УДК 004

К.Василенко, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖЕВИХ CLOUD-СИСТЕМАХ

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

захист персональних даних, Cloud-система

Постановка проблеми. Стандартизація необхідна для ефективного функціонування будь-якої галузі, і ринок хмарних послуг не є виключенням. Його повноцінний розвиток неможливо без стандартів захисту інформації, переносимості даних і додатків, оцінки рівня надаваного сервісу й т.д. Причому їхній вплив може бути настільки ж великий, як і законодавчих вимог і норм. Проте забезпечення належної відповідності їм, а також сертифікація залишаються комерційною справою кожного провайдеру, якщо немає відповідної вимоги регулятора. Ключову роль у прийнятті необхідних стандартів і розвитку ринку може грати уряд – потенційно найбільш великий споживач хмарних сервісів. Підтримка хмарних обчислень припускає прийняття безлічі різних стандартів, що – з урахуванням наявності десятків органів по стандартизації – чревате їхньою фрагментарністю, непогодженістю й взаємним дублюванням. У свій час Європейська комісія навіть виразила заклопотаність із цього приводу, назвавши «мішанину стандартів» головною перешкодою на шляху переходу до хмар, що гальмує розвиток ринку. Найбільше побоювання викликало те, що галузь не зможе прийти до згоди відносно інтероперабельності сервісів і переносимості даних. Кожний великий гравець прагне до домінування на ринку, а тому, на думку комісії, не зацікавлений у стандартизації. У результаті замовники можуть виявитися прив'язаними до конкретного провайдеру, не маючи можливості його перемінити. Крім того, комісія виразила тривогу із приводу відсутності стандартів для забезпечення безпеки даних, відповідно до яких можна було б сертифікувати провайдерів хмарних послуг, їхню інфраструктуру й сервіси, що дозволило б гарантувати схоронність користувальницьких даних і допомогло галузі розвиватися.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи захисту персональних даних у мережевих cloud-системах.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи захисту персональних даних у мережевих Cloud-системах.

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

– Огляд існуючих систем захисту персональних даних у мережевих Cloud-системах.

– Дослідження системи захисту персональних даних у мережевих Cloud-системах.

– Програмна реалізація системи захисту персональних даних у мережевих Cloud-системах.

Об'єктом дослідження є процес захисту персональних даних у мережевих Cloud-системах.

Предметом дослідження є методи захисту персональних даних у мережевих Cloud-системах.

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

Виклад основного матеріалу. Релевантними для провайдерів стандартами ISO із групи 27000 є ISO 27002 на методи й засоби інформаційної безпеки й ISO 27005 на керування ризиками в області інформаційної безпеки. У першому більш докладно розглядаються засоби керування, що перераховуються в додатку до ISO 27001. Обидва стандарти (27002 і 27005) є рекомендаційними, сертифікація на відповідність їм не передбачається. Проте провайдер може замовити незалежну оцінку, щоб перевірити, якою мірою дотримуються запропоновані рекомендації. Деякі замовники запитують таку оцінку замість сертифікації по 27001. Всі три стандарти не є специфічними для провайдерів. Тим часом улітку 2014 року ISO опублікувала стандарт ISO 27018:2015 про захист персональних даних у хмарі, а наприкінці 2015 року – ISO 27017:2015 про засоби контролю інформаційної безпеки для хмарних рішень.

В ISO 27017 передбачаються додаткові елементи безпеки для хмари, відсутні в ISO 27002. Повна офіційна назва цього стандарту: «Звід правил для засобів керування інформаційною безпекою на базі ISO/IEC 27002 для хмарних сервісів» («Code of practice for information security controls based on ISO/IEC 27002 for cloud services»). Незважаючи на те що його фінальна редакція була опублікована лише 30 листопада 2015 року, Amazon Web Services уже має відповідний сертифікат, отриманий ще в жовтні 2015-го. Тим часом, будучи доповненням до ISO 27002, новий стандарт не припускає сертифікації, однак через його популярність багато органів сертифікації планують це робити: імовірно, будуть видавати «свідчення про відповідність». У всякому разі, на дане питання ще немає ясної відповіді.

Конкретні рекомендації стосовно до хмарних сервісів даються до 37 з більш ніж сотні засобів керування безпекою, які визначені в ISO 27002. Вони адресовані не тільки провайдерам хмарних послуг, але й замовникам, чим підкреслюється їхня взаємна відповідальність за безпеку сервісів: замовник повинен розробити політикові використання хмарних сервісів, а провайдер – надати йому необхідну інформацію. Найбільші зміни стосуються розділу, присвяченого контролю доступу: розглядаються реєстрація й вихід користувача, надання доступу, керування привілейованим доступом, обмеження доступу до інформації й використання привілейованих службових програм. Крім того, уводяться сім нових елементів керування:

– загальні ролі й відповідальність у хмарному середовищі;
– видалення й повернення активів клієнта хмарних сервісів;
– сегрегація у віртуальних обчислювальних середовищах;
– посилення віртуальних машин;
– операційна безпека адміністратора;
– моніторинг хмарних сервісів;
– узгодження керування безпекою для віртуальних і фізичних середовищ.

Звичайно, це далеко не всі стандарти, навіть якщо обмежитися тільки інформаційною безпекою. Чим їх більше, тим сутужніше в них розібратися. Як би те не було, ISO 27001 представляється найкращим базовим стандартом для всіх компаній, що бажають захистити свою інформацію (і єдиним із серії стандартів інформаційної безпеки ISO, на який видається реальний сертифікат). Залишаючи осторонь питання про захист персональних даних (ISO 27018 і/або 152-ФЗ), можна сказати, що реалізований постачальником хмарних послуг комплекс рекомендацій ISO 20001 і 20017 є необхідним «джентльменським набором» в

області інформаційної безпеки, якщо провайдер хоче розсіяти сумніву замовника в безпеці хмарних сервісів.

