МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

21-22 квітня 2022 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 21-22 квітня 2022 р**.** - Одеса, Видавництво ОНТУ, 2022 р. – 251 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова - д.т.н., проф., **Єгоров Б.В.**, ректор ОНТУ

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНТУ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНТУ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м.Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц., Київський національний університет імені Тараса Шевченка

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНТУ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНТУ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНТУ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ “Львівська політехніка”,
Жуков І.А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською та англійською мовами.
Редактор збірника Котлик С.В.

Висновки. Забезпечення безпеки інформації в системі є ключовою складовою у якості роботи ІАС. Розроблена система захисту дає змогу повністю виключити можливість стороннього втручання до системи та гарантує повне забезпечення інформаційної конфіденційності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 Магических мер разработки безопасногопрограммного обеспечения [Электронный ресурс]. URL: https://cyberrus.com/wp-content/uploads/2015/12/vkb_13_1.pdf.
2. Киверина Н. Ш. АНАЛИЗ УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ / Н. Ш. Киверина // Международный научно-исследовательский журнал. — 2015. — №5 (36) Часть 2. — С. 73—74. — URL: https://research-journal.org/technical/analiz-uyazvimosti-informacionnoj-sistemy/.
3. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем: М.: Изд-во ВПК, 2008
4. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. №1(1). С. 44-48.
5. Безкоровайный М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем. Руководство системного аналитика. 2-е изд., доп.: М.: Вооружение. Политика. Конверсия, 2002. 305 с.
6. Зубарев И.В., Жидков И.В., Кадушкин И.В., Медовщикова С.А. Уязвимости информационных систем «Information and mathematical technologies in science and management» 2016

УДК 004.056.55

ШИФРУВАННЯ ДАНИХ ЯК ОДИН З МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

В.Р.ПОПОВА, І.С.БОБРІКОВА
(bobrikova.irina@gmail.com)
Одеський національний технологічний університет

Захист персональної конфіденційної інформації знаходиться під загрозою у зв'язку з сучасним технологічним прогресом. Значна більшість людей налаштовує комунікації завдяки електронним технічним засобам. Інформація у великих обсягах передається, обробляється та зберігається на носіях. У зв'язкуз високим рівнем діджиталізації багатьох сфер діяльності людства та впливу мережі Інтернет - інформація набуває значущу роль у житті багатьох людей. Стає багато питань щодо конфіденційності, цілісності та ідентифікованості даних при передачі, обробці та зберігані інформації. Питання шифруванняданих стає все більш актуальним у наш час.

Вступ і постановка проблеми

У сучасному світі проблема захисту інформації викликає велику зацікавленість не тільки з боку військових або державних діячів, але й у звичайних людей. Сьогодні зловмисники мають можливість аналізувати інтернет-контент та інші дані користувачів аж до додатків на їх смартфонах, за допомогою яких забезпечується передача особистих повідомлень. У зв'язку з цим актуальність захисту даних зумовлена необхідністю шифрування інформації, що передається для того, щоб вивчити її могли тільки ті особи, кому вона призначається.

Методи шифрування

- Симетричне шифрування
- Асиметричне шифрування

- Необоротне шифрування

Симетричне шифрування

Симетричне шифрування з'явилося першим. Для шифрування даних використовується ключ, який слугує і для дешифрування даних. [1] Якщо є ключ, тоді розшифрувати дуже просто.

Алгоритми з симетричними ключами мають дуже високу продуктивність. Криптографія з симетричними ключами стійка, що робить практично неможливим процес дешифрування без знання ключа. За інших рівних умов стійкість визначається довжиною ключа.

Асиметричне шифрування

Асиметричне шифрування вирішує проблему передачі ключа по мережі, тому що для даного виду шифрування використовуються два ключи: відкритий і закритий. За допомогою спеціалізованої програми генерується пара з відкритогоі закритого ключа.

Відкритий ключ застосовується для шифрування, а для дешифрування потрбіен закритий ключ.

Необоротне шифрування

Даний метод відрізняється тим, що використовуваний алгоритм перетворює дані тільки в одну сторону, зворотне перетворення (дешифрування)неможливо.[2]

Необоротний метод застосовується для шифрування паролів. І щоб перевірити чи правильно ввів користувач пароль введені дані також шифруються, і результат порівнюється з зашифрованим паролем, що зберігаються в базі.

Сфери застосовання алгоритмів шифрування

Шифрування даних застосовується для зберігання важливої, конфіденційної інформації на надійних носіях, а також для передачі її через незахищені канали зв'язку. Різні алгоритми шифрування постійно застосовуються в банківських і корпоративних мережах для захисту від промислового шпигунства або взлому. Всі канали та сервери в таких системах є захищеними, тобто підданими обробці тим чи іншим алгоритмом шифрування. Такі системи вимагають обов'язкового поточного шифрування каналів зв'язку намережевому рівні і вище, що забезпечує захист переданого трафіку від компрометації при передачі по потенційно скомпрометованим провайдерським каналам, а потенційно скомпрометованим каналом для банку вважається будь- який канал, який не забезпечується самим банком як провайдером.

Важливість шифрування

Як відомо, у світі інформаційних технологій, кількість кіберзлочинів зростає, і це змушує користувачів комп'ютерів захищати свої дані від хакерів. Великі корпорації та уряди вимагають високого рівня шифрування для захисту своїх конфіденційних планів, таких як комерційні секрети і конфіденційні дані. Це також дає нам впевненість в тому, що наші дані не потраплять в чужі руки.

Висновок

Спільне використання шифрування як передачі даних, так і їх зберігання на диску забезпечить найбільший рівень захисту, ніж використання якого- небудь одного з цих видів шифрування. Експерти з безпеки називають такий спосіб «глибокого захисту». Використовуючи кілька способів захисту даних можливо досягти максимального рівня безпеки. Ідеальним способом захисту від широкого кола загроз стане як шифрування даних, які зберігаються на пристрої, так і переданих в мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. https://uk.wikipedia.org/wiki/Шифрування

2. https://sites.google.com/view/blog-ua/основні-поняття-криптографії-та- захисту-інформації/криптографія-з-відкритим-ключем-різновидності- алгоритм

XXII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

21-22 квітня 2022 р

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.