КОМП'ЮТЕРНІ НАУКИ

DOI: 10.32782/2220-8674-2024-24-2-26
УДК 004.056

Д. В. Лубко, к.т.н., ORCID: 0000-0002-2506-4145
М. Ю. Мірошниченко, к.т.н, ORCID: 0000-0003-4596-3110
Таврійський державний агротехнологічний університет імені Дмитра Моторного
e-mail: di75ma@gmail.com

МЕХАНІЗМИ БЕЗПЕКИ ІНФОРМАЦІЇ ТА ЇХ ВИКЛИКИ

Анотація. Метою статті є розгляд механізмів безпеки інформації та їх викликів, а також розглянути програми безпеки та вимоги до захисту інформації. Механізми безпеки інформації – це різні заходи, що мають захищати дані від несанкціонованого доступу, модифікації, розголошення чи знищення. Вони грають ключову роль у запобіганні витоку чи пошкодженню даних, що може призвести до фінансових втрат чи порушень конфіденційності. Шифрування, аутентифікація та контроль доступу - основні засоби безпеки, що допомагають у захисті інформації. Організації повинні розробляти та підтримувати ці механізми, а також постійно вдосконалювати свої системи з урахуванням нових викликів, таких як швидкий розвиток технологій та збільшення кіберзагроз.

Ключові слова: механізми безпеки інформації, шифрування даних, безпека, аутентифікація та авторизація, захист від кібератак, контроль та моніторинг.

Постановка проблеми. В сучасному світі інформація – це скарб, що визначає багато напрямків. Вона не лише допомагає в прийнятті рішень та розвитку бізнесу, а й може бути предметом зловживань. Саме тому забезпечення безпеки даних стало критичним для будь-якої організації, незалежно від її розміру чи сфери діяльності. Безпека даних – це не лише обмеження доступу, а й гарантія конфіденційності, цілісності та доступності інформації. Конфіденційність стає гарантом того, що доступ до даних мають лише уповноважені особи. Цілісність забезпечує, що інформація залишається незмінною та не пошкодженою. А доступність – це забезпечення доступу до інформації в потрібний момент. Існує безліч загроз, що стоять перед безпекою даних: від природних катастроф до кібератак та знехтування правилами безпеки. Для запобігання цим проблемам використовують різноманітні механізми захисту, такі як шифрування, аутентифікація, контроль доступу, фізичний захист, моніторинг та аналіз безпеки, стратегії резервного копіювання та відновлення даних, а також відповідність стандартам та вимогам щодо захисту інформації.

Аналіз останніх досліджень. Області інформаційної безпеки виділяють кілька класів безпеки, які використовуються для класифікації даних та систем відповідно до їхньої важливості та чутливості. Ці класи безпеки допомагають організаціям розробляти та впроваджувати ефективні заходи безпеки для захисту своїх даних. Нажаль кількість кібер-злочинів росте з кожним днем, велика частка цих злочинів це крадіжка особистих даних. Частіше всього це стається через халатність та необізнаність користувачів. Саме тому все це і є проблемою, яку потрібно вирішувати як особисто там і колективно.

Як показує проведений аналіз останніх досліджень і публікацій з даної проблемної області (з виявлення механізмів безпеки, з питань захисту інформації та даних, питань інформаційної безпеки, питань безпеки, тощо) багато вчених та науковців активно працювали в цьому. А саме, це такі фахівці та науковці як: Пархуць Ю.Л. [1], Михайлов А.О. [2], Шевчук Д.Т. [3], Скрипка М.В. [4], Тівецька А.В. [5], Говорущенко Т.О. [5], Олешко І.В. [6], Шевченко С. [7], Близнюк І. [8], Легка О.В. [10], Чунарьова А. [11], Шемет А. [12], Федоренко Р.М. [13], Оксіюк О.Г. [14], Зінченко Д.А. [15], Думанська Н.О. [16].

Закордоні вчені також активно долучаються до аналізу даної предметної області та багато вже чого зробили, а саме це: Michaelsen J.R. [18], Grossman J. [19], Michael Whitman [22], Herbert Mattord [22], Smieliauskas W. [23], Cardwell Kevin [24], Porter B. [25], Hatherly D. [25], Jason A. [26], Jason A. [27], Shanon C.E. [28].

