М.П. Савченко, Д.М. Ізосімов, В.В. Мороз // Створення та модернізація озброєння і військової техніки в сучасних умовах: Тринадцята наук.-техн. конф., 5-6 вер. 2013 р., м. Феодосія: тези доп. – Феодосія: ДНВЦ, 1013. – С. 187-188.
15. Кожанова А.С. Визначення основних напрямків досліджень щодо створення системи технічної діагностики інтегрованих інформаційних систем / А.С. Кожанова, О.А. Смірнов, А.В. Челпанов // Проблемні питання розвитку озброєння та військової техніки Збройних Сил України: IV наук.-техн. конф., 16-20 груд. 2013 р., м. Київ: зб. тез. – Київ: ЦНДІ ОВТ ЗСУ, 1013. – С. 293.
16. Коваленко А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Інформатика та системні науки : V Всеукр. наук.-практ. конф., 13–15 бер. 2014 р., м. Полтава : зб. тез. – Полтава: ПУЕТ, 1014. – С. 292-294.
17. Коваленко А.С. Створення систем технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Проблеми і перспективи розвитку ІТ-індустрії: VI між нар. наук.-практ. конф., 17-18 квіт. 2014 р., м. Харків: зб. тез. – Харків: ХНЕУ, 1014. – С. 241.
18. Коваленко А.С. Визначення понятійного апарату та напрямів досліджень для синтезу систем технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Комп'ютерне моделювання у наукоємних технологіях (КМНТ-2014): наук.-техн. конф. з міжнар. участю, 18-31 трав. 2014 р., м. Харків: зб. наук. праць. – Харків: ХНУ, 1014. – С. 190-193.
19. Коваленко А.С. Розробка структури бази даних інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Проблеми і перспективи розвитку ІТ-індустрії: VII міжнар. наук.-практ. конф., 17-18 квіт. 2015 р., м. Харків: зб. тез. – Харків: ХНЕУ, 1015. – С. 15.
20. Коваленко А.С. Дослідження елементів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Комбінаторні конфігурації та їх застосування: XVII між нар. наук.-практ. сем., 17-18 квіт. 2015 р., м. Кіровоград: зб. тез – Кіровоград: КНТУ, 1015. – С. 5.

УДК 004

М.Жупило, магістр гр. КІ-21МЗ,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ ХМАРНИХ СЕРВІСІВ

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення конфіденційності даних хмарних сервісів. Метою розробки є дослідження та програмна реалізація системи забезпечення конфіденційності даних хмарних сервісів. Об'єктом дослідження є процес забезпечення конфіденційності даних хмарних сервісів. Предметом дослідження є методи забезпечення конфіденційності даних хмарних сервісів. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення конфіденційності даних хмарних сервісів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, конфіденційність даних, хмарні сервіси

Постановка проблеми. Незалежно від того, чи виконуєте ви робочі навантаження в загальнодоступній хмарі, приватній хмарі, гібридній інфраструктурі чи мультихмарі з декількома хмарними провайдерами, вам потрібно дотримуватися правил обробки даних і гарантувати безпеку своїх даних.

Недотримання правил щодо даних і наступне порушення може призвести до грошових втрат і шкоди авторитету бренду. Щоб забезпечити захист даних у хмарі, ви можете застосувати різні методи, такі як шифрування, контроль доступу, захист кінцевих точок і моніторинг.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи забезпечення конфіденційності даних хмарних сервісів.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи забезпечення конфіденційності даних хмарних сервісів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем забезпечення конфіденційності даних хмарних сервісів.
– Дослідження системи забезпечення конфіденційності даних хмарних сервісів.
– Програмна реалізація системи забезпечення конфіденційності даних хмарних сервісів.

Об'єктом дослідження є процес забезпечення конфіденційності даних хмарних сервісів.

Предметом дослідження є методи забезпечення конфіденційності даних хмарних сервісів.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Захист даних означає стратегічні та процедурні кроки, вжиті для захисту конфіденційності, доступності та цілісності конфіденційних даних, і часто взаємозамінно використовується з терміном «безпека даних». Ці захисні заходи, критичні для організацій, які збирають, обробляють або зберігають конфіденційні дані, спрямовані на запобігання пошкодженню, втраті чи пошкодженню даних. В епоху, коли генерація та зберігання даних зростає безпрецедентною швидкістю, важливість надійної стратегії захисту даних є першорядною. Основна мета захисту даних полягає не лише в захисті конфіденційної інформації, а й у забезпеченні її доступності та надійності, таким чином зберігаючи довіру та відповідність операціям, орієнтованим на дані.

Принципи захисту даних

Ось ключові аспекти керування даними, пов'язані із захистом даних:

– Доступність даних.
– Управління життєвим циклом даних.
– Управління життєвим циклом інформації.

Конфіденційність даних

Конфіденційність даних – це вказівка щодо того, як слід збирати та обробляти дані, виходячи з їхньої конфіденційності та важливості. Конфіденційність даних зазвичай застосовується до особистої інформації про здоров'я (PHI) та інформації, що дозволяє ідентифікувати особу (PII). Це включає фінансову інформацію, медичні записи, номери соціального страхування або ідентифікаційні номери, імена, дати народження та контактну інформацію.

Проблеми щодо конфіденційності даних стосуються всієї конфіденційної інформації, яку обробляють організації, включно з інформацією про клієнтів, акціонерів і співробітників. Часто ця інформація відіграє життєво важливу роль у бізнес-операціях, розвитку та фінансах.

