УДК 623.618

А.В. Снігуров, В.Ю. Балашов, А.Ю. Нестеренко

Харківський національний університет радіоелектроніки, Харків

ПІДХІД ДО ПРОГНОЗУВАННЯ ТА ОЦІНКИ СИТУАЦІЇ ПРИ КОМПЛЕКСНІЙ ІНФОРМАЦІЙНІЙ АТАЦІ НА ОРГАНІЗАЦІЮ З ВИКОРИСТАННЯМ ІНДИКАТОРІВ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В статті представлений підхід до прогнозування та оцінки ситуації при комплексній інформаційній атаці на організацію. Для вирішення даного завдання пропонується використовувати теорію ризиків інформаційної безпеки та індикатори реалізації даних ризиків. Цій підхід пропонується для реалізації при створенні систем менеджменту інформаційної безпеки організацій (підприємств).

Ключові слова: *комплексна інформаційна атака, ризики інформаційної безпеки, індикатори ризиків.*

Вступ

Постановка задачі. Однією з найнебезпечніших видів інформаційних атак на організації є комплексні спрямовані атаки. Під спрямованістю атаки ми розуміємо сплановану зловмисником атаку на конкретну організацію, наприклад, за замовленням її конкурентів. Під комплексністю атаки ми розуміємо сплановані за метою, завданнями, часом та об'єктами атаки дії зловмисників з використанням різноманітних технічних, програмних або (та) психологічних методів та засобів.

Об'єктами таких інформаційних атак можуть бути:

– управлінські організації – міністерства, управління тощо;

– телекомунікаційні компанії;

– промислові підприємства;

– засоби масової інформації та комунікації (ЗМІ та К),

– організації, які надають послуги для населення (наприклад, послуги страхування, медичні послуги, продаж будь-якої продукції) та інші.

Метою зловмисника, при цьому можуть бути:

1) нанесення збитку комерційним інтересам організації: зрив контрактів, партнерських взаємин;

2) нанесення збитку репутації організації, її дискредитація;

3) дезорганізація діяльності організації, погіршення морального клімату в колективі, зниження ефективності функціонування організації.

Комплексна атака на організацію може включати наступні дії зловмисників:

– отримання зловмисником конфіденційної інформації організації через різні канали перехоплення інформації: кібератаки на інформаційну мережу, перехоплення інформації через побічні електромагнітні випромінювання та наводки (ПЕМВН) комп'ютерної техніки, акустичні канали прослуховування, підкуп персоналу та інше;

– атаки на відмову в обслуговуванні (DoS) інформаційних ресурсів організації;

– психологічні атаки на керівництво та співробітників організації;

– розповсюдження інформації об організації в ЗМІ та К, яка її дискредитує (атака на клієнтів організації);

– внесення шкідливих програм в інформаційну мережу організації та інше.

Комплексна атака, як правило, розтягнута в часі, може бути підготовчий період, при якому зловмисник вивчає організацію, її основні та допоміжні процеси, персонал, клієнтуру, систему захисту.

Класичним прикладом проведення комплексної спрямованої атаки проти організації є атака на страхову компанію «Оранта», що наведена в [1]. Зміст даної атаки:

1) 10 грудня 2008 року об 11:30 у вигляді спаму було розіслано інформаційне повідомлення, в якому йшлося про те, що страхова компанія «Оранта» заявляє про банкрутство. Ця інформація поширилася на тисячі адрес та потрапила у ЗМІ та К. У повідомленні говорилося про те, що компанія з 31 грудня 2008 року припиняє виконувати взяті перед клієнтами обов'язки;

2) о 12:31 на сайті «Економічні новини» з'являється повідомлення про банкрутство компанії «Оранта».

3) протягом двох годин з початку атаки всі поштові сервери компанії «Оранта» були виведені з ладу, тому спростування в мережі затрималося;

4) протягом ще кількох годин ряд видавництв ЗМІ та К підхопили цю інформацію та опублікували її на своїх ресурсах;

5) представники компанії «Оранта» із запізненням на добу публікують спростування неправдивої інформації про банкрутство компанії, яка розповсюджується видавництвами ЗМІ та К.