Також всі ці питання та вирішення даної проблематики періодично висвітлюють і викладачі ТДАТУ, такі як Шаров С.В. [17], Мірошниченко М.Ю. [29] та Лубко Д.В [17, 29].

Незважаючи на велику кількість праць та досліджень у цій сфері, недостатньо висвітлено ще багато аспектів питань забезпечення інформаційної безпеки та захисту даних.

Формулювання мети статті. Розглянути механізми безпеки інформації та їх виклики, а також розглянути програми безпеки та вимоги до захисту інформації.

Основна частина. Шифрування даних – це ключовий механізм безпеки, що забезпечує конфіденційність та захист інформації під час передачі чи зберігання. В сучасному цифровому світі, де обмін даними відбувається безперервно, шифрування виступає як надійний щит, що захищає від несанкціонованого доступу та можливих загроз. Шифрування забезпечує те, що дані перетинають мережі та зберігаються у вигляді незрозумілого тексту для всіх, крім тих, кому призначено розшифрувати їх [16, с. 23]. Це забезпечується за допомогою спеціальних алгоритмів, які перетворюють звичайний текст у незрозумілий шифрований вигляд, який може бути

розкодований лише з допомогою відповідного ключа. Існує два основних типи шифрування: симетричне та асиметричне. Симетричне шифрування використовує один і той же ключ для шифрування та дешифрування даних. Ключ шифрування відомий лише авторизованим користувачам. Асиметричне шифрування, ж використовує два ключі: ключ шифрування та ключ дешифрування. Ключ шифрування відомий будь-кому, а ключ дешифрування відомий лише авторизованим користувачам. Існує багато різних алгоритмів шифрування, які використовуються для різних цілей.

Деякі з найпоширеніших алгоритмів шифрування включають:

1. DES (Data Encryption Standard) - це алгоритм симетричного шифрування, який був розроблений Національною лабораторією Лоуренса Лівермора в США. DES був широко використовуваний у минулому, але він вважається застарілим.
2. AES (Advanced Encryption Standard) - це алгоритм симетричного шифрування, який був розроблений Національним інститутом стандартів і технологій (NIST) США. AES є найпоширенішим алгоритмом шифрування в даний час.
3. RSA (Rivest-Shamir-Adleman) - це алгоритм асиметричного шифрування, який був розроблений Роєм Ривестом, Аді Шаміром і Леонардом Адлеманом. RSA є одним із найнадійніших алгоритмів шифрування, який використовується в даний час.

Шифрування даних використовується для захисту різноманітних типів даних, включаючи:

1. Шифрування електронної пошти може використовуватися для захисту конфіденційних повідомлень від несанкціонованого доступу;
2. Шифрування файлів може використовуватися для захисту даних, які зберігаються на комп'ютері, від крадіжки або розголошення;
3. Шифрування баз даних може використовуватися для захисту даних, які зберігаються в базі даних, від несанкціонованого доступу або зміни;
4. Шифрування мережевих повідомлень може використовуватися для захисту конфіденційних даних, які передаються через мережу, наприклад, даних електронної комерції.

Для використання шифрування даних необхідно мати програмне забезпечення або обладнання, яке підтримує шифрування. Існує багато різних програмних продуктів і пристроїв, які підтримують шифрування даних. Для шифрування даних за допомогою програмного забезпечення необхідно створити ключ шифрування. Ключ шифрування може бути створений за допомогою спеціальної програми або вручну. Після створення ключа шифрування його необхідно зберегти в безпечному місці. Для шифрування даних за

допомогою обладнання необхідно використовувати пристрій, який підтримує шифрування. Пристрої, які підтримують шифрування, часто називаються шифрувальними пристроями.

Шифрування даних є ефективним методом захисту інформації, але воно не є абсолютно надійним. Шифрування даних може бути скомпрометовано, якщо ключ шифрування буде втрачений або викрадений.

Щоб підвищити безпеку шифрування даних, необхідно:

1. Використовувати надійні алгоритми шифрування;
2. Створювати довгі та складні ключі шифрування;
3. Зберігати ключі шифрування в безпечному місці.

Аутентифікація та авторизація також є важливими аспектами безпеки, які допомагають захистити інформацію від несанкціонованого доступу.

