УДК 004.02
В. В. ГЛОВАЦЬКИЙ,
Національний авіаційний університет, Київ

МЕТОДИ ОЦІНЮВАННЯ СТАНУ БЕЗПЕКИ ТА ЗАГРОЗ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Досліджено методи оцінювання стану безпеки та загроз щодо інформаційних ресурсів. Досліджено традиційні підходи до аналізу стану безпеки інформаційних ресурсів за допомогою кількісних і якісних методів. Виявлено переваги та недоліки зазначених методів. Подано рекомендації стосовно розробки алгоритму оцінювання стану безпеки інформації.

Ключові слова: інформаційна безпека; загрози; захист інформації; інформаційна система; ризики щодо безпеки; методи аналізу.

Вступ

Будь-яка сучасна організація незалежно від виду діяльності та форми власності не в змозі успішно розвиватися й вести господарську або управлінську діяльність без створення належних умов для надійного функціонування системи захисту власної інформації.

Відсутність у багатьох керівників установ чіткого уявлення з питань захисту інформації призводить до того, що їм складно повною мірою усвідомити потребу створення надійної системи захисту інформації на очолюваному ним підприємстві, а тим більше — визначити конкретні дії, необхідні для оцінювання та захисту тих чи інших конфіденційних відомостей. Загалом кажучи, управлінці вдаються до створення охоронних служб, повністю ігноруючи при цьому питання інформаційної безпеки.

Паралельно з розвитком засобів обчислювальної техніки та появою нових способів порушення безпеки інформації розвивалися й удосконалювалися засоби оцінювання стану безпеки. Варто зазначити, що колишні види атак нікуди не зникають, а нові тільки ускладнюють ситуацію. Утім сучасні підходи до оцінювання стану безпеки інформаційних ресурсів усе ж відмінні від тих, що застосовувалися на перших порах. Головна особливість новітніх концепцій полягає в тому, що сьогодні не йдеться про один універсальний засіб захисту, а формуються цілі системи на базі сучасних методів виявлення загроз.

Аналіз досліджень і публікацій

Аналіз стану безпеки інформації та відповідних загроз стає дедалі важливішим компонентом організаційних операцій.

Інформаційна безпека — порівняно молода галузь інформаційних технологій, що швидко розвивається. Словосполучення «інформаційна безпека» в різних контекстах може набувати різного змісту. Під інформаційною безпекою розуміють захищеність інформації та підтримувальної інфраструктури від випадкових або навмисних впливів природного чи штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації та відповідної інфраструктури.

Що ж до ***захисту інформації***, то це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Вочевидь, для розв'язання проблеми оцінювання безпеки інформаційних ресурсів необхідно дослідити загальні принципи побудови інформаційних систем і мереж, зокрема й таких, що мають спеціальні засоби захисту. Це питання докладно розглянуто в [1], завдяки чому маємо змогу встановити ті параметри, які є сенс оцінювати щодо захищеності ресурсів. У [2] здійснено аналіз тенденцій забезпечення захищеності інформаційної безпеки для автоматизованих систем. Спираючись на дані, уміщені в зазначеній публікації, маємо всі підстави прогнозувати розробку відповідних методик оцінювання інформаційної безпеки. Процедури вибору та застосування програмних засобів для розробки й упровадження систем відповідних оцінок описано в [3]. У [4] відзначено деякі аспекти щодо створення системи оцінювання, які реалізовано в політиці запобігання загроз інформаційній безпеці в практичній діяльності.

Баскервіль [5] із середини 1980-х років здійснює фундаментальні дослідження в галузі аналізу загроз інформаційній безпеці. Він визначив контрольний список аналізу ризиків для інструментів, що використовуються з метою розробки заходів із забезпечення інформаційних систем. Хан [7] запропонував підхід до аналізу ризиків стосовно інформаційної безпеки, яка передбачає безперервність функціонування експлуатаційного середовища. Кілька методик спираються на такі види аналізу, як матричний підхід [6], парне порівняння тощо. Деякі дослідники розробили комплексні інструменти для оцінювання стану інформаційних ресурсів: **ISRAM** (*Information Security Risk Analysis Method*), **OCTAVE** (*The Operationally Criti-*

cal Threat, Asset, and Vulnerability Evaluation), **FRAP** (*Facilitated Risk Assessment Process*).

Наведені факти переконливо підтверджують актуальність проблеми забезпечення ефективного захисту інформації. При цьому постають завдання щодо визначення методів і засобів управління інформаційною безпекою та класифікації їх згідно з потребами користувача; огляду переваг і недоліків відомих методів та підходів, а також формування рекомендацій, спрямованих на оцінювання стану безпеки інформаційних ресурсів та відповідних загроз.

