бинарное представление. Логический (высокий) уровень объекта является носителем его смысловой насыщенности (факта). Собственно СЦДИ затрагивают разные аспекты своего инструментария по отношению к этим интерпретационным уровням – целостности на низком и достоверности на высоком уровнях.

3. Инструментарий СЦДИ позволяет на низком уровне выявлять и корректировать ошибки, на среднем (граничном) – только их выявлять. Особенности субъективного восприятия объекта позволяют полностью нивелировать степень достоверности факта объекта посредством подмены его контекста.

4. Анализируя объективно-субъективный континуум, можно говорить об определенных законах воздействия на субъект (при наличии детерминированного объекта), а именно:

- различимости: механизмы воздействия средствами низкого и среднего уровня на объект субъектом различимы, потенциально ожидаемы и, по большей части, прогнозируемы; механизмы воздействия высокого уровня субъективно неразличимы, что позволяет осуществить тонкую коррекцию факта (в сравнении с грубой на нижних уровнях);
- многонаправленности: интерпретационное восприятие объекта субъектом восприимчиво как к официальному (информационному), так и неофициальному (дезинформационному) каналам трансляции объектов;
- активной роли субъекта: в информационном мире процесс трансляции объектов одновременно формирует сами объекты;
- многослойности: объект содержит в себе не только факт, но и его интерпретацию, поэтому заимствование факта с иным объектом несет в себе и иную интерпретацию, что в подавляющем большинстве случаев не воспринимается субъектом; объект формируется как источником, так и потребителем;
- информационного усиления: искривление информационного пространства достигается за счет значимости объекта, а удержание внимания со стороны субъекта возможно только при качественной мотивации.

Методология анализа достоверности объекта, предложенная в статье, позволяет комплексно подойти к оценке контекста любых информационных событий, электронных документов и отрезков известных форматов различных потоков данных глобальной информационной сети.

Литература: 1. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ / Под. ред. Р. Л. Добрушина, С. И. Самойленко. – М.: Мир, 1976. 2. ДСТУ 34.310-95. 3. Почепцов Г. Информация и дезинформация // Досье секретных служб, № 3, 2001

УДК 681.31

ВАРІАНТ ПІДВИЩЕННЯ ШВИДКОСТІ ФОРМУВАННЯ ОЗНАК ЦІЛІСНОСТІ В МЕХАНІЗМАХ КОНТРОЛЮ ЦІЛІСНОСТІ

Микола Будько, Вячеслав Василенко, Руслан Балидін
ВАТ "КП ОТІ", м. Київ

Анотація: **Запропоновано варіант організації контролю цілісності та варіант прискорення формування ознак цілісності при модифікації інформаційного об'єкту.**

Summary: **The article presents variant of organization of the control of integrity and variant of acceleration of formation of integrity attributes at updating information object.**

Ключові слова: **Захист інформації, цілісність інформації, контроль, імітостійкість, ознака цілісності.**

Вступ

Однією із основних властивостей захищеності інформації є її цілісність [1–3], забезпечення якої дозволяє з певною гарантією стверджувати про можливість запобігти несанкціонованій модифікації чи знищенню програмних засобів або інформації комп'ютерних систем. Цілісність інформації забезпечується в першу чергу механізмами захисту від несанкціонованого доступу, та виявлення порушень цілісності інформації. В статті розглядаються варіант організації контролю цілісності та можливості підвищення швидкості формування ознак цілісності. Під контролем цілісності інформації розуміється процес перевірки наявності модифікації цієї інформації в комп'ютерних системах, незалежно від причин та походження модифікації (навмисна чи ненавмисна).

І Організація контролю цілісності

При побудові систем захисту інформації розробці механізмів та засобів забезпечення контролю цілісності приділяється значна увага. Так, в [4] наведено один з можливих механізмів контролю цілісності (КЦ) інформації та її поновлення. Цей механізм передбачає розподілення контрольованої інформації на блоки – базові кодові слова (БКС) та узагальнені кодові слова (УКС). Як БКС використовуються інформаційні блоки довжиною, наприклад у 32 байти. З декількох таких БКС шляхом їх перемежування створюється УКС. Ознака цілісності (ОЦ) для контрольованої інформації розраховується за правилами коду Умовних лишків. При цьому здійснюється перетворення інформації, для якої обраховується ОЦ. Ця ознака цілісності зберігається для подальшого контролю цілісності. При контролі цілісності розраховується нове значення ОЦ для інформації, що контролюється, яке порівнюється із збереженим значенням попередньо розрахованої ознаки цілісності. Якщо вони збігаються, то цілісність інформації, що контролюється, не порушено, інакше – цілісність порушено.