Аутентифікація - це процес підтвердження особи користувача. Аутентифікація може бути реалізована за допомогою різних методів, таких як:

1. Паролі - це найпоширеніший метод аутентифікації. Паролі повинні бути довгими та складними, щоб їх було важко вгадати;
2. Біометричні характеристики - це фізичні або поведінкові характеристики людини, які можна використовувати для аутентифікації. Біометричні характеристики включають відбитки пальців, обличчя, райдужну оболонку ока та голос;
3. Сертифікати цифрових підписів - це електронні документи, які підтверджують особу користувача. Сертифікати цифрових підписів використовуються для підписання електронних документів, щоб гарантувати їх цілісність.

Авторизація - це процес надання дозволів користувачеві на виконання певних дій.

Авторизація може бути реалізована за допомогою різних методів, по типу [1, с. 5]:

1. Контроль доступу на основі ролей (RBAC) - це метод авторизації, який заснований на ролях користувача. Роль визначає, які дії користувач може виконувати [3, с. 58];
2. Контроль доступу на основі атрибутів (ABAC) - це метод авторизації, який заснований на атрибутах користувача та ресурсу. Атрибут - це характеристика користувача або ресурсу [2, с. 44];

Аутентифікація та авторизація часто працюють разом, щоб забезпечити безпеку.

Наприклад, аутентифікація може використовуватися для визначення того, хто є користувачем, а авторизація - для визначення того, які дії користувач може виконувати. Сучасні виклики аутентифікації включають:

1. Забезпечення того, щоб аутентифікація була надійною, але водночас легкою у використанні;

2. Зупинення атак на основі підбору паролів;

3. Забезпечення аутентифікації для мобільних пристроїв і пристроїв Інтернету речей (IoT).

Сучасні виклики для авторизації включають:

1. Забезпечення того, щоб авторизація була точною, але водночас не надто суворою;

2. Забезпечення авторизації для хмарних додатків і послуг;

3. Забезпечення авторизації для даних, які зберігаються в різних системах.

До сучасних тенденції в аутентифікації та авторизації можна включити зростання та використання біометричних характеристик, а також розвиток хмарних технологій і збільшення використання мобільних пристроїв. Ці тенденції створюють нові виклики для аутентифікації та авторизації, але також відкривають нові можливості для підвищення безпеки.

Інший механізм це контроль доступу - це один з найважливіших аспектів фізичного захисту даних [4, с. 12]. Він дозволяє регулювати доступ до фізичних об'єктів, таких як будівлі, серверні кімнати та робочі станції. Контроль доступу може бути реалізований за допомогою різних методів, таких як паролі, картки-ключі, біометричні сканери та відеокамери.

Паролі - це найпоширеніший метод контролю доступу. Паролі повинні бути довгими та складними, щоб їх було важко вгадати. Картки-ключі - це ще один популярний метод контролю доступу. Картки-ключі можуть бути використані для відкриття дверей, замків та інших фізичних об'єктів. Біометричні сканери - це методи контролю доступу, які використовують фізичні або поведінкові характеристики людини, такі як відбитки пальців, обличчя, райдужна оболонка ока або голос. Біометричні сканери вважаються більш надійними, ніж паролі або картки-ключі. Відеокамери - це ще один важливий елемент контролю доступу. Відеокамери можуть бути використані для моніторингу фізичного середовища та виявлення несанкціонованих дій.

Фізичне середовище, в якому зберігаються дані, також є важливим фактором фізичного захисту даних [14, с. 238].

Фізичне середовище – інший важливий аспект, воно повинно бути безпечним і захищеним від несанкціонованого доступу.

До заходів, які можна вжити для підвищення безпеки фізичного середовища, відносяться:

1. Встановлення фізичних бар'єрів, таких як двері, замки та стіни;

2. Встановлення систем безпеки, таких як сигналізація та відеокамери;

3. Контроль доступу до фізичних об'єктів;

4. Забезпечення освітлення в темних місцях.

Не варто забувати про кібератаки, вони є серйозною загрозою для організацій і приватних осіб. Вони можуть призвести до витоку конфіденційних даних, фінансових втрат або навіть зупинки бізнесу. Кібератаки сьогодні – це не просто загроза, вони стали реальністю, що неминуче впливає на всі сфери життя – від державних структур до приватних домогосподарств. Ці напади виявляють уразливості в цифрових системах, використовуючи технологію для зловживання даними, знищення інфраструктури чи крадіжку конфіденційної інформації. Нинішні кібератаки стали складнішими, хитрішими і масштабнішими, вимагаючи постійного вдосконалення та підвищення рівня захисту. Їхні наслідки можуть бути руйнівними як для індивідуальних користувачів, так і для великих корпорацій чи навіть цілих країн.