Аналіз даної атаки показує, що для досягнення своєї мети зловмисниками були використані як ін-

формаційно-технічні, так і інформаційно-психологічні методи впливу, які здійснювалися за єдиним задумом.

Причинами ефективності комплексних спрямованих атак проти організацій є:

1) активні дії зловмисника. При проведенні комплексної атаки зловмисником здійснюється ретельне планування об'єктів нападу, способів та засобів нападу, проводиться пошук вразливих місць в захисних механізмах організації. Можуть активно використовуватися методи соціальної інженерії;

2) помилки в побудові захисних механізмів організації, політиках та процедурах інформаційної безпеки (ІБ), орієнтованість системи менеджменту інформаційної безпеки (СМІБ), в першу чергу, проти неорганізованих зловмисників, ніж проти сторони, що має можливості провести комплексну атаку;

3) несподіваність дій зловмисника;

4) низька кваліфікація співробітників підрозділів ІБ щодо захисту організації від комплексних атак;

5) недостатня глибина та частота контролю інформаційної ситуації в організації та в інформаційному просторі навколо організації. Так, якщо комп'ютерна мережа сучасних організацій контролюється більш-менш адекватно сучасній ситуації у сфері інформаційного протиборства, то морально-психологічна ситуація в колективах контролюється набагато гірше. В той же час контроль ЗМІ та К на рівні організацій практично не здійснюється;

6) низький рівень взаємодії підрозділів ІБ організацій із структурами держави, що забезпечують інформаційну та національну безпеку.

Для забезпечення ІБ організацій в цих умовах важливо розуміти, почалася проти організації комплексна атака або відбуваються неузгоджені та ненаправлені загрози від різних зовнішніх зловмисників, інсайдерів або безграмотні дії персоналу та керівництва.

Для рішення даного завдання в роботі пропонується використовувати теорію ризиків ІБ, яка має високу ефективність при побудові СМІБ [2] та теорію індикаторів ризику, яка добре зарекомендувала себе в системі митного контролю [3].

Аналіз літератури. Питання прогнозування в сфері інформаційної безпеки досліджувалися в джерелах [4–6]. Але підхід прогнозування та оцінки ситуації з використанням теорії ризиків інформаційної безпеки та індикаторів ризиків у відомій літературі відсутній.

Мета статті – запропонувати підхід до прогнозування та оцінки ситуації в сфері інформаційної безпеки навколо організації з метою виявлення початку комплексної атаки з використанням теорії ризиків ІБ.

Виклад основного матеріалу

Визначення поняття ризику ІБ

Традиційно ризики ІБ визначаються за формулою (1):

$$R = P_{загр} \cdot P_{вразл} \cdot Ст, \quad (1)$$

де $P_{загр}$ – ймовірність реалізації атаки (ймовірність загрози);

$P_{вразл}$ – ймовірність того, що атака подолає систему захисту, тобто показник, який враховує ефективність системи захисту активу (ймовірність вразливості);

Ст – ступінь важливості активу для організації, тобто ступінь втрат для організації в разі реалізації успішної атаки на актив.

При цьому ризик ІБ фактично виступає в якості прогнозу можливих дій зловмисника з урахуванням рівня важливості активу та його захищеності. Застосуємо дану теорію для оцінки комплексної атаки.

