MATHEMATICS

Методика визначення ймовірності негласного отримання інформації потенційним порушником

О. А. Лаптєв

Державний Університет телекомуникацій, м.Київ,Україна
Corresponding author. E-mail: alaptev64@ukr.net

Paper received 30.05.19; Accepted for publication 16.06.19.

https://doi.org/10.31174/SEND-NT2019-200VII24-06

Анотація. У статті розглядається математичне моделювання ймовірності негласного отримання інформації потенційним порушника яке зводиться до моделювання впливу порушника на захищаєму систему з цілю отримання можливого каналу витоку інформації і являє собою формалізований опис сценаріїв у вигляді логіко-алгоритмічної послідовності дій порушників, кількісних значень, що характеризують результати дій і функціональних (аналітичних, чисельних або алгоритмічних) залежностей, що описують протікають процеси взаємодії порушників з елементами захіщаемого об'єкта. Однак подібні підходи до моделювання не дозволяють кількісно оцінити актуальність загрози атак та врахувати цю найважливішу характеристику. Тому запропоновано варіант кількісної оцінки можливості несанкціонованого отримання інформації з окремій інформаційної системи, розроблена універсальна методика. Універсальність цієй методиці дозволяє порівнювати між собою складності реалізації різнорідних атак, заснованих на різних принципах реалізації, в загальному випадку використовують абсолютно різні за своєю природою канали витоку інформації. На основі запропонованій методиці розроблен підхід по математичному моделюванню ймовірності отримання порушником несанкціонованого доступу до інформації вже на першому підготовчому етапе комплексної перевірки, що в подальшому дозволить реально оцінити фінансові, оперативні і технічні засоби захисту інформації.

Ключові слова: *захист інформації, математичне моделювання, методика визначення ймовірності, засоби негласного отримання інформації.*

Вступ. Захист інформації-досить дороге заняття, що потребує не тільки разових, а й постійних витрат. Тому захищати необхідно тільки ту інформацію, витік якої може привести до економічного, морального або іншого збитку підприємству, організації, її керівництву. Необхідно розуміти не тільки, що и навіщо треба захищати, а й наскільки слід захистити конкретний вид охоронюваних відомостей. Це дозволити диференціювати заходи забезпечення безпеки інформації та скоротіти тім самим витрати на їх проведення. Зарубіжній и вітчизняний досвід проведення робіт з виявлення засобів негласного отримання інформації (далі по тексту НОІ) показує, що дії по підготовці и проведенню комплексних спеціальних перевірок приміщень доцільно умовно розділити на три етапи: підготовчій, етап безпосередньо проведення спеціальної перевірки приміщень та заключний етап. Найважливіше місце серед робіт підготовчого етапу комплексної спеціальної перевірки приміщень займає виявлення або уточнення ймовірного противника, який здійснює перехоплення інформації за допомогою засобів НОІ. Ризик НОІ інформації з інформаційній системи неможливо оцінити без побудови моделі потенційного порушника безпеки вже на першому етапе робіт.

Короткий аналіз літературних даних та постановка проблеми Більшість відомих підходів до моделювання, що відрізняються тим, які параметри при моделюванні ними використовуються в якості вхідної інформації і які характеристики модельованої системи розраховуються і надходять на вихід моделі (Будуються моделі з використанням теорії ймовірностей, випадкових процесів, мереж Петрі, теорії автоматів, теорії графів, нечітких множин, теорії катастроф, ентропійного підходу і ін.), передбачає використання в якості найпростішого елемента безпеки загрозу атаки на інформаційну систему [1, 4-5].

Разом с тим у всіх зазначених джерелах математичне моделювання порушника зводиться до моделювання впливу порушника на захищаєму систему з цілю отримання можливого каналу витоку інформації і являє собою формалізований опис сценаріїв у вигляді логіко-алгоритмічної послідовності дій порушників, кількісних значень, що характеризують результати дій і функціональних (аналітичних, чисельних або алгоритмічних) залежностей, що описують протікають процеси взаємодії порушників з елементами захіщаемого об'єкта . Однак подібні підходи до моделювання не дозволяють кількісно оцінити актуальність загрози атак та врахувати цю найважливішу характеристику. Тому потрібно запропонован варіант кількісної оцінки можливості несанкціонованого знімання інформації інформаційної системи замовника.

