# СТАТЬИ ПО МАТЕРИАЛАМ СЕКЦИОННЫХ ДОКЛАДОВ
# ARTICLES BASED ON THE MATERIALS OF SECTIONAL REPORTS

УДК 004.9

## БЕЗОПАСНОСТЬ ДАННЫХ В СПОРТИВНЫХ ПРИЛОЖЕНИЯХ

С.А. Зайкова
*Учреждение образования «Гродненский государственный университет имени Янки Купалы», г. Гродно, Республика Беларусь*

**Аннотация.** Рассмотрены практические методы, используемые при разработке комплексного подхода к защите и шифрованию данных в мобильных приложениях, включая спортивное направление. Исследованы угрозы, с которыми сталкиваются разработчики подобных приложений, а также создание эффективных мер по обеспечению конфиденциальности, целостности и доступности данных пользователей.
**Ключевые слова:** мобильное приложение; защита данных; шифрование; угрозы безопасности; персональные данные.

## DATA SECURITY IN SPORTS APPS

S. Zaikova
*Educational Institution "Yanka Kupala State University of Grodno", Grodno, Republic of Belarus*

**Abstract.** This article examines practical methods used in developing a comprehensive approach to protecting and encrypting data in mobile apps, including those in the sports sector. It explores the threats faced by developers of such apps, as well as the development of effective measures to ensure the confidentiality, integrity, and availability of user data.
**Keywords:** mobile application; data protection; encryption; security threats; personal data.

В наше время новых возможностей, которые предоставляют пользователям современные спортивные и фитнес приложения, приходят и новые вызовы, особенно в контексте защиты личных данных. В мире, где цифровые следы наших действий становятся все более яркими и запутанными, защита персональной информации становится крайне важной, а ее утечка или использование в противоправных целях могут иметь серьезные последствия для нашей частной жизни [1, 2].

Спортивные приложения предоставляют уникальные возможности для отслеживания физической активности, анализа тренировок, и обмена опытом с сообществом единомышленников. Однако, с ростом популярности этих приложений возрастает и необходимость обеспечения их безопасности и защиты данных пользователей.

Проблема безопасности в спортивных мобильных приложениях становится все более актуальной, поскольку они хранят и обрабатывают чувствительные личные данные [3]. Пользователи доверяют такого рода приложениям свои персональные данные, связанные со здоровьем.

Разработчику необходимо предусмотреть не только интуитивно понятный интерфейс приложения, но и обеспечить высокий уровень конфиденциальности этой информации.

Несанкционированный доступ к данным пользователя может привести к серьезным последствиям, таким как: утечка персональных данных, медицинской истории и результатов тренировок. Кроме того, некорректная передача данных через сеть может привести к их перехвату.

Психологический аспект: утечка личных данных в сфере здоровья и физической активности может повлечь за собой эмоциональные и психологические последствия для пользователя, нарушая его чувство конфиденциальности и безопасности. Доверие пользователей: утечка данных может серьезно подорвать доверие пользователей к приложению и специалистам, разработавшим приложение.

Эффективная защита от утечки личных данных в спортивных мобильных приложениях требует комплексного подхода, включая использование современных методов шифрования, строгие политики доступа, регулярное тестирование безопасности и обучение пользователей основам безопасности.

Разработанное программное решение предусматривает следующие шаги: регистрация (ввод логина и пароля), ввод личных данных (название аккаунта, имя, возраст, место проживания), шифрование данных с помощью соли, внос в базу данных уже зашифрованные данные (хэш и соль). Затем пользователь мобильного приложения может проверить свои данные (вводит логин и пароль, если все верно, то данные дешифруются из базы данных и выводятся).

В начале программы пользователь выбирает, что ему надо сделать (проверить регистрацию и получить данные или зарегистрироваться). Затем выполняется проверка на правильность выбора, после чего пользователь вводит данные для регистрации в приложении. Демонстрация шифрования данных приведена на рис. 1.

Алгоритм AES является одним из самых широко используемых алгоритмов симметричного шифрования. Он обеспечивает высокую степень безопасности при относительно высокой скорости выполнения операций. AES использует блоки фиксированной длины (128 бит) и ключи различной длины (128, 192 или 256 бит).

Отметим, что защита персональных данных пользователя в базе крайне важна. При разработке прототипа предложено шифровать данные с помощью алгоритмов шифрования и соли. Злоумышленник, который получит данные, будет видеть только хэш, который он не сможет использовать. Чувствительные данные останутся в безопасности.

В результате проведенной работы выполнен анализ уязвимостей и угроз безопасности приложения, включая outline, разработаны

и применены некоторые методы шифрования данных. Практическая реализация предложенных мер безопасности реализована в прототипе спортивного мобильного приложения. Разработаны рекомендации конечным пользователям такого рода приложений с целью повышения их осведомленности в вопросах безопасности персональных данных.

```
        // Generate a unique salt for each user field
                byte[] passwordSalt = GenerateSalt();
                byte[] nameSalt = GenerateSalt();
                byte[] ageSalt = GenerateSalt();
                byte[] residenceSalt = GenerateSalt();

                // Encrypt user data
                string encryptedPassword = AesEncryptionHelper.EncryptData(password,
passwordSalt);
                string encryptedName = AesEncryptionHelper.EncryptData(name, nameSalt);
                string encryptedAge = AesEncryptionHelper.EncryptData(age, ageSalt);
                string encryptedResidence = AesEncryptionHelper.EncryptData(residence,
residenceSalt);

                // Save user to database
                RegisterUser(username, encryptedPassword, encryptedName, encryptedAge,
encryptedResidence, Convert.ToBase64String(passwordSalt),
Convert.ToBase64String(nameSalt), Convert.ToBase64String(ageSalt),
Convert.ToBase64String(residenceSalt));

            }
```

Шифрование данных в приложении
Encrypting data in the application

## Список использованных источников

1. Меры по обеспечению защиты персональных данных: учебное пособие / А. И. Гавриленко [и др.]; под общ. ред. А.А. Гаева, М.А. Городецкой. – Минск: РИВШ, 2025. – 78 с.

2. Защита персональных данных : учебное пособие / А.А. Гаев. [и др.]; под. общ. ред. М.Г. Коршекевича, М.А. Городецкой. –. Минск: РИВШ, 2024. – 124 с.

3. Зайкова С.А. Обеспечение безопасности процесса аутентификации с использованием дополнительных факторов / С. А. Зайкова // Технические средства защиты информации: матер. XXIII Междунар. науч.-техн. конф., Минск, 8 апр. 2025 г. – Минск: БГУИР, 2025. – С. 161–164.

## References

1. Measures to Ensure the Protection of Personal Data: A tutorial / A.I. Gavrilenko, [et al.]; edited by A.A. Gaev, M.A. Gorodetskaya. Minsk: RIVSh, 2025. – 78p.

2. Personal Data Protection: A tutorial / A.A. Gaev, [et al.]; edited by M.G. Korshekevich, M.A. Gorodetskaya. Minsk: RIVSh, 2024. – 124p.

3. Zaikova S.A. Ensuring the Security of the Authentication Process Using Additional Factors / S.A. Zaikova // Technical Means of Information Protection: Proc. of the XXIII Int. Scientific and Technical Conf., Minsk, April 8, 2025. – Minsk: BSUIR, 2025. – P. 161–164.

## Сведения об авторе

**Зайкова С.А.,** канд. физ.-мат. наук, доц., доцент кафедры СПиКБ, учреждение образования «Гродненский государственный университет имени Янки Купалы», sunny@mf.grsu.by.

## Information about the author

**Zaikova S.,** Cand. Sci. (Phys. and Math. Sciences), Associate Professor, Department Lecturer, Educational Institution "Yanka Kupala State University of Grodno", sunny@mf.grsu.by.