УДК 004.7:004.056.53

М. П. Карпінський[1], У. О. Яциковська[2], А. В. Балик[3], М. Александер[4]
[1]Department of Computer Science, University of Bielsko-Biala, Bielsko-Biala, POLAND,
[2]кафедра комп'ютерних наук, Тернопільський національний технічний університет імені Івана Пулюя, Україна, м. Тернопіль,
[3]Обчислювальний центр, Тернопільський національний педагогічний університет імені Володимира Гнатюка, Україна,
[4]Institute of Engineering, State Higher Vocational School in Nowy Sacz, Poland

АТАКИ НА ВІДМОВУ В ОБСЛУГОВУВАННІ КОМП'ЮТЕРНИХ МЕРЕЖ

Розглянуто задачі DoS/DDoS/DRDoS-атак на клієнт-серверні моделі комунікації. Побудовані формалізовані математичні моделі такого класу атак дають змогу враховувати структуру мережі та на основі вагових коефіцієнтів міру впливу кожного виду атак, що дозволяє ефективно проектувати системи захисту інформації із урахуванням інформаційних загроз.

Ключові слова: формалізована математична модель, клієнт-серверна модель комунікації, DoS/DDoS/DRDoS-атаки.

COMPUTER NETWORKS SERVICE DENIAL ATTACKS

In this article problems of DoS/DDoS/DRDoS – attacks on client-server model of communication are discussed. We've built formal mathematical model of this class of attacks which allows to design a system of information security according to security threats and network topology using weighting coefficients for each type of attacks.

Key words: formal mathematical model, client-server model of communication, DoS/DDoS/DRDoS –attacks.

Постановка проблеми

Зростання кіберзлочинності останніми роками уможливлює несанкціонований доступ до ресурсів комп'ютерних мереж (КМ). Серед найпоширеніших численних атак зловмисників на КМ – переривання і спотворення пакетного трафіка. Найруйнівнішими атаками сьогодні є атаки, спрямовані на відмову в обслуговуванні легітимних послуг. У цьому випадку ініціатор атак компрометує вузол-користувача, експлуатуючи його ресурси, щоб забезпечити повне керування вузлом. Ініціатор атак спрямовує велику кількість підробленого трафіка до вузла-користувача, споживаючи пропускну здатність суттєвого обсягу, що призводить до неможливості обслуговувати легітимний трафік [1].

До такого класу атак належать: DoS (Denial of Service) – під час якої спостерігається підвищена витрата ресурсів процесора та зменшення пропускної здатності каналу зв'язку, що може призвести до істотного уповільнення роботи всієї КМ; DDoS (Distributed Denial of Service) – розподілена атака, спрямована на комп'ютер користувача в КМ з наміром зробити інформаційні ресурси недоступними, DRDoS (Distributed Reflection Denial of Service) – розподілена віддзеркалена атака, яка спрямована на поглинання пропускної здатності мережі. Тому розроблення формалізованої математичної моделі впливу різних видів DoS/DDoS/DRDoS-атак є актуальним завданням.

Аналіз останніх досліджень та публікацій

Під час проектування та побудови систем захисту комп'ютерних мереж враховують різні чинники, що можуть вплинути на безпеку: топологію мережі, середовище користувачів, склад програмного та апаратного забезпечення, налаштування параметрів системи тощо. Ці чинники впливають на рівень захищеності комп'ютерної мережі. Інтегральне кількісне врахування цих чинників дає можливість визначати рівень захищеності й досягається розв'язанням завдання оцінювання захищеності компонентів комп'ютерної мережі.

Є різні підходи та моделі, які оцінюють захищеність корпоративної мережі та її ресурсів, – дерево атак (attack tree) та формалізованіша модель – граф атак (attack graph). У цих моделях розглядаються можливі атаки на систему, які експлуатують відомі вразливості кожного із сервісів мережі. Згідно з цими підходами, для пошуку можливих шляхів проникнення до системи будують відповідний граф, який враховує топологію мережі. Недоліком такого підходу є необхідність виконання перебору всіх можливих шляхів атак. При цьому потрібно враховувати можливість послідовної експлуатації вразливостей на кожному хості мережі, що для мереж великих розмірів є трудомістким обчислювальним завданням. Цей підхід може використовуватися для аналізу вже створених мереж, але не дає змогу синтезувати топологію мережі, для якої зменшується ймовірність атак.