На основі цього механізму авторами розроблені програмні засоби контролю цілісності файлів персональних комп'ютерів в середовищі Windows 95/98/NT. Програмні засоби призначені для забезпечення контролю цілісності у відповідності до вимог захисту інформації в комп'ютерних системах, які передбачені нормативними документами систем ТЗІ України [2].

До складу програмних засобів для контролю цілісності входять наступні компоненти:

1. Управління;
2. Ідентифікації та автентифікації користувачів;
3. Тестування;
4. Захисту ключових наборів;
5. Формування довільного ключового набору;
6. Формування стандартного ключового набору;
7. Формування базових констант перетворення;
8. Формування ознак цілісності в загальному та вибірковому режимах;
9. Формування бази даних;
10. Контролю цілісності в загальному та вибірковому режимах;
11. Аудиту.

Компонент управління забезпечує активізацію процесу КЦ, вибір та установку режимів, а також зручний для користувача інтерфейс, який виконано в стандарті вікон Windows. Активізація процесу контролю цілісності може бути здійснена при старті комп'ютера, за таймером та за запитом користувача.

Виконання контролю цілісності програмними засобами КЦ є можливим в режимах:

а) Контроль за запитом (на вимогу адміністратора);

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

б) Контроль при старті програмного засобу (при включенні комп'ютера);
в) Контроль за таймером.

В кожному з режимів контроль цілісності передбачає наступні етапи:

- ідентифікація та автентифікація користувача;
- самоконтроль цілісності при старті;
- вибір інформаційного об'єкту для формування ОЦ чи КЦ;
- формування чи вибір ключового набору;
- формування базових констант перетворення;
- формування ОЦ чи КЦ;
- формування бази даних.

В процесі ідентифікації та автентифікації користувачів здійснюється введення ідентифікатора користувача та його паролю. В разі спроби активізувати засоби контролю цілісності з боку не авторизованих користувачів (при введенні не вірних паролів) дозволяється ще дві спроби введення паролю, і в разі трикратного введення неправильного паролю формується звуковий сигнал, здійснюється фіксація цієї події в журналі реєстрації, забезпечується попередження адміністратора звуковими сигналами та візуально і здійснюється блокування роботи комп'ютера поки не буде введений вірний пароль.

При самотестуванні здійснюється автоматичний (без участі користувача) самоконтроль засобів контролю цілісності шляхом перевірки цілісності власного файлу для виконання при старті програмного засобу. Для здійснення самоконтролю при інсталяції формується ОЦ файлу для виконання. Ця ознака цілісності використовується при перевірці цілісності файлу для виконання під час самоконтролю.

Засобами захисту ключів забезпечується шифрування ключів, що зберігаються в базі даних. Для закриття (викривлення) ключового набору, який записується в базу даних, застосовується порозрядне додавання по модулю 2 до цього набору (який записується) псевдовипадкової послідовності. ЇЇ формування здійснюється програмним генератором псевдовипадкових чисел, для якого першим (початковим) числом служить пароль, який вводиться користувачем власноручно. При перевірці цілісності здійснюється спочатку розшифровування ключового набору. Для цього користувач власноручно вводить такий же пароль, як і при формуванні ОЦ, за допомогою якого програмним датчиком псевдовипадкових чисел генерується ідентична послідовність символів. Ця послідовність шляхом порозрядного додавання по модулю 2 до ключового набору, який записано в базі даних, дешифрує його. Після цього цей ключовий набір використовується для перевірки цілісності.

Засобами формування довільного та стандартного ключових наборів забезпечується реалізація функцій вибору за бажанням користувача ключового набору довільної чи стандартної (наперед визначеної) довжини, що забезпечує формування довільної чи стандартної довжини ОЦ, а також формування елементів ключового набору власноручно користувачем чи в автоматичному режимі з використанням програмних датчиків псевдовипадкових чисел. При ручному формуванні ключового набору користувач вибирає із масиву номерів елементів ключів ті елементи, на яких він буде формувати ОЦ для інформаційного об'єкту. При використанні програмних датчиків псевдовипадкових чисел генерується псевдовипадкова послідовність номерів елементів для формування ОЦ.

Засобами формування базових констант перетворення забезпечується створення відповідно до **ключових наборів** масивів констант, **які є невідомими для** не авторизованих користувачів та необхідними для формування ОЦ.