Кібератака - це будь-яка спроба отримати несанкціонований доступ до комп'ютерної системи або мережі. Кібератаки можуть бути здійснені з різних мотивів, таких як крадіжка даних, саботаж або викуп.

Існує широкий спектр методів, які можуть використовуватися для кібератак. Деякі з найпоширеніших методів включають [15, с. 120]:

1. Взлом паролів – використання програмного забезпечення або ручних методів для зламу паролів користувачів.

2. Соціальна інженерія – обман користувачів, щоб вони надали конфіденційну інформацію або виконали небажані дії.

3. Зловмисне програмне забезпечення – завантаження на комп'ютер жертви шкідливого програмного забезпечення, яке може використовуватися для крадіжки даних, саботажу або викупу;

4. Зловмисні атаки на мережу – використання вразливостей у мережі для отримання несанкціонованого доступу до комп'ютерів або систем.

Існує безліч заходів, які можна вжити для захисту від кібератак. Деякі з найважливіших заходів включають:

1. Створення міцних паролів, паролі повинні бути довгими, складними і унікальними для кожної системи;

2. Використання багатофакторної аутентифікації, цей метод вимагає від користувачів ввести додаткову інформацію, наприклад, код з мобільного телефону, для аутентифікації;

3. Оновлення програмного забезпечення, програмне забезпечення часто містить вразливості, які можуть бути використані для кібератак. Важливо регулярно оновлювати програмне забезпечення, щоб закрити ці вразливості;

4. Використання брандмауера;

5. Використання антивірусного програмного забезпечення;

6. Співробітники повинні бути поінформовані про кібератаки і про те, як їх уникнути.

Багатофакторна аутентифікація (MFA) – це додатковий рівень безпеки, який вимагає від користувачів ввести додаткову інформацію, наприклад, код з мобільного телефону, для аутентифікації [7, с. 22]. MFA робить кібератаки набагато складнішими, оскільки зловмиснику потрібно буде отримати не тільки пароль, але й доступ до іншого пристрою, наприклад, мобільного телефону. Програмне забезпечення часто містить вразливості, які можуть бути використані для кібератак. Важливо регулярно оновлювати програмне забезпечення, щоб закрити ці вразливості. Виробники програмного забезпечення регулярно випускають оновлення для виправлення вразливостей.

Брандмауер - це пристрій або програмне забезпечення, яке допомагає захистити комп'ютер або мережу від несанкціонованого доступу. Брандмауер працює, блокуючи доступ до комп'ютера або мережі з неавторизованих джерел.

Антивірусне програмне забезпечення [8, с. 66] допомагає захистити комп'ютер від шкідливого програмного забезпечення, такого як віруси, троянські коні та шкідливі програми. Антивірусне програмне забезпечення працює, скануючи ваш комп'ютер на наявність шкідливого програмного забезпечення та видаляючи його, якщо воно знайде. Співробітники повинні бути поінформовані про кібератаки і про те, як їх уникнути. Співробітники повинні знати про поширені методи кібератак, такі як соціальна інженерія, і як їх розпізнати. Співробітники також повинні знати про важливість створення міцних паролів і використання багатофакторної аутентифікації. Важливо регулярно перевіряти свої комп'ютери та мережі на наявність вразливостей.

Вразливості - це помилки в програмному забезпеченні [6, с. 5], які можуть бути використані для кібератак. Ви можете використовувати інструменти для сканування на наявність вразливостей, щоб знайти вразливості у своєму програмному забезпеченні. Резервні копії даних - це важливий засіб захисту від кібератак. Якщо ваші дані будуть втрачені або пошкоджені внаслідок кібератаки, ви зможете відновити їх з резервних копій. Ви повинні створювати регулярні резервні копії своїх даних і зберігати їх у безпечному місці. Важливо розробити і впровадити плани реагування на кібератаки. План реагування на кібератаки визначає, що робити в разі кібератаки.

План реагування на кібератаки повинен включати в себе такі елементи, як:

1. Процедура виявлення кібератаки

2. Процедура реагування на кібератак

3. Процедура відновлення після кібератаки

Також потрібно моніторити та аналізувати безпеку - це важливі процеси, які допомагають організаціям захистити свою інформацію та активи від кібератак [13, с. 24]. Моніторинг безпеки передбачає постійне спостереження за системою безпеки, щоб виявити будь-які потенційні загрози. Аналіз безпеки передбачає оцінку даних, зібраних під час моніторингу, щоб визначити, чи є ці загрози реальними.

