УДК 004.9

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ВИРТУАЛЬНОГО ТРЕНАЖЕРА «ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ»

Гатауллин Б.И., студент 6 курса кафедры систем информационной безопасности
Научный руководитель – Тумбинская М.В., кандидат технических наук, доцент
ФГБОУ ВО «КНИТУ-КАИ»

Ключевые слова: *виртуальный тренажер, методические указания, защита информации, образование, средства защиты информации.*

В работе рассмотрены методические указания по выполнению лабораторных работ по разделу «Защита информации от утечки по техническим каналам» с использованием виртуального тренажера.

Введение. На сегодняшний день наблюдается устойчивый рост интереса к технологиям виртуальной и дополненной реальности. Основными драйверами развития данного рынка являются внедрение VR и AR в промышленность, медицину, образование, маркетинг и авиационную отрасль. В этих сферах высокий спрос на технологии виртуальной реальности обусловлен необходимостью практической подготовки специалистов. Использование виртуальной реальности позволяет воспроизводить реальные процессы в цифровой среде без дополнительных затрат и потенциальных рисков. Например, при обучении специалистов в области информационной безопасности применение подобных технологий дает возможность закрепить теоретические знания на практике и максимально приблизить процесс обучения к реальным условиям. Такие технологии обеспечивают более глубокое и эффективное усвоение материала по сравнению с традиционными подходами к обучению.

Цель работы. Целью виртуальной лаборатории является повышение качества подготовки специалистов в сфере информационной безопасности.

Результаты исследований. Для выполнения лабораторной работы были разработаны методические указания по работе с виртуальной лабораторией «Защита информации от утечки по техническим каналам». Цель лабораторной работы: формирование практических навыков по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях.

Шаг 1. Запустить первый модуль виртуальной лаборатории по защите информации на объектах информатизации «Технический канал утечки информации».

После запуска будет представлена виртуальная комната, содержащая экраны со справочным материалом по каждому средству технической защиты информации, используемому в данном модуле виртуальной лаборатории, и панель управления процессом перемещения между VR-комнатами, проверки корректности установки средств защиты и перезапуска виртуальной комнаты.

Шаг 2. Запуск первой VR-комнаты

Необходимо открыть первую VR-комнату, нажав на кнопку «1». В первой VR-комнате представлена доска с доступными техническими средствами защиты информации.

Шаг 3. Перемещение средств защиты информации в инвентарь комнаты.

Необходимо поближе подойти к доске и направить курсор на средства защиты информации. Затем, нажав на клавиатуре клавишу «E», подобрать предметы в инвентарь. Для того, чтобы открыть/закрыть инвентарь, необходимо нажать на клавиатуре клавишу «I».

Шаг 4. Перемещение средств защиты информации из инвентаря в быстрые слоты.

Левой кнопкой мыши необходимо переместить средства защиты информации в быстрые слоты, размещенные под инвентарём (рис. 1). Необходимо придерживаться ограничения в максимальном количестве предметов в инвентаре, соответствующее количеству слотов (15 ед.).



Рисунок 1. – Интерфейсная часть (быстрый слот)

Шаг 5. Выбор места установки средств защиты информации.

Необходимо выбрать средство защиты информации из быстрого слота клавишами 1-8 соответственно. Затем подобрать место установки выбранного средства и навести на данное место курсор. Зажав клавишу «Alt», нажать левую кнопку мыши. Средство защиты информации пропадёт из быстрого слота и установится на выбранном месте.

Шаг 6. Проверка корректности установки средств защиты информации.

После завершения процесса установки средств защиты информации по объекту информатизации необходимо проверить их корректность размещения. Для этого следует нажать на кнопку . На доске будет представлена информация о количестве корректно установленных средств защиты информации. Если средство защиты было размещено в установленном по правилам месте, оно окрасится в зеленый цвет. Красными метками будут обозначены места, рекомендуемые для установки средств защиты информации.

Шаг 7. Запуск второй VR-комнаты.

Необходимо открыть вторую VR-комнату, нажав на кнопку «2».

Шаг 8. Прохождение второй VR-комнаты.

Необходимо повторить шаги 3-6.

Выводы. На сегодняшний день популярность виртуальной и дополненной реальностей растёт. Современные технологические решения призваны обеспечить высококачественное и безопасное освоение практических компетенций. В этом контексте особое значение приобретает создание виртуальных тренажёров и лабораторий. Погружение в симулированную среду позволяет обучающимся принять на себя роль специалиста, взаимодействовать со средствами защиты информации и отрабатывать методы предотвращения кибератак. Такой подход гарантирует доступное, безопасное и достоверное моделирование реальных рабочих сценариев.

Библиографический список:

1. Борисенко, А. В. Эмуляция программного модуля имитации атаки на беспроводную сеть / А. В. Борисенко, В. Л. Акапьев, Е. Г. Ковалева, Е. А. Новикова // Экономика. Информатика. – 2025. – Т. 52, № 4. – С. 873-886. – DOI 10.52575/2687-0932-2025-52-4-873-886.

2. Petrovsky, V. The history and prospects of information security at Russian enterprises / Petrovsky V., Tumbinskaya M. В сборнике: Proceedings - 3rd International Conference on Computer Technology in Russia and in the Former Soviet Union, SoRuCom 2014. 3. 2015. С. 143-146.

3. Тумбинская М.В. Процесс распространения нежелательной информации в социальных сетях // Бизнес-информатика. 2017. № 3 (41). С. 65-76.

4. Тумбинская, М.В. Виртуальный тренажер по обработке конфиденциальной информации на физических носителях / Тумбинская, М.В., Хаерова Э.И., Гатауллин Б.И. // Вестник компьютерных и информационных технологий. 2024. Т. 21. № 8 (242). С. 49-55.

5. Тумбинская М.В. Информационная поддержка при обеспечении защищенности систем интернет-банкинга // Национальные интересы: приоритеты и безопасность. 2015. Т. 11. № 15 (300). С. 48-58.

6. Yakimov, I. Creation of a unified industrial basis for the development and supply of applied research program packages at the kazan computer factory / Yakimov I., Tregubov V., Tumbinskaya M. В сборнике: Selected Papers - 2017 4th International Conference "Computer Technology in Russia and in the Former Soviet Union", SoRuCom 2017. 4. 2017. С. 126-130.

METHODICAL INSTRUCTIONS FOR WORKING WITH THE VIRTUAL TRAINER "PROTECTION OF INFORMATION FROM LEAKAGE THROUGH TECHNICAL CHANNELS"

Gataullin B.I.
Scientific supervisor – Tumbinskaya M.V.
FSBEI HE "KNITU-KAI"

Keywords: *virtual simulator, guidelines, information protection, education, and information security tools.*

The paper discusses the prospects for using virtual reality in the educational process. When developing a virtual simulator, the author has created and presented guidelines for working with the virtual simulator.