Засобами формування ознаки цілісності з використанням базових констант

перетворення забезпечується обчислення ОЦ інформаційного об'єкту, яка є образом (відображенням) інформаційного об'єкту, для якого ця ОЦ формується. **В зв'язку з тим, що для формування ОЦ використовуються базові константи перетворення, які є невідомими для не авторизованих користувачів, значення її елементів не можуть бути сформованими цими не авторизованими користувачами з метою маскування своїх дій з модифікації (підміні чи вилученні) інформації файлу, що захищається даною ОЦ, чи набору даних так, щоб значення елементів ОЦ, що формуються не авторизованими користувачами, відповідали б справжнім.** Останнє і є метою формування ОЦ. Цим, до речі, забезпечується потрібна імітостійкість даної програми. Наслідком етапів формування ОЦ є відповідні записи (рядки) в журналі реєстрації (час, дата, ім'я та шлях до контрольованого файлу) та видача повідомлень про здійснення формування ОЦ.

Засобами формування бази даних забезпечується архівація інформації про всі файли чи набори даних, для яких сформовані ОЦ. База даних (ознака цілісності, зашифровані ключі, довжина ключа, час формування ОЦ) дозволяє здійснювати в подальшому контроль цілісності цих інформаційних об'єктів.

Засобами контролю цілісності забезпечується формування поточної ОЦ для інформаційного об'єкту, що контролюється, на тому ж ключовому наборі (і, звичайно, з тими ж базовими константами перетворення). Це поточне значення ОЦ порівнюється з контрольним (обчисленим раніше). На підставі цього порівняння формується ознака наявності чи відсутності порушення цілісності інформації, що контролюється. Наслідком етапів контролю цілісності є відповідні записи (рядки) в журналі реєстрації (час та дата КЦ, стан, ім'я та шлях до контрольованого файлу) та формування повідомлень про стан цілісності контрольованого файлу.

В запропонованому в [4] алгоритмі розрахунку ОЦ при перестановці в інформаційному об'єкті блоків інформації таким же розміром, як і УКС, розрахунок ОЦ для не модифікованого інформаційного об'єкту та інформаційного об'єкту, в якому зроблені перестановки, дає однакові значення ОЦ. Цьому можна запобігти декількома способами. Як варіант тут використовується спосіб накопичення інформації у змінній К. Він полягає в тому, що при розрахунку ОЦ кожного з наступних УКС використовується змінна К, яку можна отримати шляхом використання порозрядної операції за модулем 2 від усіх попередніх байтів. Початкове ж значення К1 формується шляхом порозрядного додавання за модулем 2 над обрахованими базовими константами.

II Варіант прискорення формування ознак цілісності при модифікації інформації

Описаний механізм ефективно діє при контролі інформаційних об'єктів, які змінюються достатньо рідко (квазістатичні). Але на практиці часто зустрічаються випадки, коли є необхідність санкціонованої модифікації інформаційного об'єкту типу накопичення інформації в файлах, таблицях бази даних та т. п. При цьому виникає потреба повторного здійснення операції формування ОЦ для модифікованого інформаційного об'єкту. При великих об'ємах інформації, та при досить частих модифікаціях операції формування нового значення ОЦ можуть займати значний час.

Цьому недоліку можна запобігти, використовуючи для формування нового значення ОЦ операції розрахунку ОЦ лише для інформації, яка дописується, та ОЦ для попереднього інформаційного об'єкту. Крім цього для формування нового значення ОЦ із попередньої інформації слід використати останнє УКС, оскільки особливостями останнього з УКСn (див. рис. 1) є те, що воно є зв'язком між попереднім та новим інформаційними об'єктами.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Тобто для попереднього інформаційного об’єкту останнє УКС є кінцевим інформаційним блоком, до якого буде приєднуватись нова інформація при формуванні нового значення ОЦ модифікованого інформаційного об’єкту.

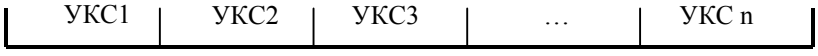

Рисунок 1 - Представлення інформації для формування її ОЦ

При дописуванні нової інформації до попереднього інформаційного об’єкту можливо виникнення одного з трьох випадків, в залежності від розміру УКС та довжини інформаційного об’єкту.

У першому випадку останній УКС заповнюється інформацією не повністю і, згідно з існуючим алгоритмом, останні недописані байти заповнюються нулями. В цьому випадку при приєднанні нового інформаційного об’єкту виникає інформаційний розрив. Тому, щоб цьому запобігти, нулі в останньому УКС потрібно заповнювати інформацією, що записується.

