системи захисту інформації інформаційно-телекомунікаційних систем на стадії модернізації.

Основний матеріал. У відповідності до [8] захист інформації в ІІТС це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі. Дане визначення дозволяє сформулювати поняття захисту інформації як цілеспрямований процес з єдиною (що є принциповим) метою – недопущення несанкціонованих дій стосовно інформації під час всього життєвого циклу ІІТС. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" дає визначення комплексної системи захисту інформації (КСЗІ) як взаємопов'язаної сукупності організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. Варто зазначити, що у наведеному визначенні КСЗІ розглядається ізольовано від зовнішнього середовища, а саме від умов функціонування та

умов застосування системи.

У роботах [9-11] використовується поняття зовнішнього середовища, як основної умови забезпечення функціонування ІТС, якість якої залежить не тільки від ступеня захисту інформації яка циркулює в ній, а й від здатності запобігання негативного впливу зовнішнього середовища та шкідливого програмного забезпечення. В основному всі автори, які розглядають в своїх роботах поняття «зовнішнє середовище» оцінюють тільки його негативний вплив на якість функціонування системи. Зовнішнє середовище розглядається як джерело загроз інформації: діяльність організацій (окремих осіб), вплив стихійного лиха, тощо. Такий підхід до розгляду зазначеного поняття має раціональне підґрунтя, а саме розгляду тільки негативного впливу, так як позитивний не призводить до зниження якості функціонування ІТС в цілому. Разом із тим, зовнішнє середовище може здійснювати і позитивний вплив на функціонування СЗІ або компенсувати окремі негативні дії. В рамках такого підходу зовнішнє середовище ІТС розглядається не тільки з негативної сторони, а як неконтрольований вплив на функціонування системи в цілому.

Дамо визначення поняття "навколишнє середовище" в рамках терміну "захист інформації", а саме як сукупність об’єктів, які не входять в СЗІ (КСЗІ) та безпосередньо не приймають участь в процесі захисту інформації, але здійснюють вплив на досягнення мети захисту інформації. В подальшому поняття "навколишнє середовище" будемо розуміти як сукупність умов функціонування та умов застосування системи захисту інформації.

В загальному, функціонування системи захисту інформації можна представити як складну людино-машинну (ергатичну) систему з множиною можливих станів яка взаємодіє із зовнішнім середовищем та оперує власними ресурсами із завданням досягнення мети (рис. 1).

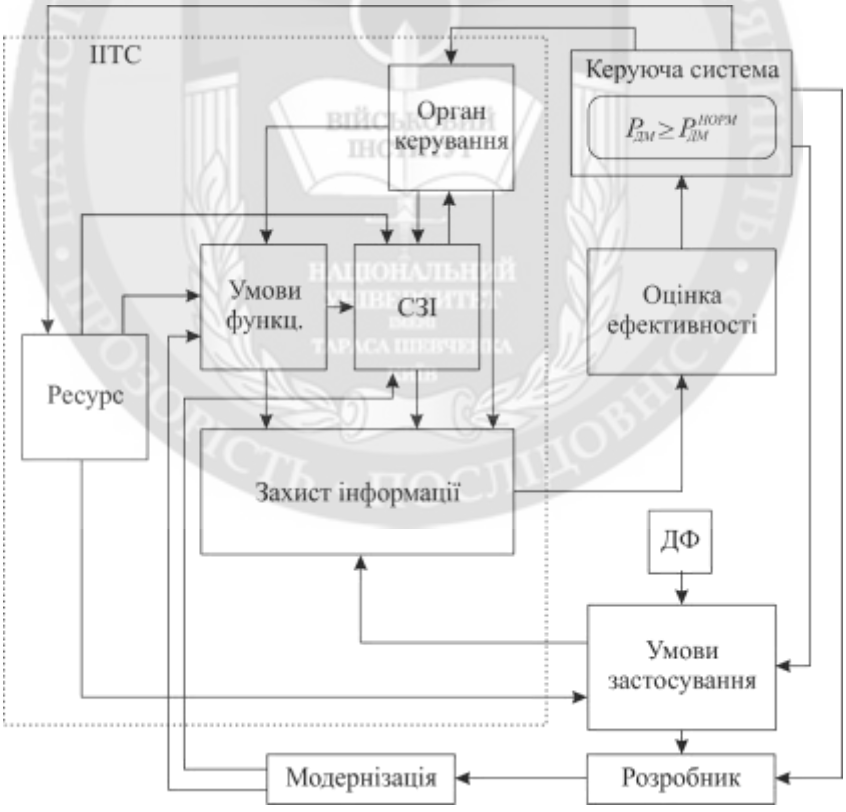

Рис. 1. Узагальнена структура функціонування СЗІ

По відношенню до ІТС «зовнішнім середовищем» вважаються умови застосування системи на які діють різного типу дестабілізуючі фактори об’єктивного характеру, а також керуюча система та процес модернізації розробником.

