Захист інформації. – 2021. – Т. 23, № 1.

Ключко, О. М. Інформаційна система з біосенсором та захистом даних: розробка концептуальних напрямків / О. М. Ключко // Захист інформації. – 2021. – Т. 23, № 1. – С. 6-20.

Метою виконаної роботи є детальний аналіз можливостей розробки специфічних способів захисту даних у інформаційних системах, реалізованих із застосуванням технічних пристроїв – біосенсорів. Вони є інкорпорованими до інформаційних систем як їх елементи та пов'язані функціонально завдяки електричним сигналам на виході біосенсорів; у публікації аналізуються специфічні можливості кодування інформації у такій комплексній системі. У процесі роботи були застосовані методи фізичного моделювання біосенсорів як елементів інформаційних систем, розробки інформаційної системи моніторингу із базами даних, методики компаративного аналізу характеристик вхідних та вихідних електричних інформаційних сигналів біосенсора. Розглянуто поняття біосенсорів та їх властивості, у тому числі у експериментальній системі із реєстрацією вихідних електричних інформаційних сигналів, властивість кодування інформаційних сигналів таким біотехнічним пристроєм та ряд інших. Розроблена фізична модель та наведені деякі результати випробування пристрою. Коротко розглянуто функції нейроподібного біосенсора: приймач вхідних інформаційних сигналів – фільтр – аналізатор – кодер/декодер. Показано у табличному вигляді відповідність інформаційних сигналів на вході біосенсора (хімічні сигнали) та після кодування на виході (електричні сигнали). Як приклад розглянута інформаційна система із базами даних та біосенсорами для моніторингу наявності та ідентифікації шкідливих хімічних речовин у довкіллі аеропортів. Результати виконаної роботи можуть створити нові можливості для захисту даних у інформаційних системах.

Лізунов, С. І. Захист мовної інформації з використанням систем активного звукопридушення / С. І. Лізунов, Є. В. Філобок // Захист інформації. – 2021. – Т. 23, № 1. – С. 20-25.

Проводиться аналіз існуючих каналів витоку акустичної інформації, методів та засобів її захисту. Частково вирішується проблема захисту мовної інформації від несанкціонованого доступу під час проведення перемовин, забезпечення надійного захисту інформації у виділеному приміщенні, що є актуальним завданням захисту інформації з обмеженим доступом. Запропоновано модель системи захисту інформації, яка використовує систему активного звукопридушення з підвищеною ефективністю, запропоновано покращену систему акустичної захищеності. Така система має підвищену швидкодію і може ефективніше придушити майже усі звукові хвилі, які виходять за межі контрольованої зони, використовуючи щонайменше два мікрофони, електронний блок управління та динамік.

Коломицев, М. В. Аудит изменений таблиц базы данных SQL Server / М. В. Коломицев, С. О. Носок // Захист інформації. – 2021. – Т. 23, № 1. – С. 25-30.

Неотъемлемым компонентом информационных систем является подсистема регистрации и аудита. Все современные СУБД обладают возможностью регистрировать и обрабатывать информацию о выполняемых операциях. SQL Server начиная с версии с 2008 имеет возможность определять спецификацию аудита [1] на уровне сервера или базы данных. Однако данные системного аудита не учитывают требования бизнес-модели информационной системы. Возникает необходимость настройки процесса регистрации с учетом специфики предметной области. Кроме того, важнейшей задачей защиты БД является обеспечение целостности данных. В современных сложных ИС многие таблицы должны быть защищены от нежелательных операций изменений (вставок, обновлений и удалений). Данные аудита могут использоваться для отмены таких нежелательных действий. В этом случае, информации в системных журналах недостаточно. В данной статье рассматривается подход к решению задачи аудита изменений в таблицах БД с целью предотвращения нежелательных изменений данных. Такой подход реализован в виде методики создания объектов базы данных, с помощью которых осуществляется регистрация действий пользователей и отмена нежелательных изменений. Для решения задачи регистрации всех действий пользователя предлагается использовать отдельную схему БД для аудита, специальную таблицу аудита и триггеры информационных таблиц БД. Для отмены нежелательных изменений предложены SQL-процедуры. Для каждого этапа методики приведена программная реализация, что позволяет использовать ее как часть автоматизированной защиты БД. Неотъемлемым компонентом информационных систем является подсистема регистрации и аудита. Все современные СУБД обладают возможностью регистрировать и обрабатывать информацию о выполняемых операциях. SQL Server начиная с версии с 2008 имеет возможность определять спецификацию аудита [1] на уровне сервера или базы данных. Однако требования бизнеса могут потребовать более тонкой

настройки процесса регистрации. Кроме того, если возникает задача отмены нежелательных действий, то информации в системных журналах недостаточно. В современных сложных ИС многие таблицы должны быть защищены от нежелательных операций изменений данных (вставок, обновлений и удалений). В данной статье рассматривается подход к решению задачи аудита и предотвращения нежелательных изменений таблиц БД. Для решения задачи регистрации всех действий пользователя предлагается использовать отдельную схему БД для аудита, специальную таблицу аудита и триггеры информационных таблиц БД.

Трофименко, О. Г. Питання кібербезпеки медичних комп'ютерних систем / О. Г. Трофименко // Захист інформації. – 2021. – Т. 23, № 1. – С. 30-39.