Сучасні тенденції в моніторингу та аналізі безпеки включають:

1. Зростання використання автоматизації:

1.1. Автоматизація моніторингу та аналізу безпеки може допомогти організаціям економити час і ресурси.

2. Зростання використання штучного інтелекту:

2.1. Штучний інтелект може використовуватися для підвищення ефективності моніторингу та аналізу безпеки.

3. Зростання використання хмарних технологій:

1.2. Хмарні технології можуть використовуватися для централізації моніторингу та аналізу безпеки.

Інший важливий механізм це – резервне копіювання та відновлення даних – це важливі процеси, які допомагають організаціям захистити свою інформацію та активи від втрати або пошкодження. Резервне копіювання - це процес створення копії даних, які можна використовувати для відновлення в разі втрати або пошкодження оригіналів.

Відновлення - це процес відновлення даних з резервної копії. Мета резервного копіювання та відновлення даних - це забезпечення того, щоб організація могла відновити свої дані в разі втрати або пошкодження. Це може бути важливо з багатьох причин, наприклад, у разі:

1. Кібератак – можуть призвести до втрати або пошкодження даних.

2. Природних катастроф, таих як пожеж або повеней, можуть призвести до втрати або пошкодження даних.

3. Знехтуваннь, наприклад, несвоєчасне оновлення програмного забезпечення, може призвести до втрати або пошкодження даних.

Існує два основних види резервних копій – це повні резервні копії містять копії всіх даних, та диференціальні резервні копії що містять копії лише даних, які змінилися з моменту останньої повної резервної копії. А також інкрементальні резервні копії що містять копії лише даних, які змінилися з моменту останньої резервної копії, будь то повної або диференціальної [12, с. 224]. Частота резервного копіювання залежить від важливості даних та ймовірності втрати або пошкодження даних. Для критичних даних може знадобитися

щоденне резервне копіювання, тоді як для менш важливих даних може бути достатньо резервного копіювання раз на тиждень або навіть раз на місяць. Резервні копії повинні зберігатися в безпечному місці, яке не є доступним для зловмисників. Це може бути фізичне місце зберігання, наприклад, сейф або серверна кімната, або хмарне сховище. Важливо мати процедуру відновлення даних, яка визначає, як відновлювати дані в разі втрати або пошкодження.

Процедура відновлення даних повинна включати в себе такі елементи, як:

1. Інформація про розташування резервних копій
2. Інформація про тип резервних копій
3. Інформація про програмне забезпечення, яке використовується для відновлення даних

Сучасні тенденції в резервному копіюванні та відновленні даних включають:

1. Зростання використання хмарних технологій що можуть використовуватися для зберігання резервних копій, що може зробити резервне копіювання більш зручним і економічно ефективним.
2. Зростання використання автоматизації даних може допомогти організаціям економити час і ресурси.
3. Зростання використання штучного інтелекту, може використовуватися для підвищення ефективності резервного копіювання та відновлення даних.

Резервне копіювання та відновлення даних - це важливі процеси, які допомагають організаціям захистити свою інформацію та активи від втрати або пошкодження. Організації повинні розробити і впровадити ефективні стратегії резервного копіювання та відновлення даних, щоб захиститися від збитків, викликаних втратою або пошкодженням даних.

Регулятивні стандарти та вимоги до захисту інформації - це набори правил і процедур, які встановлюють мінімальні вимоги до безпеки інформації для організацій, що підпадають під їхню юрисдикцію [9, с. 34]. Регуляторні стандарти та вимоги до захисту інформації розробляються з метою захисту конфіденційності, цілісності та доступності інформації. Існує безліч різних регуляторних стандартів та вимог до захисту інформації. Деякі з найбільш поширених типів включають закони та нормативні акти які встановлюють обов'язкові вимоги до захисту інформації для організацій, що підпадають під їхню юрисдикцію. Наприклад, Закон про захист персональних даних ЄС (GDPR) встановлює вимоги до захисту персональних даних для організацій, що обробляють персональні дані громадян ЄС [10, с. 40]. Також керівні принципи та рекомендації вони не є обов'язковими, але їх часто використовують

