DOI: 10.18372/2410-7840.22.14976
УДК 004.056:351.861

МОДЕЛЬ ЗАХИСТУ КІБЕРПРОСТОРУ CYBERSEC

Юлія Ткач

У статті запропоновано модель захисту кіберпростору CyberSec, що орієнтована на виконання функції «кіберзахисту». Дана модель є функціональною, складається з п'яти етапів, об'єднує в собі низку методів й моделей, є циклічною, а тому дозволяє створити самоналагоджувану систему захисту у кіберпросторі. На першому етапі «Розвідка та виявлення» здійснюється опис середовища безпеки, тобто формується модель загроз, що є повним переліком усіх можливих загроз, які існують або можуть виникнути в даній ситуації. Другим етапом «Озброєння» є вибір засобів захисту та побудова системи захисту кіберпростору (СЗК). Проведення контролю системи (кібепростору) є третім етапом «Контроль». На четвертому етапі «Протидія» побудови захищеного кіберпростору виконується оцінка дієвості запропонованої СЗК. На п'ятому етапі «Активна протидія» здійснюється підготовка нормативних документів, інформування корпорацій щодо інцидентів кібербезпеки активна протидія на рівні держави, тобто відбувається застосування контрзаходів. Модель захисту кіберпростору CyberSec дозволяє на практиці побудувати захищений кіберпростір як окремої корпорації, так і держави в цілому.

Ключові слова: *кіберпростір, модель захисту, національна безпека, захищений кіберпростір.*

ВСТУП

Фундаментом інформаційної безпеки України є безпека кіберпростору держави. Вирішення усіх інших завдань забезпечення національної безпеки країни можливе саме за умов стійкої безпеки в кіберпросторі. З іншого боку, справжня інформаційна безпека існує тільки за умови надійного захисту національних інтересів України від будь-якого силового чи інформаційного тиску. Тому серед головних передумов національної безпеки України є кібербезпека держави, в цьому контексті пріоритетного значення набуває побудова захищеного кіберпростору.

МЕТА РОБОТИ

Побудувати модель захисту кіберпростору CyberSec, яка дозволить на практиці побудувати захищений кіберпростір як окремої корпорації, так і держави в цілому.

ПОСТАНОВКА ЗАДАЧІ

Не існує єдиного рішення задля забезпечення кібербезпеки держави.

Розв'язування завдання побудови системи захисту інформації (СЗІ) ускладнюється такими її властивостями [3]:

- складний опосередкований взаємозв'язок показників якості СЗІ з показниками якості інформаційної системи;

- необхідність урахування великої кількості показників (вимог) СЗІ в оцінюванні та виборі її раціонального варіанта;

- переважно якісний характер показників (вимог), що враховуються під час аналізу та синтезу СЗІ;

- істотний взаємозв'язок та взаємозалежність цих показників (вимог), що мають суперечливий характер;

- труднощі, пов'язані з отриманням початкових даних, необхідних для розв'язування задач аналізу та синтезу СЗІ, особливо на ранніх етапах проектування.

Все це значно ускладнює процес аналізу та узагальнення будь-якої інформації щодо системи. Таким чином, існуючі класичні математичні підходи (моделі, статистика, теорія ймовірності, оптимізаційні методи тощо) в умовах некоректної постановки завдання не дають бажаного результату.

Тому виникає необхідність розробки нових підходів, побудови нових моделей, орієнтованих на специфіку процесу забезпечення безпеки інформації в кіберпросторі держави.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У відповідності до стандарту ISO/IEC 15408-99 [1] розробка моделі захисту припускає виконання наступних операцій:

1. Описати пропоновану сферу, пов'язану з безпекою функціонування в ній інформації.

2. Визначити стратегію протистояння кожній загрозі і сформувати відповідні цілі захисту.

На цьому етапі фактично визначається область дії моделі.

Цілі захисту слід розділити на цілі, досягнення яких покладається на об'єкт оцінки, і меті досягнення яких покладається на середовище.

3. Використати каталог функціональних вимог безпеки з частини 2. Загальні вимоги для специфікації функціональних можливостей, спрямованих на досягнення цілей захисту для кіберпростору держави.