Вважаємо, що дано i, $i = \overline{1,I}$ активів організації, на які можливі атаки зловмисником під час проведення комплексної атаки. При цьому активом можуть бути як інформаційні ресурси організації, інформаційна система, так і керівництво, співробітники, клієнти організації. Для кожного активу проводиться окрема оцінка ризику ІБ. На кожний актив існує певна кількість типів атак q, $q = \overline{1,Q}$. Для кожного з q типів атак є ймовірність реалізації, тобто ймовірність того, що зловмисник проведе саме таку атаку, $P_{загр_q}$, $q = \overline{1,Q}$. Кожна із атак може бути реалізована через одну або декілька вразливостей активів z, $z = \overline{1,Z}$. Ймовірність вразливості до q-го типу атаки – $P_{вразл_q^z}$, $z = \overline{1,Z}$. Якщо актив не вразливий до q-го типу атаки, то $P_{вразл_q^z} = 0$.

Ступінь впливу на актив q-го типу атаки через всі існуючі z вразливостей визначається згідно виразу (2):

$$P_{впливу_q} = 1 - \prod_{z=1}^{Z} (1 - P_{загр_q} \cdot P_{вразл_q^z}). \quad (2)$$

Ступінь впливу на актив всіх q атак визначається згідно виразу (3):

$$P_{впливу} = 1 - \prod_{q=1}^{Q} (1 - P_{впливуq}). \quad (3)$$

Тоді ризик успішного нападу на і-й актив з урахуванням множини атак на даний актив та множини вразливостей його системи захисту описується формулою (4):

$$R_i = P_{впливуі} \cdot Ст_i. \quad (4)$$

Ступінь важливості активу для організації $Ст_i$ в теорії ризиків ІБ прийнято вимірювати або в реальних втратах, які виражають в грошовому еквіваленті, або в безрозмірних величинах. В даній статті пропонується вимірювати даний показник в межах від 0 до 1 (0 – ступінь важливості активу $Ст_i$ – мінімальна; 1 – максимальна).

Оцінка ризиків здійснюється завчасно до будь-яких дій зловмисників і має на меті підготувати СМІБ до дій у відповідь в разі початку комплексної атаки. При цьому в роботі пропонується здійснювати оцінку поточної ситуації (оцінка сценарію комплексної атаки) та прогноз її розвитку за допомогою індикаторів ризиків.

Використання індикаторів ризиків ІБ для оцінки ситуації

Індикатор ризику комплексної атаки – це певні події ІБ (показники розвитку ситуації), поява яких вказує, що може розвиватися ризикова ситуація.

На даний час в СМІБ одним з основних процесів є процес обробки інцидентів ІБ. Це достатньо складний процес, який показує як ситуацію в сфері ІБ в організації, так і якість СМІБ. Даний процес орієнтований, в першу чергу, на своєчасне реагування на інциденти ІБ, їх виявлення, реалізацію заходів на вирішення проблеми, яка виникла, розумінню причин виникнення інцидентів. Тому інциденти ІБ є індикаторами ризиків ІБ.

Але є кілька проблем використання в якості індикаторів ризику комплексної атаки тільки інформацію о інцидентах ІБ.

При розробці політики обробки інцидентів ІБ дуже важливим етапом є визначення в організації переліку інцидентів ІБ з сукупності подій ІБ. Не кожна подія ІБ є інцидентом ІБ. В рекомендаціях щодо побудови СМІБ спеціалістами ІБ акцентується увага, що помилкове включення в перелік інцидентів ІБ подій, які такими не є, приводить к перевитраті ресурсів групи обробки інцидентів (людських, часових, матеріальних) та знижує ефективність її роботи. Це обумовлено тим, що термін «інцидент ІБ» вимагає реалізації певних, прописаних в політиці, дій групи обробки інцидентів. Тому в перелік інцидентів ІБ в організації будуть, як правило, включаться ті події ІБ, які по розумінню представників організації є реальною загрозою та чітко фіксуються.

При цьому може виникнути ситуація, при якій проявляється індикатор ризику, але інцидентом для організації він не буде. Наприклад, поява негативних публікацій у ЗМІ та К про організацію, різних чуток, різного роду мітингів, акції протесту проти організації тощо, або специфічна кібератака на комп'ютерну мережу організації, яка не подолала системи захисту (як правило, це буде подією ІБ, а не інцидентом ІБ).