Керуюча система (розпорядник ІІТС) безпосередньо не входить до складу СЗІ як

підсистеми ІТС, але здійснює безпосередній вплив на наявність ресурсів системи, визначає умови застосування та, через орган керування, умови функціонування ІІТС. Наприклад, у прикордонному відомстві розпорядником ІТС є Адміністрація ДПС України. При створенні ІТС визначаються технічні умови розгортання зазначеної системи, розпорядником виділяються ресурси на її створення. Реалізуючи розпорядчу функцію Адміністрація через відповідні керівні документи формує порядок застосування СЗІ в органах охорони державного кордону. Наявність зворотного зв'язку, через оцінку ефективності СЗІ дозволяє Адміністрації здійснювати корегування умов функціонування та застосування системи в цілому. При потребі модернізації існуючої системи розпорядник системи надсилає розробнику технічне завдання на модернізацію системи. Розробник, в свою чергу, отримавши завдання на модернізацію системи враховує умови застосування та здійснює зміни в системі, в тому числі стосовно СЗІ.

Таким чином, модернізація складових ІІТС приводить до зміни показника ефективності процесу захисту інформації, який після її оцінки порівнюється з нормативним значенням та на цій підставі приймається рішення керуючою системою щодо запровадження внесених змін, зміни умов функціонування системи чи визначення допустимих умов застосування ІІТС або регулювання ресурсів, які виділяються на процес ЗІ з метою дотримання відповідності показника ефективності захисту інформації заданому критерію. Такий підхід передбачає вирішення зворотної задачі оцінювання ефективності СЗІ, а саме задачу синтезу СЗІ при заданих умовах застосування та функціонування. Вищенаведене вимагає використання інших критеріїв: переваги та оптимальності, що виходить за межі статті.

На систему захисту інформації в ІТС впливають: орган керування, який визначає умови функціонування ІТС та СЗІ, зокрема; наявний ресурс, що забезпечує функціонування СЗІ та визначає умови функціонування ІТС в цілому. Безпосередньо на сам процес захисту впливають умови функціонування (внутрішній фактор) та умови застосування (зовнішній фактор), структура та організація СЗІ, орган керування.

Аналіз узагальненої структури функціонування показав, що вплив дестабілізуючих факторів на процес захисту інформації здійснюється опосередковано через умови застосування системи. Керуюча система з метою дотримання заданого (нормативного) рівня захисту має можливість визначати допустимі умови застосування.

Під умовами функціонування СЗІ будемо розуміти сукупність факторів, які впливають на характеристики СЗІ (стабільність, надійність, відновлюваність, керованість, тощо). До умов функціонування віднесемо також природні та техногенні умови в яких функціонує система, способи її застосування (постійний, періодичний), структуру та організацію СЗІ, кількість та якість ресурсів. У якості прикладу умов функціонування СЗІ наведемо мобільний програмно-технічний комплекс автоматизації прикордонного контролю який базується на автомобілі та застосовується відповідно до рішення начальника органу охорони кордону на різних ділянках відповідальності та в різний період. Таким чином, умови функціонування такого комплексу є різними (погодні умови, спосіб електроживлення, наявність каналів зв'язку, тощо), спосіб застосування – періодичний.

