Готовий прототип вебресурсу планується розмістити на платформі Heroku для доступу усім користувачам в мережі Інтернет. Дизайн вебресурсу містить патріотичні зображення, щоб його майбутнім користувачам було цікаво та незвично обмінюватися повідомленнями. У разі успішного запуску та підтримки серед суспільства – проект можна розвивати та покращувати.

Список використаних джерел:

1. Python official website. URL: https://www.python.org/
2. Django official website. URL: https://www.djangoproject.com/
3. SQLite. URL: https://sqlite.org/index.html
4. NordPass. Top 200 most common passwords. URL:https://nordpass.com/most-common-passwords-list/

Науковий керівник: доцент Ахмаметьєва Г.В.

ПОБУДОВА МОДЕЛІ СИСТЕМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кухаренко С. В.

кандидат технічних наук, доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

У тезах розглядається підхід до структуризації моделі системи забезпечення інформаційної безпеки, який може бути використаний під час моделювання систем захисту інформації.

При побудові сучасних систем забезпечення інформаційної безпеки виникає необхідність дослідження багатьох ситуацій з урахуванням впливу різних випадкових факторів. Тому виникає потреба створення комплексу математичних моделей систем інформаційної безпеки.

Введення пропонованого апарату аналізу систем інформаційної безпеки випливає з необхідності початку формального математичного опису визначених ситуацій при побудові і моделюванні систем захисту.

Об’єктом дослідження є система забезпечення інформаційної безпеки, яка має ієрархічну структуру та безліч складових її об’єктів.

Для спрощення процесу моделювання пропонується надати систему забезпечення інформаційної безпеки у вигляді узагальненої структури.

В узагальненій структурі системи забезпечення інформаційної безпеки на її верхньому рівні можна виділити чотири основні блоки:

1. Блок ресурсів. Він включає доступні системі ресурси - фінансові, технічні, інформаційні.

2. Блок небезпек. Містить базу даних можливих загроз, їх ймовірності та можливості реалізації.

3. Блок параметрів об'єкта. Містить інформацію про фізичну структуру, розташування на місцевості, канали проходження інформації.

4. Блок захисту. Включає використовувані технічні засоби захисту, засоби захисту інформації, організаційні заходи.

Блок системи розподілу ресурсів містить доступні системі ресурси – фінансові, технічні, інформаційні. В цьому блоці необхідно виділити кілька основних підблоків та зв'язків між ними. Це підблоки фінансових ресурсів, людських ресурсів, існуючих технічних засобів захисту, і навіть засобів інформаційного захисту.

Вхідна та вихідна інформація цих підблоків обробляється в блоці обробки, завдання якого - дати відповідь на запит про можливі або необхідні ресурси з урахуванням їх наявності, вартості та сумісності. Цей блок може працювати у двох режимах. По-перше, давати оптимальну інформацію з урахуванням фінансових обмежень та, по-друге, без цих обмежень, але з урахуванням необхідної якості.

Структура блоку загроз передбачає обробку та прогнозування. У ньому обробляється вхідний запит або генерується відповідна загроза або випадковим чином або на основі моделювання відповідної ситуації. У ньому необхідно також врахувати: кримінальні загрози – крадіжки, напади, агресії та ін; природні катаклізми – землетруси, несприятливі погодні умови; внутрішні загрози – неправильні дії персоналу, короткі замикання, зависання комп'ютерів, збої системи захисту; міські загрози – відключення електроенергії, обриви телефонних мереж, затори на дорогах.

Блок параметрів об'єкта визначає фізичну структуру об'єкта, межі безпеки, параметри розмежування доступу, інформаційні потоки на об'єкті. Для правильного опису структури необхідно формалізувати процес розбиття об'єкта на елементарні та локальні зони, межі безпеки. Зіставити фізичним об'єктам (будівлям, поверхам, приміщенням) інформаційні об'єкти (комп'ютери, мережеву структуру, електричні та телефонні мережі), а також систему доступу та переміщення персоналу та відвідувачів на об'єкті. Це завдання можна вирішити з урахуванням інформаційно-фізичної моделі об'єкта, введеної раніше.

Блок системи захисту є центральним блоком загальної моделі системи забезпечення інформаційної безпеки об'єкта. У ньому забезпечується взаємодія решти блоків моделі. Повинні бути передбачені два основні режими роботи – синтез та моделювання системи захисту. По-перше, на основі даних блоку параметрів об'єкта, обмежень, визначених блоком розподілу ресурсів, проектується перший варіант системи захисту об'єкта. На другому етапі дана система захисту піддається впливу загроз, які отримують з блоку загроз. Обчислюється ряд параметрів захищеності об'єкта і порівняється з бажаними. Шляхом варіювання параметрів у блоках розподілу ресурсів та у блоці параметрів об'єкта проводиться пошук оптимального варіанту системи захисту. Для точного аналізу роботи системи захисту необхідне ретельне опрацювання логічної схеми проходження

загрози через межі системи безпеки та апарат аналізу реакції системи захисту на цю загрозу.

Отже, визначивши шляхи вирішення цих завдань, можна суттєво спростити початковий етап побудови систем безпеки.

Список використаних джерел:

1. Грищук Р. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / Р. Грищук, К. Молодецька-Гринчук // *Захист інформації*. 2017. Т. 19, № 4. С. 254-262 URL: http://nbuv.gov.ua/UJRN/Zi_2017_19_4_3.
2. Kahler M. Economic security in an era of globalization. *The Pacific Review*. Vol. 17. No. 4. URL: https://www.tandfonline.com/doi/full/10.1080/09512740 42000326032?scroll=top&needAccess=true
3. Radchenko, S.G. (2015), Formalizovannie i jevristicheskie reshenija v regressionnom analize [Formalized and heuristic solutions in regression analysis], Kornijchuk, Kyiv, Ukraina.
4. Варналій З.С., Онищенко С.В., Маслій О.А. Механізм попередження загроз економічній безпеці України. Економічний часопис XXI. 2016. № 159(5-6). С. 20-24.
5. Системи забезпечення інформаційної безпеки. URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review
6. Економічна безпека підприємств, організацій та установ URL: https://pidru4niki.com/1663080551264/ekonomika/ekonomichna_bezpeka_pidpriyemstv_organizatsiy_ta_ustanov

ЗАСТОСУВАННЯ НЕЙРОМЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ КОРИСТУВАЧІВ

Ломановська А. В.

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Одним з важливих завдань є захист даних користувачів від втрати і пошкодження. Це пояснює зростаючий інтерес до способів захисту, які могли б забезпечити безпеку даних користувачів. На даний момент одним з прогресивних напрямків у цій галузі є використання нейронних мереж для вирішення цієї проблеми.

Важливою особливістю нейромереж, яка використовується у сфері забезпечення безпеки даних користувачів, є їх здатність аналізувати складні багаторівневі алгоритми умисних атак на дані користувачів.

Класичним прикладом такого використання є проект STAMINA [1].

STAMINA представляє собою нейромережу яка здатна конвертувати програмний код в монохромне зображення. Надалі зображення піддається аналізу