УДК 621.3

О.Б. Полусин [1], аспірант УАД, О.В. Тимченко [1, 2], д.т.н, професор,
І.М. Лях[3], к.т.н., доцент, В.І. Сабат [1], к.т.н., доцент

# ОРГАНІЗАЦІЯ І СТРУКТУРНІ ЕЛЕМЕНТИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

**Анотація.** В статті розглянуті елементи системи захисту інформації, їх ефективність та проведено їхній аналіз. Розкриваються основні проблеми систем захисту інформації, що використовуються та причини їх виникнення. Обгрунтовується необхідність створення систем комплексного захисту інформації, що доповнюються законодавчими і організаційними елементами.

**Ключові слова**: захист інформації, комплексна система захисту інформації, інформаційні системи, безпека інформації.

**Вступ.** Інформаційні технології, які ми знаємо на сьогоднішній день, пройшли великі і об'ємні перетворення до сучасних надтехнологій у вигляді потужних надкомп'ютерів, які опрацьовують величезні потоки інформації за лічені секунди та смартфонів, що поєднали у собі функції багатьох пристроїв і виконують функції телефону та базові функції персонального комп'ютера.

Прогрес розвитку технологій опрацювання інформації вразив цілі покоління, але із неймовірно швидким прогресом і розвитком постали загрози пов'язані із безпекою конфіденційної інформації. Захист інформації є одним з ключових факторів, які необхідних для безперебійного функціонування довільної інформаційної системи. Прогрес у цій області неможливий без виявлення несправностей чи проблем, які можна використати для завдання шкоди чи отримання та використання важливої інформації у власних цілях. На даний момент загрози, пов'язані із відставанням у розвитку інформаційного захисту, значно погіршують становище потужних компаній, банків, цілих галузей, а тому постає проблемним питання безпеки передачі, опрацювання і збереження інформації для держави в цілому.

Захист інформації сьогодні перетворюється на одну з найактуальніших і найпоширеніших задач у зв'язку з широким розповсюдження та застосуванням різноманітних систем обробки інформації, розширення комп'ютерних мереж різної топології, розширенням області їх дії і використання підключення за протоколами, якими передаються та опрацьовуються неймовірно величезні, в порівнянні з минулим, об'єми різноманітної інформації, власники якої категорично проти, щоб сторонні особи мали змогу ознайомитись або використати її у власний цілях.

[1], Українська академія друкарства
[2] Uniwersytet Warmińsko-Mazurski w Olsztynie
[3] ДВНЗ «Ужгородський національний університет»

Аналізуючи останні дослідження та матеріали, що характеризують сучасний стан забезпечення безпеки інформації, можна прийти до висновку, що на сьогоднішній день уже не залишилось безпечного місця, де б була змога цілковито забезпечити захист інформації сучасного суспільства.

Опублікування секретних файлів та документів Центрального Розвідувального Управління, США, місце зберігання та опрацювання яких здійснювалось в ізольованій мережі високої безпеки, над ними було втрачено контроль за допомогою шкідливого програмного забезпечення, щоб отримати доступ до конфіденційної інформації або перетворити довільний хост на пристрій стеження [ https://wikileaks.org/ciav7p1/].

Можемо припускати, що на даний момент методи зламування систем захисту інформації вийшли на новий, досить високий програмно-технологічний рівень. Шкідливі програми, віруси, різноманітні програми шпигування та програми «нульового дня» надають можливість доступу до технологій для збору, а також використання інформації за різноманітними напрямками призначення.

Беручи до уваги оприлюднення за останні роки матеріали, що дозволяють обійти комплексні системи захисту інформації, на сьогодні маємо можливість для доопрацювання проблемних ділянок, що допускалися при розробці сучасних інформаційних технологій, а також удосконалення та осучаснення комплексних систем захисту інформації.

**Постановка проблеми.** На теперішній момент організаційні заходи і програмно-технічні засоби для захисту конфіденційної інформації не набули достатньо досконалого характеру і потребують серйозного доопрацювання та удосконалення. Проблема в надійному захисті, що забезпечується системами захисту, з'являється у зв'язку з недбалим ставленням працівників до організаційних питань та використання неліцензованого, часто не протестованого на належному рівні або досить вузького напрямку дії, програмно-технічних засобів, що надають змогу зловмиснику отримати доступ до конфіденційної інформації. Тобто, йде мова про створення цілісної системи, що забезпечить аналіз та швидке усунення недоліків, що сприяють втраті інформації внаслідок несанкціонованого доступу.

**Метою роботи є** дослідження існуючих організаційних і структурних елементів систем захисту інформації та розгляд питання підвищення ефективності комплексного поєднання елементів, що забезпечують захист інформації.

**Виклад основного матеріалу.** Визначимо, що є захистом інформації і складові системи захисту інформації.

В різноманітних джерелах визначення авторів відрізняються, але усі ґрунтуються на певних загальних ознаках і елементах. Можна зазначити, що захист інформації - це сукупність організаційних заходів, програмно-технічних засобів і правових норм, що забезпечують запобігання завдання збитку інтересам власника інформації.