4. Використати каталог вимог довіри і безпеки з частини 3. Загальні вимоги для специфікації компонентів довіри, спрямованих на забезпечення рівня довіри і безпеки, що відповідає цілям безпеки.

5. Розробити логічне обґрунтування того, що вибрані функціональні компоненти і компоненти довіри до захисту підходять для протидії загрозам в кіберпросторі держави.

Зазначимо, що згідно з ISO/IEC 15408-99 частини 2, 3 (ще називають) «Загальні критерії - ЗК» являють собою каталоги вимог безпеки наступних типів:

- функціональні вимоги (Частина 2) - відповідають активному аспекту захисту та висуваються до функцій безпеки ЗК та механізмам, що їх реалізують.

- вимоги довіри (Частина 3) - висуваються до технології та процесу розробки, експлуатації та оцінки ЗК та покликані гарантувати адекватність реалізації механізмів безпеки.

Розглянувши відповідні стандарти та методику Cyber kill chain, нами було запропоновано власну модель захисту кіберпростору, що орієнтована на виконання функції «кіберзахисту» (рис.1). Моделі, орієнтовані на функції систем, прийнято називати функціональними [8].

Для забезпечення виконання даної функції та проектування роботи моделі треба детально проаналізувати роботу їх складових частин і їх взаємодію. Функціональна модель захисту кіберпростору складається з набору етапів та описує реалізацію переходів від етапу до етапу, а саме порядок та умови переходу починаючи від розвідки і закінчуючи активною протидією на рівні держави.

Вважаємо, що для побудови захищеного кіберпростору треба спочатку проаналізувати та захистити, а потім забезпечувати безпеку створеної СЗІ, виявляючи різноманітні активності зловмисників та реагуючи певним чином на них.

Розглянемо більш детально кожен з етапів нашої моделі.

На першому етапі «Розвідка та виявлення» здійснюється опис середовища безпеки, тобто формується модель загроз, що є повним переліком усіх можливих загроз, які існують або можуть виникнути в даній ситуації, після робляться припущення щодо зловмисника, а отже формується модель порушника.

При складанні моделей враховується середовище в якому функціонує інформація. У нашому випадку це кіберпростір корпорації. Зовнішні порушники за даних умов можуть бути з числа держави.

Формування моделі загроз. Це можна здійснити з використанням теорії ризиків, лінгвістичних термів, теорії графів при одночасній участі експертів, але бажано було б, щоб це був комплексний підхід, оскільки треба визначити не тільки перелік загроз, що існують у кіберпросторі, а і зони ризиків, що в подальшому необхідно для формування вимог довіри до безпеки, міри впливу різних концептів один на одного та на кіберпростір держави в цілому, необхідно також визначити рівень загального ризику.

Складність і трудомісткість аналізу визначається реальними умовами і можливостями її проведення.

Міра впливу трудомісткості обробки експертних даних буде залежить від обсягу і рівня деталізації вхідних даних.

Оскільки переважна більшість впливів на інформацію у випадку технічних й програмних несправностей (відмова, збій й помилка компонентів систем обробки даних, вірусне зараження тощо) носить випадковий характер, можна навіть стверджувати про їх системність, то навмисна причина впливу на інформацію притаманна людині (злочинні дії), тому вона може стати основним джерелом виникнення як суб'єктивних, так і об'єктивних причин.

Аналіз має проводитись за допомогою емпіричного підходу, на основі тривалого збору й обробки даних про реальні прояви загроз інфо-

рмації й про розміри того збитку, що при цьому мав би місце. На четвертому етапі «Протидія» побудови захищеного кіберпростору виконується оцінка дієвості запропонованої СЗК.

При рішенні практичних завдань обґрунтування вимог і оцінки дієвості системи захисту кіберпростору виникає природне питання раціонального вибору методу визначення вагових коефіцієнтів з числа існуючих методів.