Виявлення даних

Перш ніж захистити свої дані, вам потрібно знати, що у вас є та де вони розташовані. Цей процес, відомий як виявлення даних, має вирішальне значення для виявлення конфіденційної інформації та визначення найкращих способів її захисту.

Інвентаризація та класифікація

Щоб почати процес виявлення даних, ви повинні спочатку провести інвентаризацію всіх даних, які є у вашій організації. Це передбачає ідентифікацію різних типів даних, які ви зберігаєте, наприклад інформацію про клієнтів, записи про співробітників, інтелектуальну власність тощо. Отримавши вичерпний список, ви зможете класифікувати кожен тип даних на основі його чутливості та важливості.

Відображення даних

Відображення даних – це наступний крок у виявленні даних, який включає визначення розташування ваших даних і те, як вони проходять у вашій організації. Це допоможе вам зрозуміти взаємозв'язки між різними наборами даних і системами, дозволяючи вам приймати обґрунтовані рішення щодо захисту даних.

Інструменти автоматизованого виявлення

Для подальшого спрощення процесу виявлення даних багато організацій тепер використовують автоматизовані інструменти, які можуть швидко сканувати та ідентифікувати конфіденційні дані. Ці інструменти можуть допомогти вам відстежувати інвентаризацію даних і гарантувати, що ви завжди будете в курсі будь-яких змін або доповнень.

Запобігання втраті даних (DLP)

Запобігання втраті даних (DLP) є критично важливим компонентом захисту даних, призначеним для запобігання несанкціонованому доступу, витоку або крадіжці конфіденційної інформації. Технології DLP складаються з різних інструментів і процесів, які допомагають організаціям контролювати свої дані.

Політики DLP

Створення та впровадження політик DLP є важливим першим кроком у захисті ваших даних. Ці політики окреслюють правила та процедури обробки конфіденційної інформації та мають бути адаптовані до конкретних потреб вашої організації.

Моніторинг і сповіщення

Технології DLP часто включають системи моніторингу та оповіщення, які можуть виявляти потенційні порушення даних або інші інциденти безпеки. Ці системи можуть відстежувати дії користувачів, позначаючи будь-яку підозрілу поведінку або спроби отримати доступ до конфіденційних даних.

Санація

У разі потенційного порушення даних або інциденту безпеки технології DLP також пропонують варіанти виправлення. Це може включати блокування передачі конфіденційних даних, розміщення уражених файлів на карантин або автоматичне скасування доступу до зламаних облікових записів.

Зберігання з вбудованим захистом даних

Вибір правильного рішення для зберігання є важливим для забезпечення безпеки ваших даних. Сучасні технології зберігання тепер оснащені вбудованими функціями захисту даних, які пропонують додаткові рівні безпеки.

Надмірність

Одним із основних способів захисту даних у технологіях зберігання є резервування. Створивши кілька копій своїх даних і зберігаючи їх на окремих дисках або в окремих місцях, ви можете мінімізувати ризик втрати даних через збій обладнання чи інші проблеми.

Виправлення помилок

Вбудована корекція помилок є ще однією особливістю багатьох сучасних систем зберігання. Ця технологія може автоматично виявляти та виправляти пошкодження даних, забезпечуючи цілісність вашої інформації.

Резервне копіювання

Резервне копіювання ваших даних є фундаментальним аспектом захисту даних. Регулярне резервне копіювання гарантує швидке відновлення інформації у разі втрати або пошкодження даних.

Локальні та зовнішні резервні копії

Дуже важливо підтримувати як локальні, так і зовнішні резервні копії ваших даних. Локальні резервні копії забезпечують швидкий доступ до вашої інформації, тоді як зовнішні резервні копії пропонують додатковий захист від катастроф, таких як пожежі чи повені.

Інкрементні та повні резервні копії

Окрім вибору правильного місця резервного копіювання, вам також слід враховувати

тип резервного копіювання, який ви виконуєте. Інкрементне резервне копіювання зберігає лише зміни, внесені з часу останнього резервного копіювання, а повне резервне копіювання створює повну копію ваших даних. Поєднання обох типів може допомогти знайти правильний баланс між простором для зберігання та часом відновлення.

Планування резервного копіювання

Щоб гарантувати, що ваші резервні копії завжди актуальні, важливо встановити регулярний розклад резервного копіювання. Це може включати щоденне, щотижневе або навіть щомісячне резервне копіювання, залежно від потреб вашої організації та конфіденційності ваших даних.

Моментальні знімки

Знімки пропонують додатковий рівень захисту для ваших даних, створюючи копії ваших систем і файлів на певний момент часу. Ці знімки можна використовувати для швидкого відновлення ваших даних у разі інциденту безпеки.

Миттєве відновлення

Однією з головних переваг знімків є їх здатність сприяти миттєвому відновленню. Якщо вашу систему зламано, ви можете швидко повернутися до попереднього знімка, мінімізуючи час простою та втрату даних.

Керування версіями

Знімки також забезпечують форму керування версіями, що дозволяє підтримувати кілька версій ваших даних і систем. Це може бути особливо корисним для відстеження змін і визначення причини інциденту безпеки.

Ефективність зберігання

Завдяки своїй інкрементній природі знімки можуть бути більш ефективними для зберігання, ніж традиційні резервні копії. Це може допомогти вам заощадити місце, зберігаючи комплексну стратегію захисту даних.

Тиражування

Реплікація передбачає створення точної копії ваших даних і збереження її в окремому місці. Це може забезпечити додатковий захист від втрати даних і забезпечити доступність вашої інформації.

Відмовостійкість і відмова

У разі системного збою або іншого збою реплікація дозволяє швидко переключитися на репліковані дані (відмова), забезпечуючи мінімальний час простою. Після того, як проблему буде вирішено, ви зможете повернутися до вихідних даних (відновлення).

