Юдіна Л.Г.
аспірант
Національний авіаційний університет
6433061@stud.nau.edu.ua

ІНФОРМАЦІЙНА БЕЗПЕКА КОМП'ЮТЕРНОЇ СИСТЕМИ ТА МЕРЕЖІ ВІД ВНУТРІШНІХ ТА ЗОВНІШНІХ АТАК

Моделі надійності функціонування комп'ютерних мереж та систем розроблені давно і детально вивчені, а моделі безпеки тільки розробляються. Важливість та актуальність проблеми забезпечення інформаційної безпеки обумовлені тим, що сучасні рівні розвитку засобів інформаційної безпеки значно відстають від рівнів розвитку інформаційних технологій та розширення впровадження комп'ютерних та мережевих технологій у різноманітні сфери людської діяльності. Крім цього, стрімкий розвиток інформаційних технологій відкрив нові можливості для бізнесу, що призвело до появи нових загроз .

Моделі безпеки відіграють важливу роль у процесах розробки і дослідження захищених комп'ютерних систем (КС), вирішують такі задачі:

− вибір і обґрунтування базових принципів архітектури захищених КС, що визначають механізми реалізації засобів і методів захисту інформації;

− підтвердження властивостей захищених систем шляхом формального дотримання політики безпеки;

− складання формальної специфікації політики безпеки, як найважливішої складової частини організаційного та документаційного забезпечення розроблюваних захищених КС.

Основним призначенням КС є переробка (збір, збереження, обробка і передача) інформації, тому проблема забезпечення інформаційної безпеки є для КС центральною. Забезпечення безпеки припускає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування КС, а також спробам модифікації, розкрадання, виведення з ладу або руйнування її компонентів, тобто захист усіх компонентів КС – апаратних засобів, програмного забезпечення, даних і персоналу. Існують два підходи до проблеми забезпечення безпеки КС: фрагментарний і комплексний.

Фрагментарний підхід спрямований на протидію чітко визначеним погрозам у заданих умовах. Як приклади реалізації такого підходу можна вказати окремі засоби керування доступом, автономні засоби шифрування, спеціалізовані антивірусні програми. Перевагою такого підходу є висока вибірковість до конкретної погрози. Істотним недоліком даного підходу є відсутність єдиного захищеного середовища обробки інформації. Фрагментарні міри захисту інформації забезпечують захист конкретних об'єктів КС тільки від конкретної погрози. Навіть невелика видозміна погрози веде до втрати ефективності захисту.

Комплексний підхід орієнтований на створення захищеного середовища обробки інформації у КС, що поєднує в єдиний комплекс різнорідні міри протидії погрозам. Організація захищеного середовища обробки інформації дозволяє гарантувати визначений рівень безпеки КС, що є безсумнівною перевагою комплексного підходу. До недоліків цього підходу відносяться: обмеження на свободу дій користувачів КС, велика чутливість до помилок установки і настроювання засобів захисту, складність керування. Комплексний підхід застосовують для захисту великих організацій або невеликих КС, що виконують відповідальні задачі або обробляють особливо важливу інформацію. Порушення безпеки інформації в КС великих організацій може нанести величезний матеріальний збиток як самим організаціям, так і їх клієнтам. Тому такі організації змушені приділяти особливу увагу гарантіям

безпеки і реалізовувати комплексний захист. Комплексного підходу дотримують більшість державних і великих комерційних підприємств і установ. Цей підхід знайшов своє відображення в різних стандартах. Комплексний підхід до проблеми забезпечення безпеки заснований на розробленій для конкретної КС політиці безпеки.

Політика безпеки являє собою набір норм, правил і практичних рекомендацій, на яких будується керування, захист і розподіл інформації в КС. Політика безпеки регламентує ефективну роботу засобів захисту КС, вона охоплює всі особливості процесу обробки інформації, визначаючи поводження системи в різних ситуаціях.

Політика безпеки реалізується за допомогою адміністративно організаційних мір, фізичних і програмно-технічних засобів і визначає архітектуру системи захисту. Для конкретної організації політика безпеки повинна носити індивідуальний характер і залежати від конкретної технології обробки інформації і використовуваних програмних і технічних засобів. Політика безпеки визначається способом керування доступом, що визначає порядок доступу до об'єктів системи.

Основні загрози для комп'ютерних мереж та систем ґрунтуються в області конфіденційності, цілісності та доступності.

Відповідно до цього завдання інформаційної безпеки в комп'ютерних мережах полягають у:

- аутентифікації одного або декількох взаємодіючих об'єктів;
- контролі доступу та захисту від несанкціонованого використання ресурсів мережі;
- маскуванні інформаційного потоку у мережі;
- захисту від можливих відмов відправки змісту відправлених даних.