Однак, як випливає з ISO 20017, навіть проходження провайдером його рекомендаціям не знімає відповідальності із клієнта, що повинен виконати свою частину домашнього завдання й також ретельно додержуватися рекомендацій стандарту. Наприклад, відповідно до вимог контролю доступу А.9.4.1, він повинен обмежити доступ до інформації в хмарі у відповідності зі своєю корпоративною політикою.

Стандарти можуть робити настільки ж значний вплив на ринкову ситуацію, як і введення законодавчих вимог і норм. Проте при відсутності офіційних вимог забезпечення відповідності тим або іншим стандартам, а також сертифікація – це комерційна справа кожного провайдеру. У більшості країн діяльність хмарних провайдерів державою ніяк спеціальним образом не регулюється. Донедавна в жодній країні миру не було окремих законів, присвячених хмарам. Торік першопрохідником на цьому шляху стала Південна Корея.

До кінця 2017 року були прийняті необхідні правові акти по врегулюванню використання хмарних технологій при здійсненні державного керування. Однак на даний момент спеціальні нормативно-правові акти, де б установлювалися правила надання хмарних послуг, відсутні. Проте в Україні дуже багато законів, у яких і до замовників, і до постачальників послуг пред'являються досить специфічні й детальні вимоги. Головні з них – Цивільний кодекс (ГК), а також закони про інформацію й персональні дані.

Основні обмеження в частині обробки інформації стосуються персональних даних (ПДн). З юридичної точки зору у відносинах, що формуються у зв'язку з використанням хмарних послуг, беруть участь три сторони: суб'єкти даних, замовники й провайдери, – причому замовник є також оператором даних для тих суб'єктів даних, інформацію про які він збирає й потім передає в хмару. При буквальному читанні закону про персональні дані провайдер може класифікуватися як оператор ПДн залежно від обсягу надаваної хмарної послуги. У такому випадку виникає необхідність відповідати величезній кількості критеріїв, у числі яких – реєстрація в спеціальному реєстрі регулятора й відповідальність перед суб'єктом персональних даних, що перебувають у хмарі, що збільшує навантаження на провайдеру і його витрати.

Щоб уникнути цієї ситуації радимо провайдерам скористатися особливим режимом обробки даних – обробкою з доручення. Він рятує від необхідності діставати згоду на обробку ПДн у суб'єктів і дозволяє уникнути відповідальності безпосередньо перед ними: відносини провайдеру із приводу дотримання законодавства про ПДн будуть обмежені його контрактом із замовником – розбиратися з тими або іншими претензіями конкретних суб'єктів даних буде сам замовник, він же оператор даних. Для цього в договорі із провайдером повинні бути прописані наступні умови:

– перелік дій по обробці Пдн, які будуть відбуватися провайдером, а також мети обробки;

– зобов'язання провайдеру дотримувати конфіденційності Пдн і забезпечити їхня безпеку в ході обробки;

– перелік вимог до провайдеру по захисту оброблюваних Пдн.

При відсутності в договорі цих умов провайдер ризикує порушити безліч статей закону про Пдн, а при їхній наявності він хоча й звільняється від безпосередньої відповідальності перед суб'єктом даних, але відповідає за недотримання передбачених договором заходів щодо захисту Пдн.

Багато питань викликало вимогу закону про локалізацію, що вказує на те, що персональні дані українських громадян повинні оброблятися з використанням баз даних, що перебувають в Україні, і – згідно «твердому трактуванню» – винятково на вітчизняних серверах. Однак у підсумку вибрали більше м'який варіант: обробка даних українських громадян можлива й на закордонних серверах, якщо ці дані втримуються також у базах даних, розташованих на території Україні, при цьому не допускається наявності за межами

країни Пдн, які відсутні в українській базі даних. Як відзначає Микола Феоктистов, дане роз'яснення не відповідає на цілий ряд питань, наприклад: якщо нові дані створюються за рубежем і вони доступні користувачеві в Україні, те чи належні вони відразу реплікуватися в українську базу даних і яка відповідальність провайдеру в той період часу, поки ця реплікація відбувається?

Послуги хмарних обчислень – послуги з надання обчислювальних потужностей, включаючи технічні засоби й права використання програм для електронних обчислювальних машин з метою обробки й зберігання інформації органів державної влади, органів місцевого самоврядування, органів керування державними позабюджетними фондами з використанням технічних засобів, взаємодіючих через інформаційно-телекомунікаційні мережі.

Фактично в цьому визначенні хмарні сервіси розглядалися як послуги винятково для державних структур, тому після обговорення експертів згадування про органи державної влади й іже з ними було виключено (до слова, було подано всього одна пропозиція по внесенню зміни, текст якого, на жаль, недоступний; наскільки можна судити по приводяться адресам, що, електронної пошти, текст виправлень розсилався на експертизу в основному представникам бізнес-співтовариства): «Послуги хмарних обчислень – послуги з надання обчислювальних потужностей, включаючи технічні засоби й права використання програм для електронних обчислювальних машин з метою обробки й зберігання інформації з використанням технічних засобів, взаємодіючих через інформаційно-телекомунікаційні мережі».

Однак поточне формулювання як і раніше носить занадто загальний характер (наприклад, під дане визначення підходять послуги аутсорсингу обчислювальної інфраструктури, коли оператор не тільки обслуговує відомчу мережу, але й надає в оренду встаткування. Крім того, вона не відбиває специфіки хмарних сервісів: оперативне одержання послуг при мінімальній участі провайдеру, оплату за фактичне використання й інші особливості. Далі, не тільки не проводиться явного розходження між різними моделями надання хмарних сервісів («інфраструктура як сервіс» і «ПЗ як сервіс»), але вони фактично змішуються – «надання обчислювальних потужностей (IaaS), включаючи…права використання програм (SaaS)». (І нарешті, винятково редакторське зауваження – після «обчислювальних машин» необхідна кома, інакше виходить нелегкотравна фраза про «технічні засоби … з використанням технічних засобів».)

