

Научная статья

УДК 004.056

DOI 10.25205/1818-7900-2026-24-1-40-54

Виртуальная лаборатория по защите информации на объекте информатизации

**Марина Владимировна Тумбинская
Булат Ильнурович Гатауллин
Эндже Ильдаровна Хаерова**

Казанский национальный исследовательский технический университет
им. А. Н. Туполева – КАИ
Казань, Россия

tumbinskaya@inbox.ru, <https://orcid.org/0000-0003-3738-5242>

mr.bulgat12@mail.ru, <https://orcid.org/0009-0004-0202-0117>

engikhaer@gmail.com, <https://orcid.org/0009-0001-1872-2189>

Аннотация

Рост киберугроз обуславливает необходимость совершенствования методов подготовки специалистов в области информационной безопасности. В статье предложена виртуальная лаборатория, основанная на технологии виртуальной реальности (Unity3D), для моделирования практических кейсов по защите информации на объекте информатизации. Лаборатория включает сценарии по противодействию утечкам по техническим каналам, защите сетевого периметра и физической безопасности. Разработаны алгоритмы интерактивного взаимодействия, система автоматизированной проверки корректности решений и обратной связи. Экспериментальное исследование подтвердило эффективность разработки: среднее количество верно установленных средств защиты информации при использовании только виртуальной лаборатории составило на 6 % больше, чем при использовании комбинированного подхода (виртуальная лаборатория совместно с методическими указаниями).

Ключевые слова

виртуальная лаборатория, объект информатизации, технический канал утечки информации, программно-аппаратные средства защиты информации, физические средства защиты

Для цитирования

Тумбинская М. В., Гатауллин Б. И., Хаерова Э. И. Виртуальная лаборатория по защите информации на объекте информатизации // Вестник НГУ. Серия: Информационные технологии. 2026. Т. 24, № 1. С. 40–54. DOI 10.25205/1818-7900-2026-24-1-40-54

© Тумбинская М. В., Гатауллин Б. И., Хаерова Э. И., 2026

ISSN 1818-7900 (Print). ISSN 2410-0420 (Online)

Вестник НГУ. Серия: Информационные технологии. 2026. Том 24, № 1

Vestnik NSU. Series: Information Technologies, 2026, vol. 24, no. 1

Virtual Laboratory for Information Protection at the Informatization Facility

**Marina V. Tumbinskaya, Bulat I. Gataullin,
Endje I. Haerova**

Kazan national research technical university named after A. N. Tupolev – KAI
Kazan, Russian Federation

tumbinskaya@inbox.ru, <https://orcid.org/0000-0003-3738-5242>

mr.bulgat12@mail.ru, <https://orcid.org/0009-0004-0202-0117>

engikhaer@gmail.com, <https://orcid.org/0009-0001-1872-2189>

Abstract

Currently, due to the digitalization of processes and the growing number of cyber threats, many companies are in need of competent specialists with the necessary information security skills. The article offers a modern digital software product based on virtual reality technology. Virtual simulators can be actively used in the educational process. The use of such technologies makes it possible to carry out pilot industrial work in an environment as close to reality as possible. The virtual laboratory is a set of interactive models in a three-dimensional virtual space and has a wide range of practical tasks aimed at timely response to information security incidents and their prevention. The article presents an analysis of existing software tools and virtual simulators in the field of Information Security. Conclusions are drawn about the need to develop a virtual laboratory for information security at the informatization facility. The algorithm of the user's work with the virtual laboratory is presented. The interface forms and fragments of the virtual laboratory program code are described. The paper presents the stages of program development and the results of testing a virtual laboratory for information security at an informatization facility. The testing of the virtual laboratory confirmed the importance of using the simulator in the educational process as a tool for obtaining professional competencies. Based on the results of the statistical data of the experiment, it can be concluded that the use of an exclusively virtual laboratory has reduced the time spent on laboratory work by 30 minutes, while improving the quality of the absorbed material.

Keywords

virtual simulator, informatization facility, technical information leakage channel, software and hardware information protection tools, physical protection tools

For citation

Tumbinskaya M. V., Gataullin B. I., Haerova E. I. Virtual laboratory for information protection at the informatization facility. *Vestnik NSU. Series: Information Technologies*, 2026, vol. 24, no. 1, pp. 40–54 (in Russ.) DOI 10.25205/1818-7900-2026-24-1-40-54

Введение

На сегодняшний день получение знаний и навыков по различным областям нацелено на использование цифровых технологий. Все чаще в учебном процессе используют виртуальные лаборатории, AR-тренажеры, VR-симуляторы в таких областях, как энергетика, промышленность, авиация и др. [1]. На сегодняшний день популярность виртуальной и дополненной реальностей растет. Об активном развитии таких технологий свидетельствует исследование, проведенное компанией «ТМТ Консалтинг». По последним исследованиям, рынок виртуальной реальности в России в ближайшие годы будет расти в среднем на 37 % в год [2]. Такие прогнозные оценки позволяют сделать вывод, что виртуальная реальность займет важное место в тренде развития передовых технологий, в том числе в области образования. При подготовке специалистов в области защиты информации также могут применяться виртуальные тренажеры, позволяющие проводить опытно-промышленные работы в среде, максимально приближенной к реальности. Целью исследования является повышение качества подготовки специалистов в области защиты информации за счет разработки и практического применения виртуальной лаборатории, позволяющей имитировать решение профессиональных задач.

В статье описывается подход к разработке виртуальной лаборатории на базе платформы Unity3D для поддержки образовательного процесса в области технической защиты информа-

ции. Описан алгоритм взаимодействия пользователя с виртуальной лабораторией для трех сценариев практической подготовки (защита от утечки по техническим каналам, защита сетевого периметра, физическая защита объекта) в единой виртуальной среде. Проведено экспериментальное исследование, подтверждающее, что использование разработанной виртуальной лаборатории способствует повышению качества обучения за счет повышения точности выполнения кейсов и снижения частоты ошибок. Данный подход особенно актуален при подготовке специалистов по технической защите информации, поскольку традиционное практическое обучение связано с ограничениями: сложностью доступа к реальным объектам и недостаточной оснащенностью лабораторий современными средствами защиты информации. Реализация подхода позволит эффективно формировать необходимые профессиональные компетенции.

Анализ виртуальных тренажеров в области информационной безопасности

Результаты анализа литературных источников и патентного поиска показывают, что рынок технологий виртуальной и дополненной реальности в России растет с каждым годом. На сегодняшний день существуют различные виды виртуальных тренажеров для повышения компетенций в сфере информационной безопасности. К примеру, виртуальный тренажер «Технология VPN» [3], виртуальный учебник «Защита информации от искажения при передаче» [4], демонстрационная виртуальная среда «Монтаж средств ТЗИ» [5], виртуальный тренажер «Системы видеонаблюдения» [6], виртуальный тренажер «Монтаж телекоммуникационной стойки и сетевого оборудования» [7], виртуальный комплекс «Защита объекта от утечек информации по техническим каналам» [8], виртуальный комплекс «Обнаружение скрытых устройств и скрытых видеокамер» [9], виртуальный тренажер «Основы квантовой криптографии» [10].

В таблице сравнительного анализа виртуальных тренажеров в области информационной безопасности на основе патентного поиска представлены их ключевые особенности.

В процессе сравнительного анализа существующих виртуальных тренажеров, используемых для подготовки специалистов по информационной безопасности, были определены критерии сравнения: охват предметной области, количество изучаемых средств защиты информации (СрЗИ), наличие теоретического блока для изучения материала, тип проверки результатов и взаимодействия, а также доступность решения (платное или бесплатное). Сравнительный анализ существующих виртуальных тренажеров показал, что большинство проанализированных средств являются коммерческими решениями в области защиты информации, носят узкоспециализированный характер, обладают ограниченной иммерсивностью (реализованы преимущественно в формате 2D-симуляторов либо 3D-сред) без интеграции теоретического и практического блоков. Следовательно, можно сделать вывод о том, что целесообразность разработки специализированной виртуальной лаборатории, ориентированной на объект информатизации как средства повышения практических навыков и формирования профессиональных компетенций будущих специалистов в области информационной безопасности, является актуальной. Предмет исследования – виртуальный тренажер по защите информации на объекте информатизации. Методы исследования – методы системного анализа, моделирования. Практическая значимость работы заключается в применении виртуальной лаборатории в учебном процессе.