Принциповими особливостями рішення задачі вибору раціонального варіанту системи захисту, що визначає метод її рішення, є:

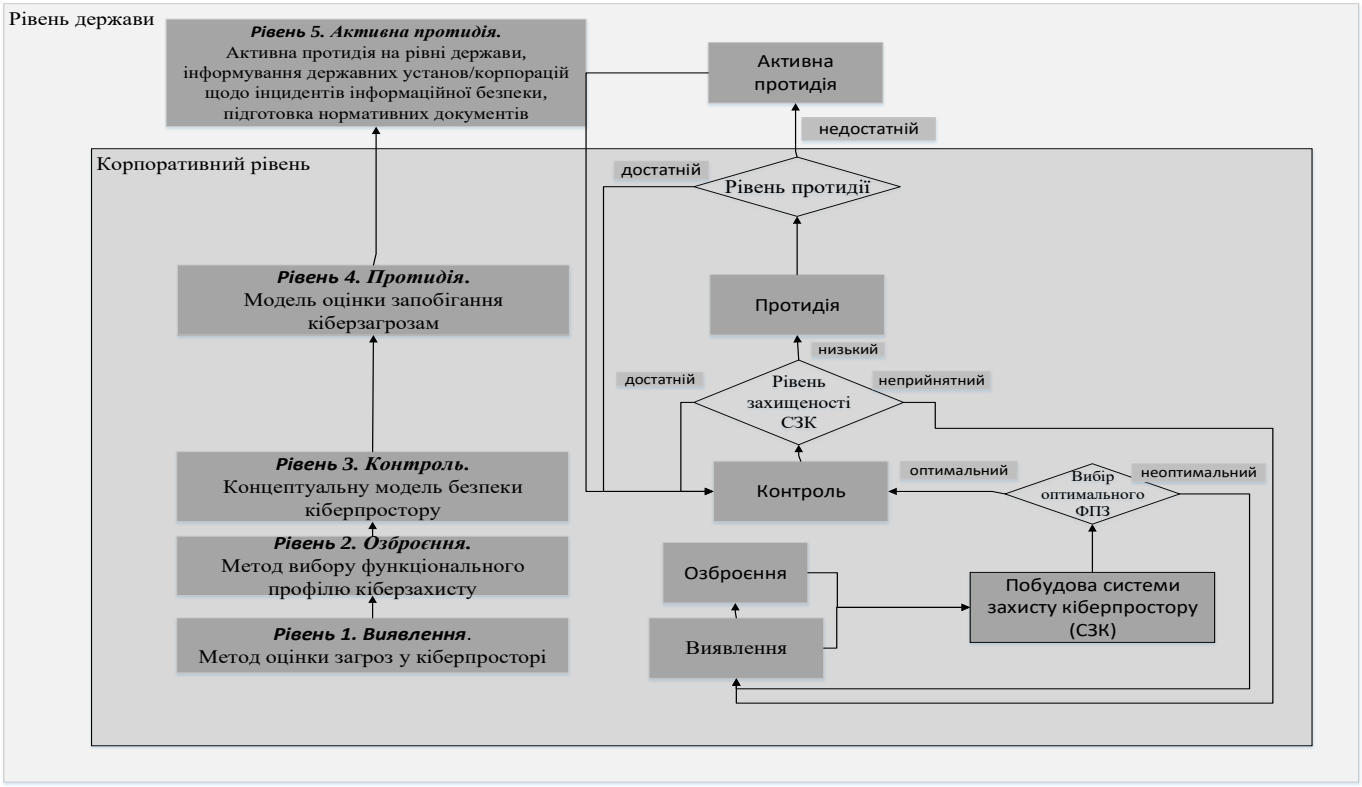

Рис.1 Модель захисту кіберпростору CyberSec

- багатокритеріальність завдання вибору;

- не лише кількісний, але і якісний опис показників якості системи захисту, що задаються у вигляді вимог;

- при якісній постановці завдання вплив на вибір методу її рішення експертної інформації, що визначає перевагу того або іншого показника.

Переважна особливість даного завдання вибору - це якісний характер показників, що трактували їм вимоги, задавалися до системи захисту кіберпростору держави.

Вибір методу рішення задачі залежить від того, в якому виді представлення експертна інформація про перевагу показників, а також від міри їх важливості (рівна і різна важливість вимог).

Відповідно до формування завдання, основними практичними етапами її рішення є:

- розробка методики формування і проведення експертних оцінок;

- розробка принципів і механізмів збору і обробки експертної інформації з характеристики загроз;

- розробка принципів і механізмів збою і обробки експертної інформації з метою визначення важливості виконання функціональних вимог для усунення відповдних загроз.