Поставлене нами завдання можна виконати з використанням різних математичних моделей. Це завдання розв'язувалось у роботах [2–5] та інших. Так, у роботі [2] запропоновано модель у вигляді графу атак, яка для системи, що існує, враховує топологію мережі, використовує інформацію про відомі вразливості та будує можливі сценарії здійснення атак. У роботі [3] розглянуто класичні моделі формальної теорії захисту інформації в електронних системах обробки даних. У роботі [4] наведено моделі захищеної комп'ютерної системи, які ґрунтуються на логіко-імовірнісному підході. Алгоритм, який наведено в [2], призначений для аудиту вже створеної системи на предмет можливості атак з використанням відомих вразливостей програмного забезпечення. Моделі, проаналізовані в роботі [3], доволі важко застосовувати на практиці в розподілених системах. У [4] обчислюється інтегральний показник захищеності всієї системи без врахування її топології.

У роботі [5] розроблено процедуру формального опису та оцінювання рівня захищеності об'єктів у інформаційно-комунікаційній комп'ютерній системі. Застосовуючи логіко-імовірнісний підхід для оцінювання рівня захищеності, автор виділяє кілька ключових етапів.

На першому етапі здійснюється побудова матриці доступу хостів між собою, а також логічної схеми мережі. Для того щоб виявити усі можливі шляхи проникнення до визначеного об'єкта системи, необхідно, ґрунтуючись на політиці безпеки (чи мережевих налаштуваннях), скласти матрицю (логічну схему) взаємної доступності хостів. Для цього можуть використовуватися топологічні сканери мережі.

На другому етапі розробляються та аналізуються сценарії можливих атак. Для створення сценаріїв атак необхідно:

а) визначити категорії зловмисників;

б) об'єкти (хости) системи, до яких зловмисники можуть отримати доступ.

Потім, на основі логічної структури мережі, перевіряють, чи можна з цих хостів, через інші хости, отримати доступ до об'єкта захисту.

У результаті аналізу усіх варіантів отримуємо сценарії атаки та послідовну множину умов, необхідних для її здійснення. Краще, щоб сценарій атаки складали спеціалісти з інформаційної безпеки.

На третьому етапі сценарій атаки подають у вигляді графу, що складається з комбінації умов, необхідних для здійснення атаки. Вершиною графу є доступ зловмисника до об'єкта захисту, листками – умови, а проміжними вершинами – логічні комбінації цих умов.

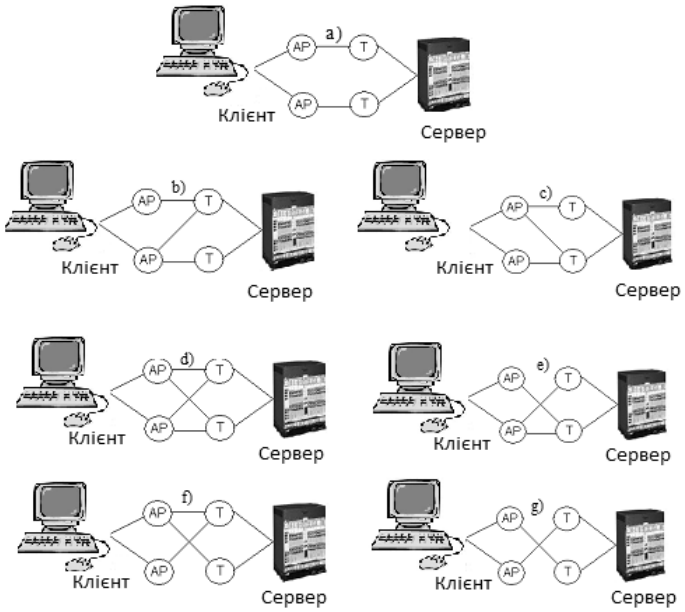
На четвертому етапі будується логічна модель атаки. На основі графу складають логічну функцію атаки.

Формулювання цілі статті

Метою роботи є розроблення та вивчення формалізованої математичної моделі класу атак DoS/DDoS/DRDoS з урахуванням структури мережі та вагових коефіцієнтів міри впливу кожного виду атак, що дасть змогу ефективно проектувати системи захисту інформації у КМ із урахуванням інформаційних загроз.