Методи оцінювання стану безпеки інформації

У XXI сторіччі інформаційні технології швидко проникли в усі сфери діяльності суспільства, і це спонукає до модернізації та формування інформаційної системи від базового (фізичного) рівня до верхнього (користувацького). Отже, людство ввійшло в нову еру — еру інформації.

Але зрештою розвиток інформаційних систем приніс не лише велику користь, а й гострі проблеми щодо загроз інформаційній безпеці. Віруси, хакерські атаки, витоки секретної інформації, відмови систем, переривання обслуговування і різні комп'ютерні злочини примножуються лавиноподібно. Згідно з дослідженнями Федерального бюро розслідувань США, економічні втрати, зумовлені неналежною мережною безпекою, щороку перевищують $ 170 млрд. За даними китайського інформаційного центру інтернет-мереж (CN CERT), у першій половині 2014 року CN CERT отримав 4780 звітів про інциденти з мережною безпекою. Отже, не дивно, що в 2015 році плата за послуги із забезпечення інформаційної безпеки в Китаї досягли 153 млрд юанів [8].

Зрештою проблеми безпеки інформаційних систем привертають пильну увагу фахівців різних сфер приватного і державного секторів. Вони застосовують різні засоби нагляду, спонукаючи агентства на всіх рівнях підвищувати поінформованість і активізувати заходи з оцінювання стану інформаційної безпеки, щоб уникнути величезних ризиків.

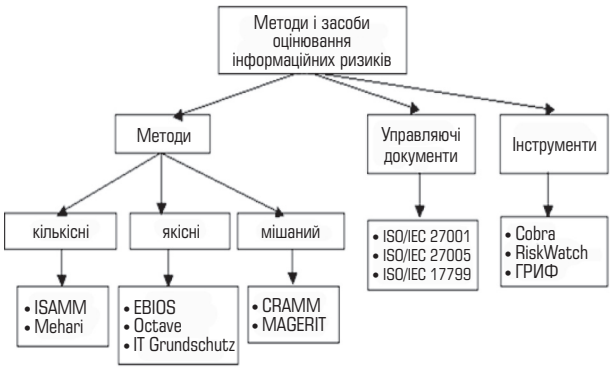
Говорячи про системи безпеки, потрібно наголосити, що вони повинні не тільки і не стільки обмежувати допуск користувачів до інформаційних ресурсів, скільки визначати і делегувати їхні повноваження у спільному розв'язанні завдань, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації та усувати їх наслідки, гнучко адаптуючи мережну структуру до виникнення відмов, часткової втрати або тривалого блокування ресурсів.

Не варто, однак, забувати про економічну доцільність застосування тих чи інших заходів забезпечення безпеки інформації, які завжди мають бути адекватні існуючим загрозам.

Надійність захисту інформації, насамперед, буде визначатися повнотою розв'язання цілого комплексу завдань. Іншими словами, на практиці захист інформації являє собою комплекс регулярно використовуваних засобів і методів, а також здійснюваних заходів із метою систематичного забезпечення необхідної надійності інформації, що генерується, зберігається й обробляється на об'єкті інформаційно-аналітичною системою та передається по каналах. Захист повинен мати системний характер, тобто для отримання найкращих результатів усі розрізнені види захисту інформації мають бути об'єднані в одне ціле й функціонувати в складі єдиної системи як злагоджений механізм, призначений для виконання завдань із забезпечення безпеки інформації. Він має містити:

- нормативно-правовий базис захисту інформації;
- засоби, способи і методи захисту;
- органи і виконавців.

Визначення інформаційних ризиків — складне завдання. Зазвичай відповідні питання розв'язуються за допомогою експертних методів, що вносять суб'єктивізм в оцінку ризику. Тому організація, спираючись на таку оцінку, може ухвалити хибне рішення інвестування в інформаційну безпеку. Помилково оцінені ризики можуть призвести до переоцінки або, що набагато гірше, недооцінки небезпеки. Ось чому вибір обґрунтованої моделі визначення інформаційних ризиків становить актуальну проблему. Методи та засоби оцінювання інформаційних ризиків у систематизованому вигляді подано на рисунку.



Методи і засоби оцінювання інформаційних ризиків

Метод розуміється як систематизована сукупність кроків, дій, що їх необхідно виконати, аби розв'язати певне завдання чи досягти поставленої мети. У даному разі дати оцінку ризиків. Тобто метод — це покрокова інструкція плюс інструмент (програмний продукт) для оцінювання ризиків.