Балансування навантаження

Реплікація також може допомогти з балансуванням навантаження, дозволяючи вам розподіляти робоче навантаження між кількома системами або розташуваннями. Це може покращити продуктивність і запобігти перевантаженню системи.

Географічна надмірність

Тиражуючи свої дані в географічно різних місцях, ви можете захистити свою інформацію від регіональних катастроф і зберегти доступ до своїх даних у разі локального збою.

Брандмауери

Брандмауери відіграють вирішальну роль у захисті даних, діючи як бар'єр між внутрішніми системами та зовнішнім світом. Вони можуть допомогти запобігти несанкціонованому доступу та захистити ваші дані від різних загроз.

Виявлення та запобігання вторгненням

Багато сучасних брандмауерів включають функції виявлення та запобігання вторгненням, які можуть ідентифікувати та блокувати потенційні загрози до того, як вони досягнуть ваших систем.

Контроль додатків

Брандмауери також можуть забезпечити контроль програм, дозволяючи обмежувати або дозволяти певним програмам доступ до ваших даних. Це може допомогти запобігти

несанкціонованому доступу та зберегти цілісність вашої інформації.

Моніторинг руху

Нарешті, брандмауери пропонують можливості моніторингу трафіку, дозволяючи відстежувати та аналізувати потік даних у вашу організацію та з неї. Це може допомогти вам виявити потенційні інциденти безпеки та відповідним чином реагувати.

Автентифікація та авторизація

Автентифікація та авторизація є важливими компонентами захисту даних, які гарантують, що лише авторизовані особи можуть отримати доступ до ваших даних. Ці процеси передбачають перевірку ідентичності користувачів і надання їм належного рівня доступу.

Багатофакторна автентифікація

Багатофакторна автентифікація (MFA) додає додатковий рівень безпеки, вимагаючи від користувачів надання двох або більше форм ідентифікації для доступу до ваших даних. Це може включати те, що вони знають (наприклад, пароль), те, що вони мають (наприклад, маркер безпеки), або те, чим вони є (наприклад, відбиток пальця).

Керування ідентифікацією та доступом

Системи керування ідентифікацією та доступом (IAM) призначені для керування ідентифікацією користувачів і правами доступу у вашій організації. Завдяки централізації процесів автентифікації та авторизації IAM може допомогти оптимізувати захист даних і підвищити безпеку.

Шифрування

Шифрування – це процес перетворення даних у код, який можуть прочитати лише авторизовані сторони. Ця технологія є критично важливим компонентом захисту даних, оскільки може допомогти запобігти крадіжці даних або несанкціонованому доступу.

Симетричне шифрування

Симетричне шифрування передбачає використання одного ключа для шифрування та дешифрування даних. Цей метод часто швидший за інші методи шифрування, але вимагає, щоб обидві сторони мали доступ до одного ключа, що є менш безпечним.

Асиметричне шифрування

Асиметричне шифрування, також відоме як шифрування з відкритим ключем, використовує два ключі: один для шифрування даних, а інший – для їх дешифрування. Цей метод повільніший за симетричне шифрування, але забезпечує більший захист, оскільки закритий ключ залишається секретним.

Наскрізне шифрування

Наскрізне шифрування – це метод шифрування, який гарантує, що дані залишаються захищеними з моменту їх надсилання до отримання одержувачем. Ця технологія зазвичай використовується в програмах для обміну повідомленнями та інших комунікаційних платформах.

Захист кінцевої точки

Кінцеві точки, такі як ноутбуки, смартфони та інші мобільні пристрої, часто є вразливими цілями для кібератак. Технології захисту кінцевих точок призначені для захисту цих пристроїв і даних, які вони містять.

Антивірус і захист від шкідливих програм

Антивірусне програмне забезпечення та програмне забезпечення для захисту від зловмисного програмного забезпечення є важливими компонентами захисту кінцевих точок, призначеними для виявлення та видалення шкідливого програмного забезпечення з ваших пристроїв.

Управління пристроєм

Захист кінцевих точок також може включати керування пристроєм, що дозволяє відстежувати та контролювати кінцеві точки з центрального розташування. Це може включати моніторинг активності пристрою, обмеження доступу до певних програм і дистанційне стирання пристроїв у разі крадіжки чи втрати.

Керування виправленнями

Керування виправленнями – це процес підтримки ваших пристроїв в актуальному стані за допомогою останніх виправлень безпеки та оновлень програмного забезпечення. Це може допомогти усунути вразливості та запобігти кібератакам з використанням відомих слабких місць.

Стирання даних

Стирання даних передбачає безпечне й остаточне видалення даних із ваших систем. Цей процес має вирішальне значення для того, щоб конфіденційна інформація не потрапила в чужі руки.

Безпечні методи видалення

Методи безпечного видалення даних передбачають перезапис існуючих даних новими, що унеможливлює відновлення вихідної інформації. Ці методи можуть включати багаторазове перезаписування даних, розмагнічування або фізичне знищення носія даних.

Політика знищення даних

Встановлення політики знищення даних має важливе значення для забезпечення належного видалення конфіденційної інформації, коли вона більше не потрібна. У цих політиках мають бути описані процедури видалення даних і типи даних, які потребують безпечного видалення.

Сертифікація та аудит

Нарешті, сертифікація та аудит можуть допомогти переконатися, що ваші процеси видалення даних є ефективними та відповідають відповідним нормам. Отримавши сертифікацію та проходячи регулярні аудити, ви можете продемонструвати свою відданість захисту даних і гарантувати, що ваші процедури залишаються актуальними.