У виправленнях даються визначення не тільки хмарних сервісів, але також хмарної інфраструктури й постачальника послуг хмарних обчислень, які по суті носять тавтологічний характер: хмарна інфраструктура – це інфраструктура для надання хмарних сервісів. Втім, якщо підходити формально, з визначення не цілком ясно, чи входять у неї мережі доступу або тільки мережі усередині ЦОДа, оскільки передача інформації (надання її клієнтові) не згадується в числі операцій з даними: «хмарна інфраструктура – сукупність програмно-технічних засобів і інформаційно-телекомунікаційних мереж, що забезпечують обробку й зберігання інформації з метою надання послуг хмарних обчислень».

Як провайдери можуть виступати як юридичні особи, так і індивідуальні підприємці. До них пред'являються три основних вимоги: постачальник повинен забезпечити доступність інформації й програмного забезпечення, можливість обробки даних (включаючи повне видалення) і, нарешті, захист інформації (відповідно до вимог ст. 16 з 5-й частини закону про інформацію). Окремо обмовляється, що постачальник не має ніяких прав на інформацію (не є її власником). Здійснювати поставку хмарних послуг державним і муніципальним органам можуть тільки українські компанії (і навіть індивідуальні підприємці), а їхня хмарна інфраструктура повинна перебувати на території України. Провайдерам необхідно буде одержати акредитацію. Крім того, міністерство зобов'язане розробити вимоги до контрактів і договорів на надання хмарних послуг. Порядок надання послуг визначить уряд України.

Перший закон про хмари був прийнятий у Південній Кореї. Його повна назва – «Закон про розвиток хмарних обчислень і захисту користувачів» («Act on the Development of Cloud Computing and Protection of Users», скорочено – Korean Cloud Act). Держава зважилася на

дерегулювання галузі, оскільки Південна Корея була однієї з деяких країн, де суспільним інститутам заборонялася орендувати хмарні сервери в приватних провайдерів. Головною причиною заборони було побоювання щодо можливих погроз інформаційної безпеки, який, як виявляється з назви, у законі приділяється особлива увага.

На розробку й прийняття цього документа пішло біля півтора років (постанова уряду бути схвалено у вересні 2013 року, а закон прийнятий у березні 2015-го й набув чинності у вересні того ж року). Причому спочатку комітет з науці, ИКТ, майбутньому плануванню й комунікаціям не квапився з його розглядом, уважаючи більше важливим рішення інших завдань, зокрема прийняття закону про віщання.

Закон поширюється на всі суспільні інститути – центральний уряд, громадські організації, установи охорони здоров'я й утворення – і покликаний стимулювати першочергове використання хмарних сервісів для підвищення продуктивності й конкурентоспроможності.

Місцевий ринок хмарних обчислень відносно невеликий і нерозвинений у порівнянні з локальним IT-ринком, щодо цього він схожий з українським. По оцінках інституту економічних досліджень Digieco, в 2014 році його обсяг склав 863 млн доларів, що порівнянно з розміром українського хмарного ринку (до знецінення гривни). Як очікується, його щорічний ріст повинен скласти 30% за рахунок наступних мір:

– нарощування інвестицій у розвиток хмарного ринку й розширення підтримки, насамперед з боку уряду;

– дозвіл і заохочення повсюдного використання хмарних сервісів, включаючи публічні сервіси;

– введення мер по забезпеченню безпеки з боку провайдерів хмарних послуг.

Корейське Міністерство науки, IT і перспективного планування надає й ряд стимулюючих преференцій, адресованих насамперед невеликим розроблювачам хмарного програмного забезпечення: податкові відрахування й технічна допомога. Крім того, такі компанії одержать пріоритет при проведенні державних тендерів на реалізацію науково-дослідних проектів у сфері хмарних технологій.

Вся відповідальність за захист даних переноситься із клієнта на провайдеру хмарних сервісів. Як затверджується, це зроблено для того, щоб компаніям без досвіду роботи в IT не доводилося додатково витрачатися на безпеку, і тоді хмарні сервіси стануть для них більше привабливими. Власники даних повинні підписати угоду із провайдером і вказати, яка збережена в хмарі інформація може бути розкрита, а яка немає.

Спочатку передбачалося, що контроль за відповідністю вимогам безпеки стане здійснювати Національне агентство розвідки (НАР). Зокрема, провайдери повинні були б повідомляти НАР про всі інциденти безпеки із хмарними сервісами. Однак побоювання у відношенні того, що НАР одержить необмежений контроль за хмарними сервісами й персональними даними, привело до суспільних протестів, і ця стаття була вилучена з підсумкового тексту. Відповідно до закону про інциденти провайдер повинен повідомляти про підозрілі випадки в галузеве міністерство, і саме воно буде ініціювати перевірку.

Вимоги до хмарних провайдерів

При виборі провайдеру клієнти повинні з'ясувати його відповідність вимогам закону про хмари. Відповідно до нового південнокорейського законодавства, на провайдерів хмарних послуг покладає ряд зобов'язань:

– провайдер зобов'язаний повідомити про факт витоку інформації, якщо такий мав місце, своїм клієнтам і в профільне міністерство; останнє може провести розслідування інциденту;

– провайдер не повинен надавати приналежним клієнтам інформацію третій стороні або використовувати неї для інших, відмінних від застережених, цілей без згоди клієнта;

– провайдер повинен повернути або видалити дані клієнта після закінчення строку контракту про надання хмарних послуг;

– при розміщенні інформації за межами Південної Кореї клієнт може зажадати від провайдеру розкрити її місцезнаходження;

– якщо клієнт поніс втрати внаслідок навмисних дій провайдеру або через його недбалість і порушення закону про хмари, то клієнт може зажадати відшкодування від провайдеру, що повинен сам доводити свою невинність;

– підзаконними актами міністерства будуть деталізовані вимоги до якості/функціональності хмарних сервісів і належних рівнів обслуговування, а також стандарти для захисту інформації;

– крім цього, планується введення системи сертифікації хмарних сервісів і стандартизованих контрактів на використання хмарних сервісів.