організації для розробки своїх власних політик та процедур безпеки. Наприклад, Міжнародна організація з стандартизації (ISO) розробила ряд стандартів безпеки інформації [5, с.82], які широко використовуються організаціями по всьому світу. Та внутрішні політики та процедури безпеки - це набори правил і процедур, які розробляються організаціями для захисту своєї інформації. Внутрішні політики та процедури безпеки повинні відповідати вимогам будь-яких відповідних регуляторних стандартів та вимог. Регулятивні стандарти та вимоги до захисту інформації є важливим інструментом для захисту інформації. Вони допомагають організаціям запобігти витоку або пошкодженню інформації, що може призвести до фінансових втрат, порушення конфіденційності або інших негативних наслідків [11, с. 50]. Організації, що підпадають під юрисдикцію регуляторних стандартів та вимог до захисту інформації, повинні розробити і впровадити ефективні програми безпеки, які відповідають цим стандартам і вимогам.

Програми безпеки повинні включати в себе такі елементи, як:

1. Політики та процедури безпеки:

1.1. Організації повинні розробити і впровадити політики та процедури безпеки, які відповідають вимогам регуляторних стандартів та вимог.

2. Освіта та навчання:

2.1. Організації повинні забезпечити, щоб їхні співробітники були поінформовані про політики та процедури безпеки і як їх дотримуватися.

3. Контроль та моніторинг:

3.1. Організації повинні регулярно контролювати та моніторити свою програму безпеки, щоб переконатися, що вона ефективна.

Висновки. Механізми безпеки інформації - це різні заходи, що мають захищати дані від несанкціонованого доступу, модифікації, розголошення чи знищення. Вони грають ключову роль у запобіганні витоку чи пошкодженню даних, що може призвести до фінансових втрат чи порушень конфіденційності. Шифрування, аутентифікація та контроль доступу - основні засоби безпеки, що допомагають у захисті інформації. Організації повинні розробляти та підтримувати ці механізми, а також постійно вдосконалювати свої системи з урахуванням нових викликів, таких як швидкий розвиток технологій та збільшення кіберзагроз.

Список використаних джерел

1. Пархуць Ю. Л. Криптографічні механізми захисту інформації в мобільному зв'язку. *Національний університет «Львівська політехніка»*. 2011. https://doi.org/10.18372/2410-7840.13.1985.

2. Михайлов А. О. Дослідження моделей та методів контролю доступу до інформаційної системи: пояснювальна записка до атестаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 121 – Інженерія програмного забезпечення. А. О. Михайлов; М-во освіти і науки України, Нац. ун-т радіоелектроніки. Харків, 2021. 83 с.

3. Шевчук Д. Т. Методи аутентифікації та авторизації у мобільних та веб-додатках. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення:* Міжнародна наукова інтернет-конференція. 2022. 56 с.

4. Скрипка М. В. Система контролю доступу до персональних даних. 2021.

5. Тівецька А. В., Невмержицька С. М. Удосконалення системи управління персоналом організації з врахуванням вимог міжнародних стандартів ISO. *Вісник Київського національного університету технологій та дизайну. Серія «Економіка і вища освіта»*. 2015.

6. Говорущенко Т. О., Мевша А. В., Криськов В. А. Класифікація відмов та вразливостей системного програмного забезпечення. 2014.

7. Олешко І. В. Моделі та методи оцінки захищеності механізмів багатофакторної автентифікації від несанкціонованого доступу. 2014.

8. Shevchenko Svitlana, Skladannyi Pavlo, Martseniuk Maksym. Аналіз та дослідження характеристик антивірусного програмного забезпечення, стандартизованого в Україні. *Кібербезпека: освіта, наука, техніка*. 2019. № 4.4. С. 62–71.

9. Близнюк І., Шорошев В. Основи нормативно-правового забезпечення захисту інформації в комп'ютерних системах державних органів України. 2002.

10. Легка О. В. Імплементація міжнародних стандартів щодо захисту права на доступ до інформації в Україні. 2023.

11. Чунарьова А. Система управління інформаційною безпекою на базі міжнародних стандартів серії ISO. 2012.

12. Шемет А. Застосування методів програмного резервування інформації: аспект резервного копіювання. метод паралельного резервного копіювання. *Вісник Хмельницького національного університету*. 2011. Вип. 3. С. 221–225.