Аварійного відновлення

Аварійне відновлення передбачає підготовку та реагування на несподівані події, які можуть загрожувати доступності або цілісності ваших даних. Цей процес має важливе значення для забезпечення безперервності роботи та може допомогти мінімізувати вплив катастроф.

Аналіз впливу на бізнес

Перш ніж ви зможете розробити план аварійного відновлення, ви повинні спочатку провести аналіз впливу на бізнес. Цей процес передбачає визначення критичних функцій і систем у вашій організації та визначення потенційного впливу збоїв.

Планування аварійного відновлення

Провівши аналіз впливу на бізнес, ви можете розробити план аварійного відновлення. Цей план має окреслювати процедури реагування на катастрофи та відновлення систем і даних.

Тестування та технічне обслуговування

Щоб забезпечити ефективність вашого плану аварійного відновлення, важливо регулярно тестувати та підтримувати свої процедури. Це може включати проведення настільних навчань або повномасштабного моделювання, а також оновлення вашого плану в міру появи нових технологій або загроз.

Найважливіші найкращі методи забезпечення конфіденційності даних

Створення політики щодо конфіденційності даних може бути складним завданням, але це не неможливо. Наведені нижче практичні поради допоможуть вам переконатися, що створені вами політики є максимально ефективними.

Інвентаризуйте свої дані

Частиною забезпечення конфіденційності даних є розуміння того, які дані у вас є, як вони обробляються та де вони зберігаються. У вашій політиці має бути визначено, як ця інформація збирається та обробляється. Наприклад, вам потрібно визначити, як часто дані скануються та як вони класифікуються після того, як вони знаходяться.

У вашій політиці конфіденційності має бути чітко вказано, які засоби захисту необхідні для різних рівнів конфіденційності ваших даних. Політики також повинні

включати процеси перевірки захисту, щоб переконатися, що рішення застосовуються правильно.

Мінімізуйте збір даних

Переконайтеся, що ваша політика передбачає збір лише необхідних даних. Якщо ви збираєте більше, ніж вам потрібно, ви збільшуєте свою відповідальність і створюєте надмірний тягар для ваших команд безпеки. Мінімізація збирання даних може також допомогти вам заощадити на пропускній здатності та сховищі.

Одним із способів досягнення цього є використання фреймворків «перевіряти, а не зберігати». Ці системи використовують дані третіх сторін для перевірки користувачів і усувають необхідність зберігати або передавати дані користувачів у ваші системи.

Будьте відкритими зі своїми користувачами

Багато користувачів знають про проблеми конфіденційності та, ймовірно, оцінять прозорість, коли мова йде про те, як ви використовуєте та зберігаєте дані. Відображаючи це, GDPR зробив згоду користувача ключовим аспектом використання та збору даних.

Ви можете бути впевнені, що включите користувачів та їхню згоду у ваші процеси, розробивши проблеми конфіденційності у своїх інтерфейсах. Наприклад, наявність чітких сповіщень для користувачів із зазначенням часу збору даних і чому. Ви також повинні включити параметри для користувачів, щоб змінити або відмовитися від збору даних.

Тенденції захисту даних

Портативність даних і суверенітет даних

Портативність даних є важливою вимогою для багатьох сучасних IT-організацій. Це означає можливість переміщення даних між різними середовищами та програмними додатками. Дуже часто портативність даних означає можливість переміщення даних між локальними центрами обробки даних і загальнодоступною хмарою, а також між різними хмарними провайдерами.

Переносимість даних також має юридичні наслідки: коли дані зберігаються в різних країнах, вони підпадають під дію різних законів і правил. Це відомо як суверенітет даних.

Традиційно дані не були переносними, і перенесення великих наборів даних в інше середовище вимагало великих зусиль. Міграція хмарних даних також була надзвичайно складною на початку розвитку хмарних обчислень. Розробляються нові технічні методи, які спрощують міграцію та роблять дані більш переносними.

Пов’язаною проблемою є переносимість даних у хмарах. Постачальники хмарних послуг, як правило, мають власні формати даних, шаблони та механізми зберігання. Це ускладнює переміщення даних з однієї хмари в іншу та створює блокування від постачальника. Все частіше організації шукають стандартизовані способи зберігання та керування даними, щоб зробити їх переносними між хмарами.

Захист мобільних даних

Захист мобільних пристроїв стосується заходів, призначених для захисту конфіденційної інформації, що зберігається на ноутбуках, смартфонах, планшетах, переносних та інших портативних пристроях. Основним аспектом безпеки мобільного пристрою є запобігання доступу неавторизованих користувачів до вашої корпоративної мережі. У сучасному IT-середовищі це критичний аспект безпеки мережі.

Існує багато інструментів безпеки мобільних даних, призначених для захисту мобільних пристроїв і даних шляхом виявлення загроз, створення резервних копій і запобігання загрозам на кінцевій точці від досягнення корпоративної мережі. IT-спеціалісти використовують програмне забезпечення для захисту мобільних даних, щоб забезпечити безпечний мобільний доступ до мереж і систем.

Загальні можливості рішень безпеки мобільних даних включають:

– Забезпечення зв’язку через захищені канали.

– Виконання надійної перевірки особи, щоб переконатися, що пристрої не скомпрометовані.

– Обмеження використання програмного забезпечення сторонніх розробників і

перегляду небезпечних веб-сайтів.

– Шифрування даних на пристрої для захисту від компрометації та крадіжки пристрою.

– Виконуйте регулярні аудити кінцевих точок, щоб виявити загрози та проблеми безпеки.