Разработка виртуальной лаборатории по защите информации на объекте информатизации

Для облегчения и ускорения работы пользователей необходимо, чтобы интерфейс виртуальной лаборатории был универсальным в использовании и предоставлял качественную ви-

Анализ виртуальных тренажеров в области информационной безопасности

Analysis of virtual simulators in the field of information security

Название	Охват предметной области	Количество изучаемых средств защиты информации	Наличие теоретического блока обучения	Тип проверки результатов	Тип взаимодействия с пользователем	Доступность решения
1	2	3	4	5	6	7
Виртуальный тренажер «Технология VPN»	Узкий (только VPN)	0 (объект изучения – программная технология и ее настройка)	Да	Автоматическая (без подсветки неправильно настроенного элемента)	2D-симулятор	Платно
Виртуальный учебник «Защита информации от искажения при передаче»	Узкий (изучения основ криптографии)	0 (модели алгоритмов)	Да	Нет	2D-симулятор	Платно
Виртуальный тренажер «Монтаж средств ТЗИ»	Узкий (навыков корректного монтажа средств защиты информации по (вибро-) акустическому каналу)	5	Нет	Автоматическая (уведомление о неверном размещении СрЗИ)	3D-среда	Платно
Виртуальный тренажер «Системы видеонаблюдения»	Узкий (монтаж, проектирование систем видеонаблюдения)	5	Нет	Автоматическая (уведомление о верном и неверном размещении СрЗИ)	3D-среда	Платно
Виртуальный тренажер «Монтаж телекоммуникационной стойки и сетевого оборудования»	Узкий (проектирование и монтаж стандартных телекоммуникационных стоек)	3–4	Да	Автоматическая (список допущенных обучаемым ошибок)	3D-среда	Платно
Виртуальный комплекс «Защита объекта от утечек информации по техническим каналам»	Узкий (исключительно технические каналы утечки информации)	10	Нет	Автоматическая (запись ошибок, допущенных в процессе)	3D-среда	Платно

Окончание табл.

1	2	3	4	5	6	7
Виртуальный тренажер «Обнаружение закладных устройств и систем видеонаблюдения»	Узкий (методы обнаружения закладных устройств и скрытых видеоканалов)	8	Нет	Автоматическая (запись ошибок, допущенных в процессе)	3D-среда	Платно
Виртуальный тренажер «Основы квантовой криптографии»	Узкий (квантовая криптография)	0	Да	Автоматическая (запись ошибок, допущенных в процессе)	2D-симулятор	Платно

зуальную информацию [11]. В программном продукте реализовано два вида взаимодействия с пользователем. Первый вид взаимодействия является визуальным с использованием отображаемых кнопок на панели управления процессом обучения. Второй вид взаимодействия – это нативный, с использованием клавиш на клавиатуре, которые принято использовать для действий в игровом сообществе [12].

Процесс разработки виртуальной лаборатории был разделен на три основных этапа. На первом этапе была разработана система инвентаря для имитации подбора предметов и добавления их в виртуальный объект информатизации. На втором этапе была выполнена разработка и программная реализация модели, обеспечивающей размещение средств защиты информации в виртуальной среде и автоматизированную оценку корректности их установки. Третий этап включал в себя проектирование и разработку визуальных составляющих практического и теоретического блоков виртуальной лаборатории. Виртуальная лаборатория была разработана на платформе Unity3D с разделением событий на отдельные скрипты на языке программирования C#.

При разработке виртуальной лаборатории были проанализированы современные подходы к моделированию и анализу технических систем, в том числе методы, основанные на искусственных нейронных сетях [13–15], что позволило разработать многоуровневую систему автоматизированной проверки корректности размещения средств защиты информации, сочетающую анализ пространственного расположения объектов, учет их функционального назначения и соответствие заданным сценариям угроз. Компоненты виртуальной лаборатории позволяют моделировать процесс выбора и размещения средств защиты информации в виртуальной среде с последующей оценкой.

Разработанная виртуальная лаборатория поддерживает два режима работы: автономный – на базе персонального компьютера с традиционным интерфейсом (клавиатура, мышь), и иммерсивный – с применением системы виртуальной реальности Pico 4, обеспечивающей эффект присутствия и естественную механику взаимодействия с объектами виртуальной среды.