Якщо ж попередній інформаційний об’єкт взагалі менший, ніж довжина УКС (у другому випадку), то дописувати нову інформацію потрібно безпосередньо до цього об’єкту, бо загальна кількість УКС для такого маленького інформаційного об’єкту буде дорівнювати 1.

У третьому випадку (його можна назвати ідеальним) останнє УКС попереднього інформаційного об’єкту заповнене інформацією повністю і інформаційний об’єкт, що записується, буде просто приєднуватись до останнього УКС попереднього інформаційного об’єкту.

Для роботи алгоритму, що пропонується, після формування ОЦ для попереднього інформаційного об’єкту інформації потрібно запам’ятати (у зовнішньому інформаційному об’єкті, файлі, БД) такі параметри:

- останнє з УКС (див. рис. 1).
- кількість байтів в УКС (N);
- змінну (К), яка використовується для запобігання перестановки блоків інформації, розміром N байтів. Цю змінну слід запам’ятовувати для розрахованих УКС, які повністю заповнені інформацією;
- ОЦ для всього попереднього інформаційного об’єкту;
- ключі, на яких здійснено формування ОЦ.

Після дописування нового інформаційного об’єкту до попереднього інформаційного об’єкту для формування нового значення ОЦ всього інформаційного об’єкту інформації потрібно додаткові параметри, що запам’ятовані, використати як вхідні для алгоритму формування нового значення ОЦ.

Алгоритм реалізує три режими оброблення інформації.

Перший режим є таким, коли загальна кількість байтів попереднього інформаційного об’єкту для формування ОЦ більша за УКС (Nсф > N).

У другому режимі загальна кількість байтів попереднього інформаційного об’єкту для формування ОЦ менша ніж УКС (Nсф < N).

Третій режим є таким, коли загальна кількість байтів попереднього інформаційного об’єкту при діленні на кількість байтів в УКС дає ціле число (Nсф/N = ціле).

Розглянемо роботу алгоритму для кожного із режимів більш докладно.

При роботі алгоритму формування нового значення ОЦ за першим режимом (Nсф > N) потрібно виконати наступні дії:

1. Виділити із ОЦ для всього попереднього інформаційного об’єкту ОЦ, яка

обраховувалась лише для повних УКС, для чого потрібно обрахувати ОЦ для останнього з УКС попереднього інформаційного об'єкту та виконати операцію порозрядного додавання по модулю 2 з ОЦ всього попереднього інформаційного об'єкту.

2. Дописати останнє неповне УКС попереднього інформаційного об'єкту інформацією із інформаційного об'єкту інформації, що дописується, та обрахувати ОЦ для даного дописаного УКС. При цьому після розрахунку базових констант не слід виконувати над ними операцію порозрядного додавання по модулю 2 для обрахування К1, а присвоїти відповідній змінній запам'ятовану К.

3. При першому виконанні операції порозрядного додавання по модулю 2 для ОЦ, потрібно використати виділену ОЦ для повних УКС попереднього інформаційного об'єкту та ОЦ, обраховану в п. 2.

4. Подальша робота алгоритму формування нового значення ОЦ відповідає існуючому, при цьому читання здійснюється з інформаційного об'єкту, що дописується, наступних байтів, які не були використані для дописування УКС в п. 2.

При роботі алгоритму формування нового значення ОЦ за другим режимом (Nсф < N) потрібно попередній інформаційний об'єкт доповнити новою інформацією та обрахувати нове значення ОЦ за існуючим алгоритмом. При цьому ОЦ, обрахованою для попереднього інформаційного об'єкту, потрібно знехтувати.

При роботі алгоритму формування нового значення ОЦ за третім режимом (Nсф/N = ціле) виконуються наступні дії:

1. Читання здійснюється з інформаційного об'єкту, що дописується. Після розрахунку базових констант не слід виконувати над ними операцію порозрядного додавання по модулю 2, а присвоїти відповідній змінній запам'ятовану К.

2. При першому виконанні операції порозрядного додавання по модулю 2 для ОЦ, потрібно використати ОЦ для всього попереднього інформаційного об'єкту та ОЦ, обраховану в п.1.

3. Подальша робота алгоритму формування нового значення ОЦ відповідає існуючому.