– Моніторинг загроз на пристрої.

– Налаштування захищених шлюзів, які дозволять віддаленим пристроям безпечно підключатися до мережі.

Програми-вимагачі

Програмне забезпечення-вимагач – це зростаюча загроза кібербезпеці, яка є головним пріоритетом безпеки майже для всіх організацій. Програми-вимагачі – це різновид зловмисного програмного забезпечення, яке шифрує дані користувача та вимагає викуп за його розповсюдження. Нові типи програм-вимагачів надсилають дані зловмисникам перед їх шифруванням, що дозволяє зловмисникам вимагати від організації, погрожуючи оприлюднити її конфіденційну інформацію.

Резервне копіювання є ефективним захистом від програм-вимагачів: якщо організація має свіжу копію своїх даних, вона може відновити її та відновити доступ до даних. Однак програми-вимагачі можуть поширюватися мережею протягом тривалого періоду часу, поки файли не шифруються. На цьому етапі програми-вимагачі можуть заразити будь-яку підключену систему, включно з резервними копіями. Коли програми-вимагачі поширюються на резервні копії, це закінчується для стратегій захисту даних, оскільки відновити зашифровані дані стає неможливо.

Існує кілька стратегій для запобігання програмному забезпеченню-вимагачу та, зокрема, запобіганню його розповсюдженню на резервні копії:

– Найпростіша стратегія полягає в тому, щоб використовувати старе правило резервного копіювання 3-2-1, зберігаючи три копії даних на двох носіях, один з яких знаходиться за межами підприємства.

– Постачальники засобів безпеки мають передові технології, які можуть виявляти програми-вимагачі на ранніх стадіях або, у гіршому випадку, блокувати процеси шифрування, коли вони починаються.

– Постачальники сховищ пропонують незмінне сховище, яке гарантує, що дані не можна буде змінити після їх збереження. Дізнайтеся, як захищене сховище Cloudian може допомогти захистити ваші резервні копії від програм-вимагачів.

Управління копіюванням даних (CDM)

Великі організації мають кілька наборів даних, які зберігаються в різних місцях, і багато з них можуть дублювати дані між собою.

Дублікати даних створюють численні проблеми – це збільшує витрати на зберігання, створює невідповідності та проблеми з роботою, а також може призвести до проблем із безпекою та відповідністю. Як правило, не всі копії даних будуть захищені однаково. Немає сенсу захищати набір даних і гарантувати його відповідність, якщо дані дублюються в іншому невідомому місці.

CDM – це тип рішення, яке виявляє дублікати даних і допомагає керувати ними, порівнюючи подібні дані та дозволяючи адміністраторам видаляти невикористані копії.

Аварійне відновлення як послуга

Аварійне відновлення як послуга (DRaaS) – це керована служба, яка надає організації хмарний віддалений сайт для аварійного відновлення.

Традиційно створення вторинного центру обробки даних було надзвичайно складним і пов’язаним із величезними витратами й актуальним лише для великих підприємств. Завдяки DRaaS організація будь-якого розміру може скопіювати свої локальні системи в хмару та легко відновити роботу в разі аварії.

Сервіси DRaaS використовують загальнодоступну хмарну інфраструктуру, що дає змогу зберігати кілька копій інфраструктури та даних у кількох географічних місцях, щоб

підвищити стійкість.

Захист даних і конфіденційність із Cloudian HyperStore

Для захисту даних потрібна потужна технологія зберігання. Пристрої зберігання Cloudian прості в розгортанні та використанні, дозволяють зберігати дані розміром у петабайт і миттєво отримувати до них доступ. Cloudian підтримує високошвидкісне резервне копіювання та відновлення з паралельною передачею даних (запис 18 ТБ на годину з 16 вузлами).

Cloudian забезпечує довговічність і доступність ваших даних. HyperStore може створювати резервні копії та архівувати ваші дані, забезпечуючи доступні версії для відновлення в разі потреби.

У HyperStore зберігання відбувається за брандмауером, ви можете налаштувати географічні межі для доступу до даних і визначити політики для синхронізації даних між пристроями користувачів. HyperStore дає вам можливості хмарного обміну файлами на локальному пристрої та контроль для захисту ваших даних у будь-якому хмарному середовищі.

Захист даних у хмарі

Захист даних у хмарі – це набір практик, спрямованих на захист даних у хмарному середовищі. Ці методи застосовуються до даних незалежно від того, де вони зберігаються або як ними керують, чи то всередині компанії, чи треті сторони. Хмарні методи захисту даних стали ключовими аспектами безпеки даних, оскільки компанії збільшують обсяг даних, що зберігаються в хмарі.

Якщо вас цікавить захист даних, ви можете дізнатися більше в нашому посібнику: Постійний захист даних.

Чому компаніям потрібен захист даних у хмарі

Багато компаній збирають і зберігають значні обсяги інформації, включно з конфіденційними. Більшість цих даних потрапляє в хмару в певний момент, під час збирання або зберігання.

Частково причиною зростання хмарного сховища даних є те, що організації все частіше працюють через веб-портали або використовують пропозиції програмного забезпечення як послуги (SaaS). Обидва вони потребують доступу до хмари. Крім того, багато компаній вирішують зберігати дані в хмарі навіть для внутрішнього використання.

Оскільки компанії використовують хмарні сервіси, захист даних стає складнішим:

– Компанії можуть не знати, де зберігаються всі програми та дані.

– Сторонній хостинг обмежує видимість доступу до даних і обміну ними.

– Спільні обов’язки щодо безпеки можуть бути неправильно зрозумілі або неправильно застосовані.

