УДК 004.681.3

Яніна Володимирівна Невойт,
Леся Миколаївна Мазуренко,
Володимир Олексійович Хорошко

ЖИТТЄВИЙ ЦИКЛ ІНФОРМАЦІЇ ТА ВИМОГИ ДО СИСТЕМ ЇЇ ЗАХИСТУ

Вступ. Сьогодні здійснюється перехід нашого суспільства від індустріального до інформаційного. Це стало можливим завдяки розвитку технологій, які дають змогу зберігати та обробляти великі масиви інформації, передавати її на великі відстані, здійснювати обмін інформацією між різними операторами.

Перехід до ринку і, відповідно, постійна конкуренція між виробниками товарів та послуг, привели до необхідності забезпечення конфіденційності взаємовідносин між різними людьми та організаціями.

Перед Україною постала задача щодо входження до європейського та світового інформаційного простору для розширення взаємних зв'язків з різними державами. Тому питання захисту та загроз інформації, яка передається, приймається та зберігається, є надзвичайно актуальними.

Термін "інформація" об'єднує відображення в людській в людській свідомості предметів та явищ довкілля, яке незалежно від форми подання (текст, зображення, звук) використовують для отримання теоретичних знань та прийняття практичних рішень.

З урахуванням рівня інформаційних технологій сучасності та розглядаючи інформацію як об'єкт діяльності, треба відзначити, що залежно від її важливості та значення для користування нею витрачають відповідні ресурси. Але важливість та значення інформації для тих чи інших суб'єктів інформаційних відносин в умовах прихованого комерційного, відомчого та державного інтересу визначати складно. Тому зрозуміло, що задоволення інформаційних потреб перебуває в пропорційній залежності від умов та методів (засобів) практичної діяльності відповідних суб'єктів, а високий рівень автоматизації, до якого прагне людство, ставить його в залежність від рівня безпеки інформаційних технологій, які воно використовує. В зв'язку з цим інформаційні ресурси потребують розмежування доступу. Виникає також потреба класифікувати її за формою подання.

Викладення основного матеріалу. Будь-яку інформацію розглядають у вигляді потоків, які діють на органи сприйняття оператора формами зображення, звуку та тексту, що призводить до породження потоків відповідних форм.

Визначення 1. Інформаційний потік — це обсяг (множина) інформаційних даних, що транслюється через умовний вузол обробки автоматизованої системи (АС) за одиницю часу.

Сучасні інформаційні технології сублімують у собі якості усіх форм, різні поточні форми можуть трансформуватися між собою.

Умовно всі трансформації даних в АС визначено як трансформації інформаційних потоків, модифікація яких ставить питання порушення цілісності та достовірності даних (властивості інформації, яка полягає у тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом). Інформаційні потоки поділяють на елементарні структурні одиниці — файли чи повідомлення.

Визначення 2. Файл — це іменована область пам'яті комп'ютера, яка містить компоненти одного типу (символи від початку до кінця файлу).

Наукова проблематика цілісності даних, яка сформульована у межах цієї статті — це цілісність окремого файлу наданого формату.

Розглядання інформаційних трансформацій на предмет реалізації поставлених вимог диктує необхідність локалізації її основних процесів.

Стосовно інформації (об'єкта) юридичні особи, організації (відомства, установи) є її джерелом, споживачем або порушником прав доступу (несанкціонованим користувачем).

Оскільки ми орієнтуємось на захист відомчих (комерційних, державних) інтересів, треба зауважити, що на всіх етапах [1, 2] трансформації даних (відомостей) витра-

чається деякий проміжок часу, тобто об'єкт має певний життєвий цикл (див. рис. 1).

Життєвий цикл інформації залежить від оцінки її цінності, а також відповідно від спроможності санкціонованих користувачів забезпечити її надійний захист, і, отже, не допустити "знецінення" інформації. Він передбачає, що інформація здобувається, обробляється (аналізується), зберігається, охороняється, використовується, транслюється, розкрадається та знищується. Тому розглянемо етапи життєвого циклу інформації з позиції цільової ознаки системи контролю цілісності та достовірності інформації (СКЦЦД) детальніше, щоб відокремити вразливі ланки трансформації, які потребують захисту. Підкреслимо, що модифікація даних охоплює всі етапи життєвого циклу. Під терміном "модифікація" будемо розуміти будь-яку зміну попереднього змісту даних стосовно етапу її створення (див. рис. 1).

