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.

```
@Bean
public PasswordEncoder delegatingPasswordEncoder() {
    PasswordEncoder defaultEncoder = new StandardPasswordEncoder();
    Map<String, PasswordEncoder> encoders = new HashMap<>();
    encoders.put("bcrypt", new BCryptPasswordEncoder());
    encoders.put("scrypt", new SCryptPasswordEncoder());

    DelegatingPasswordEncoder passworEncoder = new DelegatingPasswordEncoder(
      "bcrypt", encoders);
    passworEncoder.setDefaultPasswordEncoderForMatches(defaultEncoder);

    return passworEncoder;
}
```

Рисунок 1 – Конфігурація делегування паролів

Отже, розглянуто потужний фреймворк для побудови застосунків з використання мови програмування Java. Детально проаналізовано переваги та використовувані технології захисту інформації, персональних даних з використанням модуля Spring Security. Розглянуто новий функціонал кодування паролів, який є доступний у поточній версії Spring 5.6.2. Внесено зміни у стандартну конфігурацію програмного модуля Spring Security та отримано індивідуальний алгоритм обробки паролів, який надав змогу обробляти вхідні хеші паролів з урахуванням конфігурації програмного забезпечення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Spring Security. [Електронний ресурс]. – 2022 – Режим доступу до ресурсу: https://docs.spring.io/spring-security/reference/index.html

[2] What is Spring security. [Електронний ресурс]. – 2021 – Режим доступу до ресурсу: https://www.javadevjournal.com/spring/what-is-spring-security/

УДК 004.056.5

УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ (ІАС) ПРИЙМАЛЬНОЇ КОМІСІЇ ОНТУ (ОНАХТ)

МОРОЗ А.М., ПОХЛЄБІНА Н.О.
ОНТУ (Україна)

Анотація

В роботі розглянуто особливості захисту інформаційних ресурсів приймальної комісії, яка використовується, як засіб обробки та зберігання персональних даних абітурієнтів та вже студентів, що вже вступили до університету, що значно полегшує роботу приймальної комісії та прискорює якість надання даних до відділу навчання. Було виявлено основні недоліки та розглянути шляхи для удосконалення системи безпеки та збереження повної конфіденційності персональних даних вступників. Представлена схематична структура часткового алгоритму із захисту системи.

Ключеві слова: персональні данні, захист інформаційних баз, інформаційно-аналітична система

Проблема захисту є багатоплановою і комплексною і охоплює низку важливих завдань. Проблеми інформаційної безпеки постійно посилюються процесами проникнення в усі сфери суспільства технічних засобів обробки та передачі даних та, насамперед, обчислювальних

систем.

При розробці інформаційних систем із збереженням персональних даних людей, питання збереження конфіденційної інформації стає першочерговим. На сьогодні сформовано 3 базові принципи, що повинні забезпечити інформаційну безпеку:

- цілісність даних – безпосередньо захист від збоїв, що можуть призвести до втрати інформації;
- конфіденційність інформації;
- доступність інформації до уповноважених осіб, а саме секретарів приймальної комісії

В основі класифікації вразливостей ІАС використовуються такі класифікаційні ознаки:

- сфера походження вразливості;
- типи недоліків систем;
- місце виникнення або прояву вразливостей в ІАС.

Вразливості ІАС за місцем виникнення поділяються на такі типи:

- у загальному (загальносистемному) програмному забезпеченні;
- у прикладному програмному забезпеченні;
- у спеціальному програмному забезпеченні;
- у технічних засобах;
- у мережевому (комунікаційному, телекомунікаційному) обладнанні;
- у засобах захисту.

Таким чином, якість та повнота виявлення загроз безпеки інформації залежать від якості оцінки можливостей порушника щодо реалізації цієї загрози та повноти оцінки та аналізу вразливостей у системі захисту інформації ІАС.

Після аналізу існуючих вразливостей різних ІС було вирішено розробити та вбудувати комплекс системи захисту в ІАС для забезпечення безпеки, така система показана на рис.1, що дала змогу повністю виключити такі можливості зовнішнього впливу, як взлом системи, ймовірність помилок у самому коді, вразливостей, що можуть сприяти втраті інформації.

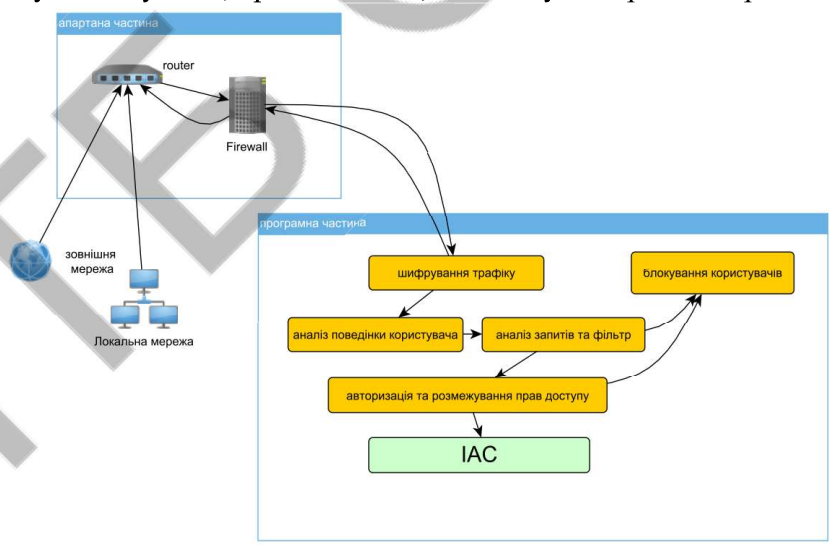

Рис.1 – Схематичне зображення системи безпеки автоматизованої інформаційно-аналітичної системи приймальної комісії ОНТУ (ОНАХТ)

Також дана система допомагає відстежувати користувачів та їх дії у АІС. Для того аби авторизуватись у системі існує система логінів та паролів, що встановлюються адміністратором системи та уповноваженими особами. Безпосередньо користувач системи не має змоги редагувати вхідні данні та уразі втрати повинен звернутися до адміністратора ІАС. Окремо слід виділити програмне забезпечення, яке аналізує трафік, обчислює та блокує небезпечну інформацію, дозволяючи уникнути зараження вірусом або витоку даних. Згідно представленій схемі був додатково встановлений фільтр трафіку, що не дає змоги підключення інших регіонів та держав.

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

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.