Також можна відмітити, що існує багато таких типів інформаційних атак, які фактично не виявляються технічними засобами. Про факт реалізації такої атаки можна здогадатися за неявними ознаками. Наприклад, про перехоплення зловмисником інформації через ПЕМВН за допомогою пасивних засобів радіоперехоплення, можна здогадатися через розміщення в зоні 2 навколо комп'ютерів організації невстановленого транспортного засобу в часи їх роботи (особливо в часи початку роботи, коли вводиться логін та пароль). Натяк на подібну ситуацію описаний в [4]. При цьому без фізичного догляду цього транспортного засобу чітко встановити факт перехоплення інформації неможливо. Наявність такої ситуації не буде відноситися до інциденту ІБ, але до індикатору ризику її віднести можна.

Таким чином індикатор ризику може сигналізувати про можливість виникнення ризикової ситуації, але при цьому інцидентом ІБ може і не бути. З іншого боку інцидент ІБ також не обов'язково сигналізує про наявність виникнення ризикової ситуації початку комплексної спрямованої атаки, так як інцидентами ІБ є і порушення ІБ внаслідок халатності персоналу, вихід з ладу технічних засобів та інше.

Порядок дій підрозділів з ІБ підприємства щодо захисту від комплексних атак повинен бути наступним:

1). Підбір профілів ризиків відповідно до діяльності організації.

Профіль ризику – сукупність відомостей про область ризику (процеси організації, які являють собою ризики, а також активи, що забезпечують функціонування цих процесів), рівень ризиків для цих активів та процесів, індикатори ризику, а також заходи щодо мінімізації ризику.

2). Оцінка ситуації і співвіднесення одержуваної інформації з індикаторами ризику в профілях ризику.

3). Визначення рівня сумарного ризику початку комплексної атаки згідно індикаторів ризиків, які виявлені системою захисту.

4). Прийняття рішення про наявність ризикової події.

Даний механізм пропонується використовувати в двох напрямках. Перший напрямок – виявлення сценарію комплексної атаки, другий – оцінки динаміки розвитку ситуації та її прогнозування.

Для виявлення сценарію комплексної атаки необхідно мати дані щодо множини можливих її сценаріїв $C_x = \{a_1, a_2, ..., a_X\}$.

Далі формується матриця (5), в якій для кожного сценарію визначається сукупність ризиків, які можуть проявитися при реалізації того чи іншого сценарію.

$$M_{\text{сценаріїв}} = \begin{array}{c|cccc} & R_1 & R_2 & \dots & R_Y \\ C_1 & \mu_1^1 & \mu_1^2 & \dots & \mu_1^Y \\ C_2 & \mu_2^1 & \mu_2^2 & \dots & \mu_2^Y \\ \dots & \dots & \dots & \dots & \dots \\ C_X & \mu_X^1 & \mu_X^2 & \dots & \mu_X^Y \end{array}, \quad (5)$$

де μ_x^y – ступінь можливості реалізації у-го ризику в х-му сценарії комплексної атаки, $x = \overline{1,X}$, $y = \overline{1,Y}$, $\mu_x^y = [0,1]$.

В умовах оцінки обстановки фіксуються індикатори ризику та розраховуються вагові коефіцієнти для кожного сценарію:

$$C_x = \sum_{y=1}^{Y} \mu_x^y \left(R_y^{\text{інд}} \right), \quad (6)$$

де $\mu_x^y \left(R_y^{\text{інд}} \right)$ – ступінь можливості реалізації у-го ризику, підтвердженого індикаторами, в х-му сценарії КА.

Ступінь реалізації х-го сценарію КА знаходиться з виразу (7):

$$G_x = \frac{C_x}{C_{x_{max}}}, \quad (7)$$

де $C_{x_{max}} = \sum_{y=1}^{Y} \mu_x^y(R_y)$, $\mu_x^y(R_y)$ – ступінь можливості реалізації у-го ризику, що прогнозується, в х-му сценарії КА.