Мета. Розробка варіанту кількісної оцінки ймовірній можливості несанкціонованого отримання інформації з інформаційної системи замовника.

Виклад основного матеріалу. Математична модель потенційного порушника повинна враховувати зацікавленість зловмисника в реалізації атаки на конкретну інформаційну систему з метою отримання інформації або порушення її цілісності тобто враховуєтеся потенційна можливість НОІ.

Відзначимо, що побудова моделі порушника є ключовим питанням не тільки при визначенні можливих каналів НОІ але і характеристик безпеки інформаційних систем в цілому.

В даний час моделі потенційного порушника безпеки формуються як набір припущень про можливого

порушника безпеки, його кваліфікації, технічних і матеріальних можливостях і т.п. При цьому будується неформальна модель порушника, що відображає причини і мотиви дій, апріорні знання, переслідувані цілі, їх пріоритетність для порушника, основні шляхи досягнення поставлених цілей: способи реалізації вихідних від нього загроз, місце і характер дії, можлива тактика і т.п. В кінцевому рахунку подібна модель використовується з метою виявлення сукупності актуальних атак для конкретної інформаційної системи, для якої планується робота по виявленню і блокування засобів негласного отримання інформації, саме актуальних, оскільки потенційно можливі каналі витоку визначаються можливістю їх технічної реалізації (архітектура, використовувані програмні і апаратні засоби і т.п.). Модель порушника повинна враховувати досить багато факторів, не всі з яких піддаються формалізованому опису. Це, перш за все, рівень зацікавленості в отриманні несанкціонованого доступу до конкретної інформації, це рівень кваліфікації порушника, що дозволяє йому здійснити ту чи іншу атаку, його інформованість про виявлення й усунення різному роду вразливостей, наявність відповідних інструментальних засобів для здійснення атаки, інформованість про реалізовану в конкретній інформаційній системі технологію (можливість отримання подібної інформації), в тому числі технологіях захисту інформації, програмному забезпеченні, регламенти та інше. Складність обліку всіх цих (отже важко формалізованих) чинників обумовлюється не тільки їх кількістю і різноманітністю, але і складністю формалізації будь-яких залежностей між ними (наприклад, порушник може найняти висококваліфікованого фахівця для здійснення атаки, може придбати відповідні автоматизовані засоби здійснення атаки - реалізувати складну атаку, не володіючи при цьому належну кваліфікацію, і т.п.). Разом з тим, нам необхідна якась інтегральна оцінка, причому кількісна, що дозволяє врахувати всі ці фактори, інакше неможливо приступити до робіт по перевірці приміщень на наявність засобів негласного отримання інформації для конкретної інформаційної системи. [1]

Вкрай важливим є і наступний момент порушник зацікавлений в отриманні конкретної інформації, оскільки саме до оброблюваної інформації зловмисником і здійснюється несанкціонований доступ. Для цього введемо поняття подібної інформаційної системи, під якою будемо розуміти систему, обробну подібну (зміст, обсяг), в ідеалі для проектування аналогічну інформацію.

Виходячи з того, що порушник інформаційної системи може бути охарактеризований складністю реалізованих їм атак на інформаційну систему, визначим, як кількісно оцінити складність атаки, введемо кількісну міру складності атаки, оскільки в загальному випадку слід говорити про те, чи готовий (зацікавлений і може) порушник реалізувати атаку певної складності. При цьому, як відзначали, і можливі каналі витоку інформації , і власне реально використанні каналі по своїй суті різнорідні, кількісна ж міра повинна бути єдиною.

Звернемося до основ теорії інформації, розуміючи, що для успішного здійснення НОІ (атаки) щодо окремо взятого каналу витоку інформації порушник повинен володіти відповідною інформацією щодо можливості НОІ – інформацію про те, що така вразливість їм виявлена і не вирішено власником інформації, тобто певної кількістю інформації щодо загрози НОІ інформації.