Модель порушника. Порушник – це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення захищеності інформації. Модель порушника відображає його практичні та потенційні можливості, апріорні

знання, час та місце дії тощо. Порушники можуть бути внутрішніми (з числа персоналу/ користувачів АС), або зовнішніми (з числа сторонніх осіб).

Представники організацій – це особи, що взаємодіють з питань технічного забезпечення (енерго-, водо- теплопостачання, співробітники сервісних центрів тощо) і внаслідок чого мають доступ на територію розташування АС та діють на цій території чи за її межами, або з числа осіб, які зацікавлені в порушенні робіт АС, але доступу у контрольовану зону не мають [2].

На модель порушника впливають такі факти:

- розташування приміщення, в якому розміщено АС, на території, яка має систему надійної фізичної охорони, що практично виключає неконтрольоване проникнення у приміщення сторонніх осіб;

- ретельний підбір співробітників на відповідні посади, що практично виключає виконання ключових функціональних ролей "випадковими" особами; усі співробітники, що задіяні на таких ключових ділянках, повинні мати достатній досвід роботи;

- повсякденний візуальний контроль адміністратора безпеки за станом опечатування системних блоків, що зводить до мінімуму ризик несанкціонованого підключення до ЗОТ;

- обмеження складу встановленого програмного забезпечення та апаратних засобів відповідними затвердженими переліками, ведення паспортів на всі автоматизовані системи, де відбиваються всі відомості щодо складу їх програмного та апаратного забезпечення, а також наявність регулярних звірок паспортних даних з реальними.

Другим етапом «Озброєння» є вибір засобів захисту та побудова системи захисту кіберпростору (СЗК). Для цього нами необхідно розробити підхід, що дозволить зробити оптимальний (який забезпечує найкращі (оптимальні) показники захисту) вибір функціонального профілю кіберзахисту, при цьому витратити на це менше часу, ніж зазвичай.

За умови обрання оптимального функціонального профілю захищеності переходимо до наступного етапу, в іншому випадку повертаємось до початку.

Проведення контролю системи (кібепростору) є третім етапом «Контроль». Для цього здійснюється аналіз основних завдань захисту інформації, визначається реальний рівень зацікавленості суб'єктів, що забезпечують безпеку, у дотриманні всіх вимог до захищеності кожної з властивостей інформації (наприклад, достатній, низький, неприйнятний) відповідних загроз (вибір оптимального методу визначення важливості вимог), а також розрахунок взаємозалежних показників; розробка математичної моделі і алгоритму вибору раціонального варіанту побудови системи захисту (раціонального завдання вимог, тобто формування профілю) відповідно до поставленого завдання як завдання математичного моделювання.

Отже, необхідно визначити безпосередньо ефективність застосованих заходів за допомогою деякого кількісного показнику, який відображав би залежність цього показника від ймовірностей запобігання впливу атак на інформацію.

Таким чином, ми зможемо встановити доцільність вживання тих чи тих засобів протидії та зробити висновок про рівень протидії (достатній, недостатній).

На п'ятому етапі «Активна протидія» здійснюється інформування корпорацій щодо інцидентів кібербезпеки та активна протидія на рівні держави, тобто відбувається застосування контрзаходів, також на цьому етапі може відбуватись підготовка відповідних нормативних документів, з метою запобігання повторення реалізації загроз у майбутньому.

ВИСНОВКИ

Отже, для забезпечення представлення міри залежності вимог безпеки заданому рівню якості, необхідно використати низку понять, функцій та математичних моделей. У теорії нечітких великих кількостей є декілька методів побудови функції залежності вимог безпеки заданому рівню якості. Існують методи побудови функції залежності засновані на статистичних даних, на експертних оцінках, на разових оцінках, а також використовуються параметричних підхід. При виборі методу необхідно враховувати, як правило, складність отримання експертної інформації, трудомісткість

алгоритму обробки інформації при побудові функції залежності. Таким чином, задля побудови захищеного кіберпростору держави має бути застосований цілий комплекс заходів у чітко визначеній послідовності.

ЛІТЕРАТУРА

[1] *ISO/IEC 15408-99* [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://infobezlikbez.ru/terminy/standarty/266-mezhdunarodnyj-standart-iso-15408-obshchij-kriterij.