– Якщо компанії використовують кілька хмарних провайдерів або гібридну інфраструктуру, безпека може бути непослідовною.

– Дані можуть підпадати під дію нормативних актів щодо захисту даних, наприклад Загального регламенту захисту даних ЄС (GDPR), Каліфорнійського закону про конфіденційність споживачів (CCPA) або Закону США про перенесення та підзвітність медичного страхування (HIPAA).

Проблеми захисту даних у хмарі

Під час налаштування захисту даних у хмарі ваша організація, ймовірно, зіткнеться з кількома з наведених нижче проблем.

– Цілісність – системи мають бути розроблені таким чином, щоб гарантувати надання лише авторизованого доступу. Конфігурації також повинні гарантувати, що дозволи на зміну або видалення даних надаються відповідним користувачам.

– Локальність – правила щодо даних застосовуються відповідно до фізичного розташування даних, місця їх збору та використання. У розподіленій системі це може бути важко визначити та контролювати. Системи мають бути спроектовані таким чином, щоб чітко визначати, де постійно знаходяться дані.

– Конфіденційність – дані мають бути захищені відповідно до рівня конфіденційності. Це вимагає належного обмеження дозволів і застосування шифрування для обмеження читабельності. Так само облікові дані адміністратора та ключі шифрування мають бути захищені, щоб гарантувати дотримання цих обмежень.

– Хмарна інфраструктура зберігання даних повністю контролюється постачальником. Це означає, що компанії повинні покладатися на постачальників, щоб забезпечити безпеку фізичної інфраструктури, мереж і центрів обробки даних.

Найкращі методи безпеки хмарних даних

Щоб забезпечити ефективність створених вами засобів захисту, додайте наведені нижче практичні поради.

Оцініть вбудовану безпеку

Будь-який обраний вами хмарний постачальник повинен мати надійні внутрішні засоби контролю та пропонувати надійні інструменти, які допоможуть вам захистити дані. Шукайте постачальників, які пропонують угоди про рівень обслуговування, які гарантують належний захист систем.

Крім того, обов'язково перевірте, які політики мають постачальники, щоб відповідати вимогам. Якщо постачальники не сертифіковані, можливо, ви не зможете відповідати стандартам відповідності.

Використовуйте шифрування на рівні файлу

Більшість хмарних провайдерів пропонують певну міру шифрування як під час передавання, так і під час спокою. Вам слід увімкнути обидва параметри. Вам також слід розглянути можливість додавання додаткового шифрування на рівні файлу. Найпростіший спосіб зробити це – зашифрувати дані перед перенесенням їх у хмарне сховище.

Якщо ви не можете зашифрувати на рівні файлу, подивіться, чи можете ви «розшардувати» свої дані. Шардинг зберігає частини даних або програм у різних місцях. Це може ускладнити зловмисникам повторно зібрати ваші дані, навіть якщо вони отримають до них доступ.

Обмежте доступ за допомогою надійних облікових даних

Ви повинні застосовувати як сувору політику облікових даних, так і суворі дозволи доступу. Суворі дозволи гарантують, що користувачі та програми можуть отримати доступ лише до тих даних, які їм потрібні. Сувора політика облікових даних гарантує, що зловмисники не зможуть зловживати дозволами, наданими цим користувачам і програмам.

Періодично перевіряйте свої дозволи та встановлюйте життєві цикли паролів. Ви хочете переконатися, що всі облікові дані у вашій системі активно використовуються. Ви також хочете переконатися, що паролі досить важко вгадати, і що користувачі не використовують паролі повторно.

Захистіть пристрої кінцевих користувачів

Кінцеві точки є однією з найбільш вразливих частин вашої системи, особливо якщо кінцевими точками керує користувач. Наприклад, смартфони, підключені до вашої мережі в рамках політики використання власного пристрою (BYOD). Ці пристрої можуть бути проблемою, оскільки групи безпеки зазвичай не мають повного контролю над заходами безпеки, такими як оновлення чи шифрування.

Щоб запобігти зловживанню цими пристроями, вам слід запровадити рішення для захисту кінцевих точок. Ці рішення допомагають відстежувати та обмежувати трафік на периметрі вашої мережі, а також можуть допомогти вам обмежити вихід або надходження даних у ваші системи.

Захист даних за допомогою Cloudian HyperStore

Захист даних у хмарі може бути складним завданням, особливо коли мова йде про розподілену та складну інфраструктуру, як-от мультихмарні та гібридні хмари. Якщо ви користуєтеся кількома постачальниками хмарних технологій або кількома хмарними службами, вам доведеться більше працювати, щоб захистити свої дані.

Захист даних стає набагато легшим, коли ви переміщуєте дані локально. Cloudian

надає локальні пристрої зберігання даних, які прості в розгортанні та використанні, дозволяють зберігати дані розміром у петабайти за низькою ціною та миттєво отримувати до них доступ. Cloudian підтримує високошвидкісне резервне копіювання та відновлення з паралельною передачею даних (запис 18 ТБ на годину з 16 вузлами).

Cloudian HyperStore забезпечує довговічність і доступність ваших даних. Ви можете використовувати HyperStore як пристрій для швидкого та надійного зберігання даних. HyperStore може створювати резервні копії та архівувати ваші дані, забезпечуючи доступні версії для відновлення в разі потреби.

У HyperStore зберігання відбувається в межах брандмауера, ви можете налаштувати географічні межі для доступу до даних і визначити політики для синхронізації даних між пристроями користувачів. HyperStore дає вам можливість хмарного обміну файлами та масштабованість на локальному пристрої.

Розробка структурної схеми

На рисунку 1 зображена структурна схема системи забезпечення конфіденційності даних хмарних сервісів.

