**Тарас Ромашенко**
студент 1 СТН курсу спеціальності 073 «Менеджмент»
Науковий керівник: **Мушеник І.М.**
к.е.н., доцент кафедри інформаційних технологій,
Подільський державний аграрно-технічний університет,
м. Кам’янець-Подільський

# АСПЕКТИ БЕЗПЕКИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаної з носієм, може легко і швидко копіюватися і передаватися по каналах зв'язку. Відомо дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку зовнішніх порушників, так і з боку внутрішніх порушників.

Радикальне вирішення проблем захисту електронної інформації може бути отримано тільки на базі використання криптографічних методів, які дозволяють вирішувати найважливіші проблеми захищеної автоматизованої обробки та передачі даних. При цьому сучасні швидкісні методи криптографічного перетворення дозволяють зберегти вихідну продуктивність автоматизованих систем. Криптографічні перетворення даних є найбільш ефективним засобом забезпечення конфіденційності даних, їхньої цілісності і справжності. Тільки їх використання в сукупності з необхідними технічними та організаційними заходами можуть забезпечити захист від широкого спектру потенційних загроз.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи:

– Перехоплення інформації - цілісність інформації зберігається, але її конфіденційність порушена;
– Модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і відсилається адресату;
– Підміна авторства інформації. Дана проблема може мати серйозні наслідки.

Наприклад, хтось може надіслати листа від вашого імені (цей вид обману прийнято називати спуфінга) або Web - сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

Потреби сучасної практичної інформатики призвели до виникнення нетрадиційних завдань захисту електронної інформації, однією з яких є автентифікація електронної інформації в умовах, коли обмінюються інформацією сторони не довіряють один одному. Ця проблема пов'язана зі створенням систем електронного цифрового підпису. Теоретичною базою для вирішення цієї проблеми було відкриття двухключевой криптографії американськими дослідниками Діффі і Хеміманом в середині 1970-х років, яке стало блискучим досягненням багатовікового еволюційного розвитку криптографії. Революційні ідеї двухключевой криптографії призвели до різкого зростання числа відкритих досліджень в галузі криптографії і показали нові шляхи розвитку криптографії, нові її можливості і унікальне значення її методів у сучасних умовах масового застосування електронних інформаційних технологій.

Технічною основою переходу в інформаційне суспільство є сучасні мікроелектронні технології, які забезпечують безперервне зростання якості засобів обчислювальної техніки і служать базою для збереження основних тенденцій її розвитку - мініатюризації, зниження електроспоживання, збільшення обсягу оперативної пам'яті (ОП) і місткості вбудованих і знімних накопичувачів, зростання продуктивності і надійності, розширення сфер і масштабів застосування. Дані тенденції розвитку засобів обчислювальної техніки призвели до того, що на сучасному етапі захист комп'ютерних систем

від несанкціонованого доступу характеризується зростанням ролі програмних та криптографічних механізмів захисту в порівнянні з апаратними.

Зростання ролі програмних і криптографічних засобів зашитий проявляється в тому, що виникають нові проблеми в галузі захисту обчислювальних систем від несанкціонованого доступу, вимагають використання механізмів і протоколів з порівняно високою обчислювальною складністю і можуть бути ефективно вирішені шляхом використання ресурсів ЕОМ.

Однією з важливих соціально-етичних проблем, породжених все більш розширюється застосуванням методів криптографічного захисту інформації, є протиріччя між бажанням користувачів захистити свою інформацію і передачу повідомлень і бажанням спеціальних державних служб мати можливість доступу до інформації деяких інших організацій та окремих осіб з метою припинення незаконної діяльності . У розвинених країнах спостерігається широкий спектр думок про підходи до питання про регламентації використання алгоритмів шифрування. Висловлюються пропозиції від повної заборони широкого застосування криптографічних методів до повної свободи їх використання. Деякі пропозиції відносяться до вирішення використання тільки ослаблених алгоритмів або до встановлення порядку обов'язкової реєстрації ключів шифрування. Надзвичайно важко знайти оптимальне рішення цієї проблеми. Як оцінити співвідношення втрат законослухняних громадян і організацій від незаконного використання їх інформації і збитків держави від неможливості отримання доступу до зашифрованої інформації окремих груп, що приховують свою незаконну діяльність? Як можна гарантовано не допустити незаконне використання криптоалгоритмів особами, які порушують і інші закони? Крім того, завжди існують способи прихованого зберігання і передачі інформації. Ці питання ще належить вирішувати соціологам, психологам, юристам і політикам.

Виникнення глобальних інформаційних мереж типу INTERNET є важливим досягненням комп'ютерних технологій, однак, з INTERNET пов'язана маса комп'ютерних злочинів.

Результатом досвіду застосування мережі INTERNET є виявлена слабкість традиційних механізмів захисту інформації та відставання у застосуванні сучасних методів. Криптографія надає можливість забезпечити безпеку інформації в INTERNET і зараз активно ведуться роботи з впровадження необхідних криптографічних механізмів в цю мережу. Не відмова від прогресу в інформатизації, а використання сучасних досягнень криптографії - ось стратегічно правильне рішення. Можливість широкого використання глобальних інформаційних мереж та криптографії є досягненням і ознакою демократичного суспільства.

Володіння основами криптографії в інформаційному суспільстві об'єктивно не може бути привілеєм окремих державних служб, а є нагальною необхідністю для самих широких верств науково-технічних працівників, що застосовують комп'ютерну обробку даних або розробляють інформаційні системи, співробітників служб безпеки і керівного складу організацій і підприємств. Тільки це може служити базою для ефективного впровадження та експлуатації засобів інформаційної безпеки.

Одна окремо взята організація не може забезпечити досить повний і ефективний контроль за інформаційними потоками в межах всієї держави і забезпечити належний захист національного інформаційного ресурсу. Однак, окремі державні органи можуть створити умови для формування ринку якісних засобів захисту, підготовки достатньої кількості фахівців і оволодіння основами криптографії та захисту інформації з боку масових користувачів.

У Росії та інших країнах СНД на початку 1990-х років чітко простежувалася тенденція випередження розширення масштабів і сфер застосування інформаційних технологій над розвитком систем захисту даних. Така ситуація у певній мірі була і є типовою і для розвинених капіталістичних країн. Це закономірно: спочатку повинна виникнути практична проблема, а

потім будуть знайдені рішення. Початок перебудови в ситуації сильного відставання країн СНД в області інформатизації в кінці 1980-х років створило благодатний грунт для різкого подолання сформованого розриву.

Приклад розвинених країн, можливість придбання системного програмного забезпечення і комп'ютерної техніки надихнули вітчизняних користувачів. Включення масового споживача, зацікавленого в оперативній обробці даних та інших достоїнствах сучасних інформаційно-обчислювальних систем, у вирішенні проблеми комп'ютеризації призвело до дуже високим темпам розвитку цієї області в Росії та інших країнах СНД. Однак, природне спільне розвиток засобів автоматизації обробки інформації і засобів захисту інформації в значній мірі порушилося, що стало причиною масових комп'ютерних злочинів. Ні для кого не секрет, що комп'ютерні злочини в даний час складають одну з дуже актуальних проблем.

Використання систем захисту зарубіжного виробництва не може виправити цей перекіс, оскільки надходять на ринок Росії продукти цього типу не відповідають вимогам через існуючих експортних обмежень, прийнятих у США - основному виробнику засобів захисту інформації. Іншим аспектом, що має першорядне значення, є те, що продукція такого типу повинна пройти встановлену процедуру сертифікації в уповноважених на проведення таких робіт організаціях.

Сертифікати іноземних фірм та організацій, ніяк не можуть бути заміною вітчизняним. Сам факт використання зарубіжного системного та прикладного програмного забезпечення створює підвищену потенційну загрозу інформаційних ресурсів. Застосування іноземних засобів захисту без належного аналізу відповідності виконуваних функцій і рівня захисту, який він може багаторазово ускладнити ситуацію.

Форсування процесу інформатизації вимагає адекватного забезпечення споживачів засобами захисту. Відсутність на внутрішньому ринку достатньої кількості засобів захисту інформації, що циркулює в комп'ютерних системах, значний час не дозволяло в необхідних масштабах здійснювати заходи щодо

захисту даних. Ситуація погіршувалася відсутністю достатньої кількості фахівців у галузі захисту інформації, оскільки останні, як правило, готувалися тільки для спеціальних організацій. Реструктурування останніх, пов'язане із змінами, що відбуваються в Росії, привело до утворення незалежних організацій, що спеціалізуються в області захисту інформації, що поглинув вивільнені кадри, і як наслідок виникнення духу конкуренції, що призвела до появи в даний час досить великої кількості сертифікованих засобів захисту вітчизняних розробників.

Однією з важливих особливостей масового використання інформаційних технологій є те, що для ефективного вирішення проблеми захисту державного інформаційного ресурсу необхідно розосередження заходів щодо захисту даних серед масових користувачів. Інформація повинна бути захищена в першу чергу там, де вона створюється, збирається, переробляється і тими організаціями, які несуть шкоди безпосередній при несанкціонованому доступі до даних. Цей принцип раціональний і ефективний: захист інтересів окремих організацій - це складова реалізації захисту інтересів держави в цілому.

## Список використаних джерел

1. Острейковскій В.А. Інформатика: Учеб. посібник для студ. середовищ. проф. навч. закладів. - М.: Вищ. шк., 2001. - 319с.

2. Економічна інформатика / під ред. П.В. Конюховского і Д.М. Колесова. - СПб.: Пітер, 2000. - 560с.

3. Інформатика: Базовий курс / С.В. Симонович та ін - СПб.: Пітер, 2002. - 640с.

4. Молдовян А.А., Молдовян Н.А., Рад Б.Я. Криптографія. - СПб.: Видавництво "Лань", 2001. - 224с., Іл. - (Підручники для вузів. Спеціальна література).