Для оцінки поточної ситуації з інформаційною безпекою в організації пропонується використовувати інформацію про динаміку реалізації ризику через оцінку індикаторів ризику, за рівні проміжки часу відповідно до формули (8).

$$R_\Sigma^{\text{інд}}(t) = \sum_{y=1}^{Y} R_y^{\text{інд}}(t), \quad (8)$$

де $R_y^{\text{інд}}(t)$ – *у*-й ризик, який підтверджений індикаторами ризику к заданому моменту часу t;

$R_\Sigma^{\text{інд}}(t)$ – сумарний ризик порушення ІБ для організації, який підтверджується індикаторами ризиків к заданому моменту часу t. Таку оцінку можна здійснювати як по кожному сценарію комплексної атаки, так і відповідно до загального ризику для організації.

Для прогнозування рівня сумарного ризику $R_\Sigma^{\text{інд}}(t)$ в наступні періоди часу при допущенні, що динаміка зміни даного параметру має приблизно лінійний характер, можна використовувати лінійну функцію:

$$R_\Sigma^{\text{інд}}(t) = a + b \cdot t, \quad (9)$$

де $R_\Sigma^{\text{інд}}(t)$ – значення досліджуваного параметру (сумарного ризику комплексної атаки, який проявився через індикатори ризику) на t-му моменті часу;

t – порядковий номер моменту часу з початку оцінки ситуації;

a та b – коефіцієнти регресії прогнозної моделі.

Для знаходження коефіцієнтів регресії a та b використовуються формули (9) та (10) (отримані на основі наявних статистичних даних методом найменших квадратів):

$$b = \frac{n\sum_{i=1}^{n} t_i R_{\Sigma i}^{\text{інд}} - \sum_{i=1}^{n} t_i \sum_{i=1}^{n} R_{\Sigma i}^{\text{інд}}}{n\sum_{i=1}^{n} t_i^2 - \left(\sum_{i=1}^{n} t_i \right)^2}; \quad (10)$$

$$a = \frac{1}{n}\left(\sum_{i=1}^{n} R_{\Sigma i}^{\text{інд}} - b\sum_{i=1}^{n} t_i \right), \quad (11)$$

де n – кількість спостережень,

i – порядковий номер спостереження.

Для обчислення розрахункових (згладжених) та прогнозних значень в отримане рівняння тренду слід підставити порядковий номер прогнозного моменту часу, починаючи з першого моменту часу базисного періоду.

Наведемо приклад розрахунків. Наприклад, аналіз індикаторів ризиків виявив такі дані в перші 4 години спостереження (табл. 1).

Таблиця 1

Приклад розрахунку прогнозу розвитку ризику комплексної атаки

Часові інтервали	1-а година	2-а година	3-а година	4-а година
Кількість індикаторів ризиків, які були виявлені	2	2	3	4
Значення ризиків, які відповідають виявленим індикаторам ризиків	$R_1^{\text{інд}} = 0,$ $R_2^{\text{інд}} = 0,$	$R_1^{\text{інд}} = 0,$ $R_2^{\text{інд}} = 0,$	$R_1^{\text{інд}} = 0,$ $R_2^{\text{інд}} = 0,$ $R_3^{\text{інд}} = 0,$	$R_1^{\text{інд}} = 0,$ $R_2^{\text{інд}} = 0,$ $R_3^{\text{інд}} = 0,$ $R_4^{\text{інд}} = 0,$
Сумарний ризик, який відповідає виявленим індикаторам ризиків	$R_{\Sigma\,1}^{\text{інд}} = 0$	$R_{\Sigma\,2}^{\text{інд}} = 0$	$R_{\Sigma\,3}^{\text{інд}} = 0$	$R_{\Sigma\,4}^{\text{інд}} = 1$

Результати прогнозу ризику КА на 5 годину $R_{\Sigma\,5}^{\text{інд}} = 1,4$. Тобто видно, що ситуація для організа-

ції погіршується, що вимагає негайної реакції системи менеджменту інформаційної безпеки.

