УДК 623.618

Якобінчук О.В., к. військ. н.

Національний університет оборони України імені Івана Черняховського

Математична модель інфокомунікаційної мережі спеціального призначення

Резюме. Розроблена модель інфокомунікаційної мережі спеціального призначення з урахуванням взаємовпливу усіх складових процесу нанесення втрат. За допомогою запропонованої моделі здійснюється визначення типів загроз, активів, які підлягають захисту та вразливостей, які притаманні мережам. Це дозволяє найбільш точно визначити ризики та втрати, які наносяться типам об'єктів оцінювання та на цій основі сформулювати конкретизовані вимоги з безпеки.

Ключові слова: математична модель, інфокомунікаційна мережа, захищеність.

Математическая модель инфокоммуникационной сети специального назначения

Резюме. Разработана математическая модель инфокоммуникационной сети специального назначения с учетом взаимного влияния всех составных процесса нанесения ущерба. С помощью предложенной модели осуществляется определение типов угроз, активов, подлежащих защите и уязвимостей, присущих сетям. Это дает возможность наиболее точно определять риски и потери, наносимые объектам оценивания, и на этой основе сформулировать конкретизированные требования безопасности.

Ключевые слова: математическая модель, инфокоммуникационная сеть, защищенность.

The mathematical model of infocomm network of the special purpose

Resume. A mathematical model of infocomm network of the special purpose account the mutual influence of all components of the process of damage is developed. With the proposed model is carried out to determine the types of threats, assets to be protected and vulnerabilities that are inherent in networks. This allows to more accurately determine the risks and losses that are applied object type estimation and on this basis to formulate the specified security requirements.

Keywords: Mathematical model, infocomm network, security.

Постановка проблеми. Аналіз останніх досліджень і публікацій. Під інфокомунікаційною мережею спеціального призначення (ІМСП) будемо розуміти технологічну систему, яка містить мережу електрозв'язку та засоби зберігання, обробки і пошуку інформації для забезпечення зв'язком та доступом до інформації відомчих (корпоративних) користувачів. Внаслідок зростання ролі та значення ІМСП підвищується їх вразливість до різнорідних загроз, отже питанню безпеки слід приділяти достатньо уваги. Захищеність ІМСП є ключовим питанням на усіх етапах функціонування мереж та одним із найважливіших показників ефективності їх функціонування разом із пропускною спроможністю, стійкістю та ін. Обгрунтування вимог до безпеки ІМСП, окремих засобів забезпечення захищеності та оцінювання їх ефективності можливе на основі математичних моделей.

Організація забезпечення захищеності повинна бути комплексною та ґрунтуватись на ретельному аналізі можливих негативних наслідків від реалізації загроз [1]. Аналіз негативних наслідків передбачає обов'язкову ідентифікацію можливих джерел загроз, факторів, які сприятимуть їх виявленню, визначенню загроз безпеці інформації, можливих наслідків реалізації загроз, аналіз можливих втрат, вибір заходів захисту, які сприятимуть мінімізації можливих втрат [1-5]. Виходячи з цього модель слід розробляти з урахуванням взаємного впливу таких елементів: загроза; фактор впливу (вразливість); актив; максимально можливий ризик; максимально можливі втрати; заходи захисту; залишковий

фактор впливу; залишковий ризик; залишкові втрати.

Метою статті є розробка математичної моделі інфокомунікаційної мережі спеціального призначення.