Оскільки нас цікавить виключно ймовірність того, що канал отримання інформації присутній в інформаційній системі– загроза атаки реальна, при цьому можливі два результату події: канал для отримання інформації присутнє або ні, тобто кількість інформації щодо вразливості в даному випадку слід розглядати як імовірнісну міру. У нашому випадку невизначеність можна розглядати стосовно будь-якої можливості отримання інформації, яка може використовуватися порушником при здійсненні атаки, ймовірність присутності якої в системі визначається як $1 - P$оа (де Pоа ймовірності перекриття каналу отримання інформації) [2]

Порушник для здійснення успішної атаки повинен володіти відповідною інформацією щодо присутності каналів витоку інформації в загальній інформаційній системі власника інформації, тобто отримати дані, що зменшують невизначеність у відношенні даного каналу отримання інформації. Очевидно, що чим вище загрози отримання інформації значення Pоа ймовірності перекриття каналу отримання інформації, тим складніше порушнику здійснити відповідну атаку. З урахуванням сказаного складність реалізації атаки (позначимо її Sa) може інтерпретуватися як імовірна міра кількості інформації $I(P$оа), якими повинен володіти зловмисник для реалізації НОІ по виявленому каналу, яка може бути визначена наступним чином [2]:

Sа $= I(P$оа$) = -\log_2(1 - Poa)$

Коректність використання даної методики для оцінки реалізації знімання інформації по виявленому каналу обґрунтовується використанням логарифмічної функції (у нашому випадку за основою 2, оскільки у події можливі два результату), що дозволяє відповідним чином врахувати не лінійність функції зміни складності реалізації порушником знімання інформації від зміни значення ймовірності Pоа: Sа$=f(P$оа$)$

Проілюструємо сказане прикладом, для чого порівняємо складності реалізації двох можливих каналів знімання інформації , нехай для одного з них (припустимо з виброакустичному каналу) значення характеристики Pоа становить 0,7, а для іншого (електромагнітного випромінювання) – 0,99. Бачимо, що в першому випадку Sа1=1,74, у другому випадку Sа2 =6,64, тобто реалізація знімання інформації по другому каналу для порушника в 3,82 рази складніше, ніж реалізація можливості знімання інформації по першому каналу (тобто йому знадобиться в 3,82 рази більше кількості інформації про можливий канал знімання інформації) з метою зняття невизначеності щодо наявності в системі цього каналу.

Одиниця складності реалізації загрози уразливості Sа $= I(P$оа$) = 1$ задається умовою Pоа $= 0{,}5$, що визначає те, що канал знімання інформації з рівною ймовірністю присутня в інформаційній системі власника чи ні.

Оскільки загрозу атаки створює відповідна сукупність виявлених і не усунутих в системі каналів витоку інформації, складність атаки для порушника в загальному випадку визначається сукупною складністю атак через кожен розкритий можливий канал знімання інформації. Якщо розглянути атаку як послідовність ви-

користання порушником виявлених і не усунутих в системі каналів знімання інформації , що мають характеристики $Poar$ і Sar, r=1,...,R, можна ввести кількісну характеристику складності атаки $I(P$оа) (позначимо її Sа), де Sа= $I(P$оа), яка визначається кількістю інформації, якою повинен володіти порушник для здійснення успішної атаки, якої створюють загрозу каналу отримання інформації R виявлених в системі і не усунутих власником інформації (з урахуванням того, що події виникнення каналів несанкціонованого отримання інформації є незалежними, а умовою реалізації порушником безпосереднього отримання інформації є наявність в системі одночасно різноманітних каналів витоку інформації:

$Sa= I(Poa) = -\log_2(1 - Poa) = -\log_2 \prod_{r=1}^{R}(1 - Poar)$

де Pоа =1-$\prod_{r=1}^{R}(1 - Poar)$,– ймовірність того, що в будь-який момент часу можливе отримання інформації.