Виклад основного матеріалу

Для того, щоб з'ясувати ключові задачі архітектури, стійкої до нападу КМ, спочатку розглянемо спрощену модель комунікації клієнт-сервер, яка зображена на рисунку.



Модель комунікації клієнт-сервер:
AP – точка доступу, T – точка призначення

У цих моделях обмежимося двома точками входу й двома точками призначення. Лінії, що сполучають точки входу й точки призначення, моделюють комунікацію між ними в КМ.

Під стійкістю мережі розуміють здатність мережі забезпечити альтернативну комунікацію під час зруйнування (чи спроб зруйнувати) хоча б одного шляху між клієнтом і сервером [6].

У результаті аналізу класифікації DoS/DDoS/DRDoS-атак ми запропонували формалізовану математичну модель (1), яка дає змогу визначити рівень впливу показників атак на КМ [7, 8]:

$$\begin{aligned} P_{DoS} &= \beta_1 P_{Smurf} + \beta_2 P_{Fraggle} + \beta_3 P_{SYNFlood} + \beta_4 P_{DNS}, \\ P_{DDoS} &= \delta_1 P_{Trinoo} + \delta_2 P_{TFN/TFN2K} + \delta_3 P_{Stacheldraht}, \\ P_{DRDoS} &= \mu_1 P_{Smurf} + \mu_2 P_{Fraggle} + \mu_3 P_{DNS} + \mu_4 P_{SNMP}, \end{aligned} \quad (1)$$

де β_i, δ_i, μ_i – вагові коефіцієнти впливу показників DoS-, DDoS-, DRDoS-атак, причому $\sum_{i=1}^{4} \beta_i = 1$, $\sum_{i=1}^{3} \delta_i = 1, \sum_{i=1}^{4} \mu_i = 1$.

Вагові коефіцієнти визначають внесок основних видів атак DoS/DDoS/DRDoS у КМ та дають змогу врахувати зазначені атаки під час розроблення та експлуатації систем захисту інформації. За допомогою цих показників та коефіцієнтів можна визначити основні види загроз та їх вплив на рівень безпеки КМ, що дасть змогу ефективно проектувати системи захисту інформації з урахуванням інформаційних загроз.

Побудуємо формалізовані математичні моделі імовірності інформаційних загроз із характером DoS/DDoS/DRDoS-атак лінійного виду на основі використання методу вагових коефіцієнтів:

$$\begin{aligned} P\_I3(P) &= \alpha_1 P_{Конф.} + \alpha_2 P_{Ціл.} + \alpha_3 P_{Дост.}, \\ P\_DoS(P) &= \beta_1 P_{Smurf} + \beta_2 P_{Fraggle} + \beta_3 P_{SYNFlood} + \beta_4 P_{DNS}, \\ P\_DDoS(P) &= \delta_1 P_{Trinoo} + \delta_2 P_{TAN/TF2K} + \delta_3 P_{Stacheldraht}, \\ P\_DRDoS(P) &= \mu_1 P_{Smurf} + \mu_2 P_{Fraggle} + \mu_3 P_{DNS} + \mu_4 P_{SNMP}, \end{aligned} \tag{2}$$

де P_I3_(P) – імовірність інформаційних загроз; P_DoS(P) – імовірність DoS-атак; P_DDoS(P) – імовірність DDoS-атак; P_DRDoS(P) – імовірність DRDoS-атак; α_i, β_i, δ_i, μ_i – вагові коефіцієнти, причому $\sum_{i=1}^{3}\alpha_i = 1$, $\sum_{i=1}^{4}\beta_i = 1$, $\sum_{i=1}^{3}\delta_i = 1$, $\sum_{i=1}^{4}\mu_i = 1$ відповідно.

