УДК 004.93

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛИЗИРОВАННОЙ ИНФРАСТРУКТУРЕ

Гатауллин Б.И.[1], студент гр. 4504, V курс, Хаерова Э.И.[2], студент гр. 4165, I курс
Научный руководитель: Тумбинская М.В.[1], к.т.н., доцент
[1] Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ
г. Казань
[2] Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ, г. Казань

История вычислительной техники [1] неразрывно связана с развитием технологий виртуальной и дополненной реальности. В настоящее время данные технологии широко используются в различных сферах деятельности, в том числе в области образования [2].

В работе предлагается специальное программное обеспечение (ПО) – виртуальная лаборатория для приобретения профессиональных компетенций в области информационной безопасности (рис. 1). В виртуальном пространстве собраны все технологии и инструменты для получения и отработки практических навыков по защите от угроз и киберинцидентов. Виртуальная лаборатория представляет собой набор виртуальных комнат, имеющих различную тематику защиты информации и пул практических кейсов. Виртуальная лаборатория содержит шесть VR-пространств.

Рис. 1 - Виртуальная лаборатория с функциональными комнатами

1. VR-пространство - комната регистрации. Пользователь вводит данные аутентификации идентификации на виртуальной стойке.

2. VR-пространство - комната по изучению нормативной базы (нормативно-правовых документов) в области защиты информации. Пользователю

предлагается решить несколько практических задач по обезличиванию персональных данных.

3. VR-пространство - комната по изучению технических методов и средств защиты информации. VR-пространство содержит технические устройства для физической защиты информации, поиска и детектирования источников несанкционированного съема информации. Пользователям предлагается решить несколько кейсов в области инженерно-технической защиты информации.

4. VR-пространство - комната программно-аппаратной защиты информации, в котором предложены этапы работы с программно-аппаратными средствами информационной безопасности.

5. VR-пространство - комната «Защита объектов от утечек информации с применением системы контроля управления доступом», в котором предлагается решение эффективного применения элементов системы контроля управления доступом (далее СКУД) для предотвращения несанкционированного доступа к информации и защиты помещения. Пользователю предлагается решить несколько кейсов для приобретения компетенций по проектированию и внедрению системы защиты информации контролируемой зоны объекта информатизации.

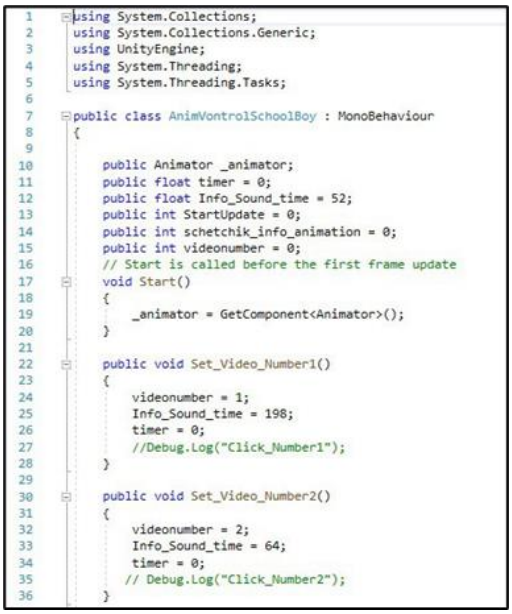
6. VR-пространство - комната оценки знаний. Помимо совершенствования своих практических навыков посредствам прохождения VR-пространств, пользователи могут проверить теоретические и практические знания в области защиты информации.

В основе виртуальной лаборатории лежит платформа Unity3D - кроссплатформенная среда разработки компьютерных игр, разработанная компанией Unity Technologies, в Unity для расчётов физики используется физический движок PhysX от NVIDIA.