[2] *Державна служба спеціального зв'язку та захисту інформації України* [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: www.dsszzi.gov.ua.

[3] Домарев В.В. *Безопасность информационных технологий. Системный подход* / Домарев В. В. – К.: ДиаСофт, 2006. – 904 с.

[4] Синенко М.А. Математична модель методів активного захисту інформації / Синенко М.А., Ткач Ю.М. // *Технічні науки та технології : науковий журнал* / Чернігів. нац. технол. ун-т. – Чернігів: ЧНТУ, 2020. – № 2 (20). – С.109-115.

[5] Ткач Ю.М. Моделі систем захисту інформаційної сфери держави // *Сучасна спеціальна техніка*. – 2020. – №2 (61). – С.59-66.

[6] Ткач Ю.М. О развитии киберпространства и его защищенности // Безпека ресурсів інформаційних систем : *збірник тез І Міжнародної науково-практичної конференції* (м. Чернігів 16-17 квітня 2020 р.). – Чернігів: НУЧП, 2020. – С.173-177.

МОДЕЛЬ ЗАЩИТЫ КИБЕРПРОСТРАНСТВА CYBERSEC

В статье предложена модель защиты киберпространства CyberSec, ориентированная на выполнение функции "киберзащиты". Данная модель является функциональной, состоит из пяти этапов, объединяет в себе ряд методов и моделей, является циклической, а потому позволяет создать самоналагоджувану систему защиты в киберпространстве. На первом этапе «Разведка и обнаружения» осуществляется описание среды безопасности, то есть формируется модель угроз, является полным перечнем всех возможных угроз, которые существуют или могут возникнуть в данной ситуации. Вторым этапом «Вооружение» является выбор средств защиты и построение системы защиты киберпространства (СЗК). Проведение контроля системы (кибепростору) является третьим этапом «Контроль». На четвертом этапе «Противодействие» построения защищенного киберпространства выполняется оценка действенности, предложенной СЗК. На пятом этапе «Активное противодействие» осуществляется подготовка нормативных документов, информирование корпораций по инцидентам кибербезопасности активное противодействие на уровне государства, то есть происходит применения контрмер. Модель защиты киберпространства CyberSec позволяет на практике построить защищенный киберпространство как отдельной корпорации, так и государства в целом.

Ключевые слова: киберпространство, модель защиты, национальная безопасность, защищенное киберпространство.

CYBER SPACE PROTECTION MODEL CYBERSEC

The article proposes a cyberspace protection model CyberSec, which is focused on performing the function of "cyber protection". This model is functional, consists of five stages, combines a number of methods and models, is cyclical, and therefore allows you to create a self-configuring protection system in cyberspace. At the first stage of "Intelligence and Detection" is a description of the security environment, ie a threat model is formed, which is a complete list of all possible threats that exist or may arise in this situation, then assumptions are made about the attacker, and therefore the violator model is formed. The second stage of "Armament" is the choice of means of protection and construction of a system of cyberspace protection (SSC). To do this, it is necessary to develop an approach that will make the optimal (which provides the best (optimal) protection) choice of the functional profile of cybersecurity, while spending less time than usual. Carrying out control of the system (cyberspace) is the third stage of "Control". To do this, the analysis of the main tasks of information security, determines the real level of interest of security entities in compliance with all requirements for the security of each of the properties of information (for example, sufficient, low, unacceptable). At the fourth stage of "Counteraction" to the construction of secure cyberspace, the evaluation of the effectiveness of the proposed SZK is performed. In the fifth stage of "Active Counteraction", normative documents are prepared, corporations are informed about cybersecurity incidents, active counteraction is carried out at the state level, ie countermeasures are applied. The CyberSec cyberspace protection model allows you to build a secure cyberspace in practice for both an individual corporation and the state as a whole.

Keywords: cyberspace, protection model, national security, protected cyberspace.

Ткач Юлія Миколаївна – доктор педагогічних наук, професор, завідувач кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет.
E-mail: tkachym79@gmail.com.
ORCID ID: 0000-0002-8565-0525.

Ткач Юлия Николаевна – доктор педагогических наук, профессор, заведующая кафедрой кибербезопасности и математического моделирования, Черниговский национальный технологический университет.

Tkach Yuliia – Doctor of Pedagogical Science, Professor, Head of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology.