УДК 681.322.067

М.О. Справа, магістрант
Житомирський державний технологічний університет

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У ВИЩОМУ НАВЧАЛЬНОМУ ЗАКЛАДІ

(Представлено д.т.н., проф. Самотокіним Б.Б.)

Викладено основні поняття та положення щодо організації захисту інформації від несанкціонованого доступу. Проаналізовані потенційні загрози безпеки інформації. Наведені основні методи захисту інформації.

Актуальність і постановка проблеми. Проблема захисту інформації не є новою. Вона з'явилася ще задовго до появи комп'ютерів. Стрімке вдосконалення комп'ютерних технологій позначилося й на принципах побудови захисту інформації. З самого початку свого розвитку системи інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло призвести до величезних жертв, у тому числі й людських. Тому конфіденційності (тобто нерозголошенню інформації) в перших системах безпеки приділялася особлива увага. Очевидно, що надійно захистити повідомлення й дані від розголошення і перехоплення може тільки повне їхнє шифрування. Принципова особливість сучасної ситуації полягає в тому, що найважливішим завданням сьогодні стає захист інформації в комп'ютерних мережах. Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

Аналіз існуючих рішень в області захисту інформації. Існуючі методи та засоби захисту інформації від несанкціонованого доступу можна поділити на такі категорії:

- законодавчі;
- організаційні;
- апаратні;
- програмні.

Мета законодавчих заходів – попередження та стримування потенційних зловмисників. Функціонування даного комплексу здійснюється через створення та введення в дію законів, постанов та інструкцій, що регулюють юридичну відповідальність осіб-користувачів та технічного персоналу обслуговування інформаційної системи за витік, втрату або модифікацію інформації, за яку вони несуть відповідальність.

В Україні питання регулювання інформаційного обміну розглядаються, зокрема, в таких законах:

- Закон України “Про інформацію”;
- Закон України “Про науково-технічну інформацію”;
- Закон України “Про авторське право та суміжні права”;
- Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”;
- Закон України “Про електронний цифровий підпис”.

Організаційні заходи із захисту інформації в комп’ютеризованих системах мають охоплювати етапи проектування, розробки, виготовлення, випробування, підготовки до експлуатації системи. Витік інформації про важливі характеристики системи може призвести до зниження безпечності інформаційного обміну через можливість використання зловмисником слабких місць у реалізації системи або певних конструкційних особливостей апаратури. До організаційних заходів захисту інформації належать:

- створення відповідних режимів роботи з інформаційною системою з урахуванням ступеня секретності інформації;
- створення та впровадження інструкцій та положень із забезпечення режимів секретності;
- створення захищених зон інформаційної системи з обмеженим доступом та організацією служби безпеки;
- розмежування кола задач за певними виконавцями та обмеження доступу до інформації в цілому;
- постійний контроль за виконанням режимів секретності та облік доступу до інформації відповідно до кожного оператора;
- встановлення та розподілення відповідальності за витік інформації за службами безпеки та конкретними особами.

Апаратні засоби захисту використовуються для обмеження доступу до фізичних носіїв інформації, контролю та перевірки цілісності інформації та допоміжної апаратури для її обробки.

Програмні засоби захисту призначені для захисту структури інформації від випадкових або злочинних маніпуляцій, приховування структури та змісту інформації тощо.

Метою досліджень є розробка системи захисту інформації для деканату і кафедри університету.

Викладення основного матеріалу. Початковий етап розвитку комп'ютерної безпеки міцно пов'язаний із криптографією. Головні умови безпеки інформації – її доступність і цілісність. Інакше кажучи, користувач може в будь-який час запросити необхідний йому набір сервісних послуг, а система безпеки повинна гарантувати при цьому його правильну роботу. Будь-який файл або ресурс системи, при дотриманні прав доступу, має бути доступним користувачеві в будь-який час. Якщо якийсь ресурс недоступний, то він непотрібний. Інше завдання захисту – забезпечити незмінність інформації під час її зберігання або передачі. Це так звана умова цілісності.

Виконання процедур шифрування й дешифрування у будь-якій системі інформаційного процесу сповільнює передачу даних і зменшує їхню доступність, тому що користувач буде занадто довго чекати свої "надійно захищені" дані, а це неприпустимо в деяких сучасних комп'ютерних системах. Тому система безпеки повинна в першу чергу гарантувати доступність і цілісність інформації, а потім уже (якщо необхідно) її конфіденційність.