Висновки

Таким чином, даних підхід використання теорії ризиків ІБ і індикаторів ризиків дозволяє проводити оцінку ситуації з інформаційною безпекою в організації, виявляти сценарій комплексної атаки, аналізувати динаміку реалізації комплексної атаки. Подальші дослідження будуть присвячені побудові методики реалізації запропонованого підходу для забезпечення інформаційної безпеки складних організаційно-технічних систем.

Список літератури

1. Додонов А.Г. Живучесть информационных систем / А.Г. Додонов, Д.В. Ландэ. – К.: Наук. думка, 2011. – 256 с.

2. Міжнародний стандарт ISO/IEC 27001-2013. Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги. – ISO, 2013. – 38 с.

3. Курбанлы У.К. Оценивание профилей риска и индикаторов риска с использованием матрицы подозрительных свіязей / У.К. Курбанлы // Телекоммуникации. – 2014. – № 7. – С. 39-42.

4. Костогрызов А.И. Прогнозирование рисков для обеспечения эффективности систем информационной безопасности в их жизненном цикле / А.И. Костогрызов, В.М. Лазарев, А.Е. Любимов // Правовая інформатика. – 2013. – № 4. – С. 4-14.

5. Шабуров А.С. Моделирование оценки угроз безопасности информационных систем персональных данных / А.С. Шабуров, С.А. Юшкова, А.В. Бодерко // Электротехника, информационные технологии, системы управления. – 2013. – № 7. – С. 149-159.

6. Заркумова-Райхель Р.Н. Прогнозирование количества инцидентов в системе информационной безопасности предприятия при помощи динамической модели / Р.Н. Заркумова-Райхель, А.Ж. Абденов // Фундаментальные исследования. – 2012. – № 6 (часть 2). [Електронний ресурс] – Режим доступу до ресурсу: https://www.fundamental-research.ru/ru/article/view?id=30007.

7. Мінфін поскаржився на "підозрілий фургон" біля будівлі відомства [Електронний ресурс] // ТСН. Офіційний веб-сайт. – 15.05.2017. – Режим доступу до ресурсу: https://tsn.ua/ukrayina/minfin-poskarzhivsya-na-pidozriliy-furgon-bilya-budivli-vidomstva-929608.html.

Надійшла до редколегії 18.05.2017

Рецензент: д-р техн. наук проф. В.В. Бараннік, Харківський національний університет Повітряних Сил, Харків.

ПОДХОД К ПРОГНОЗИРОВАНИЮ И ОЦЕНКЕ СИТУАЦИИ ПРИ КОМПЛЕКСНОЙ ИНФОРМАЦИОННОЙ АТАКЕ НА ОРГАНИЗАЦИЮ С ИСПОЛЬЗОВАНИЕМ ИНДИКАТОРОВ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Снігуров, В.Ю. Балашов, А.Ю. Нестеренко

В статье представлен подход к прогнозированию и оценке ситуации при комплексной информационной атаке на организацию. Для решения данной задачи предлагается использовать теорию рисков информационной безопасности и индикаторы реализации данных рисков. Данный подход предлагается для использования при создании систем менеджмента информационной безопасности организаций (предприятий).

Ключевые слова: *комплексная информационная атака, риски информационной безопасности, индикаторы рисков.*

AN APPROACHT OF ORECASTING AND AS SESSING A SITUATION UNDER COMPLEX IN FORMATION ATTACK ON AN ORGANIZATION USING RISK INDICATORS OF INFORMATION SECURITY

A. Snigurov, V. Balashov, O. Nesterenko

The paper presents an approach to forecasting and assessing the situation with a complex information attack on an organization. To solve this problem, it is proposed to use the theory of information security risks and indicators of realization of these risks. This approach is proposed for implementation when creating management systems of information security in organizations (enterprises).

Keywords: *complex information attack, risk of information security, risk indicators.*