Процес створення та знищення інформації, тобто відображення або стирання на деякому матеріальному носії, папері або електронній копії накопичення даних з урахуванням визначених завдань до розроблення документів здійснюються авторизованими користувачами (у разі знищення це не має значення). Після створення документа (масиву) здійснюється його оцінка на предмет відповідності абстрактним і конкретним вимогам для подальшого спрямування та використання у визначених (дозволених) межах. Зберігання вимагає розроблення порядку та правил підготовки до зберігання інформації на паперових носіях та в електронному вигляді на машинних носіях (жорстких, гнучких дисках) з наступною технологією (обмеженням) доступу. Вибірка інформації та подальша оцінка вибору зумовлена конкретністю поставленої задачі. Критичність щодо даних настає з моменту вибірки та подальшого їхнього опрацювання.

Обробка та використання інформації суб'єктами розподіленої системи, які зумовлюють практичне використання інформації при прийнятті рішень та реалізації тих чи інших життєвих процесів, дає змогу виділити найуразливішу ланку захищеної системи — етап її передавання, де є можливість несанкціонованих дій (перегляду, модифікації, знищення) з боку неавторизованих користувачів.

Засоби контролю цілісності та достовірності інформації функціонують на різних структурних рівнях її обробки. Це низький, середній та високий: низький (структурний рівень), середній (семантичний рівень подання інформації) та високий (логічний рівень контексту інформації) рівні. Розглядання високого рівня оцінки виходить за межі статті, засоби середнього рівня аналізуються у цій роботі.

На низькому (структурному) рівні обробки інформації ПЕОМ [2, 3] функціонують методи, які відповідають СКЦДІ.

Отже, вирішення проблеми цілісності та достовірності інформації зумовлює розгляд елементів його сигнатурного аналізу та побудови функцій хешування даних, які оформлюються з урахуванням з систематизації переліку загроз інформації та класифікація характеристик файлу, які критичні для модифікування.

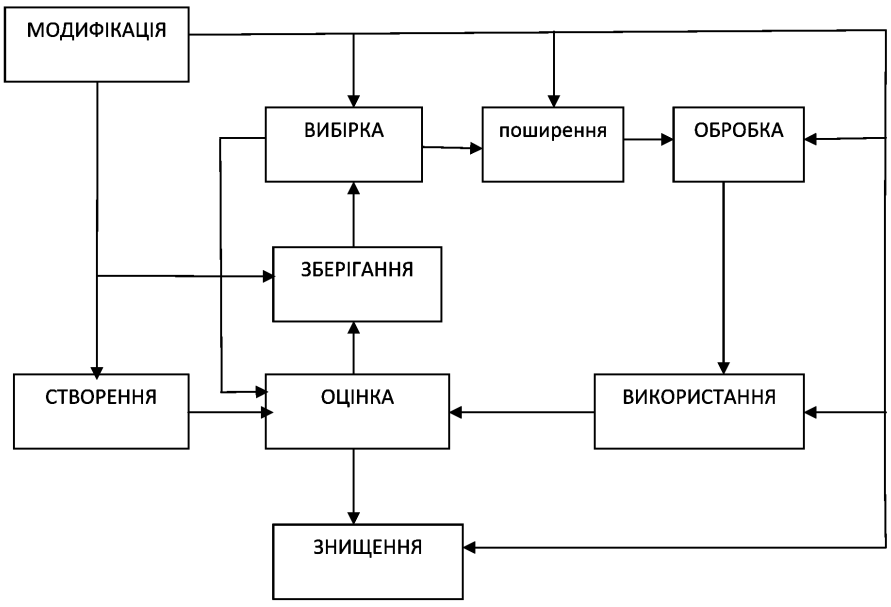

Рис. 1. Життєвий цикл інформації

Обробка інформації пов'язана з формою подання на подразники остаточної інформації (текст, зображення, звук). Крім перелічених потоків, існують ще деякі службові дані, що характеризують програмне середовище та відображають його функціональність (відповідність призначенню). Тобто інформаційний потік залежно від сприйняття поданий в формі текстового, звукового (аудіо), графічного потоку, потоку відеозображень та службового потоку, який циркулює на рівні функціонування вузлів обробки інформації, АС та забезпечує існування перерахованих потоків в сучасних засобах мультимедіа.

На низькому рівні інформаційні потоки — це послідовність байтів стандартного оформлення (формати даних). Модифікація файлів розуміє модифікацію потоку, оскільки перший є структурною одиницею потоку.

Визначення 3. Загроза інформаційної безпеки АС — це можливість реалізації впливу на інформацію, що призводить до створення, знищення, копіювання, блокування доступу до інформації, а також можливість впливу на компоненти АС, що призводить до втрати знищення або збою функціонування носія інформації, засобів взаємодії з носієм або засобів його управління.