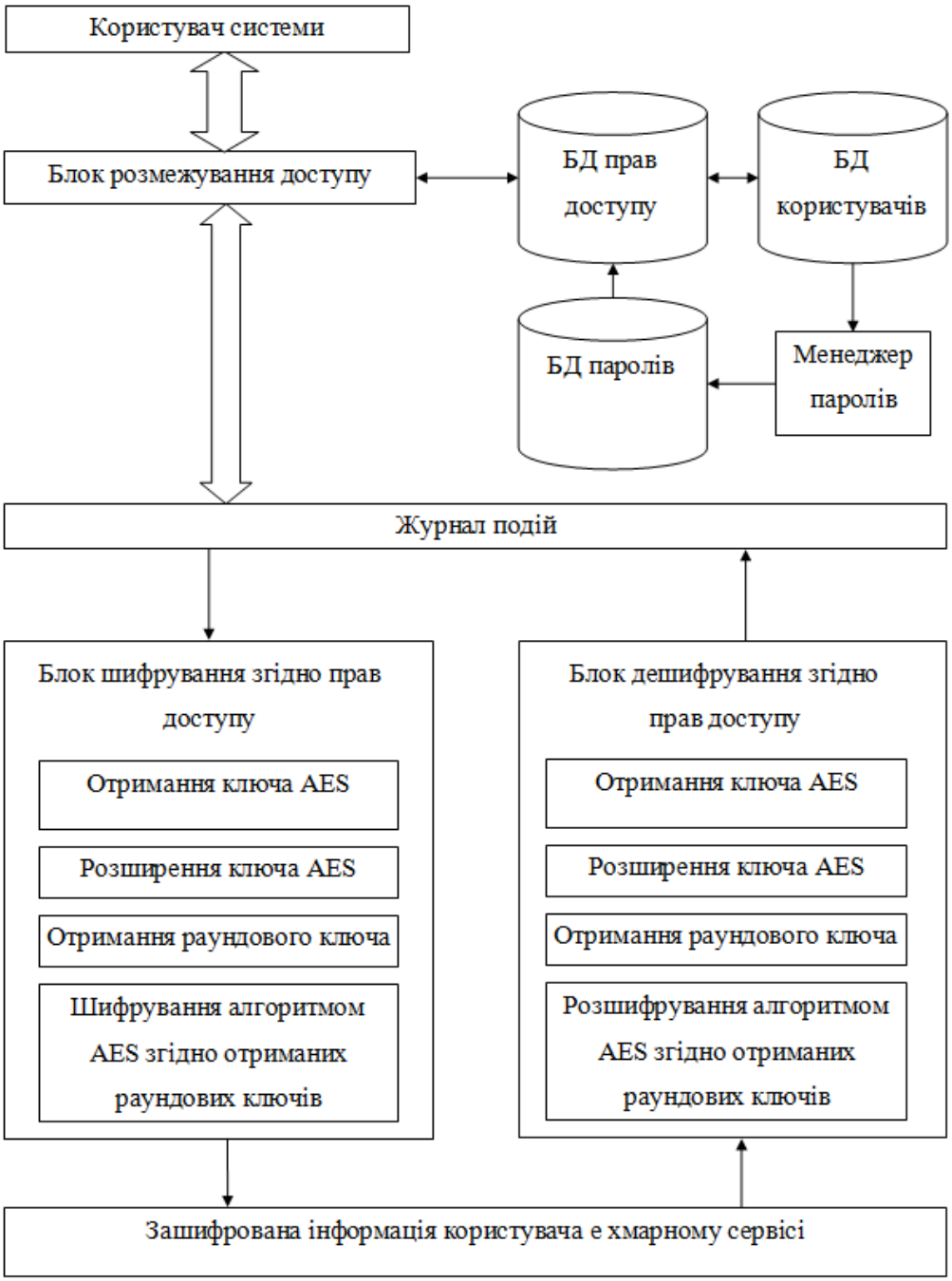

Рисунок 1 – Структурна схема системи

Забезпечення безпеки інформації при зберіганні й обробці більших інформаційних масивів у хмарних сервісах – одна із самих актуальних проблем сучасних інформаційних технологій. Інтенсивний розвиток методів розподіленої обробки даних і різке збільшення обсягів інформації, що накопичується в комп'ютерних системах, привели останнім часом до кардинальної зміни методів довгострокового зберігання даних. Традиційні підходи до організації зберігання великих інформаційних масивів перестали задовольняти зрослим вимогам до ємності носіїв і швидкості доступу до даних. Всі частіше споживач довіряє зберігання своєї власної інформації зовнішнім центрам або мережам зберігання даних (так званий аутсорсинг). Одна з основних сфер застосування мережного зберігання даних – формування банків даних електронних документів, а також електронних архівів і бібліотек. Такі сховища даних можуть бути як публічними, так і обмеженого доступу, залежно від характеру документів, що накопичуються в них.

Нерідко перед приміщенням документів у мережні сховища вони піддаються стиску або іншим спеціальним видам кодування. У зв'язку із цим загострюється необхідність забезпечення керованості, надійності й безпеці зберігання й доступу до електронних документів, а також процедур їхньої передачі між прикладними програмами й пристроями зберігання.