Ці вагові коефіцієнти можна визначити експериментальним методом для кожної конкретної мережі, тобто спроектувати архітектури мереж, поданих на рис. 1, і встановити інтенсивність атак різного виду на мережу. За допомогою спрощеної моделі комунікації системи клієнт-сервер і математичних моделей (1) та (2) визначаємо матриці активності мережі, згідно з якими формуємо висновок про здійснення виду атаки [4]:

$$\begin{aligned} \alpha_{інф.загр.} &= \begin{bmatrix} \alpha_1^a & \alpha_2^a & \alpha_3^a \\ \alpha_1^b & \alpha_2^b & \alpha_3^b \\ \alpha_1^c & \alpha_2^c & \alpha_3^c \\ \alpha_1^d & \alpha_2^d & \alpha_3^d \\ \alpha_1^e & \alpha_2^e & \alpha_3^e \\ \alpha_1^f & \alpha_2^f & \alpha_3^f \\ \alpha_1^g & \alpha_2^g & \alpha_3^g \end{bmatrix}, \beta_{DoS} = \begin{bmatrix} \beta_1^a & \beta_2^a & \beta_3^a & \beta_4^a \\ \beta_1^b & \beta_2^b & \beta_3^b & \beta_4^b \\ \beta_1^c & \beta_2^c & \beta_3^c & \beta_4^c \\ \beta_1^d & \beta_2^d & \beta_3^d & \beta_4^d \\ \beta_1^e & \beta_2^e & \beta_3^e & \beta_4^e \\ \beta_1^f & \beta_2^f & \beta_3^f & \beta_4^f \\ \beta_1^g & \beta_2^g & \beta_3^g & \beta_4^g \end{bmatrix}, \\ \delta_{DDoS} &= \begin{bmatrix} \delta_1^a & \delta_2^a & \delta_3^a \\ \delta_1^b & \delta_2^b & \delta_3^b \\ \delta_1^c & \delta_2^c & \delta_3^c \\ \delta_1^d & \delta_2^d & \delta_3^d \\ \delta_1^e & \delta_2^e & \delta_3^e \\ \delta_1^f & \delta_2^f & \delta_3^f \\ \delta_1^g & \delta_2^g & \delta_3^g \end{bmatrix}, \mu_{DRDoS} = \begin{bmatrix} \mu_1^a & \mu_2^a & \mu_3^a & \mu_4^a \\ \mu_1^b & \mu_2^b & \mu_3^b & \mu_4^b \\ \mu_1^c & \mu_2^c & \mu_3^c & \mu_4^c \\ \mu_1^d & \mu_2^d & \mu_3^d & \mu_4^d \\ \mu_1^e & \mu_2^e & \mu_3^e & \mu_4^e \\ \mu_1^f & \mu_2^f & \mu_3^f & \mu_4^f \\ \mu_1^g & \mu_2^g & \mu_3^g & \mu_4^g \end{bmatrix}. \end{aligned} \tag{3}$$

Отже, взявши загальну кількість атак за 100 %, можна визначити, скільки процесів належатиме кожному виду атак. Тоді коефіцієнти обчислюватимуться згідно з таким співвідношенням:

$$\begin{aligned} \alpha_1^a &= \frac{n_{Конф.}^a}{100\%}, \alpha_2^a = \frac{n_{Ціл.}^a}{100\%}, \alpha_3^a = \frac{n_{Дост.}^a}{100\%}, \\ \beta_1^a &= \frac{n_{Smurf}^a}{100\%}, \beta_2^a = \frac{n_{Fraggle}^a}{100\%}, \beta_3^a = \frac{n_{SYNFlood}^a}{100\%}, \beta_4^a = \frac{n_{DNS}^a}{100\%}, \\ \delta_1^a &= \frac{n_{Trinoo}^a}{100\%}, \delta_2^a = \frac{n_{TFN/TFN2K}^a}{100\%}, \delta_3^a = \frac{n_{Stacheldraht}^a}{100\%}, \\ \mu_1^a &= \frac{n_{Smurf}^a}{100\%}, \mu_2^a = \frac{n_{Fraggle}^a}{100\%}, \mu_3^a = \frac{n_{DNS}^a}{100\%}, \mu_4^a = \frac{n_{SNMP}^a}{100\%}, \end{aligned} \tag{4}$$

де $n_{Конф.}^a$, $n_{Ціл.}^a$, $n_{Дост.}^a$ – кількість показників інформаційних загроз на мережу типу *a*; n_{Smurf}^a, $n_{Fraggle}^a$, $n_{SYNFlood}^a$, n_{DNS}^a – кількість показників атак виду DoS на мережу типу *a*; n_{Trinoo}^a, $n_{TFN/TFN2K}^a$, $n_{Stacheldraht}^a$ –

кількість показників атак виду DDoS на мережу типу *a*; n^a_{Smurf}, $n^a_{Fraggle}$, n^a_{DNS}, n^a_{SNMP} – кількість показників атак виду DRDoS на мережу типу *a*.