Умови застосування СЗІ – сукупність факторів організаційно-ситуаційного характеру, які впливають на ситуацію в якій СЗІ виконує свої завдання та визначає допустимі результати виконання завдань функціонального характеру. До умов застосування ІТС ДПСУ відноситься оперативно-стратегічна обстановка, як некерований фактор, що визначається дійсним розвитком прикордонного відомства так і впливом ризиків та загроз його розвитку. Крім того, стратегія майбутнього використання ІТС визначає основний характер їх цільового застосування. Зазначені фактори за своєю суттю є випадковими, тобто до моменту запуску в експлуатацію ІТС (або після модернізації) їх значення невідомі. Це призводить до неможливості отримання розрахункового значення показника ефективності. Тому, з метою усунення цієї невизначеності необхідно визначити ймовірнісні характеристики всіх випадкових факторів

Відповідно до визначення, поняття "захист інформації" можна розглядати як сукупність (послідовність) узгоджених дій протягом певного часу які спрямовані на досягнення мети

цього процесу. При оцінці ефективності необхідно звернути увагу на те, що це властивість процесу, а не самої системи. Тому в подальшому під поняттям ефективності захисту інформації будемо розуміти комплексну властивість цілеспрямованого процесу, який характеризується ступенем досягнення мети, а саме захисту інформації.

При оцінюванні якості СЗІ, яка описується n-вимірним векторним показником $Y_{\langle n\rangle}$ необхідно визначити сукупність критеріїв, які належать класу критеріїв придатності $\{G\}$, математичне формулювання якого має вигляд [12]:

$$G:\left(Y_{\langle n\rangle}\in\left\{Y_{\langle n\rangle}^{A}\right\}\right), \tag{1}$$

де $Y_{\langle n\rangle}$ - показник якості СЗІ;

$\left\{Y_{\langle n\rangle}^{A}\right\}$ - множина допустимих значень показника якості СЗІ.

Таким чином, СЗІ для якої виконується умова (1) придатна до використання за призначенням та виконує свої функції.

Серед множини властивостей системи захисту інформації істотними є ті, які визначають якість процесу захисту інформації. Структурою критеріїв захищеності інформації [13] визначені функціональні критерії які описують вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів: конфіденційності, цілісності, доступності, спостереженості, що визначає множину типів показників якості СЗІ (властивостей інформації):

$$p=\{i,c,a,u\}, \tag{2}$$

де i – цілісність (**i**ntegrity);

c – конфіденційність (**c**onfidentiality);

a – доступність (**a**vailability);

u – спостереженість (acco**u**ntability).

Разом із тим, в процесі захисту інформації витрачаються ресурси задля підтримання функціонування СЗІ на заданому рівні ефективності. Таким чином, СЗІ в будь-який момент часу можна охарактеризувати трійкою властивостей:

результативністю – властивістю системи забезпечити захист інформації;

ресурсоємністю, яка характеризується витратою ресурсів системи (матеріально-технічних, часових, енергетичних, фінансових, людських тощо);

оперативністю – властивістю системи здійснювати захист інформацій протягом зазначеного терміну часу.

Із зазначеного вище можна зробити висновок, що якість захисту інформації не може бути охарактеризована окремими властивостями, а визначається тільки їх сукупністю, тобто трійкою властивостей.

Введемо позначення зазначених властивостей:

$V_{\langle n_1\rangle}$ – показник результативності захисту інформації;

$R_{\langle n_2\rangle}$ – показник витрат ресурсів;

$T_{\langle n_3\rangle}$ – показник часу.

Тоді, показником якості СЗІ буде *n*–вимірний вектор, котрий містить три групи властивостей:

$$Y_{\langle n\rangle}=\left\langle V_{\langle n_1\rangle},R_{\langle n_2\rangle},T_{\langle n_3\rangle}\right\rangle, \tag{3}$$

де $n=n_1+n_2+n_3$.

Всередині груп можливо згортання часткових показників шляхом введення узагальнених показників. Так, в більшості випадків витрати ресурсів можна привести до витрат коштів, тоді

(3) прийме вигляд:

$$Y = \langle v_i, v_c, v_a, v_u; r; \tau \rangle, \tag{4}$$

де v_i – показник цілісності;

v_c – показник конфіденційності;

v_a – показник доступності;

v_u – показник спостереженості;

$r = \sum_{r_i \in R} r_i$ - показник витрат ресурсів;

τ – показник часу.

Разом із тим необхідно врахувати, при згортанні різнорідних показників узагальнений показник губить фізичний сенс, тому при багатокритеріальному аналізі коректним є згортання показників тільки всередині груп показників результатів. Згортання показників якості функціонування систем із різних груп є недопустимим.

Фізичний сенс показників результативності захисту інформації полягають у визначенні часу, протягом якого властивість інформації не буде порушена.

Фізичний сенс показника часу полягає у визначенні часу роботи всіх засобів забезпечення захисту при якому забезпечується нормативний рівень їх функціонування. З точки зору надійності це напрацювання до відмови та описується відомими функціональними залежностями теорії надійності. Даний показник являється складовим у формуванні показників результативності захисту інформації та може бути згорнутий в них.