Виклад основного матеріалу. На етапі проектування та розроблення засобів безпеки мережа характеризується зовнішніми та внутрішніми факторами. До зовнішніх відносяться загрози активам, джерелом яких є зовнішнє середовище і які створюють загрозу роботі мережі та від яких необхідний захист. Безпосередньо ІМСП характеризується активами, які підлягають захисту та існуючими вразливими місцями, через які можливе здійснення атаки. Метою створення математичної моделі є врахування найбільш суттєвих факторів, які впливають на ІМСП для визначення необхідного комплексу заходів захисту активів. Тому при розгляді моделі ІМСП слід враховувати взаємний вплив трьох множин [1]:

$A = \{a_j\}, j = \overline{1, J}$ – множина активів (інформації або ресурсів), які підлягають захисту;

$Y = \{y_i\}, i = \overline{1, I}$ – множина загроз активам, які надходять з навколишнього середовища і створюють загрозу роботі мережі та від яких необхідний захист;

$V = \{v_k\}, k = \overline{1, K}$ – множина вразливих місць ІМСП, які характеризують її стан і властивості та можуть сприяти успішній реалізації загрози або можуть бути використані для здійснення загрози.

Елементи цих множин взаємодіють і характеризують ІМСП при впливі загроз активам. Множина взаємозв'язків "загроза – вразливість – актив" утворюють граф $\{\langle Y, V, A\rangle\}$, який характеризує можливості впливу загроз на певні активи через окремі вразливості ІМСП, тобто нанесення збитку.

Мірою, яка характеризує потенційну можливість навмисного або ненавмисного нанесення збитку шляхом реалізації загроз через вразливі місця на певні активи приймемо ризик. Множину ризиків визначимо, як декартів добуток множини загроз, множини вразливостей та множини активів ІМСП:

$$R = Y \times V \times A = \left\{r_c = \left\langle y_i, v_k, a_j \right\rangle\right\},$$

$$c \equiv ikj = \overline{1, C},\ C = I \times K \times J.$$

Елемент множини ризиків r_c характеризує ризик нанесення збитку при реалізації загрози i-го виду через вразливість k-го типу на j-у область активів.

Деякі комбінації $\left\langle y_i, v_k, a_j \right\rangle$ не утворюють ризику, оскільки існують активи, пов'язані з вразливостями, для яких не існує загроз, або активи, для яких існують загрози, але ці загрози не пов'язані з вразливостями, тобто виконується умова

$$(\exists y_i)(\exists v_k)(\exists a_j) \Rightarrow (\exists r)\left(r_c = \left\langle y_i, v_k, a_j \right\rangle\right),$$

$$y_i \in Y,\ v_k \in V,\ a_j \in A,\ r_c \in R.$$

У цьому випадку елемент множини ризиків сприймається рівним нулю.

Множина ризиків нанесення втрат визначається множиною втрат U, внаслідок впливу загроз безпеки через певні вразливості на окремі активи. Множину втрат визначимо декартовим добутком множини ризиків R та множини цінностей активів S, тобто

$$U = R \times S = \{u_c\} = \{r_c, s_c\}, c = \overline{1, C},$$

де s_c – цінність активу (в будь-якій шкалі вимірювань), для якого існує ризик нанесення втрати r_c.

Внаслідок цього отримуємо п'ятиелементний граф "загроза – вразливість – актив – ризик – втрати", який є формальною базовою моделлю об'єкта оцінювання (без засобів забезпечення безпеки активів), та характеризує взаємодію елементів безпеки та результати цього взаємовпливу (рис. 1).

Об'єкт оцінювання характеризується своєю структурою (складом і конфігурацією) та видом активів, які підлягають захисту. Для їх відображення запровадимо множину видів інформації $E = \{e_n\}, n = \overline{1, N}$, яка циркулює в ІМСП і підлягає захисту, та множину елементів ІМСП $O = \{o_s\}, s = \overline{1, S}$ і сформуємо три умовних підмножини:

$$Y^* = Y/(E, O) = \{y_{i*}(e_n, o_s)\} = \{y_i/(e_n, o_s)\},$$

$$Y^* \subset Y, i^* = \overline{1, I^*}, I^* \le I;$$

$$A^* = A/(E, O) = \{a_{j*}(e_n, o_s)\} = \{a_j/(e_n, o_s)\},$$

$$A^* \subset A, j^* = \overline{1, J^*}, J^* \le J;$$

$$V^* = V/(E, O) = \{v_{k*}(e_n, o_s)\} = \{v_k/(e_n, o_s)\},$$

$$K^* \subset K, k^* = \overline{1, K^*}, K^* \le K.$$

Отже, існує набір правил $e_n, o_s \to \{y^*\}$, $e_n, o_s \to \{a^*\}$, $e_n, o_s \to \{v^*\}$, згідно яким кожному елементу (e_n, o_s) множини "елемент ІМСП – вид інформації" $\{O, E\}$

знаходять відповідні елементи y_i, a_j, v_k множин Y, A, V та утворюють підмножини Y^*, A^*, V^*.