У законі про хмари поки немає якої-небудь прив'язки до міжнародних стандартів. У ряді країн для оцінки провайдеру хмарних послуг регулювальні органи орієнтуються, наприклад, на рекомендації ISO/IEC 27001 і ISO/IEC 27018. Передбачені останнім інструменти контролю відповідають багатьом положенням південнокорейського закону (і навіть пред'являють більше тверді вимоги), тому в тих провайдерів, які вже забезпечили відповідність ISO/IEC 27018, не повинне виникати яких-небудь проблем з його виконанням.

Як сподіваються в Південній Кореї, прийняття цього закону, з одного боку, активізує розвиток суміжних галузей, а з іншої, буде мотивувати недержавні компанії до використання хмарних сервісів. Розвиток необхідної інфраструктури для надання хмарних сервісів повинне сприяти росту таких зв'язаних галузей, як телемедицина, фінансові послуги й Інтернет речей. А як показує досвід Китаю, що у цьому випадку є прикладом, впровадження хмарних послуг у державному секторі сприяє їхній популяризації в приватному секторі.

Розуміння основ комп’ютерної безпеки ще ніколи не було таким важливим. З огляду на те, що наше життя дедалі більше перебуває в Інтернеті, захист вашої особистої інформації є ключем до збереження вашої конфіденційності та запобігання крадіжці особистих даних.

Комп'ютерна безпека охоплює широкий спектр практик, протоколів і технологій, спрямованих на захист IT-систем від несанкціонованого доступу, витоків даних та кіберзагроз. Вона передбачає впровадження різних заходів безпеки, включаючи брандмауери, антивірусний захист, персональний брандмауер та інструменти шифрування, всі з яких розроблені для захисту конфіденційної інформації від зловмисників.

Перш ніж ми поговоримо про послуги комп’ютерної безпеки, давайте розглянемо визначення комп’ютерної безпеки. Комп’ютерна безпека включає захисні заходи та практики, які ви впроваджуєте для запобігання несанкціонованому доступу до IT-систем. Водночас вона забезпечує цілісність, конфіденційність та доступність ваших даних та цифрової інформації.

Якщо ви хочете досягти надійної комп'ютерної безпеки, потрібен багатогранний підхід, який включає різні компоненти. Зазвичай це включає шифрування даних для захисту конфіденційної інформації, гарантуючи, що навіть у разі перехоплення дані залишатимуться нечитабельними без відповідних ключів розшифрування. Стандарти шифрування також відіграють значну роль у забезпеченні безпеки ваших даних.

Контроль доступу є життєво важливим для обмеження дозволів користувачів та доступу до системи лише уповноваженими особами, тим самим мінімізуючи потенційні вразливості. Методи автентифікації, такі як захист паролем, біометричне сканування та багатофакторна автентифікація, забезпечують додаткові рівні безпеки, перевіряючи особу користувачів.

Разом ці елементи створюють комплексну систему, необхідну для захисту ваших цифрових активів від потенційних загроз та порушень.

Важливість комп'ютерної безпеки для захисту даних

Ефективні заходи захищають конфіденційну інформацію від таких загроз, як крадіжка особистих даних та витоки даних, зокрема тих, що виникають внаслідок підозрілих електронних листів.

У сучасному цифровому середовищі, де величезні обсяги особистої та фінансової інформації поширюються онлайн, наслідки недостатньої безпеки можуть бути руйнівними. Це може призвести не лише до фінансових втрат, але й до значного порушення довіри між користувачами. Ви повинні розуміти ризики, пов’язані із незахищеними системами, оскільки один недогляд може призвести до несанкціонованого доступу до особистих даних. Захистіть свої IT-системи від несанкціонованого доступу, застосовуючи надійні заходи безпеки.

Складний взаємозв'язок між комп'ютерною безпекою та конфіденційністю в Інтернеті стає дедалі важливішим, що підкреслює необхідність надійних захисних заходів.

Надаючи пріоритет безпеці, ви можете краще гарантувати конфіденційність своїх даних, тим самим зберігаючи свою конфіденційність в епоху кіберзагроз. Розгляньте можливість використання VPN для безпечного з’єднання Wi-Fi та уникнення публічних Wi-Fi, щоб покращити свою конфіденційність в Інтернеті.

Види загроз комп'ютерній безпеці та онлайн-загроз

Вам слід знати про різні типи загроз комп’ютерній безпеці, які становлять значні ризики для захисту даних. До них належать:

– кібератаки;

– фішингові атаки;

– шкідливе програмне забезпечення, що походить з підозрілих електронних листів.

Всі вони прагнуть використати вразливості в IT-системах, включаючи вразливості програмного забезпечення та програмне забезпечення сторонніх розробників.

Поширені загрози безпеці даних

Хочете знати, які поширені загрози безпеці даних? Ось огляд для вас: шкідливе програмне забезпечення, фішингові атаки та несанкціонований доступ – це вважаються поширеними загрозами безпеці даних.

Вони можуть призвести до серйозних наслідків, таких як крадіжка особистих даних та витік даних, які впливають як на організації, так і на окремих користувачів. Впровадження заходів безпеки програм та захисту електронної пошти може зменшити ці ризики.