Аналогічно, показник витрат ресурсів також залежить від часу функціонування системи. Разом із тим, розгортання об’єкта інформаційної діяльності (ОІД) передбачає витрату певних ресурсів та при їх відсутності або недостатній кількості дозвіл на функціонування ОІД не надається. Таким чином, даний показник не потребує дослідження і може бути виключений із вектору показників якості СЗІ та враховуватись окремо при порівнянні двох систем з однаковими значеннями показника якості.

Враховуючи вищенаведене, вектор показників якості функціонування СЗІ (4) прийме вигляд:

$$Y = \langle v_i, v_c, v_a, v_u \rangle. \tag{5}$$

Варто зазначити, що компоненти вектору Y являються кількісними характеристиками кількісних результатів самого процесу захисту інформації. Будемо вважати, що їх якісна характеристика завчасно забезпечується ще до початку експлуатації СЗІ. Аналогічне зауваження застосуємо до якісної характеристики ресурсного забезпечення.

Система захисту інформації, як взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту [8] повинна мати властивості системи, а не бути просто сукупністю певних засобів. Крім того, системний підхід повинен застосовуватись на всіх етапах життєвого циклу – від підготовки технічного завдання до експлуатації СЗІ. Зазначимо, що система такого типу повинна мати чітке призначення, причому чим конкретніше сформульована мета системи, тим адекватніше буде її описувати показник ефективності. Складність формулювання мети СЗІ ІІТС полягає у її значній розосередженості та багатофункціональності, причому кожна із підсистем постійно підлягає модернізації. При такому підході значущість властивостей окремих елементів СЗІ зменшується, а загальносистемні завдання, такі як визначення раціональної структури і режимів функціонування, організація взаємодії між складовими системи, вплив умов застосування та функціонування системи збільшується. Системне об’єднання складових СЗІ створюють ефект

емержентності, тобто появи властивостей які не притаманні жодному елементу окремо.

Наочно, що аналіз ефективності функціонування СЗІ вимагає формування та вирішення завдання кількісного оцінювання характеристик системи. Зазначені дані, які отримані або математичним моделюванням, або експериментальним шляхом повинні описувати властивості системи, основним з яких є ефективність функціонування СЗІ. Дана властивість системи агрегує в собі інші системні властивості, такі як надійність, керованість, оперативність відновлення після збоїв, тощо. Разом із тим, кількісна оцінка ефективності дозволяє здійснити порівняння системи при експлуатації в різних умовах та визначити допустимі межі експлуатаційних умов, при яких дотримується нормативне значення показника захисту інформації.

В більшості випадків при проектуванні СЗІ застосовують емпірично-інтуїтивний підхід, що наглядно показано в оцінюванні рівня безпеки інформаційних систем, коли оперують нечіткими поняттями, наприклад «достатньо захищений» [14]. Нечітке визначення у відношенні до інформаційної безпеки пов'язане з нечіткою постановкою завдання, вимог до захисту в умовах стохастичних впливів дестабілізуючих факторів. Як правило, це пояснюється тим, що СЗІ проектується після розробки основного функціоналу ІТС та не є складовою системи на стадії проектування.

Для оцінювання ефективності функціонування системи захисту інформації необхідно розробити показник ефективності процесу захисту інформації, який повинен відповідати основним вимогам [12]: показовість (адекватність), критичність (чутливість), комплексність (повнота), стохастичність, простота.

На показники результативності СЗІ впливають зовнішні та внутрішні фактори, які визначаються середовищем її функціонування.

Кожна з компонент вектору Y залежить від характеристик СЗІ та її організації, умов функціонування та умов застосування системи.

$$Y = Y(A_1, A_2, B_1, B_2), \tag{6}$$

де A_1 - характеристики СЗІ;

A_2 - характеристики організації процесу ЗІ;

B_1 - характеристики умов функціонування ЗСІ

B_2 - характеристики умов застосування ЗСІ.