Використовуючи ж відповідне властивість логарифмів, можемо записати:

$Sa = I(Poa) = \sum_{r=1}^{R} I(Poar) = \sum_{r=1}^{R} Sar$

При цьому інформація, яку одержав порушник використовуючи канал знімання інформації, розглядається з точки зору її корисності (цінності) для досягнення поставленої практичної мети – в нашому випадку для здійснення порушником успішного знімання інформації з інформаційної системи власника.

Використання в інформаційній системі системи захисту збільшує значення складності реалізації відповідної атаки на інформаційну систему на величину захисту інформації.

Зазначимо, що характеристика ΔSa може розглядатися в якості так званої теорії інформації прагматичної міри кількості інформації, визначається в даному

випадку за формулою:

$\Delta Sa=\log_2(1 - Poaicx) - \log_2(1 - Poazax) = \log_2 \frac{(1-Poaicx)}{(1-Poazax)})$

де Poaicx і Pоазах – імовірності готовності до безпечної експлуатації ісходної і захищеної (при використанні системи захисту) інформаційних систем.

Універсальність даної методики обумовлюється тим, що вона дозволяє порівнювати між собою складності реалізації різнорідних атак, заснованих на різних принципах реалізації.

Для подальшої побудови моделі порушника введемо поняття коефіцієнта готовності порушника здійснити НОІ - Кга .

Коефіцієнт готовності порушника здійснити атаку Kга потрібно визначати стосовно до конкретної інформаційної системи, до конкретних каналах витоку інформації з інформаційної системи і системи її захисту. На практиці при вирішенні задачі захисту інформації може розглядатися якась подібна інформаційна система (аналог), що характеризується обробкою аналогічної інформації, що і визначає зацікавленість і можливості порушника. Щодо аналога, як правило, існує відповідна статистика реалізованих (у тому числі і відбитих) на інформаційну систему атак в процесі її експлуатації.

З урахуванням сказаного математична модель порушника (інтегральна кількісна оцінка зацікавленості та можливості реалізації зловмисником для атаки на конкретну інформаційну систему) може бути представлена наступним чином[3]:

Saн = max$\{Sanm, m = 1, \dots, M\}$,

де Saн – максимальна складність реалізованих (з урахуванням і відбитих) в подібній інформаційній системі атак, які характеризуються Poaн, визначена на множині виявлених каналів витоку інформації з подібної інформаційної системи (аналог) в процесі її експлуатації $Sanm, m = 1, \dots, M$.

Маючи значення характеристики Sа – характеристика складності реалізації варіанту знімання інформації з інформаційної системи, і значення характеристики Saн– характеристика максимальної складності реалізованих в подібній інформаційній системі атак, можна визначити шукану

характеристику коефіцієнта готовності (або ймовірності) порушника здійснити атаку складності Sа на конкретну інформаційну систему Kга:

$K\text{га}=\begin{cases} \text{Say}/\text{Sa}, \text{якщо Sан} < \text{Sa} \\ 1, \text{якщо Sан} \geq \text{Sa} \end{cases}$

Виходячи ж з того, що

$K\text{га} = \frac{\text{Sан}}{\text{Sa}} = \frac{\log_2(1-\text{Poап})}{\log_2(1-\text{Poa})} = \log_{1-\text{Poa}}(1 - \text{Poап})$

КоефіцієнтKга може інтерпретуватися як значення ступеня, у яку треба звести значення імовірності здійснення атаки на інформаційну систему $(1 - Poa)$, для отримання значення ймовірності атаки, яку може успішно реалізувати порушник$(1 - Poa$п).