Висновки

Описаний варіант організації контролю цілісності у відповідності до вимог, передбачених нормативними документами систем ТЗІ України, забезпечує контроль цілісності в режимах: контроль за запитом (на вимогу адміністратора), контроль при старті програмного засобу (при включенні комп'ютера), таймерний контроль. Крім цього, запропонований спосіб підвищення швидкості формування ознак цілісності дозволяє більш ефективно використовувати механізм контролю цілісності інформації, наведений в [4]. Цей спосіб особливо ефективний у випадках, коли є необхідність санкціонованої модифікації інформаційного об'єкту типу збільшення об'єму інформації в файлах, таблицях бази даних та т.п. При великих об'ємах інформації, та при досить частих модифікаціях це дасть змогу підвищити швидкість контролю цілісності.

Література: 1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. 2. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. 3. НД ТЗІ 2.2-002-98. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. 4. Будько М. М., Василенко В. С., Короленко М. П. Механізми контролю цілісності інформації та її поновлення. // Правове, нормативне та метрологічне забезпечення системи захисту

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

інформації в Україні. НТУУ ”КПІ”. К. 2000. - с. 130-138.

УДК 621.396: 621.391

КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В СТАНДАРТЕ СОТОВОЙ СВЯЗИ GSM

Александр Корнейко, Денис Кравченко, Юрий Черевко
Киевский военный институт управления и связи

Анотація: **Розглянуті криптографічні властивості алгоритмів A3A8 і A5, що використовуються у стандарті системи стільникового зв'язку GSM. Показано, що при розробці алгоритмів криптоперетворень стандарту GSM був допущений ряд помилок, що знижують їх криптостійкість. Визначено, що для криптоаналізу алгоритму A3A8 можна застосувати так звану “атаку з обраним викликом” за умови забезпечення фізичного доступу до SIM-карти, а для A5 – атаку типу “балансування час-пам'ять”.**

Summary: **The cryptographic properties of the A3A8 and A5 algorithms, used in the cellular communications standard GSM, are considered. It was shown that there is a number of breaches in the design of the cryptographic transformations which reduce the crypt security. It was determined that one can use so called «attack with chosen call» for the crypt analysis of A3A8 provided the physical access to SIM-card, and «time-memory trade off attack» – for A5.**

Ключові слова: **Стандарт стільникового зв’язку GSM, криптоалгоритми A3, A5, A8, криптостійкість.**

Введение

В настоящее время системы сотовой связи (ССС) стандарта GSM находят все большее применение в обеспечении надежной и мобильной автоматической телефонной связи субъектов предпринимательской деятельности государственной и частной форм собственности, а также законодательных и исполнительных структур органов государственной власти. Однако в ССС передача информации между мобильной и базовой станциями происходит по радиоканалу, что накладывает достаточно жесткие требования на обеспечение их информационной безопасности, которая реализуется на основе соответствующих криптографических алгоритмов.

I Анализ встроенных механизмов криптографической защиты информации стандарта GSM

Стандарт GSM (Global System of Mobile Communications), который в настоящее время наиболее массово используется в ССС Европы в диапазонах частот 900 (GSM-900) и 1800 (DCS-1800) Мгц, а также в Америке в диапазоне 1900 (PCN-1900) МГц, уже при его разработке изначально предполагал достаточно мощные механизмы обеспечения информационной безопасности ССС. Так действующие нормативные документы организации разработчиков стандарта GSM определяют, что все ССС этого стандарта должны обеспечивать следующие механизмы защиты системных и информационных ресурсов:

- защита от несанкционированного доступа к мобильной станции (МС) с помощью парольного метода защиты;
- идентификация мобильного абонента ССС с помощью его уникального международного идентификационного номера (МИН);
- аутентификация (определение подлинности) абонента при каждом вхождении в связь с помощью алгоритма A3;
- конфиденциальность передаваемой по радиоканалу информации путём её шифрования с помощью алгоритма A5, где ключ шифрования вычисляется алгоритмом A8;
- секретность местонахождения абонента и направления его вызова.

Общее описание применения данных механизмов защиты информационных ресурсов ССС стандарта GSM приведено в Рекомендации ETSI\GSM 03.21. В данном документе указывается, что криптографическая защита информационных ресурсов ССС обеспечивается за счет использования алгоритмов A3, A5 и A8, носителем которых, за исключением A5, является SIM-карта абонента. Данная карта выполнена в виде съёмного блока МС и кроме алгоритмов A3 и A8 содержит также МИН и индивидуальный ключ аутентификации *i*-го пользователя (Ki).

Рассмотрим более детально перечисленные выше механизмы защиты стандарта GSM.

Исключение несанкционированного доступа к SIM-карте реализуется с помощью проверки пароля (PIN

ISBN 966-622-022-9