розширити вибір видів праці, а також є варіантом для більшої «легалізації» роботи працівників, як наприклад, ІТ-сфера, де виконуються короткострокові проєкти та завдання.

Список використаних джерел:
1. Кодекс законів про працю України : Закон від 10.12.1971 №322-VIII (редакція станом на 01.10.2023) URL: https://zakon.rada.gov.ua/laws/show/322-08#n123
2. Трудові договори з нефіксованим робочим часом: порівняння міжнародного й українського досвіду URL: https://www.kadrovik.ua/content/trudovi-dogovory-z-nefiksovanym-robochym-chasom-porivnyannya-mizhnarodnogo-j-ukrayinskogo-dosvidu

ПРАВОВІ МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ

СТЕФАНИКА Марія Сергіївна
здобувач вищої освіти
Харківський національний університет
міського господарства імені О.М. Бекетова

Тема механізму захисту інформації надзвичайно актуальна в сучасному світі, оскільки ми переживаємо епоху цифрової трансформації. Інформація є ключовим ресурсом для багатьох організацій і особистих користувачів, і її безпека стає основною проблемою.

Окрім того, зростає загроза з боку кіберзлочинців, які постійно вдосконалюють свої методи атак і намагаються знайти слабкі місця в системах захисту. Також існує ризик внутрішніх загроз, пов'язаних з недбалістю співробітників або недостатньою освітою з питань кібербезпеки.

Існує велика кількість механізмів для захисту інформації таких як: конфіденційність, цілісність, доступність, ідентифікація і аутентифікація, авторизація, шифрування, захист від зловмисних програм, фізична безпека, аудит і моніторинг, резервне збереження і відновлення, постійне вдосконалення.

Основним аспектом механізму захисту інформації є забезпечення конфіденційності, що означає, що інформація повинна бути доступною лише для авторизованих користувачів і має захищатися від несанкціонованого перегляду, копіювання або зміни. Це передбачає використання різних технічних та організаційних засобів, а також встановлення чітких політик та процедур для забезпечення приватності та обмеження доступу до конфіденційної інформації лише тим, хто має відповідні права і дозволи.

Захист інформації означає гарантування її непорушеної цілісності, що інформація залишається без змін та недоторканою, і будь-які можливі зміни чи пошкодження мають бути попереджені та виявлені тільки з відповідними дозволами. Це досягається за допомогою різних технічних засобів та

механізмів контролю, які усувають можливість незаконних втручань та порушень цілісності інформації.

Доступність інформації означає, що коректні користувачі повинні мати можливість отримувати необхідну інформацію в потрібний момент без зайвих перешкод чи запізнень, щоб забезпечити продуктивну та безперебійну діяльність організації.

Важливою частиною механізму захисту інформації є визначення особистості користувачів та перевірка їхнього права на доступ до інформації перед наданням цього доступу. Це процес ідентифікації і аутентифікації, який гарантує, що лише правомірні особи отримують доступ до конфіденційної інформації.

Наданням користувачам конкретних прав доступу, які обмежують їх здатність взаємодіяти з інформацією відповідно до їхніх повноважень та потреб є авторизація. Це гарантує, що кожен користувач має лише обмежений доступ до інформації, який відповідає його ролі.

Застосування шифрування з метою приховування та захисту інформації від несанкціонованого доступу та потенційних змін. Цей процес перетворює дані в формат, який стає нерозбірливим без відповідного ключа або паролю, забезпечуючи конфіденційність та цілісність інформації.

Захистом від зловмисних програм називають стратегію забезпечення безпеки інформації шляхом запобігання потенційним загрозам та мінімізації можливої шкоди. Однією із місій є впровадження превентивних та заходів виявлення для уникнення і своєчасного реагування на шкідливі програми, включаючи віруси, шпигунське програмне забезпечення та зловмисні додатки.

Одним із визначальних компонентів механізму захисту інформації є його фізична безпека, завданням якої є забезпечення безпечної та контрольованої охорони серверних приміщень та інших ресурсів, де зберігається чи оброблюється інформація. Це включає в себе застосування фізичних заходів безпеки, таких як контроль доступу та нагляд за об'єктами для уникнення несанкціонованого доступу до важливих областей.

Важливим пунктом захисту інформації є аудит і моніторинг. Він включає в себе регулярний контроль та документування подій та активності з метою виявлення можливих загроз і реагування на інциденти. Ця процедура сприяє вчасному виявленню аномалій і допомагає забезпечити безпеку системи інформації.

Ще однією ланкою в механізмі захисту інформації є резервне збереження і відновлення, яке забезпечує проведення систематичного створення резервних копій та створення можливості для відновлення даних у випадку аварій та надзвичайних ситуацій. Цей процес дозволяє інформації залишається доступною та не пошкодженою навіть в екстремальних ситуаціях, забезпечуючи надійність інформаційних ресурсів під час кризових подій.

Дотримання вимог і стандартів інформаційної безпеки та відповідність законодавству є невід'ємною частиною механізму захисту інформації. Це означає, що організації та індивіди повинні не лише встановлювати та

впроваджувати технічні та організаційні заходи для захисту інформації, але також повинні бути у відповідності до чинного законодавства та стандартів безпеки даних. Дотримання цих правил і норм гарантує надійність заходів безпеки та сприяє зменшенню ризику порушення безпеки даних та відповідних правових наслідків.

Останнім сегментом механізму захисту інформації є постійне вдосконалення. Ця практика передбачає систематичне оновлення та вдосконалення заходів безпеки, з метою відповіді на постійно змінні виклики та потенційні загрози в інформаційному середовищі. Це гарантує, що механізм захисту інформації завжди залишається ефективним і надійним, забезпечуючи високий рівень безпеки в умовах швидкого розвитку технологій та загроз.

Таким чином, питання механізму захисту інформації є актуальними у сучасному цифровому світі. Забезпечення безпеки інформації, яка є цінним активом, вимагає постійної уваги та вжиття відповідних заходів. Зростання обсягу даних, наявність кіберзагроз, суворі законодавчі вимоги та залежність від технологій підкреслюють необхідність ефективних засобів захисту. Забезпечення конфіденційності, цілісності та доступності інформації є важливим завданням як для організацій, так і для окремих користувачів. Розуміння цих аспектів має критичне значення для забезпечення безпеки даних в світі, де інформація вважається найціннішим ресурсом.

Список використаних джерел:

1.Технології захисту інформації. Ужгородський національний університет. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186 (дата звернення: 16.10.2023).

2.Ткачук Н. Правовий механізм захисту інформаційних прав та свобод людини і громадянина в Україні url: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/34761/1/ПРАВОВИЙ%20МЕХАНІЗМ%20ЗАХИСТУ.pdf (дата звернення: 16.10.2023).

СОЦІАЛЬНО-ПРАВОВІ АСПЕКТИ БОРОТЬБИ ІЗ ЗАБРУДНЕННЯМ ПРИРОДНИХ ОБ'ЄКТІВ ВІДХОДАМИ

ШПАКОВА Ірина Михайлівна,
здобувач вищої освіти
Харківський національний університет
міського господарства імені О. М. Бекетова

Забруднення навколишнього природного середовища є світовою проблемою, що з кожним роком набуває все більшої актуальності. Щороку кількість відходів зростає, а найбільш розповсюдженим способом їх утилізації є їх захоронення. Переповнення полігонів та відсутність розвиненої інфраструктури для переробки відходів зумовлює їх накопичення в лісах та водних об'єктах. Проблема забруднення навколишнього середовища