2. Башмаков Д.А. Точність передбачення пікселів фонових областей цифрових зображень у задачі стеганоаналізу методом Weighted Stego // Кібернетика та програмування. 2018. №2. З. 38-47.
3. Сівачов А.В., Прохожев Н.М., Михайличенко О.В., Башмаков Д.А. Ефективність стеганоаналізу на основі методів машинного навчання// Питання кібербезпеки. 2017. №2 (20). 3. 53-60. DOI: 10.21681/2311-34562017-2-53-60.
4. Макаренко С.І. Еталонна модель взаємодії стеганографічних систем та обґрунтування на її основі нових напрямків розвитку теорії стеганографії// Питання кібербезпеки. 2014. №2 (3). С. 24-32.
5. Парасич А. В., Парасич В. А., Парасич І. В. Формування навчальної вибірки в завданнях машинного навчання // Інформаційно-керуючі системи. 2021. № 4. С.61-70.
6. Atlasov I., Solodukha R. Cample Representativeness Estimation як Preliminary Stage of Statistical Steganalysis / 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), 2021, pp. 78-84.

УДК 004.056.53:621.39(043.2)

Ласкавчук М.А.
здобувач вищої освіти
Зелінська О.В.,к.т.н., доцент
доцент кафедри інформаційних технологій

ЗАСОБИ ТА ЗАХОДИ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Донецький національний університет імені Василя Стуса, м. Вінниця

Фізичні засоби захисту - це засоби, необхідні для зовнішнього захисту обчислювальної техніки, об'єктів на базі ПК, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та інформації, що захищається [1].

Надійним і простим заходом, щоб захистити інформацію від загроз несанкціонованого доступу є режим автономного використання комп’ютера одним користувачем у спеціально виділеному приміщенні, доступ до якого наданий лише одній особі. Замкненим контуром захисту є виділене приміщення, а захистом фізичним - підлого, вікна, стеля, стіни та двері. Якщо стеля, стіни, двері і підлога міцні, вікна і двері обладнані сигналізацією, підлога не має люків, які з'єднуються з іншими приміщеннями, то стійкість захисту визначається технічними характеристиками сигналізації при відсутності користувача в неробочий час.

Більш складні засоби контролю доступу включають технологічний підхід. Сканери ідентифікаційних карток і ідентифікаційні картки - це методи фізичної аутентифікації, які служби безпеки можуть використовувати для перевірки осіб, які входять і виходять з різних об’єктів. Використовуючи тактично встановлені перешкоди, організації можуть ускладнити зловмисникам доступ до цінних

активів та інформації. Подібним чином ці бар'єри збільшують час, необхідний суб'єктам загрози для успішного здійснення актів крадіжки, вандалізму чи тероризму. Чим більше перешкод існує, тим більше часу мають організації, щоб реагувати на фізичні загрози безпеці та стримувати їх.

Коли комп'ютер працює, то є можливість витоку інформації каналами побічного електромагнітного випромінювання. Для того, щоб уникнути виникання такої загрози, здійснюється низка спеціальних досліджень, які націлені на апаратні засоби та їх випромінювання, основним їхнім змістом є категорювання та атестування об'єктів і засобів електронно-обчислювальної техніки, з видачею відповідного дозволу на експлуатацію. Також, двері приміщення повинні бути обладнані замком, він може бути електромеханічним або механічним. На період тривалої відсутності користувача за комп'ютером, коли відсутня охоронна сигналізація, радять машинні носії інформації та системний блок зберігати у сейфі.

Фізична безпека може набувати різних форм . Наприклад, стратегії, методи та бар'єри, які організації використовують для підтримки загальної безпеки фізичних інформаційних технологій, суттєво відрізняються від тих, що використовуються для забезпечення постійної безпеки фізичної мережі.

Ось кілька прикладів фізичної безпеки, які використовуються для стримування та контролю реальних загроз:

Log and trail maintenance

Ведення записів про те, до чого здійснюється доступ – і те, до чого люди намагаються отримати доступ – це надійний спосіб не лише перешкодити неавторизованим користувачам, але й створити середовище даних, сприятливе для криміналістики [2].

Risk-based approach

Одним із найефективніших способів оптимізації інвестицій у фізичну безпеку є використання підходу, що ґрунтується на оцінці ризику. Це техніка аналізу даних, яка використовується для оцінки сценаріїв на основі профілю ризику [2].

Accountable access control

Зв'язавши контроль доступу з окремими особами, організація може покращити видимість діяльності персоналу. Уявіть, що до певної кімнати можна отримати доступ лише за допомогою одного ключа, і цей ключ дають двом людям. Якщо актив у цій кімнаті зникає, то лише ці дві людини несуть відповідальність за його зникнення [2].

Отже, фізична безпека — це захист персоналу, апаратного забезпечення, програмного забезпечення, мереж і даних від фізичних дій і подій, які можуть завдати серйозної шкоди підприємству, агентству чи установі [2].

Список використаних джерел

1. *Засоби та методи захисту інформації [Електронний ресурс]. Режим доступу: https://buklib.net/books/28625/. (Дата звернення: 08.11.2022)*
2. *Physical security [Електронний ресурс]. Режим доступу: https://www.techtarget.com/searchsecurity/definition/physical-security. (Дата звернення: 08.11.2022)*

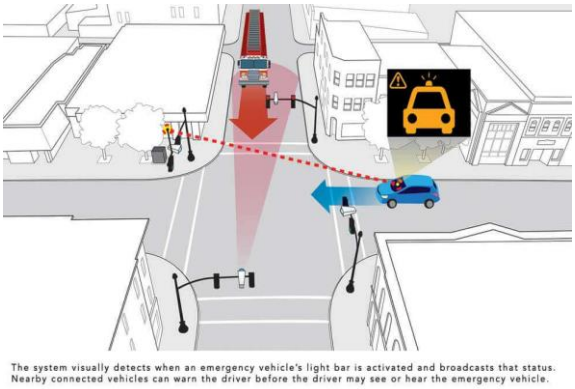
УДК 004.942+656.052.1

Лухверчик С.А. здобувач 3 курсу спеціальності 122 «Комп'ютерні науки»
Оврамець І.В. здобувач 3 курсу спеціальності 122 «Комп'ютерні науки»
Ніколюк П. К. професор, доктор фізико-математичних наук.

ІНТЕЛЕКТУАЛЬНА ТРАНСПОРТНА СИСТЕМА 4.0.

Донецький національний університет імені Василя Стуса, м. Вінниця

Ми не тільки знаємо, але кожен з нас відчуває на собі особисто проблему переповненості міста автотранспортом. З кожним роком дедалі більше місто задихається в заторах – погіршується комфортність міста, величезного стресу зазнає екологічна обстановка. Традиційні технології керування дорожнім трафіком, включаючи релейну «зелену хвилю», повністю вичерпали свої можливості вже не в змозі оптимізувати дорожній рух, рівномірно розподілити автотранспорт по місту. Досвід розвинених країн показує, що проблему можуть вирішити лише сучасні інтелектуальні системи керування дорожнім рухом (ІТС), які побудовані на технологіях штучного інтелекту, машинного навчання і розподілених граничних обчислень. Даний підхід дозволяє здійснити розумну взаємодію перехресть між собою, керувати дорожнім рухом в залежності від завантаження доріг транспортом, пішоходами, часу доби, пори року, надзвичайних ситуацій, потреб служб екстреного реагування. ІТС синхронізує між собою перехрестя міста та автоматично коригує потоки автотранспорту, чим гарантує істотне зниження коефіцієнту заторів, зменшення часу простою транспорту і збільшення середньої швидкості руху. Згідно із джерелами [1,2].



Зображення взято із джерела [1]