90/5a/91/24/1a/14/4b/40/STM32F7_Peripheral_DCMI/files/STM32F7_Peripheral_DCMI.pdf/jcr:content/translations/en.STM32F7_Peripheral_DCMI.pdf

5. Dogan Ibrahim. Camera Projects Book: 39 Experiments with Raspberry Pi and Arduino. Elektor International Media; Main edition. 2019. 254 p. ISBN: 978-1907920776.

Ключові слова: Мікроконтролери, відеоспостереження, Arduino, Raspberry Pi, машинне навчання.

Ключевые слова: Микроконтроллеры, видеонаблюдение, Arduino, Raspberry Pi, машинное обучение.

Keywords: Microcontrollers, CCTV, Arduino, Raspberry Pi, machine learning.

Чепурна Олена Євгенівна

Національний університет «Одеська юридична академія»,

доцент кафедри кібербезпеки, кандидат фіз. - мат. наук

Кулешова Євгенія Романівна

викладач математики і інформатики ЗОШ №15 м.Одеси

МЕТОДИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ В СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розвиток інформаційного суспільства диктує нові правила взаємодії між людьми, підприємствами, державними інституціями і світовими державами взагалі. Інтернет, який «видає», «поглинає» та обробляє великі об’єми інформації стає не тільки джерелом комфортного життя, але і найнебезпечніших загроз. Росте залежність від комп’ютерних технологій, додаток «Дія», наприклад, містить всю основну інформацію про людину: ID картка, ІПН, свідоцтво народження дитини, водійські права, документи підприємця та податкові декларації. Всі головні документи знаходяться в смартфоні, відомості

карткових рахунків і багато іншої особистої інформації. Великі маркетплейси і звичайні інтернет магазини при здійснені операцій використовують особисті дані. Захист інформації, в такому випадку, стає нагальною необхідністю. З точки зору кібербезпеки, ще більші загрози виникають при забезпеченні національної безпеки країни [1].

Тривалий час розуміння інформаційної безпеки в наукових та нормативно-правових джерелах ототожнювалося тільки з безпекою інформації, що значно звужувало її сутність. Саме тому, з низки питань, присвячених розгляду проблеми забезпечення інформаційної безпеки, найбільш вивченими та дослідженими її аспектами є безпека інформації (інформаційно-технічна безпека). Різні аспекти забезпечення інформаційної безпеки та вдосконалення управління нею досліджено у працях багатьох вітчизняних і зарубіжних учених, зокрема визначення змісту інформаційної безпеки, аналіз загроз та індикаторів інформаційної безпеки висвітлено в працях О.Ф. Бєлова, О.І. Барановського, М.А. Бендикова, М.М. Єрмошенка, Я.А. Жаліла, Т.Т. Ковальчука, Г.В. Козаченка, Н.О. Лоханова, О.М. Ляшенко, В.І. Мунтіяна, Є.А. Олейнікова, С.К. Реверчука та ін.[2].

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: «Кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі»[3].

Застосування методів математичного моделювання, наприклад, моделі часових рядів AR(P), MA(Q), ARIMA(P,D,Q), лінійний дискримінантний аналіз (LDA), алгоритми дискримінантного аналізу, квадратичний дискрімінатний аналіз, на наш погляд, корисно на етапі прогнозування та попередження реальних і потенційних загроз.

Крім описаних моделей, досвід показує, що в роботі щодо забезпечення інформаційної безпеки, можуть використовувати специфічні прийоми

моделювання та особливі різновиди моделей. Найбільш прийнятними тут є логіко-математичні та розумові моделі, так як їх створення і вивчення найбільш доцільно у випадках з незаконним доступом до службової інформації.

Кіберзагрози не існують окремо від особи, яка спричиняє такі протиправні дії. В частині моделювання дій порушника інформаційної безпеки потрібно проводити аналіз поведінки такої особи(або групи осіб) з точки зору виділення ним ресурсів на напад, визначити ймовірності виділення кількості ресурсів, додати аналіз існуючих моделей порушників, вивчати статистику нападів на інформаційні мережі та системи

Додатково, доцільно, також залучити методи імітаційного моделювання, і реалізувати їх, наприклад, за допомогою GPSS (з англ. General Purpose Simulation System – системи моделювання загального призначення), які застосовують для дослідження систем масового обслуговування, так звані випадкові Марковські процеси. З точки зору теорії Марковських процесів, відносно до загрози виникнення вразливості атаки (при усуненні вразливості зникає і загроза атаки), інформаційну систему можна розглядати як систему з відмовами та відновленням характеристик інформаційної безпеки.

На сьогоднішній день існує багато задач оптимізації складних систем, що не можуть бути вирішені за допомогою аналітичних моделей. У такому випадку, на наш погляд, потрібно здійснювати нейромережеве моделювання для прогнозування рівня інформаційної безпеки.

Ефективному розвитку систем інформаційної і кібербезпеки, сприяє багато факторів, серед яких можна виділити застосування методів математичного моделювання на різних етапах її реалізації.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України»: Указ Президента України. №447/2021, URL: https://www.president.gov.ua/documents/4472021-40013

2. Убийвовк І. І. Інформаційна безпека діяльності підприємств

Причорноморські економічні студії. 2016. №9. С. 2.

3. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Левченко Є. Г. , Рабчун А. О. Оптимізаційні задачі менеджменту інформаційної безпеки. *Сучасний захист інформації*. 2010. №1 (1), С. 16-24.

Ключові слова: математична модель, інформаційна безпека, часові ряди

Ключевые слова: математическая модель, информационная безопасность, временные ряды

Keywords: mathematical model, information security, time series

Янковський Олег Георгійович

Національний університет «Одеська юридична академія»,

доцент кафедри інформаційних технологій,

кандидат технічних наук, доцент

ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ FACE ID

Сучасний світ неможливо уявити без використання інформаційних технологій у найрізноманітніших сферах людської діяльності. Обсяг електронної інформації, що використовується, стрімко зростає з кожним днем. Значну частину цієї інформації складає особиста інформація і саме тому питання захисту конфіденційних даних не втрачає своєї актуальності.

Сучасні системи контролю доступу до власних інформаційних ресурсів досить різноманітні та використовують різні підходи. Процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора називається автентифікацією. З позицій інформаційної безпеки автентифікація є частиною процедури надання доступу для роботи в