13. Федоренко Р. М. Контент-моніторинг інформаційного простору як чинник забезпечення інформаційної безпеки держави у воєнній сфері. *Сучасний захист інформації*. 2015. Вип. 2. С. 21–25.

14. Оксіюк О. Г., Шестак Я. В. Методологія розробки комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2015. Вип. 50. С. 236–243.

15. Зінченко Д. А., Макарова О. П. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі. 2021.

16. Думанська Н. О. Шифрування даних в інформаційних системах. *Математичні методи, моделі та інформаційні технології в управлінні підприємством:* тези доповідей V студентської вузівської наукової конференції (9 листопада 2020 р., м. Вінниця). Вінниця, 2020. С. 23–25.

17. Lubko D., Sharov S., Strokan O. Software development for the security of TCP-connections. *Modern development paths of agricultural production: trends and innovations.* 2019. Ch. I. P. 99–109.

18. Michaelsen J. R., Vacca J. W. Information security risk management: A guide to managing risks to information assets. *Springer*, 2018.

19. Grossman J. et al. XSS Attacks: Cross site scripting exploits and defense. *MA: Syngress*, 2007. 463 c.

20. *NIST*. National institute of standards and technology. Cybersecurity framework. URL: https://www.nist.gov/cyberframe-work (дата звернення 15.09.2024).

21. ISO/IEC 27005:2011. Information security risk management.

22. Michael Whitman, Herbert Mattord. Information security: principles and practices. Publisher: Cengage learning. 2017. 656 p.

23. *Smieliauskas W., Bewley K.* Auditing: An International Approach. McGraw-Hill Ryerson Higher Education, 2006. 800 p.

24. Cardwell Kevin. Building Virtual Pentesting Labs for Advanced Penetration Testing. Birmingham: Packt Publishing Ltd, 2014. 412 p.

25. Porter B., Hatherly D., Simon J., Principles of External Auditing. 3rd edition. Wiley, 2008. 816 p.

26. Jason A. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Waltham: Syngress, 2014. 240 p.

27. Jason A. Use of Elliptic Curves in Cryptography. *Advances in Cryptology. Crypto'22. LNCS 218*. 2022. P. 503–518.

28. Shanon C. E. Communication Theory of Secrecy System. *Bell System Technical Journal.* 2011. Vol. 103, n.87. P. 345–401.

29. Лубко Д. В., Мірошниченко М. Ю. Аналіз сучасних підходів та методик в області захисту інформації та даних. *Вісник Херсонського національного технічного університету.* 2024. №1(88). С. 231–236.

Стаття надійшла до редакції 15.09.2024 р.

D. Lubko, M. Miroshnichenko
Dmytro Motornyi Tavria State Agrotechnological University

INFORMATION SECURITY MECHANISMS AND THEIR CHALLENGES

Summary

The purpose of the article is to consider information security mechanisms and their challenges, as well as to consider security programs and information protection requirements. Information security mechanisms are various measures that are intended to protect data from unauthorized access, modification, disclosure, or destruction. They play a key role in preventing data leakage or damage that may result in financial losses or privacy breaches. Encryption, authentication, and access control are the main security tools that help protect information. Organizations must develop and maintain these mechanisms and continually improve their systems to meet new challenges, such as rapid technological advances and increasing cyber threats.

Regulatory standards and information security requirements are sets of rules and procedures that establish minimum information security requirements for organizations under their jurisdiction. Regulatory standards and requirements for information protection are developed to protect the confidentiality, integrity and availability of information. There are many different regulatory standards and information protection requirements. Some of the more common types include laws and regulations that establish mandatory information protection requirements for organizations under their jurisdiction. For example, the General Data Protection Regulation (GDPR) establishes requirements for the protection of personal data for organizations that process personal data of citizens. Also, they are not mandatory guidelines and recommendations, but they are often used by organizations to develop their own security policies and procedures. Internal security policies and procedures are sets of rules and procedures that organizations develop to protect their information. Internal security policies and procedures must meet the requirements of any relevant regulatory standards and requirements. Regulatory standards and requirements for information protection are an important tool for information protection. They help organizations prevent information leakage or corruption that could lead to financial losses, privacy breaches, or other negative consequences. Organizations subject to regulatory standards and information protection requirements must develop and implement effective security programs that meet those standards and requirements.

Key words: information security mechanisms, data encryption, security, authentication and authorization, cyber defense, control and monitoring.