котором она производится. Далее, достаточно запустить главный исполняемый файл.

Для запуска получившейся программы потребуются подключенная гарнитура виртуальной реальности, установленный SteamVR, который доступен в библиотеке Steam и, при необходимости, программное обеспечение для гарнитуры виртуальной реальности.

Таким образом, результатом работы стал интерактивный проект, отвечающий следующим требованиям: наличие виртуального пространства, в котором будет находиться пользователь; наличие предметов интерьера в проекте; возможность пользователя взаимодействовать с предметами и перемещать их.

Список использованных источников

1. SteamVR Plugin | Integration | Unity Asset Store [Электронный ресурс] – Режим доступа: https://assetstore.unity.com/packages/tools/integration/steamvr-plugin-32647

2. Unity - Manual: Asset Workflow [Электронный ресурс] – Режим доступа: https://docs.unity3d.com/Manual/AssetWorkflow.html

3. Free: House Interior | 3D Interior | Unity Asset Store [Электронный ресурс] – Режим доступа: https://assetstore.unity.com/packages/3d/props/interior/free-house-interior-223416

УДК 004.056.53

Д.С. Соловьев, И.А. Соловьева,
А.В. Самохвалов, Д.А. Саратов
Тамбовский государственный университет имени Г.Р. Державина
Тамбов, Россия

АНАЛИЗ ПРИЧИН И РАЗРАБОТКА РЕКОМЕНДАЦИЙ К ПОВЫШЕНИЮ ВЗЛОМОУСТОЙЧИВОСТИ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ДИАГРАММЫ ИСИКАВЫ

Аннотация. *Существующие средства защиты от несанкционированного копирования обладают низкой взломоустойчивостью, что требует анализа причин для их улучшения. Для этого используется диаграмма Исикавы, которая*

выделяет основные причины проблемы. Из диаграммы следует, что причинами являются нерациональное использование средств и механизмов операционной системы, тривиальное логическое устройство программы и повышенные требования к ресурсам ЭВМ. Приводятся рекомендации по повышению взломоустойчивости средств защиты.

D.S. Solovjev, I.A. Solovjeva, A.V. Samohvalov, D.A. Saratov
Derzhavin Tambov State University
Tambov, Russia

CAUSES ANALYSIS AND RECOMMENDATIONS DEVELOPMENT FOR IMPROVING THE ANTI-COPYING SOFTWARE'S RESISTANCE TO UNAUTHORIZED COPYING USING AN ISHIKAWA DIAGRAM

Abstract. *Existing anti-copying software tools have low resistance to hacking, which requires an analysis of the reasons for their improvement. To do this, an Ishikawa diagram is used, which identifies the main causes of the problem. The diagram shows that the reasons are irrational use of operating system tools and mechanisms, trivial logical structure of the program, and increased requirements for computer resources. Recommendations are provided for improving the resistance of anti-copying software tools.*

В настоящее время защита от несанкционированного копирования является одной из самых актуальных проблем в сфере информационных технологий [1]. Различные компании и разработчики создают средства защиты, которые должны обеспечивать надежную защиту от копирования и распространения программного обеспечения. Однако, несмотря на все усилия, имеющиеся на данный момент, средства защиты обладают низкой взломоустойчивостью.

Для анализа причин низкой взломоустойчивости существующих средств защиты от несанкционированного копирования можно использовать диаграмму Исикавы [2]. Эта диаграмма позволяет выделить основные причины проблемы и определить направления улучшения защиты. Диаграмма Исикавы анализа причин низкой взломоустойчивости существующих средств защиты от несанкционированного копирования представлена на рис. 1.

Из диаграммы, представленной на рис. 1, видно, что основными причинами слабой взломоустойчивости являются нерациональное использование средств и механизмов операционной системы Windows, тривиальное логическое устройство программы и повышенные требования к ресурсам ЭВМ.

Рис. 1 - Диаграмма Исикавы анализа причин низкой взломоустойчивости существующих средств защиты от несанкционированного копирования

Первой причиной слабой взломоустойчивости является нерациональное использование средств и механизмов операционной системы Windows. Для защиты от копирования используются идентификаторы, которые могут быть одинаковыми для серии накопителей. Это позволяет злоумышленникам легко подделывать идентификаторы и обходить защиту. Кроме того, данные с USB-накопителя могут быть считаны из статических текстовых документов, таких как файлы реестра, что делает защиту бесполезной.

Второй причиной слабой взломоустойчивости является тривиальное логическое устройство программы. Для защиты от копирования используются классические криптоалгоритмы, которые могут быть легко взломаны при отсутствии секретного ключа. Кроме того, защита может быть слабой и уязвимой к средствам обратного проектирования, что позволяет злоумышленникам легко обходить ее.

Третьей причиной слабой взломоустойчивости являются повышенные требования к ресурсам ЭВМ. Все данные хранятся в оперативной памяти, что делает их уязвимыми к атакам на память. Кроме того, защита может быть сложной в переносимости на другие операционные системы, что делает ее менее эффективной.

Таким образом, в разрабатываемых средствах защиты от несанкционированного копирования предлагается:

1) в качестве ключевых идентификаторов использовать PNPID, который обладает большей степенью индивидуальности;

2) применять двухуровневую проверку подлинности накопителя;

3) воздержаться от хранения идентификатора, посредством которого происходит шифрование в пользовательской части программного обеспечения;

4) вместо прямого обращения к файлам реестра использовать WMI, специализированный механизм Windows, который служит для получения информации о состоянии операционной системы;

5) применять криптоалгоритм собственной разработки, что затруднит его анализ при попытке взлома программного обеспечения.

В целом, низкая взломоустойчивость имеющихся на данный момент средств защиты от несанкционированного копирования является серьезной проблемой для разработчиков программного обеспечения. Для повышения уровня защиты необходимо разработать новые, более надежные средства защиты, которые будут устойчивы к современным методам взлома и обхода защиты. Кроме того, необходимо использовать более рациональные механизмы и средства операционной системы для обеспечения более надежной защиты от копирования.

Список использованных источников

1. Абулгазина А.Н. Защита от копирования на основе систем шифрования / А.Н. Абулгазина, Н.Д. Зюляркина, С.А. Родивилов // Наука ЮУрГУ. Секции технических наук. материалы 74-й научной конференции. – Министерство науки и высшего образования Российской Федерации Южно-Уральский государственный университет. – 2022. – С. 147-152.

2. Рассел Дж. Диаграмма Исикавы / Дж. Рассел, Р. Кон. – М.: Книга по Требованию, 2013. – 58 с.

УДК 338.43; 631/635; 336.6

М.П. Самоховец
Белорусский государственный экономический университет
Минск, Беларусь

АДАПТАЦИОННЫЙ ПОТЕНЦИАЛ АГРАРНОГО СЕКТОРА К КЛИМАТИЧЕСКИМ ИЗМЕНЕНИЯМ: ВОЗМОЖНОСТИ ЦИФРОВЫХ ТЕХНОЛОГИЙ