Організація захисту інформації, що опрацьовується і зберігається в

сучасних інформаційних технологіях базується на комплексному підході та взаємодії різноманітних напрямків.

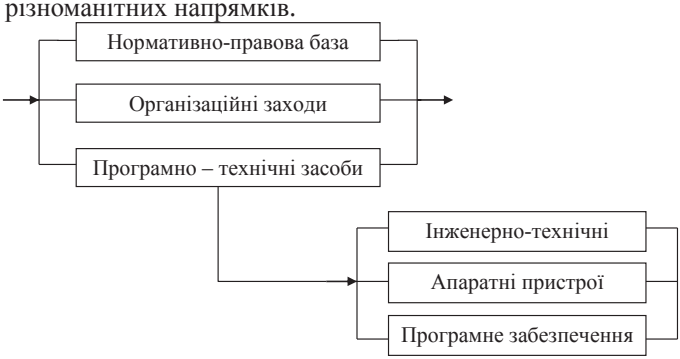


Рис. 1. Елементи системи захисту інформації

Для забезпечення надійного захисту, збереження і опрацювання інформації повинна покладатись відповідальність на осіб, що мають доступ до інформації, а також на осіб які мають наміри заволодіти важливою інформацією. Тому перш за все необхідно забезпечити відповідний рівень інформаційного захисту на законодавчому (нормативно-правовий) рівні. Законодавчі засоби захисту визначаються законодавчими актами, які регламентують правила використання, опрацювання і передачі інформації та встановлюють загальні правила, що виключають або значно затруднюють неправоміне заволодіння інформацією, покладаючи відповідальність на осіб за порушення цих правил.

Не менше необхідними вважаються організаційні та морально-етичні методи захисту інформації. Втрата великих об'ємів інформації найчастіше відбувається через недбалість та недостатню кваліфікованість працівників під час роботи з інформацією.

Ключовим елементом захисту будь-якого типу інформації вважається розвиток комплексного, програмно-технічного підходу, для забезпечення надійності збереження інформації. Програмно-технічні засоби захисту до яких на даний момент відносять інженерно-технічні, апаратні і програмні засоби, що найчастіше використовуються в поєднанні для більшої надійності і безперебійного функціонування систем обробки інформації.

Інженерно-технічні засоби реалізуються у вигляді автономних пристроїв і систем і забезпечують загальний захист об'єктів, на яких опрацьовується інформація;

Апаратні засоби являють собою пристрої для збереження реквізитів доступу, таких як паролі чи коди ідентифікації, ідентифікація індивідуальних характеристик людини, пристрої для шифрування інформації (криптографічні методи), що вбудовуються безпосередньо в обчислювальну техніку.

Програмні засоби, що складають сукупність системного та прикладного

програмного забезпечення, використовують з метою ідентифікації, шифрування та контролю доступу. Використання програмних засобів захисту інформації має цілий ряд переваг – універсальність, гнучкість, надійність, простота у використанні та можливість модифікації.

Використання надійного та ліцензійного програмного забезпечення, відповідних технічних засобів, контроль за дотриманням вимог до захисту інформації та експлуатації цих програмно-технічних засобів захисту, забезпечить високу надійність і зменшить шкоди, що зможуть завдаватись зловмисниками.

Велика кількість факторів, що дозволяють несанкціонованим доступом заволодіти інформацією повинні закликати до застосування та вдосконалення комплексних заходів захисту, що включають в себе:

- навчання та підвищення кваліфікації персоналу, що мають доступ і працюють з конфіденційною інформацією;
- забезпечення від втручання в роботу засобів радіозв'язку;
- організація охорони приміщень і забезпечення комп'ютерних систем та мереж програмно-апаратними засобами захисту інформації, використання криптографічних методів шифрування;
- періодичне тестування приміщень і програмно-технічних пристроїв та ліній зв'язку в яких опрацьовується інформація.

Актуальним на даний момент для розвитку вважаються усі напрямки забезпечення безпечного зберігання і опрацювання даних. Розвиток у законодавчому напрямку повинна забезпечити держава, організаційні заходи застосовуються індивідуально, відповідно кваліфікаційних навичок і обов'язків працівників.

Програмно-технічні засоби, що постають основною перешкодою на шляху отримання конфіденційної інформації, мають необхідність в удосконаленні, оскільки складна архітектура спричиняє витік інформації з причин користувача або навпаки, проста, що дозволяє зловмиснику зламати системи захисту із сторонніх ліній зв'язку, наприклад, таких як глобальна мережа Internet.

Організація побудови надійної системи захисту інформації включає в себе наступні елементи структури:

- проведення аудиту ІТ та систем захисту;
- моніторинг подій інформаційної безпеки;
- розробка і впровадження методів інформаційної безпеки;
- сканування для виявлення вразливих вузлів і компонентів;
- процеси усунення вразливостей;
- програми для обізнаності і підвищення рівня кваліфікації користувачів.