Ці загрози діють за допомогою різних механізмів, спрямованих на вразливості в системах, мережах або поведінці людини. Наприклад, шкідливе програмне забезпечення може проникнути на пристрій користувача через заражені вкладення електронної пошти або завантаження шкідливого програмного забезпечення, зрештою компрометуючи конфіденційну інформацію. Фішингові атаки часто маскуються під законні повідомлення, обманом змушуючи людей розкривати особисті дані або облікові дані для входу. Несанкціонований доступ зазвичай передбачає використання слабких паролів або застарілих заходів безпеки, що дозволяє кіберзлочинцям порушувати бази даних та витягувати конфіденційні дані.

Реальні приклади, такі як витік даних Equifax та злом мережі Sony PlayStation Network, підкреслюють руйнівний вплив цих загроз безпеці – не лише на постраждалі організації, але й на мільйони людей, чиї дані можуть бути використані неналежним чином.

Розуміння кібератак

Кібератаки – це зловмисні спроби порушення безпеки IT-систем та мереж з метою отримання доступу, викрадення або маніпулювання конфіденційними даними. Такі порушення можуть призвести до серйозних наслідків як для окремих осіб, так і для організацій, включаючи проблеми з безпекою обладнання.

Ці загрози можуть виникати з різних мотивів, включаючи фінансову вигоду, політичні цілі або особисту помсту. Кіберзлочинці використовують низку методів, таких як фішингові електронні листи, програми-вимагачі та розподілені атаки типу «відмова в обслуговуванні» (DDoS), для використання вразливостей у системах та IT-обладнанні.

Гучні інциденти, такі як витік даних Equifax у 2017 році та атака програм-вимагача WannaCry, служать яскравим нагадуванням про руйнівний вплив, який ці порушення можуть мати на конфіденційність, фінансову стабільність, цілісність організації та IT-системи.

Щоб зменшити ці ризики, як підприємства, так і приватні особи повинні впроваджувати надійні заходи безпеки. Регулярні оновлення програмного забезпечення, навчання співробітників та передові системи виявлення загроз можуть значно посилити захист від постійно мінливого ландшафту кіберзагроз. Розгляньте можливість звернутися за порадою до споживачів з авторитетних джерел, таких як PCMag, Wired та The Guardian, щоб дізнатися про найновіші методи безпеки.

Найкращі практики для комп'ютерної безпеки

Щоб захистити вашу конфіденційну інформацію та зменшити ризики, пов’язані з кіберзагрозами, впровадження найкращих практик комп’ютерної безпеки може допомогти вашій організації.

Надаючи пріоритет наступним практикам, ви можете покращити загальний рівень безпеки та захистити критично важливі дані від потенційних вразливостей.

1. Впровадження надійних паролів та автентифікації

Номер один: впровадження надійних паролів та багатофакторної автентифікації – це фундаментальний крок у захисті даних, який значно знижує ризик несанкціонованого доступу до конфіденційної інформації та IT-систем. Уникайте використання особистої інформації у своїх паролях та будьте обережні з підозрілими електронними листами із запитом на введення облікових даних.

Вживаючи цих заходів безпеки, ви можете створити надійну лінію захисту від кіберзагроз. Надійний пароль повинен складатися з комбінації великих і малих літер, цифр і спеціальних символів, в ідеалі довжина пароля повинна перевищувати 12 символів. Ця складність ускладнює для зловмисників злом паролів методами грубої сили. Не поширюйте свої паролі через незахищені канали, такі як демонстрація екрана або публічні Wi-Fi.

Багатофакторна автентифікація забезпечує додатковий рівень безпеки, вимагаючи від вас підтвердження вашої особи за допомогою другого засобу, такого як код текстового повідомлення або додаток для автентифікації. Такий підхід суттєво мінімізує ймовірність несанкціонованого доступу, навіть якщо паролі скомпрометовані, особливо у віддаленому місці.

Найкращі практики також включають регулярне оновлення паролів та використання менеджера паролів для безпечного зберігання, що ще більше покращує загальну гігієну ваших паролів. Переконайтеся, що ваш менеджер паролів захищений надійними стандартами шифрування.

2. Регулярні оновлення програмного забезпечення та управління патчами

Звичайно, всі ми знаємо, що нам слід регулярно оновлювати наші пристрої, але це особливо важливо для безпеки даних. Регулярні оновлення програмного забезпечення та ефективне управління виправленнями допомагають вашій організації усунути вразливості безпеки, які кіберзлочинці часто використовують для отримання несанкціонованого доступу до IT-систем та конфіденційних даних. Це включає забезпечення актуальності програмного забезпечення сторонніх розробників для запобігання зловживанням.

Слідкування за цими оновленнями не лише зміцнює ваш захист від потенційних порушень, але й підвищує загальну продуктивність і надійність системи. В епоху, коли витоки даних стають дедалі поширенішими, важливість управління виправленнями важко переоцінити.

Правильно впроваджені оновлення знижують ризик експлуатації, усуваючи лазівки, якими можуть скористатися кіберзлочинці. Найкращі практики включають встановлення послідовного графіка оновлень, визначення пріоритетів критичних виправлень на основі оцінки ризиків та використання інструментів автоматизації, коли це можливо, для оптимізації процесу. Організації також повинні впроваджувати налаштування конфіденційності для контролю доступу до конфіденційної інформації.

Крім того, організації отримують користь від навчання персоналу важливості обслуговування програмного забезпечення, сприяючи колективному зобов'язанню щодо

захисту конфіденційної інформації. Такі ресурси, як програми навчання з безпеки від Microsoft, можуть бути безцінними в цьому відношенні.

3. Стратегії резервного копіювання даних

Впровадження ефективних стратегій резервного копіювання даних допомагає запобігти втраті даних через кібератак, збої обладнання або випадкове видалення. Це гарантує, що ваша цінна інформація залишатиметься доступною та безпечною протягом усього її життєвого циклу. Розгляньте можливість використання хмарного резервного копіювання та регулярного тестування резервних даних, щоб забезпечити їх цілісність.