Минимальные системные требования платформы:

1. Операционная система: Windows 7
2. Процессор: Intel Core 2-ядерный, аналогичный AMD или лучше
3. Оперативная память: 4 Гб
4. Видеокарта: Nvidia GeForce GT 710, Intel HD Graphics 630 или лучше
5. Свободное место на диске: 2 Гб

Применение описанной выше кроссплатформенной среды разработки, позволит решить проблемы оптимизации на этапе проектирования системы и подбирать более гибкие методы реализации функционала (рис. 2) [3 - 6].



```
using System.Collections;
using System.Collections.Generic;
using UnityEngine;
using System.Threading;
using System.Threading.Tasks;

public class AnimVontrolSchoolBoy : MonoBehaviour
{

    public Animator _animator;
    public float timer = 0;
    public float Info_Sound_time = 52;
    public int StartUpdate = 0;
    public int schetchik_info_animation = 0;
    public int videonumber = 0;
    // Start is called before the first frame update
    void Start()
    {
        _animator = GetComponent<Animator>();
    }

    public void Set_Video_Number1()
    {
        videonumber = 1;
        Info_Sound_time = 198;
        timer = 0;
        //Debug.Log("Click_Number1");
    }

    public void Set_Video_Number2()
    {
        videonumber = 2;
        Info_Sound_time = 64;
        timer = 0;
       // Debug.Log("Click_Number2");
    }
```

Рис. 2 – Фрагмент программного кода по созданию контроля анимации

Виртуальная лаборатория предоставит возможность обучающимся работать с реальными сценариями инженерно-технической защиты информации, визуализацией и анализом результатов без необходимости использования дорогостоящего оборудования. Лаборатория также предлагает интеграцию с базами данных, что делает возможным сохранять результаты в системе и использовать их в дальнейшем. Виртуальная лаборатория «Комплексная система защиты информации объекта информатизации» позволит повысить компетентность, технологическую грамотность и инициативность студентов, а также будет полезна для повышения квалификации опытным специалистам по таким направлениям, как «Комплексная защита объектов информации» и «Техническая защита информации».

Список литературы:

1. OpenCV-Python Tutorials [Электронный ресурс] - https://docs.opencv.org/4.x/d6/d00/tutorial_py_root.html (дата обращения: 13.01.2025)
2. Детекция объектов с помощью YOLOv5 [Электронный ресурс] - https://habr.com/ru/articles/576738/ (дата обращения: 01.02.2025)
3. Официальный репозиторий YOLOv5 на GitHub [Электронный ресурс] - https://github.com/ultralytics/yolov5 (дата обращения: 22.01.2025)
4. Хаерова Э.И. Обнаружение поддельных новостей с использованием нейронных сетей LSTM // Бюллетень I Международной молодежной конференции по информационной безопасности, 16 мая 2023 г.: Сборник тезисов/ отв. ред. А.Ж. Мартиросян, Р.Н. Шангараев Дипломатическая академия МИД России. – М., 2023. — С. 88-95. ISBN ISBN-978-5-6048376-1-0
5. Гатауллин Б.И. Исследование перспективных методов сокрытия информации в цифровых и аналоговых сигналах // МНПК-2024: материалы Всероссийской молодёжной научно-практической конференции. Казань,

27–29 мая 2024 г. Сборник докладов. Казань: Изд-во ИП Сагиев А.Р., 2024. — С. 237-239. ISBN ISBN 978-5-6053147-0-7

6. Мухаматханов Р.М., Михайлов А.А., Баянов Б.И., Тумбинская М.В. Классификация DDOS-атак на основе нейросетевой модели // Прикладная информатика. 2019. Т. 14. № 1 (79). С. 96-103.
7. Тумбинская М.В., Галиев Р.А. Идентификация фейк-новостей с помощью веб-ресурса на основе нейронных сетей // Программные продукты и системы. 2023. № 4. С. 590-599.
8. Sharipov R., Tumbinskaya M., Abzalov A. Analysis of users' keyboard handwriting based on gaussian reference signals. В сборнике: Proceedings - 2019 International Russian Automation Conference, RusAutoCon 2019.