Побудова надійної системи захисту інформації неможлива без попереднього аналізу можливих загроз для системи. Аналіз складається з таких етапів:

- ознайомлення з характером зберігання інформації в системі;

- оцінка цінності інформації;
- побудова моделі зловмисника;
- визначення та класифікація загроз інформації в системі;
- визначення затрат часу і матеріальних ресурсів для злому системи зловмисниками;
- оцінка припустимих витрат часу, засобів і ресурсів для організації захисту системи.

Комплексні системи захисту інформації являються інструментами для забезпечення безпеки інформації, що виконують функцію із забезпечення захисту інформаційної системи і контролю її захищеності.

Система захисту інформації повинна виконувати такі функції:

- реєстрація і облік користувачів, носіїв інформації, інформаційних масивів;
- забезпечення цілісності системного та прикладного програмного забезпечення та інформації яка оброблюється;
- захист комерційної таємниці, включаючи використання сертифікованих засобів криптографічного захисту і електронного цифрового підпису;
- управління і доступ системи інформаційного захисту виконується централізовано;
- ефективний захист систем у вигляді антивірусного програмного забезпечення.

Аналіз і дослідження випадків, спричинених несанкціонованим доступом до інформації показують, що причини можна розділити на випадкові і навмисні. Навмисні загрози несуть більш вагомий характер і наслідки, оскільки зловмисник націлено намагається отримати важливу конфіденційну інформацію. Реалізація таких загроз здійснюється шляхом масованої атаки несанкціонованими запитами або вірусами, що пошкоджують систему захисту і дозволяють проникнути для одержання необхідної інформації. Випадкові події навпаки стаються з причин недбалості або недостатньої кваліфікованості особи, що має доступ до певної інформації.

Оцінка вразливості інформаційної системи, побудова моделі впливів та її стійкість до зовнішніх чинників, це характеристики на яких буде здійснена побудова системи інформаційного захисту в цілому. Аналіз системи і її тестування на можливі фактори проникнення здійснюються на базі уже відомих проникнень чи витоків інформації. Звісно в кожній організації чи компанії є власні адміністратори, які відповідають за безпеку інформаційного потоку, що опрацьовується в їхній інформаційних системах.

Аналітичним центром «Info Watch» здійснюється збір і аналіз інформації про витік інформації чи атак зловмисників на різноманітні інформаційні системи. Згідно даних, що були опубліковані, 67% випадків витоку інформації сталися за участю осіб, які мали доступ і працювали з інформацією. На противагу цьому, 33% випадків сталися через злам систем

інформаційного захисту зовнішнім втручанням.

Тому маючи сподівання на стійкість системи захисту інформації і високу кваліфікованість працівників, необхідне пам'ятати основне правило інформаційного захисту: жодна система захисту не може довгий час протистояти цілеспрямованим діям зловмисника озброєного сучасними технологіями [1]. Зважаючи на це можемо зробити висновок, що велика частина організацій і корпорацій вважають проблемою саме програмно-технічні засоби. Звісно ці засоби є ключовими, але не слід забувати, що більше половини усіх випадків стаються не через проблеми в програмному чи технічному забезпеченні, а саме через недбалість чи неуважність самих користувачів до безпеки конфіденційної інформації.

**Висновки.** Захист конфіденційних даних – це головна задача, що поставлена в пріоритеті на вирішення у багатьох країнах світу, а також і в Україні. Реалізація можлива лише за допомогою комплексного підходу до поставленого завдання. Доопрацювання нормативно-правової бази у сфері політики інформаційної безпеки, покращення розвитку інформативності та навчання персоналу, використання сучасних надійно протестованих технічних засобів та ліцензованих програмних продуктів, усі вище наведені елементи необхідні в доопрацюванні та вдосконаленні для надійнішого захисту.

Отже, можна сказати, що для покращення ефективності розробки або вдосконалення інформаційних систем захисту, насамперед необхідно використовувати системи моніторингу за подіями, що відбуваються в системі, здійснювати аналіз виявлених атак, що здійснювались з моменту останнього покращення системи захисту, а також періодично здійснювати самостійне тестування системи, для виявлення прогалин, що були допущені при розробці.

Також для запобігання втрати інформації чи пошкодження системи захисту потрібно здійснювати ознайомчі та навчальні заняття для персоналу чи осіб, що володіють доступом до певної конфіденційної інформації. Ознайомлювати з основними найпростішими засобами захисту, такими як, комбіновані надійні паролі доступу, антивірусними програмами, програмними засобами firewall. Також обмежити доступ для встановлення програмного забезпечення та відкритого доступу до мережі Internet.

В наступних публікаціях планується дослідити програмно-технічні засоби систем захисту інформації, що пов'язані з розвитком сучасних інформаційних технологій, котрі допоможуть покращити захист даних від несанкціонованого доступу чи витоку.

1. *Остапов С.Е., Євсеєв С.П., Король О.Г.* Технології захисту інформації: навчальний посібник – Х. : Вид. ХНЕУ,2013. – 476 с.
2. *Гончарова Л.Л., Возенко А.Д., Стасюк О.І., Коваль Ю.О.* Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с.
3. https://wikileaks.org/ciav7p1/
4. https://infowatch.com/report2016_half

*Поступила 6.03.2017р.*