Існує кілька методів резервного копіювання, які варто розглянути, зокрема хмарні резервні копії, які забезпечують можливості зберігання даних поза офісом та автоматичну синхронізацію. Крім того, ви можете вибрати знімні варіанти сховища, такі як зовнішні жорсткі диски або USB-флеш-накопичувачі, для локального зберігання даних. Також доцільно регулярно створювати резервні копії даних для захисту від потенційних випадків витоку даних.

Регулярне резервне копіювання не лише захищає вас від непередбачених катастроф, але й відіграє життєво важливу роль у підтримці цілісності даних та забезпеченні їхнього захисту з часом.

Щоб створити надійну стратегію резервного копіювання, важливо встановити графік резервного копіювання, який відповідає частоті оновлення ваших даних, використовувати шифрування для будь-якої конфіденційної інформації та регулярно тестувати процеси відновлення, щоб переконатися, що все працює безперебійно, коли це необхідно. Використовуйте інструменти шифрування для ефективного захисту ваших даних.

Застосовуючи ці методи, ви можете ефективно захистити свої дані від різноманітних загроз та досягти спокою. Розгляньте можливість інтеграції багатофакторної автентифікації для подальшого підвищення безпеки ваших IT-систем.

Захист даних у різних середовищах

Мобільні пристрої, віддалені місця та загальнодоступні мережі Wi-Fi – дані потребують захисту в різних середовищах. Тому вам потрібно впровадити індивідуальні заходи безпеки.

Такий підхід є важливим для збереження цілісності та конфіденційності конфіденційної інформації. Переконайтеся, що IT-обладнання захищене, а параметри конфіденційності в Інтернеті налаштовані належним чином.

Захист даних на мобільних пристроях

Мобільні пристрої часто стають мішенями для кіберзагроз, включаючи шкідливе програмне забезпечення та несанкціонований доступ, через їхню портативність та зручність підключення. Використання рішень мобільної безпеки може значно підвищити безпеку пристроїв.

Впровадження надійних методів, таких як шифрування, допомагає захистити конфіденційну інформацію, навіть якщо пристрій скомпрометовано. Контроль доступу діє як перша лінія захисту, обмежуючи тих, хто може переглядати дані або взаємодіяти з ними. Використання програм безпеки, які забезпечують виявлення загроз у режимі реального часу, може ще більше посилити цей захисний рівень, а впровадження антивірусного захисту може запобігти кібератакам.

Однак, самих лише технологій недостатньо; підвищення обізнаності користувачів щодо розпізнавання потенційних загроз, таких як фішингові атаки, підозрілі завантаження або підозрілі електронні листи, є надзвичайно важливим. Застосовуючи проактивний підхід та навчаючи користувачів, організації можуть значно посилити свою мобільну безпеку, гарантуючи безпеку даних у швидкозмінному цифровому середовищі.

Захист даних під час віддаленої роботи

Віддалена робота означає доступ до конфіденційної інформації через загальнодоступні мережі Wi-Fi або незахищені мережі, оскільки ці середовища створюють

унікальні проблеми безпеки. Захист даних у такому середовищі має бути головним пріоритетом.

Для ефективного захисту конфіденційних даних важливо використовувати віртуальну приватну мережу (VPN). VPN шифрує ваше інтернет-з'єднання, значно знижуючи ризик перехоплення кіберзлочинцями. Розгляньте можливість використання особистої точки доступу як альтернативи публічному Wi-Fi для безпечнішого з'єднання Wi-Fi.

Крім того, переконайтеся, що ваші з'єднання захищені, використовуючи надійні паролі та двофакторну автентифікацію, коли це можливо. Також важливо оновлювати антивірусне програмне забезпечення та брандмауери, оскільки ці заходи додатково захищають ваші пристрої від потенційних загроз.

Регулярний перегляд та зміна налаштувань безпеки на ваших особистих пристроях допоможе створити безпечніше середовище для віддаленої роботи, захищаючи від несанкціонованого доступу та витоків даних.

Забезпечення безпеки хмарного сховища

Забезпечення безпеки хмарного сховища вимагає впровадження надійних заходів, таких як шифрування та контроль доступу, для захисту конфіденційних даних від несанкціонованого доступу та порушень. Розгляньте можливість використання стандартів шифрування та регулярного оновлення налаштувань конфіденційності для підтримки безпеки даних.

У сучасному цифровому середовищі, де витоки даних стають все більш поширеними, вкрай важливо застосовувати проактивний підхід до захисту хмарного сховища. Організації повинні усвідомлювати, що хоча хмарні рішення пропонують значні переваги, вони також несуть низку потенційних ризиків, включаючи втрату даних та викрадення облікових записів.

Використовуючи найкращі практики, такі як надійні методи шифрування, для захисту даних як під час зберігання, так і під час передачі, компанії можуть значно зменшити ймовірність компрометації своєї інформації. Регулярні аудити безпеки мають вирішальне значення для виявлення вразливостей та забезпечення актуальності протоколів безпеки.

Розуміння цих стратегій може значно покращити загальний рівень безпеки та вселити користувачам впевненість у безпеці їхніх цінних даних.

Технології безпеки даних

Технології безпеки даних допомагають вам у боротьбі з кіберзагрозами, надаючи низку методів захисту конфіденційної інформації та забезпечення цілісності ваших IT-систем.

1. Методи шифрування

Методи шифрування пропонують критично важливий рівень безпеки, який захищає цифрову інформацію від несанкціонованого доступу та витоків даних.

Ці методи шифрують конфіденційні дані як під час передачі, так і в стані спокою, гарантуючи, що лише уповноважені особи можуть розшифрувати інформацію та отримати до неї доступ. З огляду на зростаючу залежність від цифрових платформ для особистих та ділових транзакцій, важливість надійних методів шифрування неможливо переоцінити.