За умов суворого карантину через пандемію COVID-19, завдяки можливостям сучасних інформаційно-телекомунікаційних систем, значна частина медичних послуг трансформувала у цифрове середовище в режим онлайн. Позитивний ефект цього полягає насамперед у знищенні цифрового розриву та реалізації прав громадян на рівноправне отримання медичної допомоги в електронному форматі. Проте цей процес зумовив потенційні небезпеки витоків конфіденційної інформації з подачі кіберзлочинців. Наразі питання кібербезпеки медичних комп'ютерних систем є вельми актуальними та потребують комплексного і виваженого підходу до вирішення. Важливою складовою при цьому є нормативно-правовий захист конфіденційної інформації, що циркулює в медичних комп'ютерних системах. Аналіз цифрових технологій та комп'ютерних систем з надання медичних онлайн послуг показав, що гостро постають питання анонімізації медичних даних пацієнтів, захисту медичних пристроїв, долучених до мережі Інтернет, від витоку конфіденційної медичної інформації. Тому при розробленні відповідного програмного забезпечення мають бути дотримані суворі правила щодо забезпечення конфіденційності даних, які обробляються в медичних інформаційних системах. Питання захищеності інфраструктури збору, зберігання і передачі медичних даних насамперед полягає в обмеженні доступу та створенні надійної електронної бази медичної інформації. З'ясовано певні проблеми безпеки хмарних середовищ, які використовують як платформи для зберігання даних при наданні послуг у галузі охорони здоров'я, щодо їх вразливості до можливих кібератак. Для підвищення довіри і забезпечення надійного захисту конфіденційної медичної інформації, яка обробляється у таких сервісах, варто враховувати всі програмні, апаратні та організаційні аспекти. Аналіз питань кібербезпеки медичних комп'ютерних систем дозволив виявити низку проблем захисту даних, важливість багатофакторної автентифікації користувачів, контролю доступу, застосування ефективних криптографічних схем шифрування для ефективного захисту інформаційних ресурсів екосистем охорони здоров'я в інтернеті та визначити напрями подальших досліджень з надання якісних захищених медичних онлайн послуг.

Пристрій для приведення чисел за модулем з аналізом чотирьох розрядів такого числа за крок / С. Т. Тинимбаєв, С. О. Гнатюк, Р. Ш. Бердибаєв, Ю. Я. Поліщук, Ю. А. Бурмак // Захист інформації. – 2021. – Т. 23, № 1. – С. 39-47.

Сучасна криптографія з відкритим ключем (асиметрична криптографія) дає можливість не лише шифрувати дані, але й вирішувати деякі актуальні проблеми симетричної криптографії – зокрема, проблему розподілу секретних ключів. Проте, алгоритми асиметричної криптографії є досить повільними і ресурсоємними, через що потребують новітніх підходів до підвищення швидкодії та оптимізації їх реалізації на різних платформах. Авторами у статті розглядається питання підвищення швидкодії асиметричних алгоритмів криптографії і пропонується схематичне рішення (пристрій) приведення числа за модулем як одного з методів реалізації приведення цілих чисел за модулем. Відомо, що такі операції, як множення, піднесення до квадрату і приведення за модулем впливають на швидкодію апаратних пристроїв криптографії. Особливо, операція приведення за модулем є найскладнішою і громіздкою в аспекті реалізації, що потребує особливої уваги вчених і дослідників до розробки алгоритмів і апаратних рішень для цієї проблеми. Таким чином, в цій статті авторами пропонується розробка і дослідження пристрою приведення чисел за модулем з аналізом чотирьох розрядів за крок. Розроблений пристрій був верифікований шляхом перевірки створеного алгоритму опису поведінкової моделі на мові Verilog HDL за допомогою часових діаграм. Тестування показало коректність алгоритму поведінкової моделі, що підтвердило ефективність розробленого пристрою приведення чисел за модулем з аналізом чотирьох розрядів такого числа за крок, а також можливість його використання для криптографічних застосувань.

Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України / О. В. Потій, А. І. Семенченко, Д. В. Дубов, О. О. Бакалинський, Д. В. Мялковський // Захист інформації. – 2021. – Т. 23, № 1. – С. 47-59.

У статті запропоновано концептуальні засади впровадження організаційно – технічної моделі кіберзахисту. Зокрема, визначені її місія, мета, призначення та цілі. Вперше визначені сили та засоби кіберзахисту. Розглянуто архітектуру організаційно-технічної моделі кіберзахисту, яка являє собою структуровану систему, яка складається з трьох інфраструктур кіберзахисту, а саме: організаційно-керуючу інфраструктуру кіберзахисту, як сукупність суб'єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки; технологічну інфраструктуру кіберзахисту, як сукупність сил та засобів кіберзахисту, а також інфраструктури, що забезпечує функціонування сил кіберзахисту, інформаційно-комунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту та базисну інфраструктуру кіберзахисту, як сукупність об'єктів критичної інформаційної інфраструктури, критичних активів, комунікаційних і технологічних систем підприємств, установ та організацій, що віднесені до об'єктів критичної інфраструктури, а також суб'єктів господарювання, громадян України та об'єднань громадян, інших особі, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. Отже, впровадження організаційно-технічної моделі кіберзахисту спрямовано на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів та мінімізацію вразливості комунікаційних систем.