Принцип сучасного захисту інформації можна сформулювати так – пошук оптимального співвідношення між доступністю й безпекою.

Повністю захищений комп'ютер – це той, який знаходиться під замком у броньованій кімнаті в сейфі, не підключений ні до якої мережі (навіть електричної) і вимкнений. Такий комп'ютер має абсолютний захист, однак використати його не можна. У цьому прикладі не виконується вимога доступності інформації. "Абсолютності" захисту заважає не тільки необхідність користуватися захищеними даними, але й ускладнення систем захисту інформації. Використання постійних механізмів захисту, що не розвиваються, – небезпечне, і для цього є кілька причин.

Одна з них – розвиток власної мережі. Адже захисні властивості електронних систем безпеки багато в чому залежать від конфігурації мережі й використовуваних у ній програм. Навіть якщо не міняти топологію мережі, однаково доведеться коли-небудь використати нові версії раніше встановлених продуктів. Однак може трапитися так, що нові можливості цього продукту зроблять "пролом" у захисті системи безпеки.

Крім того, не можна забувати про розвиток й удосконалення засобів нападу. Техніка так швидко змінюється, що важко визначити, який новий пристрій або програмне забезпечення, використане для нападу, може обійти ваш захист.

Комп'ютерний захист – це постійна боротьба з "дурістю" користувачів й інтелектом хакерів. Навіть хакери найчастіше використовують саме некомпетентність і недбалість обслуговуючого персоналу, саме останніх можна вважати головною загрозою для інформаційної безпеки. Одна з подібних проблем – так звані слабкі паролі. Користувачі для зручності обирають паролі, що легко запам'ятовуються. Причому проконтролювати складність паролю неможливо. Інша проблема – нехтування вимогами безпеки. Наприклад, небезпечно використовувати неперевірене програмне забезпечення. Зазвичай користувач сам "запрошує" у систему віруси й "троянських коней". Крім того, багато неприємностей може принести неправильно введена команда.

Криптографія – найбільш могутній засіб захисту інформації, що виник за багато століть до нашої ери, її основний зміст полягає в перетворенні тексту на випадковий, хаотичний набір знаків. Вона розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином.

Конфіденційність інформації забезпечується симетричним та асиметричним шифруванням. Цілісність інформації та автентичність сторін досягається використанням хеш-функцій та технологій цифрового підпису. Сукупність технологій, що забезпечують конфіденційність та цілісність інформації при її передачі незахищеними каналами зв'язку, отримала назву віртуальних приватних мереж (VPN – Virtual Private Network). Реалізація даних технологій може здійснюватися програмними та програмно-апаратними засобами. Захист інформації на робочих станціях і серверах може реалізовуватися за допомогою шифрування на рівні файлової системи, криптографічних методів перевірки автентичності (цифрові сертифікати, одноразові паролі тощо), криптографічних засобів перевірки цілісності.

Для математичного аналізу криптографія використовує інструменти абстрактної алгебри. Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. Відомо більше десятка перевірених алгоритмів шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму роблять шифрований текст недоступним для криптоаналізу.

Наведемо короткий перелік деяких найвідоміших алгоритмів шифрування:

1. Метод DEC (Data Encryption Standard), який є федеральним стандартом США, розроблений фірмою IBM та рекомендований для використання Агентством національної безпеки США. Алгоритм криптографічного захисту відомий і опублікований.

Він характеризується такими властивостями: високим рівнем захисту даних проти дешифрування і можливої модифікації даних; простотою розуміння; високим ступенем складності, яка робить його розкриття дорожчим від отримуваного прибутку; методом захисту, який базується на ключі та не залежить від "секретності" механізму алгоритму; економічністю в реалізації та ефективним у швидкодії алгоритмом.

Разом з тим, йому властиві такі недоліки: малий розмір ключа, який свідчить, що для дешифрування потрібно 7×1016 операцій на секунду (на даний час апаратури, здатної виконати такі обсяги обчислень, немає, але вона може з'явитися в майбутньому); окремі блоки, що містять однакові дані, будуть виглядати однаково, що є погано з точки зору криптографії.

2. Російський стандарт шифрування даних ГОСТ 28147–89. Єдиний алгоритм криптографічного перетворення даних для великих інформаційних систем. Не накладає обмежень на ступінь секретності інформації. Має переваги алгоритму DEC і в той же час позбавлений від його недоліків. Крім того, в стандарт закладений метод, що дозволяє зафіксувати невиявлену випадкову чи навмисну модифікацію зашифрованої інформації. Однак загальним його недоліком є складність програмної реалізації.