Більшість підходів до формування моделі безпеки лише частково відображають компоненти та процеси захисту інформації та інформаційних ресурсів і є односторонніми.

Тому, головне при формуванні моделі безпеки КС – це кваліфіковано визначити межі розумної безпеки і витрат на засоби захисту з одного боку і підтримки системи в працездатному стані і прийнятного ризику з іншого.

Передбачається, що модель безпеки в рамках комплексного підходу є функцією з множини області значень складових системи інформаційної безпеки. Тобто залежить від суб'єктів інформаційних процесів, завдань захисту інформації, загроз безпеки, рівнів вразливості комп'ютерних мереж та систем.

Умовами функціонування моделі є автономність, реагування та застосування мінімальних обчислювальних ресурсів.

Необхідність класифікації загроз інформаційній безпеці зумовлена тим, що архітектура сучасних засобів автоматизованої обробки, організаційна структурна та функціональна побудова мереж, технології та умови обробки такі, що інформація потрапляє під вплив надмірної кількості чинників, за якими і потрібно формалізувати задачу описання загроз та ефективної протидії їм.

Трансляція інформації в мережах телекомунікацій відбувається у вигляді інформаційних потоків, класифікація яких залежить від сприйняття їх оператором (текстові, графічні, відео та службові потоки: кодування архівація, стиснення) та характеризується внутрішньою структурою формату потоку. Елементарною структурною одиницею потоку є файл, який будується з однотонних даних.

Постійне зростання потреби в інформації обумовлює необхідність підвищення ефективності використання інформаційних ресурсів з інтеграцією різних підсистем забезпечення безпеки, підсистем зв'язку у єдину інтегральну систему з загальними технічними засобами та подальшого вдосконалення моделі інформаційної безпеки за рахунок вагових коефіцієнтів різних видів атак, і захищеності компонентів комп'ютерних мереж та систем від внутрішніх та зовнішніх атак.

Список використаних джерел

1. Нечипорук О. П., Кашкевич С. О., Голего Н. М. “Метод децентралізованого управління мережевими ресурсами інформаційно-комунікаційних мереж”. XIX Міжнародна науково-практична конференція “Innovative approaches to solving scientific problems”, 16 – 19 травня 2023, Токіо, Японія. С. 454 – 458. URL: https://isg-konf.com/uk/innovative-approaches-to-solving-scientific-problems/
2. Кучук Н. Г., Шишацький А. В., Нечипорук В. В., Шапошнікова О. П., Кашкевич С. О. “Розробка методу оцінки захищеності складних технічних систем з використанням штучних імунних систем”. XXVIII Міжнародна науково-практична конференція “Science and development of methods for solving modern problems”, 18 – 21 липня 2023, Мельбурн, Австралія. С. 202 – 209. URL: https://isg-konf.com/uk/science-and-development-of-methods-for-solving-modern-problems/
3. Шишацький А.В., Нечипорук В.В., Кашкевич С.О. Комплексні системи захисту інформаційних систем спеціального призначення. XXVIII Міжнародна науково-практична конференція «Science and development of methods for solving modern problems», 18-21 липня 2023 р., Мельбурн, Австралія. С. 214-222.

Науковий керівник: Нечипорук В.В., к.т.н., доцент.

Ярощук В. О.
студентка
Хмельницький університет управління та права
імені Леоніда Юзькова
yaroshchuk.vitalina@gmail.com

РИЗИКИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ НА РИНКУ МІЖНАРОДНИХ ФІНАНСОВИХ ПОСЛУГ

Впровадження технологій штучного інтелекту (ШІ) в різноманітні сфери господарської діяльності є не тільки об'єктом зацікавленості, але й предметом інтенсивних досліджень та обговорень у науковій спільноті. Одним із найбільш активно розвиваючихся секторів, де ШІ знаходить широке застосування, є фінансові міжнародні послуги. Ризики використання ШІ в цьому контексті стають предметом серйозного аналізу та уваги. Розвиток технологій ШІ у фінансових послугах створює безліч можливостей для оптимізації процесів, підвищення ефективності та зменшення витрат. Однак це також супроводжується значними ризиками, які варто ретельно розглядати та аналізувати. В цьому контексті, дослідження ризиків використання ШІ у фінансових міжнародних послугах є актуальним та важливим завданням, що сприяє як науковому розвитку, так і практичному застосуванню цих технологій.

Можна виділити такі ризики, що можуть виникати на ринку фінансових послуг у разі використання технологій штучного інтелекту:

- неправильне використання даних;
- дискримінація та упередженість;
- антиконкурентна поведінка;
- система управління у контексті розгляду автоматизованих інвестиційних послуг та щодо нагляду за алгоритмічною торгівлею на оптових ринках;