Якщо навіть дані зберігаються локально, виникає інша проблема: адміністратори, що управляють СУБД і персонал так чи інакше звичайно мають права доступу до всієї збереженої інформації. Для захисту від їхніх несанкціонованих дій у деяких випадках доцільне застосування апаратно-програмних засобів шифрування даних перед записом їх на засоби зберігання. Часто шифрувальні модулі вбудовуються, наприклад, у засоби резервного копіювання даних. Однак при зберіганні шифрованих масивів утруднений пошук окремих файлів і оперативний доступ до елементів масиву, необхідним для роботи прикладних програм. Тому що масив зберігається в зашифрованому виді, і серверу, на якому він зберігається (або СУБД), не можуть бути довірені ключі шифрування, користувач (або прикладна програма від його ім'я) змушений завантажувати копії всіх файлів масиву, розшифровувати їх і потім виконувати пошук на локальній машині.

Очевидно, що такий спосіб пошуку дуже неекономічний. У зв'язку із цим вимальовується проблема забезпечення можливості пошуку даних по шифрованим і (або) стислим даним, що може бути конкретизована залежно від застосовуваної в системі моделі шифрування даних.

Для шифрування великих масивів даних, що поміщаються в зовнішні стосовно власника інформації сховища, ефективні лише симетричні схеми шифрування. Можливості їхнього практичного застосування, мабуть, визначаються можливостями організації схеми керування секретними ключами, для яких необхідно забезпечити виконання двох почасти суперечливих вимог: забезпечення високої схоронності ключів (зокрема, за рахунок резервування) і обмеження середовища їхнього поширення тільки тими пристроями, яким довіряє власник інформації.

У зв'язку із цим у деяких випадках більше раціональним виглядає застосування схем відкритого шифрування, що дає можливість невизначеному колу осіб поміщати свої дані в сховище, але доступ до них залишати лише для власників секретного ключа. Така схема може бути корисна, наприклад, для систем електронної пошти або систем планування потоків завдань (workflows), де циркулюють переважно повідомлення невеликої довжини. Для таких схем тим більше необхідні механізми пошуку за шифрованим даними, що операції розшифрування в асиметричних криптосхемах, як відомо, виконуються на кілька порядків повільніше в порівнянні із симетричними. Інша проблема, пов'язана із забезпеченням конфіденційності пошуку в масивах даних, пов'язана з бажанням унеможливити одержання адміністратором СУБД і сторонніми особами відомостей про те, до яких саме записів (або фрагментів) бази даних здійснювався доступ при кожному конкретному запиті. У

закордонній літературі це завдання зветься “Private Information Retrieval” (PIR). Вона особливо актуальна, наприклад, при обробці й зберіганні електронних документів, що містять відомості приватного характеру: фінансові, юридичні, майнові, медичні й інші. Якщо навіть самі поля бази даних зашифровані, характер і частота запитів до них уже можуть дати зловмисникові деяку непряму інформацію, розголошення якої небажано для власника. Ці завдання до визначеної міри аналогічні виникаючої в телекомунікаційних системах завданню маскування інтенсивності трафіка між вузлами, що, як відомо, вирішується шляхом суцільного заповнення каналу псевдовипадковими послідовностями.

Виходячи зі структурної схеми системи зображеної на рисунку 9, система забезпечення конфіденційності даних хмарних сервісів, працює наступним чином. Спершу при вході в систему, користувач звертається до блоку розмежування доступу. Блок розмежування доступу отримує пароль користувача, та звертається до менеджеру паролів, де отримує сеансовий пароль перевірки правильності паролю користувача, та правильності прав доступу користувача, які зберігаються у відповідних зашифрованих базах даних. Розмежування цих баз зроблено з метою підвищення стійкості системи зберігання інформації. Після підтвердження прав доступу, та правильності введеного паролю, користувачеві видається сеансовий ключ AES для роботи з інформацією.

У блоці шифрування згідно прав доступу, з отриманого ключа AES відбувається його розширення, та обирається ключ ітерації, за допомогою яких й відбувається шифрування інформації алгоритмом AES. Процедура дешифрування відбувається аналогічним чином.

Висновки. У статті теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення конфіденційності даних хмарних сервісів. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем забезпечення конфіденційності даних хмарних сервісів; Досліджена система забезпечення конфіденційності даних хмарних сервісів; На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення конфіденційності даних хмарних сервісів; Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання забезпечення конфіденційності даних хмарних сервісів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022, pp. 1-12. (Scopus).
2. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022. (Scopus).
3. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34. (Scopus).
4. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477. (Scopus).
5. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w (Scopus).
6. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143 (Scopus).
7. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207. (Scopus).

8. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58. (Scopus).
9. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256. (Scopus).
10. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114. (Scopus).
11. Smirnov O.A., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346. (Scopus).
12. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131. (Scopus).
13. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14. (Scopus).
14. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84. (Scopus).
15. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587. (Scopus).
16. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136. (Scopus).
17. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379. (Scopus).
18. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43. (Scopus).
19. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645. (Scopus).
20. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660., (Scopus).

УДК 004

І.Завірюха, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ SMART HOME З ВИКОРИСТАННЯМ ПРОТОКОЛУ X10

У статті розроблено програмне забезпечення, яке призначено для системи smart home з використанням протоколу X10. Метою розробки є дослідження та програмна реалізація системи smart home з використанням протоколу X10. Об'єктом дослідження є процес smart home з використанням протоколу X10. Предметом дослідження є методи smart home з використанням протоколу X10. Методи дослідження базуються на методах інтернету речей, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи smart home з використанням протоколу X10. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, smart home, X10

Постановка проблеми. У сучасному житлі вже звичайними й навіть обов'язковими стають різні пристрої й пристосування, що забезпечують високу якість життя й комфорт мешканців. І якщо раніше канальні кондиціонери, електроуправляємі водопровідні вентилі, індивідуальне управління кліматом і безліч світлових груп були атрибутами великого