Усі методи оцінювання ризиків можна поділити на *кількісні*, *якісні* або *мішані* (комбінація кількісних і якісних методів).

Кількісні методи використовують вимірні, об'єктивні дані для визначення числових значень

вартості активів, імовірності втрат і пов'язаних із ними ризиків.

Якісні методи використовують відносний показник ризику (низький, середній, високий) чи вартості активу на основі рейтингу або за шкалою від 1 до 10. Якісна модель оцінює дії та ймовірності виявлених ризиків у швидкий і економічно ефективний спосіб. Набори ризиків, сформовані й проаналізовані згідно з якісною оцінкою, можуть виступати основою для цілеспрямованої кількісної оцінки.

Донедавна кількісні підходи явно домінували. Проте останнім часом суто кількісне управління ризиками, пов'язане зазвичай із надзвичайно трудомісткою роботою, яка зрештою не дає відчутного виграшу, все більше поступається якісним методам оцінювання ризиків у сфері захисту інформації. Що ж до комбінації кількісних і якісних методів, то вона, вочевидь, поєднує в собі як переваги, так і недоліки обох груп методів.

Порівняльну характеристику кількісних і якісних методів наведено в таблиці.

Переваги і недоліки кількісних і якісних методів оцінювання ризиків у сфері захисту інформації

	Кількісні методи	Якісні методи
Переваги	• Дозволяють визначати наслідки виникнення інцидентів у кількісний спосіб. • Уможливлюють аналіз витрат і користі при виборі підходу до захисту. • Допомагають отримати достатньо точну картину ризикованої ситуації	• Дозволяють визначати сфери та осередки великої небезпеки в стислі терміни та без великих витрат. • Аналіз ризиків і переваг порівняно легкий і дешевий
Недоліки	• Кількісні оцінки неодмінно залежні від розміру та точності вибраної шкали вимірювання. • Результати аналізу можуть бути неточні, зокрема й через відсутність вірогідних даних про перебіг відповідних подій. • Остаточні висновки здебільшого мають спиратися на якісний опис. • Вимагають значно більших витрат, ніж якісні методи, найвищої кваліфікації виконавців і новітніх технічних засобів	• Непридатні для визначення ймовірностей результатів, здобутих чисельними засобами. • Аналіз переваг більш ускладнюється за рахунок вибору захисту. • Результати мають загальний характер, усі значення тільки наближені тощо

Завданням якісного оцінювання є визначення можливих видів ризиків та ступеня серйозності загроз, виокремлення чинників, які впливають на рівень загроз, обґрунтування різних можливих контрзаходів. Відповідні методики не надають жодних кількісних значень (зокрема у грошовому вираженні). Вони достатньо популярні й порівняно прості. В основу їх розробки покладено, як правило, вимоги міжнародного стандарту ISO 17799:2002.

Кількісне оцінювання уможливлює перехід від імовірнісної оцінки ризику до відповідного числового значення. Методики подають реальні й обґрунтовані числові значення всіх складових процесу аналізу ризиків. Цими складовими можуть бути вартість захисних заходів, цінність активу, збиток для бізнесу, частота виникнення загрози, ефективність захисних заходів, вірогідність використання уразливості і т. ін. Кількісний аналіз дозволяє обчислити конкретне значення (у відсотках) імовірності реалізації загрози.

Висновки

Пропоноване дослідження дає змогу оцінити (або здійснити переоцінку) поточного стану інформаційної безпеки організації чи установи, виробити рекомендації щодо гарантування або підвищення такої безпеки, знизити потенційні втрати завдяки досягненню більшої стійкості функціонування інформаційної мережі, розробити концепцію і політику безпеки, а також запропонувати плани захисту інформаційних ресурсів від умисного спотворення, знищення, несанкціонованого доступу, копіювання або використання.

Важливим кроком при побудові комплексної системи захисту інформації є вибір відповідних методів та інструментів. Зазвичай організації не знають, які з існуючих способів оцінювання ризиків кращі саме для їхніх умов. Тому процес оцінювання має бути адаптований до індивідуальних особливостей організації, але водночас узгоджений із найкращими стандартами та провідними практиками.

Окрім того, розкрито механізми контролю наявного стану захищеності інформаційних ресурсів і прогнозування можливих втрат у разі реалізації виявлених загроз.

Перспективи подальших досліджень у даному напрямку зумовлюються актуальністю і нагальністю порушеної проблематики. Передбачається модернізувати пропонований метод для використання його в конкретних видах діяльності, а також розробити методику оцінювання ефективності роботи із забезпечення інформаційної безпеки на основі управління інформаційними ризиками та висвітлити її на базі сучасних апаратних засобів аналізу.