Необхідність класифікації загроз інформаційної безпеки зумовлена тим, що архітектура сучасних засобів автоматизованої обробки, організаційна, структурна та функціональна побудова інформаційно-обчислювальних систем (мереж), технології та умови обробки таку, що інформація потрапляє під вплив надмірно великої кількості чинників, за якими і потрібно формалізувати задачу описання загроз та ефективності протидії їм. Перелік загроз інформаційної безпеки [2, 3, 4] будемо розглядати за цільовою ознакою класифікації та описання складових інформаційних потоків, критичних до модифікування. Аналіз цих загроз повинен бути здійснений на основі їхньої кваліфікації за низкою ознак. Кожна з ознак відображає одну із узагальнених вимог до системи захисту (конфіденційність, цілісність, достовірність):

- несанкціоноване копіювання носіїв інформації;
- необережні дії, що призводять до розголошення конфіденційності інформації або роблять її загальнодоступною;
- ігнорування організаційних обмежень (встановлених правил) під час визначення рангу системи.

Для системи визначимо перелік класів загроз (якості моделі):

- за природою винесення ;
- за ступенем навмисності;
- за безпосереднім джерелом загроз;
- за станом джерела загроз;
- за мірою залежності від активності АС;
- за мірою впливу на АС;
- за етапами доступу користувачів або програм до ресурсів АС;
- за способом доступу до ресурсів АС;
- за поточним місцем розміщення інформації, що зберігається і обробляється в АС.

Відповідно для АС будемо розглядати чотири види загроз:

- загроза порушення конфіденційності полягає в тому, що інформація стає відомою тим, хто не володіє повноваженнями до неї;
- загроза порушення цілісності включає в себе поняття будь-якої навмисної зміни інформації, що зберігається в обмежувальних системах або при її передаванні між системами;
- загроза відмови служб виникає щоразу, коли внаслідок навмисних дій блокується доступ до деяких ресурсів;
- загроза розкриття параметрів АС.

Розглядаючи питання захисту АС, доцільно використовувати чотирирівневу градацію доступу до інформації, що зберігається, обробляється та залишається в АС:

- рівень носіїв інформації;
- рівень засобів взаємодії з носіями;
- рівень подання інформації;
- змісту інформації.

Крім того, потрібно сформулювати додаткові вимоги щодо аналізу загроз інформації:

- перелік загроз повинен бути максимально повним та деталізованим. Для кожної із загроз необхідно визначити, на порушення яких властивостей інформації або АС вона спрямована (конфіденційності, цілісності, доступності, а також відмови служб АС);
- можливі методи [3] реалізації загроз.

З урахуванням технології обробки інформації та побудови моделі загроз інформації необхідно розробляти модель порушника, яка повинна бути адекватна реальному порушнику для певної АС.

Визначення 4. Модель порушника — абстрактне формалізоване або неформалізоване описання дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дій тощо.

Стосовно АС порушники можуть бути зовнішніми або внутрішніми. Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенем небезпеки для АС;
- категорії осіб, із яких може бути порушник;
- передбачення про кваліфікацію порушника;
- передбачення про характер його дій.

Метою порушника може бути одержання необхідної інформації та можливість вно-

сити зміни в інформаційні потоки згідно зі своїми намірами та завдання збитків через знищення матеріальних та інформаційних цінностей.

Будь-яка якісна система протидії апріорно передбачає високий досвід (володіння високим рівнем знань в галузі обчислювальної техніки, програмування, проектування та експлуатації АС, володіння інформацією про функції та механізм дії засобів захисту) та кваліфікацію порушника (можливість використання недоліків проектування КСЗІ за допомогою методів та засобів активного впливу на АС, які змінюють конфігурацію системи).

Також передбачається, що за місцем дій порушники можуть одержати доступ до засобів адміністрування АС та засобів управління КСЗІ.

Перелік загроз [4], оцінка їхньої реалізації, а також модель порушника є основою для аналізу ризику реалізації загроз та формулювання рис моделі реєстрації даних.

Дія моделі реєстрації даних поширюється на рівень автентифікації файлів.

Перша умова функціонування моделі — автономність СКЦДІ (незалежність від дій системного адміністрування). Умова друга — обов'язковість (застосування алгоритмів СКЦДІ до кожного елемента потоку). Умова третя — компактність засобів СКЦДІ (застосування мінімальних обчислювальних ресурсів). Умова четверта — реагування (комплекс організаційних заходів щодо порушення цілісності об'єкта).

Враховуючи, що файл є одиницею обміну між різними системами обробки і він виступає як індикатор СКЦДІ, розглядаємо характеристики файлу як одиниці, до якої можливе застосування моделі реєстрації та підтвердження їхньої цілісності.

Створення механізму ефективного захисту інформації з обмеженим доступом передбачає, насамперед, уявлення, що в основі існує стандартна система, яка складається з об'єкта нападу та суб'єкта, який намагається використати інформацію всупереч встановленим нормам поводження з нею.

Проаналізувавши життєвий цикл інформації, визначимо питання його аналізу:

1. Як транспортувати інформацію?
2. Який вид аналізу застосувати для визначення стану інформації після її транспортування?