Такі інструменти, як AES (Advanced Encryption Standard) та RSA (Rivest-Shamir-Adleman), широко використовуються завдяки своїй ефективності у підтримці цілісності даних.

Застосовуючи передові практики, такі як регулярне оновлення ключів шифрування та впровадження багатофакторної автентифікації, ви можете ще більше покращити свої заходи безпеки. У швидкозмінному цифровому середовищі інформування про нові технології шифрування є критично важливим для будь-якої організації, яка прагне захистити цінні дані від потенційних загроз.

2. Брандмауери та антивірусне програмне забезпечення

Брандмауери та антивірусне програмне забезпечення є критично важливими компонентами захисту даних, що слугують першою лінією захисту від шкідливого

програмного забезпечення та несанкціонованого доступу у ваших IT-системах. Впровадження захисту брандмауером може допомогти запобігти несанкціонованому доступу до вашої мережі.

Ці інструменти безпеки працюють шляхом моніторингу та контролю вхідного та вихідного мережевого трафіку, ефективно створюючи бар'єр між вашими довіреними внутрішніми мережами та ненадійними зовнішніми. Брандмауери ретельно перевіряють пакети даних і можуть блокувати потенційні загрози, перш ніж вони досягнуть ваших пристроїв, тоді як антивірусне програмне забезпечення виявляє, поміщає в карантин та видаляє шкідливі програми. Разом вони створюють надійну систему, яка захищає конфіденційну інформацію та забезпечує цілісність системи. Регулярний перегляд та оновлення налаштувань безпеки має вирішальне значення для підтримки ефективної безпеки мережі.

У швидкозмінному кіберсередовищі важливо регулярно оновлювати як брандмауери, так і антивірусні рішення. Таке обслуговування не лише забезпечує їх найновішими визначеннями загроз, але й підвищує їхню здатність боротися з новими вразливостями, що підкреслює важливість проактивних стратегій кіберзахисту.

3. Інструменти запобігання втраті даних

Інструменти запобігання втраті даних (DLP) є важливими для захисту конфіденційної інформації шляхом моніторингу та контролю передачі даних, що ефективно мінімізує ризик несанкціонованого доступу та витоків даних. Використання методів управління даними разом з інструментами DLP може ще більше покращити захист цифрової інформації.

У сучасному цифровому середовищі, де кіберзагрози стають дедалі складнішими та поширенішими, ці інструменти стають ще більш важливими. Рішення DLP працюють, використовуючи комбінацію методів, включаючи перевірку контенту, контекстний аналіз та поведінкову аналітику, для виявлення та захисту конфіденційних даних на різних платформах. Регулярне навчання заходам безпеки та навчання співробітників з безпеки можуть допомогти розпізнати та пом'якшити загрози.

Організації зазвичай впроваджують стратегії, що включають шифрування конфіденційної інформації, забезпечення суворого контролю доступу та навчання співробітників найкращим практикам захисту даних. Вживаючи цих заходів, ви не лише покращуєте загальний рівень безпеки, але й забезпечуєте дотримання правил, зрештою будуючи довіру з клієнтами та зацікавленими сторонами. Регулярні оновлення програмного забезпечення сторонніх розробників можуть допомогти мінімізувати вразливості програмного забезпечення, які можуть бути використані.

Відповідність нормативним вимогам та безпека даних

Дотримання нормативних вимог є вирішальним аспектом безпеки даних для вашої організації. Важливо дотримуватися різних правил захисту даних, таких як GDPR та CCPA, щоб захистити конфіденційну інформацію та зберегти довіру ваших клієнтів. Регулярне оновлення налаштувань конфіденційності даних допоможе забезпечити дотримання вимог.

Огляд правил захисту даних (GDPR, CCPA тощо)

Нормативні акти щодо захисту даних, такі як GDPR та CCPA, забезпечують важливі рамки, яких ви повинні дотримуватися, щоб забезпечити відповідність вашим практикам безпеки даних та захистити особисту інформацію людей.

Ці правила спрямовані на створення балансу між правами осіб контролювати свою особисту інформацію та вашими обов’язками як організації щодо відповідального управління цими даними. Наприклад, GDPR наголошує на суворих вимогах щодо згоди та вимагає розробки чітких протоколів обробки даних, що включає забезпечення прозорості щодо використання даних та забезпечення прав осіб на доступ до своєї особистої інформації або її видалення. Аналогічно, CCPA надає жителям Каліфорнії право знати, які персональні дані збираються та передаються, тим самим розширюючи їхню автономію щодо особистої інформації.

Наслідки цих правил виходять за рамки простого дотримання; недотримання може призвести до значних фінансових штрафів та шкоди репутації. Це підкреслює критичну важливість впровадження надійних стратегій захисту даних у вашій організації.

Організаційні обов'язки щодо безпеки даних

Організації несуть значну відповідальність за безпеку даних, що включає впровадження ефективних стратегій кібербезпеки, забезпечення дотримання нормативних актів та захист конфіденційної інформації. Поради організацій, що надають консультації споживачам, таких як Національний центр кібербезпеки (NCSC), можуть бути безцінними в цьому відношенні.

Щоб ефективно захистити дані, ви повинні застосовувати проактивний підхід, усвідомлюючи, що цифровий ландшафт постійно розвивається та створює нові загрози. Це вимагає регулярної оцінки та оновлення ваших протоколів кібербезпеки для захисту від потенційних порушень та атак шкідливого програмного забезпечення. Дотримання законів про захист даних, таких як GDPR або CCPA, має вирішальне значення для підтримки довіри клієнтів та уникнення значних штрафів.

Також важливо брати участь у програмах навчання та підвищення обізнаності співробітників, оскільки співробітники часто виступають першою лінією захисту від кібератак. Інтегруючи ці заходи, організації можуть створити надійну систему безпеки, яка не лише захищає дані, але й сприяє культурі безпеки та відповідальності.