Аналогічно знаходимо кількісні показники різного виду атак для клієнт-серверних моделей типу *b, c, d, e, f* і *g*.

З проведених досліджень і з урахуванням аналітичних виразів (4) та емерджентності моделі комунікації клієнт-сервер отримано:

$$\alpha_1^{\alpha} = \frac{3}{8}\cdot\frac{1}{k_e^{\alpha}} = 0{,}375,\ \alpha_1^{b} = \frac{3}{8}\cdot\frac{1}{k_e^{b}} = 0{,}15,\ \alpha_1^{c} = \frac{3}{8}\cdot\frac{1}{k_e^{c}} = 0{,}15,$$

$$\alpha_1^{d} = \frac{3}{8}\cdot\frac{1}{k_e^{d}} = 0{,}125,\ \alpha_1^{e} = \frac{3}{8}\cdot\frac{1}{k_e^{e}} = 0{,}15,\ \alpha_1^{f} = \frac{3}{8}\cdot\frac{1}{k_e^{f}} = 0{,}15,$$

$$\alpha_1^{g} = \frac{3}{8}\cdot\frac{1}{k_e^{g}} = 0{,}75,\ \alpha_2^{\alpha} = \frac{1}{8}\cdot\frac{1}{k_e^{\alpha}} = 0{,}125,\ \alpha_2^{b} = \frac{1}{8}\cdot\frac{1}{k_e^{b}} = 0{,}05,$$

$$\alpha_2^{c} = \frac{1}{8}\cdot\frac{1}{k_e^{c}} = 0{,}05,\ \alpha_2^{d} = \frac{1}{8}\cdot\frac{1}{k_e^{d}} = 0{,}375,\ \alpha_2^{e} = \frac{1}{8}\cdot\frac{1}{k_e^{e}} = 0{,}05, \qquad (5)$$

$$\alpha_2^{f} = \frac{1}{8}\cdot\frac{1}{k_e^{f}} = 0{,}05,\ \alpha_2^{g} = \frac{1}{8}\cdot\frac{1}{k_e^{g}} = 0{,}0625,\ \alpha_3^{\alpha} = \frac{1}{2}\cdot\frac{1}{k_e^{\alpha}} = 0{,}5,$$

$$\alpha_3^{b} = \frac{1}{2}\cdot\frac{1}{k_e^{b}} = 0{,}2,\ \alpha_3^{c} = \frac{1}{2}\cdot\frac{1}{k_e^{c}} = 0{,}2,\ \alpha_3^{d} = \frac{1}{2}\cdot\frac{1}{k_e^{d}} = 0{,}166,$$

$$\alpha_3^{e} = \frac{1}{2}\cdot\frac{1}{k_e^{e}} = 0{,}2,\ \alpha_3^{f} = \frac{1}{2}\cdot\frac{1}{k_e^{f}} = 0{,}2,\ \alpha_3^{g} = \frac{1}{2}\cdot\frac{1}{k_e^{g}} = 0{,}25.$$

Ці коефіцієнти визначаємо експериментальним методом, спроектувавши архітектури, що дають змогу визначити інтенсивність атак на мережу.

Для обчислення коефіцієнтів емерджентності k_e^a, k_e^b, k_e^c, k_e^d, k_e^e, k_e^f, k_e^g скористаємося (6):

$$K_e = \frac{n_з}{n_e}, \qquad (6)$$

де $n_з$ – кількість зв'язків, n_e – кількість компонентів.

$$k_e^a = \frac{2}{2} = 1; k_e^b = \frac{5}{2} = 2{,}5; k_e^c = \frac{5}{2} = 2{,}5; k_e^d = \frac{6}{2} = 3;$$
$$k_e^e = \frac{5}{2} = 2{,}5; k_e^e = \frac{5}{2} = 2{,}5; k_e^g = \frac{4}{2} = 2. \qquad (7)$$

Зазначимо, що найбільшим коефіцієнтом емерджентності володіє модель комунікації клієнт-сервер типу *d*. Тому її доцільно використовувати для убезпечення передавання інформаційних потоків у комп'ютерних мережах.