Як бачимо, для розрахунку значень шуканої характеристики не потрібно використання будь-яких експертних оцінок. При розглянутому підході до моделювання використовуються тільки стохастичні параметри загроз, вразливості і статистика щодо безпеки експлуатації аналогічних систем для конкретної інформаційної системи. З використанням введеного коефіцієнта готовності зловмисника здійснити успішну атаку складності Sа на інформаційну систему Кга (порушник готовий здійснити подібну атаку – характеристика порушника), яка може розглядатися як ймовірність реалізації порушником успішної атаки за умови неможливості інформаційної системи до захисту інформації по відношенню до даної атаки, що визначається умовою Poa=0, з урахуванням того, що інформаційна система готова до захисту щодо атаки задається характеристикою Poa (характеристика безпеки щодо несанкціонованого отримання інформації), формула для розрахунку ймовірності реалізації в будь-який момент часу успішної атаки на інформаційну системуPa має наступний вигляд:

Pa = Кга $\prod_{r=1}^{R}(1 - Poar)$

Ймовірність того, що успішна атака не буде здійснена на інформаційну систему, що визначається як Pоа:

Pоа = 1 − Кга$\prod_{r=1}^{R}(1 - Poar)$

Запропонована методика дозволяє вже на першому етапі провести ймовірну оцінку негласного отримання інформації противником.

Висновки. Запропонована універсальна методика, методика яка має універсальність тому, що вона дозволяє порівнювати між собою складності реалізації різнорідних атак, заснованих на різних принципах реалі-

зації, в загальному випадку використовують абсолютно різні за своєю природою канали витоку інформації. На основі запропонований методиці розроблен підхід по моделюванню ймовірності отримання порушником несанкціонованого доступу до інформації вже на першому підготовчому етапі комплексної перевірки, що в подальшому дозволить реально оцінити фінансові, оперативні і технічні засоби захисту інформації.

ЛІТЕРАТУРА

1. Белов Е.Б. Основы информационной безопасности/ Белов Е.Б, Лось В.П., Мещеряков Р.В., Шелупанов А.А-М.:Горячая линия - Телеком, 2006.-544с.
2. Вентцель Е.С. Исследование операций. - М.: Советское радио, 1972.-552с.
3. Щеглов К.А., Математические модели експлуатационной информационной безопасности / Щеглов К.А., Щеглов А.Ю. // Вопросы защиты информации. - 2014. - Вып. 106. - № 3. - С. 52-65. 4.
4. Корт С.С. Теоретические основы защиты информации: Учебное пособие - М.: Гелиос АРВ, 2004.-240с.
5. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. - М.:Горячая линия - Телеком, 2004.-280с.

REFERENCES

1. Belov E. B. Fundamentals of Information Security / Belov E.B, Los V.P, Mecheryakov R.V., Shelupanov A.A.-M .: Hotline - Telecom, 2006.-544c.
2. Ventcel E.S. Operations research. - M .: Soviet Radio, 1972.-552s.
3. Shcheglov KA, Mathematical models of information security / Shcheglov KA, Shcheglov A.Yu. // Information security issues. - 2014. - Vol. 106. - № 3. - p. 52-65. four.
4. Cort S.S. Theoretical foundations of information security: Tutorial - M .: Helios ARV, 2004.-240s.
5. Malyuk A. A. Information security: conceptual and methodological foundations of information security. - M.: Hotline - Telecom, 2004.-280s.

Methodology for determining the probability of secret information received by the potential violator

A. A. Laptev

Abstract In the article, the mathematical modeling of the probability of the tacit reception of information of a potential violator is reduced to the simulation of the influence of the offender on the protection system with the purpose of obtaining a possible channel of information leakage and is a formalized description of the scenarios in the form of a logic-algorithmic sequence of offending actions, quantitative values characterizing the results of actions and functional (analytical, numerical or algorithmic) dependencies describing the processes of interaction of violators from an element we are protecting the object. However, similar approaches to modeling do not allow to quantify the relevance of the threat of attacks and take into account this critical characteristic. Therefore, a variant of quantitative assessment of the possibility of unauthorized access to information from a separate information system is proposed, a universal methodology has been developed. The versatility of this technique allows one to compare the complexity of the implementation of heterogeneous attacks, based on different principles of implementation, in the general case, using completely different channels of information leakage by nature. On the basis of the pre-defined methodology, an approach to mathematical modeling of the probability of an offender of unauthorized access to information is developed at the first preparatory stage of the complex verification, which in the future will allow to really assess the financial, operational and technical means of information protection.

Keywords: *information protection, mathematical modeling, probabilistic methods, tacit means of obtaining information.*