Реагування на інциденти та відновлення після них

Реагування на інциденти та відновлення є важливими процесами в управлінні порушеннями даних та забезпеченні стійкості організації до кіберзагроз. Ці процеси спрямовані на відновлення нормальної роботи, одночасно захищаючи конфіденційну інформацію.

Дії, які слід вжити після витоку даних

Після витоку даних організаціям вкрай важливо вжити негайних заходів для зменшення збитків, оцінки наслідків та ініціювання процесів відновлення для захисту конфіденційної інформації та відновлення довіри.

Це передбачає швидке стримування порушення для запобігання будь-якому подальшому несанкціонованому доступу, а потім ретельне розслідування для розуміння масштабів порушення та виявлення вразливостей, які були використані. Після завершення розслідування важливо повідомити про інцидент постраждалі сторони, регуляторні органи та зацікавлені сторони, оскільки прозорість має вирішальне значення для підтримки довіри.

Зусилля з відновлення повинні бути зосереджені на відновленні систем та впровадженні заходів для запобігання повторенню. Проведення оцінки після інциденту є життєво важливим для вдосконалення протоколів безпеки, забезпечення того, щоб отриманий досвід спонукав до оновлення існуючих захисних механізмів, та підвищення загальної стійкості організації до майбутніх загроз.

Відновлення даних та систем

Відновлення даних і систем після порушення є критично важливим компонентом процесу реагування на інциденти, що гарантує, що ваша організація може відновити втрачені дані та підтримувати безпеку своєї IT-інфраструктури.

Цей процес не лише спрямований на відновлення скомпрометованої інформації, але й наголошує на впровадженні надійних заходів безпеки для запобігання майбутнім інцидентам. Організації часто покладаються на резервні дані як фундаментальний елемент своєї стратегії відновлення, що дозволяє швидко відновити роботу, мінімізуючи час простою.

Ефективне відновлення вимагає поєднання регулярного резервного копіювання даних, впровадження посилених протоколів безпеки та постійного навчання персоналу розпізнаванню потенційних загроз. Постійне вдосконалення є важливим; воно спонукає організації вдосконалювати свої системи, оцінювати вразливості та інтегрувати найновіші технологічні оновлення та виправлення.

Застосовуючи проактивний підхід до кібербезпеки, ваша організація може краще захистити критично важливі дані та підвищити загальну стійкість системи.

На рисунку 1 зображена структурна схема роботи системи. Схема розділена на три основних компоненти:

– Flash накопичувач;
– розроблена програма;
– користувач.

Коли користувач вставляє в персональний комп'ютер Flash накопичувач, відбувається розпізнання операційною системою типу пристрою й виводу меню вироблених дій.

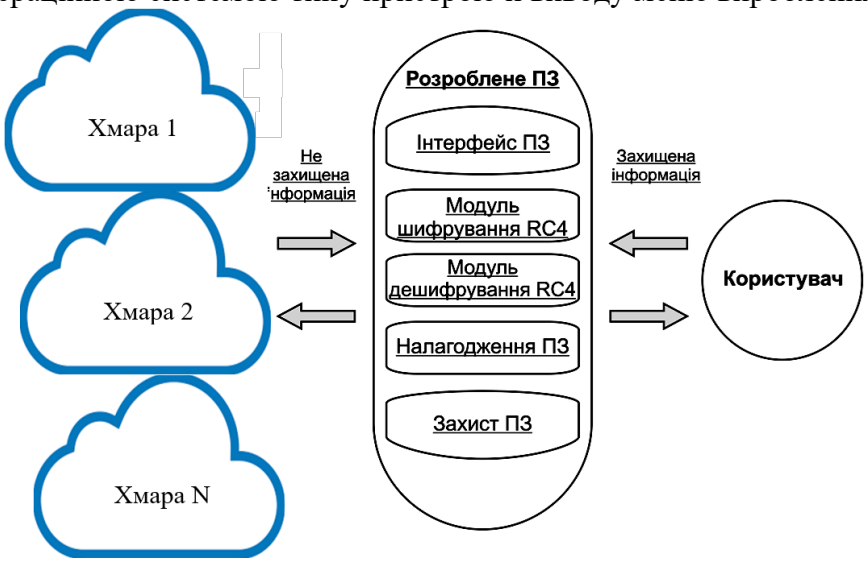

Рисунок 1 – Структурна схема роботи системи

Розроблена програма перехоплює системне повідомлення операційній системі про виклик меню вироблених дій над Flash накопичувачем і активізує власний інтерфейс програми.

Розроблена програма складається з декількох частин:

– інтерфейсу програми;
– модуля потокового шифрування RC4;
– модуля потокового дешифрування RC4;
– налаштування програми й захисту програми.

Розроблена програма управляє процесом обміну інформацією між Flash накопичувачем і персональним комп'ютером, використовуючи потоковий алгоритм шифрування інформації RC4. Завдяки такому підходу, можливо використовувати всі існуючі на даний момент Flash накопичувачі не зупиняючись на окремих реалізаціях з підвищеними вимогами захищеності Flash накопичувача (рисунок 1).

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту персональних даних у мережевих Cloud-системах. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем захисту персональних даних у мережевих Cloud-системах.
– Досліджена система захисту персональних даних у мережевих Cloud-системах.
– На основі отриманих результатів досліджень створена програмна реалізація системи захисту персональних даних у мережевих Cloud-системах. Розроблені алгоритми дозволяють успішно вирішувати завдання захисту персональних даних у мережевих Cloud-системах. 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. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025
2. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
3. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
4. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
5. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
6. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
7. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
8. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
9. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
10. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
12. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
13. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
14. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56
16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
17. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
18. 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.
19. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
20. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.

21. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
22. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
23. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
24. 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,
25. 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.
26. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
27. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
28. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
29. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
30. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
31. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
32. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.