Запровадження в модель підмножин O та E дає можливість визначити тип об'єкта оцінювання та відповідні йому підмножини Y^*, A^*, V^*.

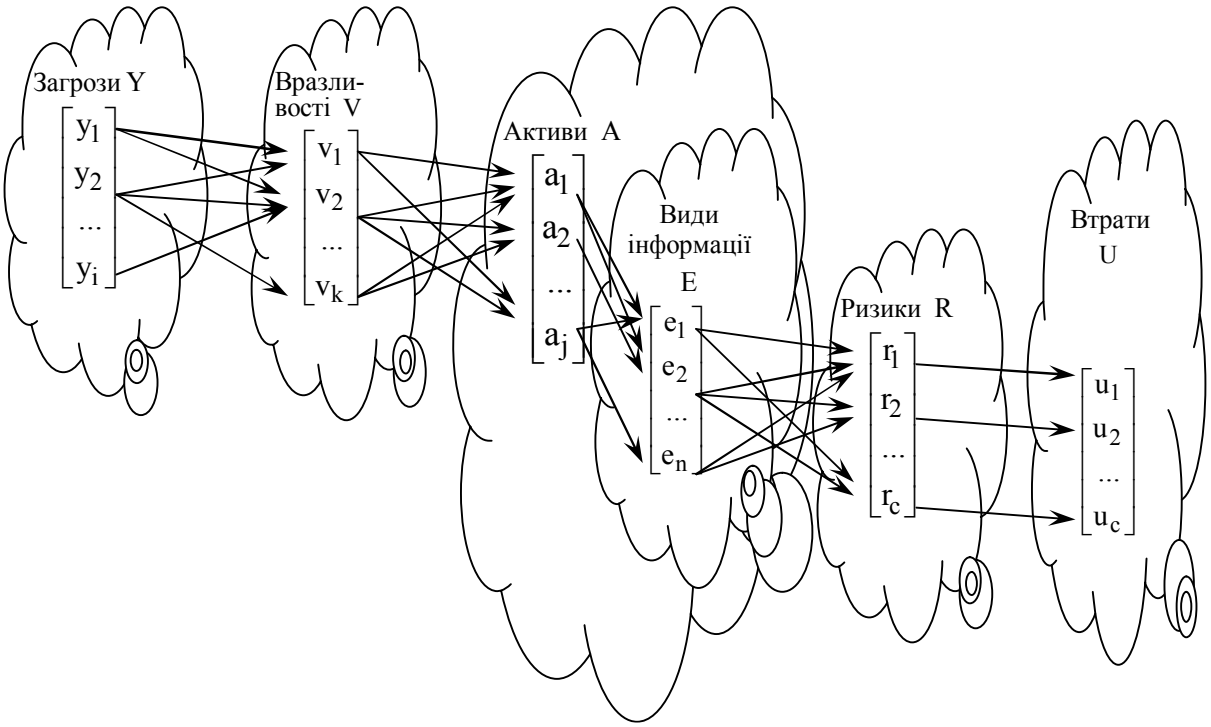

Рис. 1. Модель інфокомунікаційної мережі спеціального призначення

Під типом об'єкта оцінювання матимемо на увазі систему або продукт інформаційних технологій визначеної конфігурації, який працює з певним видом інформації.