У свою чергу, компоненти вектору Y^A допустимих значень теж залежать від умов застосування системи і визначаються керуючою системою.

$$Y^A = Y^A(B_2). \tag{7}$$

У загальному випадку на характеристики СЗІ, її організації, умови функціонування та застосування СЗІ діє множина випадкових факторів, що визначає зазначені величини як випадковими. Разом із тим, апріорі випадковими є і допустимі значення вектору Y^A, який залежить від умов застосування системи, так як завчасно невідомо, які повинні бути результати роботи СЗІ, щоб забезпечити необхідний рівень захисту. Окремі дослідження при визначенні умов застосування та функціонування системи приймають припущення про найгірший їх варіант (з точки зору захисту інформації), тобто величини B_1 та B_2 є не випадковими. Зазначене припущення призводить до неправомірно великих витрат ресурсів.

Таким чином, всі складові вектору показників якості функціонування СЗІ носять ймовірнісний характер, тому:

$$\begin{gathered} \hat{Y} = Y(\hat{A}_1, \hat{A}_2, \hat{B}_1, \hat{B}_2), \\ \hat{Y}^A = Y^A(\hat{B}_2). \end{gathered} \tag{8}$$

У результаті реальних умов експлуатації СЗІ критерій придатності (1) прийме вигляд:

$$G:\left(\hat{Y}\in\left\{\hat{Y}^{A}\right\}\right). \tag{9}$$

З виразу (8) можна зробити висновок, що придатність процесу захисту інформації – випадкова подія, яка безпосередньо не може відображати якість процесу. Тому, характеристикою якості СЗІ є ймовірність випадкової події:

$$P_{ДМ}=P\left(\hat{Y}\in\left\{\hat{Y}^{A}\right\}\right). \tag{10}$$

Таким чином, ймовірність $P_{ДМ}$ - це показник ефективності СЗІ, який визначає ступінь виконання СЗІ своїх функціональних завдань. На її основі формується критерій придатності системи, тобто $P_{ДМ}\geq P_{ДМ}^{НОРМ}$.

Висновки дослідження перспективи подальших розвідок у даному напрямку. Сформульовані семантичні аспекти щодо оцінювання ефективності системи захисту інформації та наведена узагальнена структура її функціонування в інформаційно-телекомунікаційних системах на стадії модернізації дозволила обґрунтувати поняття ефективності захисту інформації, як властивості цілеспрямованого процесу, що характеризується ступенем досягнення мети системи захисту. Дане поняття носить стохастичних характер та залежить від сукупності зовнішніх та внутрішніх чинників. Таким чином, значення ймовірності знаходження показників якості СЗІ в допустимих межах є показником ефективності процесу захисту інформації. На підставі розробленого показника сформовано критерій придатності системи.

Подальшим напрямком дослідження може бути вирішення зворотної задачі оцінювання ефективності СЗІ, а саме синтезі СЗІ при заданих умовах застосування та функціонування.

ЛІТЕРАТУРА:

1. Петренко С. А. Информационная безопасность: экономические аспекты / С. Петренко, С. Симонов, Р. Кислов // Jet Info Online. - 2003. - №10. [Электронный ресурс]. - Режим доступа: http://citforum.ru/security/articles/sec/index.shtml.

2. Архипов А. Е. Технологии експертного оценивания в задачах защиты информации / А. Е. Архипов, С. А. Архипова, С. А. Носок // Інформаційні технології та комп'ютерна інженерія : міжнар. наук.-техн. журн. – № 1. – 2005. – С. 89-94.

3. Архипов О. Є. Оцінювання ефективності системи охорони державної таємниці : монографія / О. Є. Архипов, І. Т. Бородавко, В. П. Ворожко. – К., 2007. – 63 с.

4. Архипов О. Є. Системні аспекти оцінювання рівня важливості секретної інформації / О. Є. Архипов, В. П. Ворожко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техн. зб. – К., 2007. – Вип. 2 (15). – С. 10-12.

5. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – К. : "МК-Прес", 2006. – 320 с.

6. Корченко А. Г. Экспертиза в системе ТЗИ на основе нечетких множеств / А. Г. Корченко, В. Г. Потапов, В. А. Рындюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2003. – Вип. 7. – С. 118-127.

7. Конахович Г. Ф. Оцінка ефективності систем захисту інформації в телекомунікаційних системах. / Г. Ф. Конахович, О. Г. Голубничий, О. Ю. Пузиренко. // Проблеми інформатизації та управління 3.21 (2007): 75-83.

8. Закон України Про захист інформації в інформаційно-телекомунікаційних системах / Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286

9. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах / [Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О.]. – К., 2013. – 435 с., іл.160.

10.Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. -М.: Горячая линия - Телеком, 2006. - 544 с.: ил.

11. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

12. Петухов Г.Б., Якунин В.И. - Методологические основы внешнего проектирования

целенаправленных процессов и целеустремлённых систем. – М.: АСТ, 2006. – 504 с.

13. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. Затверджено Наказом департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України від "28" квітня 1999 р. № 22. Із змінами згідно наказу адміністрації Держспецзв'язку від 28.12.2012 № 806

14. Л.А. Хмелев. Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем. // Безопасность информационных технологий»: Труды научнотехнической конференции, Пенза, июнь 2001. 2001.

REFERENCES:

1. Petrenko S. A. Informatsionnaya bezopasnost': ekonomicheskie aspekty / S. Petrenko, S. Simonov, R. Kislov // Jet Info Online. - 2003. - №10. [Elektronniy resurs]. - Rezhim dostupa: http://citforum.ru/security/articles/sec/index.shtml.

2. Arkhipov A. E. Tekhnologii ekspertnogo otsenivaniya v zadachakh zashchity informatsii / A. E. Arkhipov, S. A. Arkhipova, S. A. Nosok // Informatsiĭni tekhnologiĭ ta kompyuterna inzheneriya : mizhnar. nauk.-tekhn. zhurn. – № 1. – 2005. – S. 89-94.

3. Arkhipov O. Є. Otsinyuvannya efektivnosti sistemi okhoroni derzhavnoyi taemnitsi : monografiya / O. Є. Arkhipov, I. T. Borodavko, V. P. Vorozhko. – K., 2007. – 63 s.

4. Arkhipov O. Є. Sistemni aspekti otsinyuvannya rivnya vazhlivosti sekretnoyi informatsiyi / O. Є. Arkhipov, V. P. Vorozhko // Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiyi v Ukrayini : nauk.-tekhn. zb. – K., 2007. – Vip. 2 (15). – S. 10-12.

5. Korchenko A. G. Postroenie sistem zashchity informatsii na nechetkikh mnozhestvakh. Teoriya i prakticheskie resheniya / A. G. Korchenko. – K. : "MK-Pres", 2006. – 320 s.

6. Korchenko A. G. Ekspertiza v sisteme TZI na osnove nechetkikh mnozhestv / A. G. Korchenko, V. G. Potapov, V. A. Ryndyuk // Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiyi v Ukrayini. – K., 2003. – Vip. 7. – S. 118-127.

7. Konakhovych H. F. Otsinka efektyvnosti system zakhystu informatsiyi v telekomunikatsiynykh systemakh. / H. F. Konakhovych, O. H. Holubnychyy, O. Yu. Puzyrenko. // Problemy informatyzatsiyi ta upravlinnya 3.21 (2007): 75-83.

8. Zakon Ukrayiny Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh / Vidomosti Verkhovnoyi Rady Ukrayiny (VVR), 1994, N 31, st.286.

9. Osnovy zakhystu informatsiyi v telekomunikatsiynykh ta komp"yuternykh merezhakh / [Honcharova L.L., Voznenko A.D., Stasyuk O.I., Koval' Yu.O.]. – K., 2013. – 435 s., il.160.

10.Osnovy informatsionnoy bezopasnosti. Uchebnoe posobie dlya vuzov / E. B. Belov, V. P. Los', R. V. Meshcheryakov, A. A. Shelupanov. -M.: Goryachaya liniya - Telekom, 2006. - 544 s.: il.

11. Kavun S.V. Informatsiyna bezpeka. Navchal'niy posibnik. Ch.1 / S.V. Kavun, V.V. Nosov, O.V. Mazhay. – Kharkiv: Vid. KhNEU, 2008. – 352 s.

12. Petukhov G.B., Yakunin V.I. - Metodologicheskie osnovy vneshnego proektirovaniya tselenapravlennykh protsessov i tseleustremlennykh sistem. – M.: AST, 2006. – 504 s.

13. Kryteriyi otsinky zakhyshchenosti informatsiyi v komp"yuternykh systemakh vid nesanktsionovanoho dostupu ND TZI 2.5-004-99. Zatverdzheno Nakazom departamentu spetsial'nykh telekomunikatsiynykh system ta zakhystu informatsiyi sluzhby bezpeky Ukrayiny vid "28" kvitnya 1999 r. # 22. Iz zminamy zhidno nakazu administratsiyi Derzhspetszv"yazku vid 28.12.2012 # 806

14. L. A. Khmelev. Otsenka effektivnosti mer bezopasnosti, zakladyvaemykh pri proektirovanii elektronno-informatsionnykh sistem // Bezopasnost' informatsionnykh tekhnologiĭ»: Trudy nauchnotekhnicheskoĭ konferentsii, Penza, iyun' 2001. 2001.

Рецензент: д.т.н., проф. Андрощук О.С., Національна академія Державної прикордонної служби України імені Б. Хмельницького, м. Хмельницький

к.т.н., доц. Стрельбицкий М.А.

ОБОСНОВАНИЕ ПОКАЗАТЕЛЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА СТАДИИ МОДЕРНИЗАЦИИ

В современных условиях количество угроз информации постоянно растет. Это влияет на эффективность функционирования правоохранительных органов. С целью предотвращения реализации указанных угроз руководство пограничной службы адаптирует все составляющие

ведомства с требованиями современности. Это требует осуществлять модернизацию информационно-телекоммуникационных систем и их систем защиты информации. Указанные системы представляют собой сложные организационно-технологические структуры. Вышесказанное требует адаптации существующих подходов к оценке эффективности систем защиты информации в интегрированной информационно-телекоммуникационной системе на стадии модернизации.

Проведенный анализ понятия защиты информации показал, что в приведенном определении комплексная система защиты информации рассматривается изолированно от внешней среды. В исследованиях других авторов понятие внешней среды рассматривается только как источник угроз. Такой подход имеет рациональное обоснование, так как положительное влияние не приводит к снижению качества функционирования информационно-телекоммуникационной системы. В статье предлагается рассматривать внешнюю среду как составляющую, которая осуществляет неконтролируемое влияние на функционирование системы. Кроме того, приведено определение понятия внешней среды как совокупность объектов, не входящих на систему защиты информации и непосредственно не принимающих участие в процессе защиты информации, но оказывающие влияние на достижение цели защиты информации.

Вышеприведенные исследования позволили сформировать обобщенную структуру функционирования системы защиты информации. Анализ этой структуры показал, что влияние дестабилизирующих факторов на процесс защиты информации осуществляется опосредованно через условия применения системы. Управляющая система с целью соблюдения заданного (нормативного) уровня защиты имеет возможность определять допустимые условия применения. Под условиями применения системы защиты информации понимается совокупность факторов организационно-ситуационного характера, которые влияют на ситуацию, в которой система выполняет свои задачи и определяет допустимые результаты выполнения задач функционального характера.

Функционирование системы защиты информации описывается многомерным векторным показателем. При оценке качества системы необходимо определить совокупность критериев, принадлежащих классу критериев пригодности. Таким образом, если показатели качества системы принадлежат множеству допустимых значений, то система защиты информации пригодна к использованию по назначению и выполняет свои функции.

В результате проведенных исследований показано, что вектор показателей качества функционирования системы защиты информации состоит из четырех составляющих показателей: целостности, конфиденциальности, доступности, наблюдательности. Отметим, что компоненты указанного вектора являются количественными характеристиками количественных результатов самого процесса защиты информации. Будем считать, что их качественная характеристика заблаговременно обеспечивается еще до начала эксплуатации системы защиты информации.

В общем случае на характеристики системы защиты информации действует множество случайных факторов, определяющих указанные величины как случайные. Вместе с тем, априори случайными является значения множества допустимых значений показателя качества. Это связано с тем, что заранее неизвестно, какие должны быть результаты работы системы защиты информации, чтобы обеспечить необходимый уровень защиты. Отдельные исследования при определении условий применения и функционирования системы принимают предположение о наихудшем их варианте (с точки зрения защиты информации). Указанное предположение приводит к неправомерно большим затратам ресурсов. В результате проведенных исследований установлено, что показателем эффективности системы защиты информации является вероятность принадлежности значений случайного вектора показателей качества системы случайному множеству допустимых значений.

В статье сформулированы семантические аспекты оценки эффективности системы защиты информации, приведена обобщенная структура ее функционирования в информационно-телекоммуникационных системах на стадии модернизации. Это позволило обосновать понятие эффективности защиты информации, как свойства целенаправленного процесса, характеризующего степенью достижения цели системы защиты. Данное понятие носит стохастический характер и зависит от совокупности внешних и внутренних факторов. Таким образом, значение вероятности нахождения показателей качества системы защиты информации в допустимых пределах является показателем эффективности процесса защиты

информации. На основании разработанного показателя сформирован критерий пригодности системы.