3. Метод з відкритим ключем (RSA). Шифрування проводиться першим відкритим ключем, розшифрування – іншим секретним ключем. Метод надзвичайно перспективний, оскільки не вимагає передачі ключа шифрування іншим користувачам. Спеціалісти вважають, що системи з відкритим ключем зручніше застосовувати для шифрування даних, що передаються, ніж при збереженні інформації. Існує ще одна галузь використання даного алгоритму – цифрові підписи, що підтверджують справжність документів та повідомлень, що передаються. Проте і він не є зовсім досконалим. Його недоліком є не до кінця вивчений алгоритм. Не існує строгого доведення його надійності математичними методами.

Вибір засобів захисту інформації в автоматизованій системі інформаційного забезпечення – складна задача, при розв'язанні якої потрібно враховувати імовірності різних загроз інформації, вартість реалізації різних засобів захисту і наявність різних зацікавлених сторін. Користувачам важливо знати, що сучасна наука має в своєму розпорядженні методи, що дозволяють вибрати таку сукупність засобів захисту, яка забезпечить максимізацію міри безпеки інформації при даних витратах або мінімізацію витрат при заданому рівні безпеки інформації.

А чи потрібна криптографія в офісі, вдома чи, наприклад, в університеті? Довідавшись, що це наука про захист даних, робиш висновок, що без неї в роботі не обійтися. Як тут не згадати про перехоплення конфіденційного електронного листування, "троянських коней", що маскуються під латки для Windows, та інші витівки зловмисників. Отже, як захистити важливу для вас інформацію?

Розглянемо на прикладі деканату та кафедри університету, які найпростіші методи захисту інформації можна застосувати. В базі даних деканат–кафедра зберігаються такі документи:

- екзаменаційні відомості та контрольні заходи відповідно до робочого плану;
- результати контрольних заходів по відомостях;
- семестрові журнали;
- екзаменаційно-залікові листи в журналах перескладань;
- довідкова інформація з розкладу занять та сесії;
- результати сесій;
- списки студентів з розподілу стипендії за результатами сесії;
- рейтинги успішності;
- журнал відвідування;
- вибірки по боржниках;
- відомості про державний іспит та дипломне проектування;
- додатки до дипломів;
- оцінки студентів за певний період та ін.

Наведені дані мають різний ступінь важливості та секретності. До одних повинні мати доступ лише уповноважені особи, до інших – і працівники деканату, і студенти. Найпростіший спосіб захисту конфіденційної інформації – це приховати від небажаного перегляду файл або всю папку. Windows надає такі засоби, використовуючи атрибут файлу. У MS Office є прості й ефективні інструменти для захисту документів паролем. Цих дій цілком достатньо для випадків, коли інформація у файлах не становить великої цінності, та все-таки розголошення її небажане.

Для документів, зміна яких є небажаною, але доступ до яких необхідний багатьом працівникам і студентам, слід задати пароль дозволу запису. При цьому документ можна буде переглянути без введення пароля і зберегти його в незміненому вигляді під іншим іменем. До речі, перейменований документ теж буде захищений тим самим паролем. Щоб відредагувати захищений у такий спосіб файл,

треба буде ввести пароль. Таким чином можна захищати, наприклад, відомості з результатів сесій, журнал відвідування, розклад занять, повідомивши працівникові, який їх заповнює, правильний пароль.

Якщо немає гострої потреби захищати документ паролем, можна просто ввімкнути опцію "рекомендувати доступ тільки для читання". У цьому випадку при відкритті документу користувачу буде запропоновано переглянути його в режимі читання. У такий спосіб можна захистити дані від випадкових змін. Цей варіант найкраще використовувати для захисту базових документів. Крім того, для захисту документа від випадкової зміни можна скористатися опцією "завжди створювати резервну копію".

Слід визнати, що алгоритм захисту, який використовують у програмах MS Office, доволі примітивний, тому не треба покладатися на нього при збереженні важливих документів.