Підмножина типів об'єктів оцінювання визначається неповним декартовим добутком множини елементів ІМСП та множини видів інформації, $T = O \times E = \{t_z = \langle o_s, e_n \rangle\}, s = \overline{1,S}, n = \overline{1,N}, z = \overline{1,Z}, Z < SN$, внаслідок того, що певні елементи ІМСП не можуть оброблювати інформацію різних ступенів важливості із-за неможливості виконання вимог безпеки.

Це значить, що деякі комбінації (e_n, o_s) не утворюють окремого елементу ІМСП через відсутність можливості забезпечення необхідної захищеності активів, тобто виконується умова

$$\exists(o_s)\exists(e_n) \Rightarrow \bar{\exists}(t_z)\ (t_z = \langle o_s, e_n \rangle),$$
$$s = \overline{1,S}, n = \overline{1,N},\ z = \overline{1,Z}.$$

У випадку наявності в мережі інформації різних ступенів важливості її вид визначається найвищим ступенем важливості, проте, це не означає, що для усіх видів активів необхідно забезпечити однаковий рівень захищеності.

Кожному елементу t_z множини типів об'єктів оцінювання T відповідають визначені підмножини Y_z^*, A_z^*, V_z^*, тобто існують функціональні співвідношення

$$Y^* \subset T \times Y, A^* \subset T \times A, V^* \subset T \times V.$$

Запровадження підмножини типів об'єктів оцінювання T дає змогу визначити підмножини Y^*, A^*, V^* як сукупність образів, які утворюються при відображенні підмножини T на множини Y, A, V відповідно:

$$Y^* : T \to Y, A^* : T \to A, V^* : T \to V.$$

Підмножини T_z^*, O_z^*, E_z^* відповідають вимогам: $Y = \bigcup_{z=1}^{Z} Y_z^*, A = \bigcup_{z=1}^{Z} A_z^*, V = \bigcup_{z=1}^{Z} V_z^*$.

Зазначені множини визначають ризики нанесення втрат для певного типу об'єкту оцінювання

$$R^* = Y^* \times V^* \times A^* = \left\{ r_{c^*} = \left\langle y_i^*, v_k^*, a_j^* \right\rangle \right\},$$

$c^* = \overline{1, C^*}, C^* \le I^*, K^*, J^*$ та множина втрат $U^* = R^* \times S = \{u_{c^*}\} = \{r_{c^*}, s_{c^*}\}, c^* = \overline{1, C^*}$.

Для дотримання вимог із безпеки ІМСП необхідно вжити заходи зі зменшення кількості вразливостей. Це можливо здійснити шляхом вибору відповідного варіанта застосування

засобів забезпечення захищеності активів. Вибір варіанта застосування засобів забезпечення захищеності активів здійснюється на підставі результатів оцінювання ризиків з урахуванням вимог безпеки та інших обмежень.

Висновки та перспективи подальших досліджень. Запропонована модель ІМСП відображає взаємовплив усіх складових процесу нанесення втрат. Модель є формалізованим інструментом для подальшого отримання аналітичних виразів показників захищеності ІМСП з урахуванням усіх характеристик, які впливають на мережі, та визначення необхідного комплексу заходів захисту для дотримання вимог безпеки на основі аналізу ризиків. За допомогою запропонованої моделі здійснюється визначення типів загроз, активів, які підлягають захисту та вразливостей, які притаманні мережам. Це дозволяє найбільш точно визначити ризики та втрати, які наносяться типам об'єктів оцінювання та на цій основі сформулювати конкретизовані вимоги з безпеки.

СПИСОК ЛІТЕРАТУРИ

1. Хоффман Л. Дж. Современные методы защиты информации. – М.: Сов. Радио, 1980. – 264 с.
2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – Санкт-Петербург: Издательство "Наука и Техника", 2004. – 384 с.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – 2001. – 608 с.
4. Додонов А.Г. Живучесть информационных систем / А.Г. Додонов, Д.В. Ландэ. – К.: Наукова думка, 2011.– 256 с.
5. Барабаш О.В. Построение функционально устойчивых распределенных информационных систем / О.В. Барабаш. – К.: НАОУ, 2004.–226 с.