Література

1. ***Казакова, Н. Ф.*** *Принципи побудови захищених інтелектуальних мереж / Н. Ф. Казакова // Вісник ДУІКТ.— К. : ДУІКТ.— 2009.— № 4.— С. 381–388.*

2. ***Казакова, Н. Ф.*** *Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем / О. О. Скопа, Н. Ф. Казакова // Системи обробки інформації.— Харків: ХУПС ім. І. Кожедуба.— 2009.— № 7(79).— С. 48–54.*

3. ***Ткачук, М. В.*** *Розробка методики комплексної оцінки ефективності впровадження систем управління IT-інфраструктурою організацій / М. В. Ткачук, В. Є. Сокол, О. В. Черкашенко // Вісник*

Національного технічного університету «ХПІ».— Харків: НТУ «ХПІ».— 2012.— № 30.— С. 94–104.

4. ***Ващенко, Н. В.*** *Створення ефективної системи управління оборотними активами підприємства на основі діагностичного інструментарію / Н. В. Ващенко, Ю. І. Максимович // Сталий розвиток економіки.— 2013.— № 3.— С. 260–265.*

5. ***Baskerville, R.*** *An analysis survey of information system security design methods: Implications for Information Systems Development / R. Baskerville // ACM Computing Survey, 1993.— P. 375–414.*

6. ***Goel, S.*** *Information security risk analysis — a matrix-based approach / S. Goel, V. Chen // University, SUNY, 2005.*

7. ***Suh, B.*** *The IS risk analysis based on business model / B. Suh, I. Han // Information and Management.— 2003.— No. 2.— P. 149–158.*

8. ***Tongwei, Yuan.*** *Data Mining Applications in E-Government / Yuan Tongwei, Chen Peng // Information Security.— 2012.— P. 7.*

Рецензент: доктор техн. наук, професор **О. Г. Корченко**, Національний авіаційний університет, Київ.

В. В. Гловацкий

МЕТОДЫ ОЦЕНКИ СОСТОЯНИЯ БЕЗОПАСНОСТИ И УГРОЗ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Исследованы методы оценки состояния безопасности и угроз информационных ресурсов. Охарактеризованы традиционные подходы к анализу состояния безопасности информационных ресурсов при помощи количественных и качественных методов анализа. Выявлены преимущества и недостатки количественных и качественных методов. Даны рекомендации по разработке алгоритма оценки состояния безопасности информации.

Ключевые слова: информационная безопасность; угрозы; защита информации; информационная система; риски безопасности; методы анализа.

V. V. Glovatskyi

METHODS OF ASSESSING INFORMATION RESOURCES SECURITY CONDITION AND THREATS

The article deals with information resources methods of assessing the state of security and threats. Researched traditional methods of information security analysis, namely quantitative and qualitative methods of analysis. Detected the advantages and disadvantages of quantitative and qualitative methods of analysis. Made recommendations for the developing algorithm for information security risks state assessment.

Keywords: information security; threats; information security; information system; security risks; methods of analysis.

УДК 004.715

Т. П. ДОВЖЕНКО, аспирант;
К. П. СТОРЧАК, канд. техн. наук, доцент,
Государственный университет телекоммуникаций, Киев

Математическая модель предсказания потерь пакетов для DSREM-алгоритма активного управления очередью в сети TCP/IP

Рассматривается вопрос о построении полного факторного эксперимента для получения предсказывающей модели по отброшенным и потерянным пакетам в сети TCP/IP. Применяется план 2^3 и рассчитываются критерии Стьюдента и Фишера. Определяется адекватность полученной модели.

Ключевые слова: TCP/IP-сеть; DSREM-алгоритм; полный факторный эксперимент; дисперсия адекватности.

Введение

Математико-статистические (стохастические) методы используются в следующих целях [1–3].

1. Оценка влияния факторов, по которым нельзя построить жестко детерминированную модель.

2. Изучение и сравнение влияния факторов, не подлежащих включению в одну и ту же детерминированную модель.

3. Выделение и оценка влияния сложных факторов, которые не могут быть выражены одним определенным количественным показателем.

Основной сферой приложения стохастических моделей является проблемно-ориентированный и тематический анализ.

Построение стохастических моделей предназначено для решения ряда указанных далее задач.

1. Установление наличия или отсутствия статистически значимой связи между изучаемыми признаками.

2. Прогнозирование неизвестных значений результативных показателей по заданным значениям факторных признаков — задачи экстраполяции (интерполяции).