Организация работы пользователя в виртуальной лаборатории:

1. Выбор сценария. Студент запускает лабораторию и выбирает одно из трех виртуальных пространств для моделирования, т. е. виртуальная лаборатория состоит из отдельных модулей:

- защита информации от утечки по техническим каналам;
- программно-аппаратная защита сетевого периметра;
- физическая защита информации на объекте информатизации.

Обучающимся предлагается типовой набор виртуальных помещений (две серверные, два офисных помещения, две лаборатории), что позволяет студентам сконцентриро-

ваться на алгоритме действий, изучении средств защиты информации и их практическом применении.

2. Размещение средств защиты. Студент анализирует угрозы, каналы утечки информации и выбирает необходимые средства защиты информации из каталога. Требуется корректно разместить выбранные средства (например, камеры, датчики) на виртуальном объекте. При размещении средств защиты информации значения настраиваемых параметров их функционирования фиксируются.

3. Проверка решения. Система автоматически проверяет результат. Проверка решений в виртуальной лаборатории реализована путем сопоставления с эталонными решениями. Для каждой виртуальной комнаты экспертным путем (преподавателями-предметниками) определено эталонное решение по размещению средств защиты, основанное на действующих нормативных документах ФСТЭК России, ФСБ России, а также на положениях ГОСТ Р 50922 и руководящих документах (в том числе РД 78.36.003-2002). В разработанной виртуальной лаборатории заложена возможность множественности правильных решений. В базе данных системы хранятся несколько эталонных сценариев для каждого практического задания. Например, для контроля периметра помещения допустимы различные варианты размещения датчиков движения (в углах или на стенах) при условии обеспечения требуемой зоны обнаружения. Ошибочным считается отсутствие средства защиты в необходимой зоне либо выбор средства, не соответствующего типу угрозы (например, установка датчика движения вместо магнитоконтактного датчика для контроля открывания двери).

4. Обратная связь.

– «Корректно»: правильно установленные средства защиты информации подсвечиваются зеленым.

– «Некорректно»: ошибочные элементы выделяются красным с подсказками по исправлению.

5. Студент вносит коррективы и повторяет проверку до полного устранения ошибок.

Алгоритм взаимодействия обучаемого с программным обеспечением состоит из следующих шагов:

1. Погружение в виртуальную среду объекта информатизации.

2. Анализ уязвимостей – обследование инфраструктуры на наличие угроз информационной безопасности.

3. Выбор и изучение средств защиты информации.

4. Подготовка и установка – перенос в активную зону, выбор точек размещения и фиксация средств защиты информации.

5. Цикл – шаги 3–4 повторяются для всех необходимых средств.

6. Проверка и коррекция результата, исправление ошибок.

7. Завершение – задание считается выполненным после успешной проверки.

В виртуальной лаборатории представлено более 20 технических, программно-аппаратных и физических средств защиты информации, таких как виброакустический излучатель, коммутатор, датчик разбития стекла, камеры видеонаблюдения, магнитоконтактный датчик – геркон, датчик движения, межсетевой экран и другие. В работе представлены примеры внешнего вида технических средств (рис. 1–3).

В работе представлены интерфейсные формы пространства виртуальной лаборатории (рис. 4–6).



Рис. 1. Внешний вид виброакустического излучателя с креплением на железобетонные перекрытия, бетонных перекрытий и иных несущих конструкций
Fig. 1. Appearance of a vibro-acoustic emitter mounted on reinforced concrete floors, concrete ceilings, and other load-bearing structures



Рис. 2. Внешний вид кодонаборной панели
Fig. 2. Appearance of the code dialing panel



Рис. 3. Внешний вид коммутатора
Fig. 3. Appearance of the switch



Рис. 4. Размещение средств защиты в виртуальной комнате «Защита информации от утечки по техническим каналам» с использованием гарнитуры виртуальной реальности Pico 4

Fig. 4. Placement of security tools in the virtual room “Protecting information from leakage through technical channels” using the Pico 4 virtual reality headset

