2. НСЗУ. Єдиний веб-портал органів виконавчої влади України [Електронний ресурс]. – Режим доступу: https://nszu.gov.ua/e-data.

3. Система моніторингу поширення епідемії коронавірусу [Електронний ресурс]. – Режим доступу: https://covid19.rnbo.gov.ua/.

4. Онлайн статистика коронавируса Covid-19 в Украине [Електронний ресурс]. – Режим доступу: https://coronavirus-monitor.ru/corona/virus-v-ukraine/.

5. Защепкіна Н. М. Розробка програмного додатку для попередження захворювання населення на COVID-19 / Н. М. Защепкіна, К. О. Мешкова // XVI Міжнар. наук.-практ. конф. «Ефективність та автоматизація інженерних рішень у приладобудуванні» (8–9 грудня). – Харків : НТУУ ім. Ігоря Сікорського 2020 р.

6. Elenko E. Defining digital medicine / E. Elenko, L. Underwood. // Nature Biotechnology. – 12. – № 33. – С. 18.

7. Mobile system with network-distributed data processing for biomedical applications [Electronic resource]. – 2013. – Mode of access: https://patents.google.com/patent/US9183351B2/en.

МЕТОДИ І ЗАСОБИ ЗАХИСТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Кравчук О. А.[1], *Синюк О. М., Кравчук А. Ю.*[2]
Хмельницький національний університет
E-mail: [1]*kravchukoa2@gmail,* [2]*iiilokiiiilokiiii@gmail.com*

Інформаційна безпека - це захищеність мережевої інфраструктури і інформаційних систем від випадкового або навмисного втручання (внутрішнього або зовнішнього), крадіжки інформації та / або блокування робочих процесів, що завдають шкоди власникам і користувачам інформації [1].

Сукупність методів і засобів захисту інформації включає програмні й апаратні засоби, захисні перетворення та організаційні заходи.

Апаратний, або схемний, захист полягає в тому, що в приладах ЕОМ та інших технічних засобах обробки інформації передбачається наявність спеціальних схем, що забезпечують захист і контроль інформації (схеми контролю на чесність, які контролюють правильність передачі інформації між різними приладами ЕОМ, а також екрануючими приладами, що локалізують електромагнітні випромінювання).

Програмні методи захисту – це сукупність алгоритмів і програм, які забезпечують розмежування доступу та виключення несанкціонованого використання інформації.

Сутність методів захисних перетворень полягає в тому, що інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що виключає можливість її безпосереднього використання. Організаційні заходи із захисту інформації містять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації, чітке регламентування розробки та функціонування інформаційної системи [3]. Лише комплексне використання різних заходів може забезпечити надійний захист інформації, тому що кожний метод/захід має слабкі і сильні сторони.

Існуючі штатні заходи захисту інформації в основному будується на основі штатних вбудованих механізмах захисту інформації системного ПЗ за модульним принципом, що дозволяє доповнювати її склад додатковими програмно-апаратними засобами захисту. Адміністрування відбувається централізовано. Розробку і реалізацію технічного проєкту виконують на рівнях: правовому, організаційному, технічному.

На правовому рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо організації системи нормативно-правового забезпечення робіт з захисту інформації та контролю її виконання.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо забезпечення фізичного захисту обладнання та інших ресурсів. Для забезпечення інформаційної безпеки ресурсів на підприємстві повинні виконуватися наступні правила експлуатації ПЗ. Вимоги до засобів керування інформаційної безпеки:

– надійність засобів керування безпекою забезпечується поділом ролей і обов'язків адміністраторів;

– повинні бути присутні як мінімум інспектор із захисту інформації, адміністратор БД, користувачі;

– контроль питання перерозподілу і додавання посадових обов'язків, зв'язаних з інформаційною безпекою;

– засоби адміністрування, що відносяться до інформаційної безпеки, повинні контролюватися на предмет їхнього несанкціонованого використання, модифікації, знищення;

– у системі повинні використовуватися механізми захисту при реєстрації нових користувачів;

– повинен бути встановлений граничний час пасивності користувачів, після якого вони виключаються з числа легальних користувачів;

– системний адміністратор повинен мати можливість проводити аудит дій одного чи обраної групи користувачів;

– засоби проведення аудита повинні бути захищені від неавторизованого використання, модифікації, знищення;

– існування захисного механізму, що забезпечує доступ тільки авторизованого персоналу до виконання функцій адміністратора [2].

Література

1. [Електронний ресурс]. – Режим доступу: https://infotel.ua/ua/IT-bezopasnost-i-zacshita-informatsii-1/

2. Копылов В. В. Информационное право : учебник / В. В. Копылов. – 2-е изд., перераб. и доп. – М. : Юристъ, 2010. – 132 с.

3. Новосад О. Інформаційне забезпечення управлінської діяльності у митних органах / О. Новосад // Митниця. – 2011. – № 1. – 97 с.

РОЗПІЗНАВАННЯ ТА ІДЕНТИФІКАЦІЯ НОМЕРНИХ ЗНАКІВ ТРАНСПОРТНИХ ЗАСОБІВ

Стецюк В. І.
Хмельницький національний університет, e-mail: *sv_rt@i.ua*

Сучасний розвиток систем відеоспостереження, відеореєстрації, різноманітних програмних та апаратних засобів дозволяє вирішувати найскладніші задачі. Однак, незважаючи на зовнішню простоту поставленої задачі, розпізнавання номерних знаків транспортних засобів – потребує комплексного науково-технічного підходу.

Процедура ідентифікації номерних знаків транспортних засобі (НЗТЗ) містить наступні етапи: фото (відео) фіксація, цифрова фільтрація, сегментація, бінаризація, детектування номерного знака, статистичний аналіз, ідентифікація. В рамках процесу детектування, слід виділити один із найпростіших але досить дієвий спосіб – порівняння з шаблоном, тобто відповідність окремих частин аналізованого зображення і побудованого шаблону номерного знака [2]. Далі область, що має найбільшу схожість із шаблоном, сегментується. Очевидно, що шаблон повинен максимально відображати всі характерні ознаки, властиві області номерного знака на зображенні. Після того, як шаблон побудований, необхідно визначити спосіб знаходження ступеню кореляції виділеної областю зображення і шаблону. Найбільш часто з цією метою застосовується перехресна кореляція, яка основана на обчисленні квадрата евклідової відстані між шаблоном і зображенням:

$$d^2(u,v) = \sum_x \sum_y \left[I(x,y) - T(x-u, y-v) \right]^2$$
$$= \sum_x \sum_y \left[I^2(x,y) - 2I(x,y)T(x-u,y-v) + T^2(x-u,y-v) \right] \quad (1)$$

де $I(x, y)$ – інтенсивність зображення в точці (x, y); $T(u, v)$ – побудований шаблон.