Якщо позначка дослідження — вибір виду аналізу, то об'єктом аналізу, зважаючи на це, стає структурування інформації на електронному носії.

Сформулюємо тезисно відповіді на два питання, які були поставлені раніше. Інформаційний потік, що контролюється, переважно передаватиметься у відкритому вигляді (для безпосереднього подальшого опрацювання) з подальшою обов'язковою обробкою СКЦДІ.

За наявності такого функціонуючого механізму, у разі нападу на передану інформацію своєчасне виявлення цього факту надасть додаткові можливості щодо запобігання подальшому розвитку негативних подій.

Алгоритм цілісності та достовірності інформації будується на принципах хешування відрізків потоку даних.

Визначення 5. Одностороння хеш-функція, $H(N)$ обробляє довільне повідомлення довжини N і повертає хеш фіксованої довжини h:

$$h = H(N),$$

де h — довжин N.

Багато функцій можуть взяти вхід доцільної довжини і повернути вихід фіксованої довжини, але односторонні хеш-функції мають три додаткові характеристики, що робить їх односторонніми:

- за N легко обчислити h;
- за h важко обчислити N так, що $H(N) = h$;
- за N' важко знайти інше повідомлення N' таке, що $H(N) = H(N')$.

Довжина хеша може бути змінена користувачем. Запропонований метод припускає генерацію довшого хеша, ніж функція його виходу:

1. Згенерувати хеш-повідомлення, використовуючи односторонню хеш-функцію.
2. Додати хеш-повідомлення.
3. Згенерувати хеш конкатенації повідомленні і хеша.
4. Створити більший хеш, що будується з хеша (крок 1) і конкатенації (крок 3).
5. Повторити (кроки 1—4) до досягнення необхідної довжини хеша.

Висновки. На основі цього дослідження можна зробити такі висновки. Розгляд особливостей існування інформації в електронному вигляді дає змогу виділити такі риси інформаційної моделі реєстрації даних.

Трансляція інформації в мережах телекомунікацій відбувається у вигляді інформаційних потоків, класифікація яких залежить від сприйняття їх оператором (текстові, графічні, звукові, відео та службові потоки: кодування архівації стиснення) та характеризується внутрішньою структурною формату потоку. Елементарною структурною одиницею потоку є файл, який будується з однотипних даних.

Інформація в сучасних АС часто піддається несанкціонованій модифікації. Найуразливішим із основних етапів життєвого циклу інформації є етап її поширення між кореспондентами мережі.

Розглядаючи питання захисту АС, доцільно використовувати чотирирівневу гра-

дацію доступу до інформації, що зберігається, обробляється та захищається в АС: рівень носіїв інформації, рівень засобів взаємодії з носіями, рівень подання інформації та рівень змісту інформації.

Стосовно інформації необхідно виділити методи реалізації загроз на кожному рівні. Характеристика потенційних порушників припускає їхній високий досвід та кваліфікацію, а також передбачається, що за місцем здійснення дій порушники можуть одержати доступ до засобів адміністрування АС та засобів управління КСЗІ.

Дія моделі реєстрації даних поширюється на рівень автентифікації файлів. Виділені критичні параметри файлу, що схильні до модифікації. Це зовнішні та внутрішні якості файлу.

Умови функціонування моделі реєстрації: автономність СКЦДІ (незалежність від дій системного адміністрування), обов'язковість засобів СКЦДІ (застосування мінімальних обчислювальних ресурсів) та реагування (комплекс організаційних заходів щодо порушення цілісності об'єкта). Файли транспортують по мережі у відкритому вигляді, секретність даних підтримується організаційними заходами.

Література

1. Ленков С. В. Методы и средства защиты информации : в 2 т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. — К. : Арий, 2008. **2. Хорев А. А.** Способы и средства защиты информации, обрабатываемой ТСПИ от утечки по техническим каналам / А. А. Хорев // Специальная техника. — № 4. — 2005. — С. 58—64. **3. Ковалева Ю. Е.** Проектирование корпоративных вычислительных сетей / Ю. Е. Ковалева, Т. И. Олешко, В. А. Хорошко // Захист інформації. — № 2. — 2003. — С. 4—14. **4. Кудінов В. А.** Корпоративна мережа ОВС України та моделі її захисту від порушників безпеки / В. А. Кудінов, В. О. Хорошко // Захист інформації. — 2004. — № 1. — С. 26—36.

Рассмотрен жизненный цикл информации и требования к системам защиты. На их основе определен перечень классов угроз и внутренних и внешних нарушителей с учетом исследования угроз информации.

Ключевые слова:

The life cycle of information and requirements to security system are considered in this article. On their base list of the threats and internal and external violators classes is determined. Considering conducted study the model of the threats to information is created.

Key words: