УДК 004.056.53

ПОДХОД РАБОТЫ С ДАННЫМИ ОГРАНИЧЕННОГО ДОСТУПА ДЛЯ ПРЕДОТВРАЩЕНИЯ УЯЗВИМОСТЕЙ ТИПА "НАРУШЕННЫЙ КОНТРОЛЬ ДОСТУПА" В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ, РЕАЛИЗОВАННОМ С ПОМОЩЬЮ ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ

Ромашов В.А. (ИТМО), **Еремук В.В.** (ИТМО), **Островский Д.П.** (ИТМО)
Научный руководитель – д.т.н., доцент Гришенцев А.Ю.
(ИТМО**)**

Введение. Анализ литературы и текущей ситуации, сложившейся в сфере информационных технологий, показывает, что уязвимости типа «Нарушенный контроль доступа» (англ. «Broken access control») являются актуальной угрозой в информационных системах. Уязвимости, принадлежащие к данному типу, возглавляют рейтинги наиболее эксплуатируемых уязвимостей [1]. Эффективный контроль над доступом к информации и функциональным возможностям системы имеет важное значение для обеспечения ее безопасности и защиты от внешних угроз. В эпоху цифровой трансформации экономики и растущего числа киберпреступлений, задача разработки механизмов, направленных на обнаружение и реагирование угрозы реализации уязвимости типа «Нарушенный контроль доступа» является актуальной [2]. Задачами данной работы являются:

1. анализ информации об уязвимостях типа “Нарушенный контроль доступа”;
2. поиск некоторых существующих подходов работы с данными ограниченного доступа в языках объектно-ориентированного программирования (ООП), для предотвращения появления данных типов уязвимостей;
3. разработка собственного подхода, на основе существующих, либо на основе нового, разработанного в ходе исследования.

Целью данной работы является повышение информационной безопасности программного обеспечения (ПО), разработанного с использованием объектно-ориентированных языков программирования.

Основная часть.

В рамках настоящего исследования выполнен анализ информации об уязвимостях типа «нарушенный контроль доступа» в ПО с открытым исходным кодом, реализованным посредством языков, поддерживающих объектно-ориентированное программирование (ООП). Согласно произведенному анализу, в большинстве случаев уязвимости указанного типа возникают вследствие ошибок, допущенных при разработке программного обеспечения. Был выполнен анализ существующих решений, таких как:

1. средства мониторинга [3];
2. разные подходы к применению механизма авторизации пользователя [4];
3. использование политик контроля доступа [5].

Авторами данной работы было принято решение объединить существующий метод управления доступом с технологией ООП. Таким образом, предложен новый подход к работе с данными ограниченного доступа при разработке ПО с помощью объектно-ориентированных языков программирования. Данный подход заключается в использовании мандатного контроля доступа [6] для классов, содержащих данные ограниченного доступа. Преимущества данного метода, которые ещё предстоит апробировать: простота реализации, возможность реагировать на попытки получения несанкционированного доступа; уменьшение вероятности появления ошибки, допущенной в ходе разработки ПО. Главный недостаток состоит в том, что вероятность ошибки разработчика не исключена полностью. На основе данного подхода был создан прототип на языке поддерживающем ООП java. В рамках дальнейшей работы предполагается провести полноценное

тестирование данного подхода для сбора статистики и проведения анализа.

Выводы. В рамках работы проведен анализ уязвимостей типа «нарушенный контроль доступа» в ПО с открытым исходным кодом, проведен анализ существующих подход и предложен метод для предотвращения появления данного типа уязвимостей в ПО.

Список использованных источников:

1. Hassan M. et al. Quantitative assessment on broken access control vulnerability in web applications //International Conference on Cyber Security and Computer Science 2018. – 2018.
2. Zhong L. A Survey of Prevent and Detect Access Control Vulnerabilities //arXiv preprint arXiv:2304.10600. – 2023.
3. Anas A., Elgamal S., Youssef B. Survey on detecting and preventing web application broken access control attacks //International Journal of Electrical and Computer Engineering (IJECE). – 2024. – Т. 14. – №. 1. – С. 772-78
4. Dalton M., Kozyrakis C., Zeldovich N. Nemesis: Preventing authentication & [and] access control vulnerabilities in web applications. – 2009.
5. Son S., McKinley K. S., Shmatikov V. Fix Me Up: Repairing Access-Control Bugs in Web Applications //NDSS. – 2013.
6. Щеглов К. А., Щеглов А. Ю. Принцип и методы контроля доступа к создаваемым файловым объектам //Вестник компьютерных и информационных технологий. – 2012. – №. 7. – С. 43-47.