У поширених архіваторах WinZip і WinRar алгоритми шифрування за своєю структурою на порядок перевершують засоби шифрування в MS Office. Однак і в них виявляють "діри", що дозволяють зламати архів з цінними даними, не тільки підібравши пароль, а й використовуючи помилки в програмному коді. Тож завжди потрібно бути напоготові та застосовувати ці утиліти як засоби криптозахисту, тільки будучи впевненим у тому, що "імовірний противник" не дуже добре "підкований у сфері Hi-Tech". Під час дешифрування архіву програми злому атакують "у лоб", перебираючи всі можливі комбінації букв, цифр і спеціальних символів. Тому, захищаючи паролем важливий архів, краще задавати пароль, що складається з якомога більшої кількості символів, що включають як букви і цифри, так і спеціальні символи. У цьому випадку знайти з бази даних програм злому необхідну комбінацію стає неможливо і залишається тільки метод перебору.

Також для обміну важливими даними в мережі деканату та кафедри можна використати вільно поширюване програмне забезпечення PGP (Pretty Good Privacy), яке набуло великої популярності серед користувачів комп'ютерів завдяки простоті використання. Нині PGP стало практично стандартом для захисту електронної пошти. Розглянуті вище однорівневі способи криптографії передбачають, що сторони, які обмінюються інформацією, повинні спочатку обмінятися своїми паролями. Причому робити це бажано при особистій зустрічі, а це не завжди зручно. Системи з двома ключами (публічним і секретним), до яких належить і програма PGP, позбавлені недоліку однорівневого способу. Публічний ключ – це невеликий текстовий блок даних, який можна повідомити іншій стороні відкрито, надіславши електронною поштою. За допомогою публічного ключа друга сторона шифруватиме повідомлення, призначені для вас. У свою чергу, прочитати інформацію, відіслану іншою стороною, зумієте тільки ви, застосувавши свій неповторний секретний ключ. Для дешифрування даних не підійде пароль, заданий під час початкового шифрування конфіденційних даних. Тому система з двома ключами є дуже надійною: навіть сам відправник не розшифрує тільки що відправлений ним лист.

Ховати текстові повідомлення в графічних файлах може утиліта S-Tools. Вона використовує різні методи шифрування, у тому числі й дуже потужний алгоритм Triple DES з довжиною ключа 168 біт. Вигляд малюнка із закодованим текстом залишається практично незмінним.

Також у даному випадку можна використовувати спеціально розроблені програми для роботи у вищих навчальних закладах, що включають і захист даних від несанкціонованого доступу, і створення баз даних у деканатах, бібліотеках, на кафедрах університетів.

Висновки. Отже, документи, зміна яких є небажаною, але які не є секретними, достатньо захистити паролем або рекомендувати тільки для читання. Пароль повинен складатися з якомога більшої кількості символів. Для обміну в мережі більш важливими документами краще використовувати криптографічні системи з двома ключами. Використовуючи шифрування повідомлень в поєднанні з правильним встановленням комунікаційних засобів, належними процедурами ідентифікації користувача, можна досягнути високого рівня захисту інформаційного обміну.

ЛІТЕРАТУРА:

1. *Ван Тилборг Х.К.А.* Основы криптологии: Профессиональное руководство и интерактивный учебник : пер. с англ. / *Ван Тилборг Х.К.А.* – М. : Мир, 2006. – 148 с.
2. *Гніліцький В.В.* Засоби захисту інформації в автоматизованих системах / *В.В. Гніліцький, Ю.П. Жураковський, С.А. Лаптев* // Вісник ЖІТІ. – 2000 – № 14. – С. 175–181.
3. *Гніліцький В.В.* Захист інформації : навчальний посібник для студентів економічних спеціальностей / *В.В. Гніліцький, Є.Г. Орєхов.* – Житомир : ІМІДЖ, 2009. – С. 29–30.

СПРАВА Марина Олександрівна – магістрант кафедри автоматики та управління в технічних системах Житомирського державного технологічного університету.

Наукові інтереси:
- захист інформації від несанкціонованого доступу;
- криптографія.

Подано 17.01.2010

Справа М.О. Проблеми захисту інформації у вищому навчальному закладі
Справа М.А. Проблемы защиты информации в высшем учебном заведении
Sprava M.O. The problems of protection of information at the univercity

УДК 681.322.067

Информация "под замком" / М.А. Справа

Рассмотрены основные понятия и положения касательно организации защиты информации от несанкционированного доступа. Проанализированы потенциальные угрозы безопасности информации. Приведены основные методы защиты информации.

УДК 681.322.067

The problems of protection of information at the univercity / M.O. Sprava

The basic aspects of organization of protection of sensitive information against unauthorized access are discussed. Potential threats of security of information are analyzed. The fundamental methods of protection of information are considered.