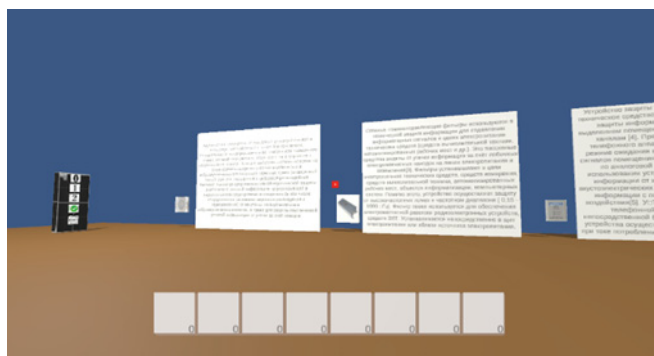


Рис. 5. Интерфейсная часть диалогового окна пространства теоретического блока обучения

Fig. 5. Interface part of the theoretical training block dialog box

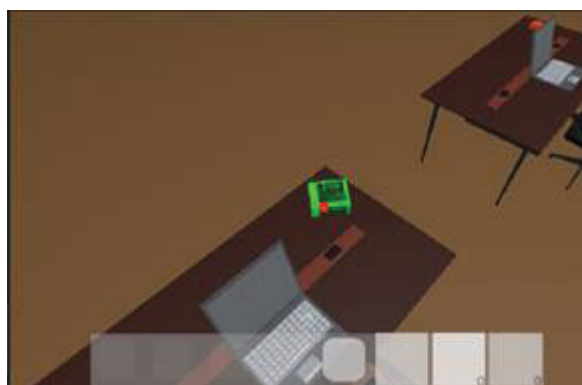


Рис. 6. Интерфейсная часть по идентификации верно и неверно установленных средств защиты информации

Fig. 6. The interface part for identifying correctly and incorrectly installed information security tools

На рис. 7 представлен фрагмент программного кода по разработке модуля системы идентификации объектов виртуальной лаборатории.

```

369 public void checkНастенныйВибро()
370 {
371     Debug.Log("Проверка настенный начало");
372     //CounterVibroSP157s = 0;
373     //Debug.Log("Я в проверкеVibroSP-157");
374     //if (КомплексныйПостановщикПомехs == null)
375     НастенныйВиброс = GameObject.FindGameObjectsWithTag("НастенныйВибро");
376     //if (Places == null)
377     НастенныйВиброPlaces = GameObject.FindGameObjectsWithTag("НастенныйВиброPlace");
378     //for (int i = 0; i <= КомплексныйПостановщикПомехs.Length; i++)
379     foreach (GameObject НастенныйВибро in НастенныйВиброс)
380     {
381         foreach (GameObject НастенныйВиброPlace in НастенныйВиброPlaces)
382         {
383             if (Vector3.Distance(НастенныйВибро.transform.position, НастенныйВиброPlace.transform.position) <= 5)
384             {
385                 CounterНастенныйВиброс++;
386                 Debug.Log("Я в проверке настенный вибро");
387                 Destroy(НастенныйВиброPlace);
388                 НастенныйВибро.GetComponent<Renderer>().material.color = Color.green;
389             }
390         }
391     }
392 }
393 }
394 foreach (GameObject НастенныйВиброPlace in НастенныйВиброPlaces)
395 {
396     НастенныйВиброPlace.GetComponent<MeshRenderer>().enabled = true;
397 }
398 }

```

Рис. 7. Фрагмент программного кода по разработке системы идентификации объектов

Fig. 7. Fragment of the software code for developing an object identification system

В работе предлагается модульная архитектура виртуальной лаборатории, благодаря которой добавление новых сценариев выполнения практических работ (например, защита речевой информации, монтаж систем контроля доступа) не требует переработки алгоритма взаимодействия пользователя с системой, инвентаря и автоматизированной проверки. Это позволяет рассматривать разработку как масштабируемую платформу для создания виртуального лабораторного практикума по технической защите информации с возможностью расширения функционала в дальнейшем без изменения базового программного ядра. Кроме того, в отличие от узкоспециализированных тренажеров, ориентированных на один тип средств или канал утечки, предложенная лаборатория объединяет технические, программно-аппаратные и физические средства защиты, что соответствует комплексному характеру профессиональной деятельности специалиста.