Ключевые слова: показатель эффективности, система защиты информации, модернизация

Ph.D. Strelbitskiy M.A.

JUSTIFICATION OF THE INDICATOR OF THE INFORMATION PROTECTION SYSTEM FUNCTIONING EFFICIENCY AT THE STAGE OF MODERNIZATION

In modern conditions the amount of threat information is growing. This affects the efficiency of law enforcement. In order to prevent the implementation of these threats border service agencies adapt all the components to the requirements of today. This requires carrying out the modernization of information and telecommunication systems and information protection systems. These systems are complex organizational and technological structures. The abovementioned requires the adaptation of existing approaches to evaluating the effectiveness of information protection in integrated information and telecommunication systems at the stage of modernization.

The analysis of the protection of information concept showed that in the suggested definition the comprehensive system of information is considered in isolation from the environment. In studies by other authors the concept of environment is considered only as a source of threats. This approach has a rational basis, since a positive influence does not lead to a decrease in the functioning quality of the information and telecommunication systems. The article proposes to consider the environment as a component that exerts an uncontrolled influence on the functioning of the system. In addition, the article gives the definition of the environment as a set of objects that are not part of information protection and are not directly involved in the process of protecting information influencing the goal of information protection.

The above studies have made it possible to form a generalized structure for the functioning of the information protection system. An analysis of this structure showed that the influence of destabilizing factors on the process of information protection is made indirectly through the conditions of the application of the system. The control system with the purpose of observing the specified (standard) level of protection has the ability to determine the allowable terms of use. The terms of application of the information protection system imply a set of organizational and situational factors that affect the situation in which the system performs its tasks and determines the allowable results of performing tasks of a functional nature.

The functioning of the information protection system is described by a multidimensional vector index. When assessing the quality of the system, it is necessary to determine the set of criteria belonging to a class of validity criteria. Thus, if the system quality indicators belong to a multitude of acceptable values, then the information protection system is usable for its intended purpose and performs its functions.

As a result of the conducted researches, the vector of performance indicators of the information protection system consists of four components: integrity, confidentiality, availability, accountability. Note that the components of this vector are quantitative characteristics of the quantitative results of the information protection process itself. We may assume that their qualitative characteristics are provided in advance before the operation of the information protection system.

The system of information protection must have the properties of the system, and not simply be a collection of certain means. In addition, the system approach should be applied at all stages of the life cycle - from the preparation of the technical assignment to the operation of the system. A system of this type should have a clear purpose, and the more concretely the goal of the system is formulated, the more adequately will the efficiency index describe it. The complexity of the formulation of the information protection system purpose in integrated information and telecommunications system of the border agency is its considerable dispersal and multifunctionality. And each of the subsystems is constantly subject to modernization. With this approach, the importance of the properties of individual elements of the protection system decreases, and the definition of a rational structure and modes of operation, the organization of interaction between the components of the system, the impact of the conditions of application and functioning of the system as a system-wide task increases. System integration of the components of the information protection system creates the effect of consistency, that is, the appearance of properties that are not inherent in any element separately.

In the general case, the characteristics of an information protection system are affected by a number of random factors that determine these values as random. At the same time, a priori the value of the set of admissible values of the quality index is random. This is due to the fact that it is not known in advance what the results of the information protection system should be in order to provide the necessary level of

protection. Some studies in determining the conditions of application and functioning of the system accept the assumption of a worst option (in terms of information protection). This assumption leads to an unjustifiably high expenditure of resources. As a result of the conducted researches it is established that the indicator of the effectiveness of the information protection system is the probability that the values of the random vector of the system's quality indicators belong to a random set of admissible values.

The article offers the semantic aspects of the evaluation of the effectiveness of the information protection system, the generalized structure of its functioning in information and telecommunication systems at the modernization stage. This allowed justifying the concept of the effectiveness of information protection, as the property of a purposeful process, which is characterized by the degree of achievement of the protection system purpose. This concept is stochastic and depends on a combination of external and internal factors. Thus, the value of the probability of finding quality indicators of the information protection system within the acceptable limits is an indicator of the effectiveness of the information protection process. Based on the developed indicator, a criterion for the suitability of the system is formed.

Keywords: indices effectiveness, information security system, modernization