Висновок

Ґрунтуючись на класифікації інформаційних загроз, характерних для атак типу DoS/DDoS/DRDoS, запропоновано формалізовані моделі лінійного виду для диференціації атак на основі методу вагових коефіцієнтів. За допомогою цих показників та коефіцієнтів можна визначити основні види загроз у КМ, що дають змогу ефективно проектувати системи захисту інформації із урахуванням інформаційних загроз.

Для того, щоб спроектувати мережу з урахуванням усіх інформаційних загроз, слід враховувати як вагові коефіцієнти різних видів атак, так і захищеність компонентів КМ від внутрішніх та зовнішніх атак.

1. Steve G. Distributed reflection denial of service [Електронний ресурс] / G. Steve // Портал: Gibson Research Corporation – Режим доступу: http://grc.com/dos/drdos.htm. – Заголовок з екрану, умовно-вільний, 15. 04. 2012. 2. Todd Hughes, Sheyner Oleg: Attack scenario graphs for computer network threat analysis and

prediction // Complexity 9(2) (ISSN: 1076-2787): 15-18 (2003). 3. Грушо А. А., Тімоніна Є. Є. Теоретичні основи захисту інформації. – М.: Видавництво Агентства "Яхтсмен", 1996. – 192 с. 4. Новіков О., Тимошенко А. Побудова логіко-ймовірнісної моделі захищеної комп'ютерної системи // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вип. 3. – С. 101–105. 5. Новіков О. М., Родіонов А. М. Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем // Інформаційні технології та комп'ютерна інженерія. – 2008. – № 1(11). – С. 170–175. 6. Яциковська У. О. Модель захищеної архітектури клієнт-сервер [Текст] / У. О.°Яциковська, І. В. Васильцов, М. П. Карпінський // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2010. – № 9 (151). – С. 74–79. 7. Яциковська У. О. Дослідження реалізації розподілених атак в комп'ютерній мережі [Текст] / У. О. Яциковська, І. В. Васильцов, М. П. Карпінський // Сучасна спеціальна техніка. – 2011. – № 2 (25). – С. 124–127. 8. Яциковська У. О. Моделювання мережного трафіка комп'ютерної мережі під час реалізації атак типу DoS/DDoS [Текст] / У. О. Яциковська, М. П. Карпінський // Інформаційна безпека. – 2011. – № 1 (5). – С. 142–145.

УДК 004.056.5:004.7

В. О. Кононова, О. В. Харкянен, С. В. Грибков
Національний університет харчових технологій,
кафедра інформаційних систем

ОЦІНКА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Розглянуто особливості захисту інформаційних ресурсів у корпоративних мережах та системах, а також описано підхід щодо їх оцінки. Розглянутий підхід щодо оцінки засобів захисту дає змогу знизити витрати на їх впровадження, він легко адаптується до конкретних потреб будь-якої організації з урахуванням специфіки її діяльності та бізнесу. Такий підхід дозволяє точніше описувати інформаційні ресурси через характерні для них вразливості, вартість самих ресурсів, а також ранжувати ризики та відповідно інформаційні ресурси за ступенем критичності для діяльності організації.

Ключові слова: захист інформації, оцінка захисту, інформаційний ресурс, комп'ютерна мережа, інформаційна безпека.

ASSESSING PROTECTION MEANS OF INFORMATION RESOURCES

The paper considers specifics of information resources protection in corporate networks and systems. An approach to assessing protection means is described which allows to reduce their deployment cost and adapts easily to specific needs of any organization with an allowance for specifics of its activities and business. Such an approach makes it possible to describe information resources more precisely through their characteristic vulnerabilities and resources cost. It also helps to rank the risks and information resources according to their criticality for organization activities.

Key words: information protection, protection assessment, information resource, computer network, information security.

Вступ

Сучасна організація режиму інформаційної безпеки стає критично важливим стратегічним чинником розвитку будь-якої вітчизняної компанії. При цьому, як правило, основну увагу звертають на вимоги і рекомендації нормативно-методичної бази в галузі захисту інформації. Разом