Экспериментальное исследование

В процессе исследования была проведена апробация виртуальной лаборатории по защите информации на объекте информатизации. Апробация проводилась в течение двух месяцев. Для апробации были привлечены группы студентов КНИТУ-КАИ им. А. Н. Туполева направления подготовки 10.03.01 «Информационная безопасность» – 42 человека. Студенты были разделены на две группы по 21 человеку. Первая использовала виртуальную лабораторию в сочетании с традиционными методическими указаниями, вторая – только виртуальный тренажер. В рамках апробации фиксировались следующие два параметра:

1. Время, затраченное на одну попытку выполнения практического задания по каждой виртуальной комнате (мин.).
2. Количество верно установленных средств защиты информации при каждой попытке выполнения практического задания по каждой виртуальной комнате (шт.).

Результат апробации показал, что среднее время размещения средств защиты информации в виртуальной комнате «Защита информации от утечки по техническим каналам» (ТКУИ) с использованием виртуальной лаборатории совместно с методическими указаниями составило 127 минут. При использовании только виртуальной лаборатории среднее время составило 105 минут. Среднее время размещения средств защиты информации сократилось на 17 % у студентов, выполнявших работу только с использованием виртуальной лаборатории «Защита информации от утечки по техническим каналам». Аналогичная тенденция наблюдалась при выполнении лабораторных работ в виртуальных комнатах «Программно-аппаратная защита сетевого периметра» и «Физическая защита информации на объекте информатизации». Среднее время сократилось на 34 и 35 % соответственно. В среднем время выполнения лабораторных работ по каждой виртуальной комнате с использованием виртуального тренажера сократилось на 30 минут. На рис. 8 представлена гистограмма распределения среднего времени размещения средств защиты информации по каждой виртуальной комнате.

Фактором снижения среднего времени выполнения лабораторной работы по каждой виртуальной комнате является снижение среднего времени размещения каждого средства защиты информации. В результате статистического анализа можно сделать вывод о том, что среднее время размещения одного средства защиты информации по виртуальным комнатам «Защита информации от утечки по техническим каналам», «Программно-аппаратная защита сетевого периметра», «Физическая защита информации на объекте информатизации» снизилось на 17; 40 и 30 % соответственно, что в среднем по трем комнатам составило примерно 32 %. На рис. 9 представлена гистограмма распределения среднего времени размещения одного средства защиты информации.

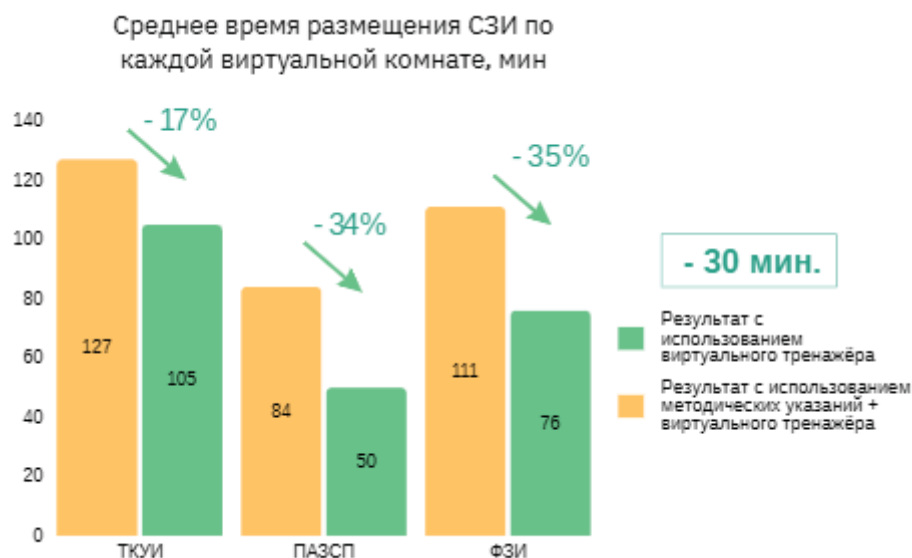


Рис. 8. Гистограмма распределения среднего времени размещения средств защиты информации по каждой виртуальной комнате

Fig. 8. Histogram of the distribution of the average placement time of information protection tools for each virtual room

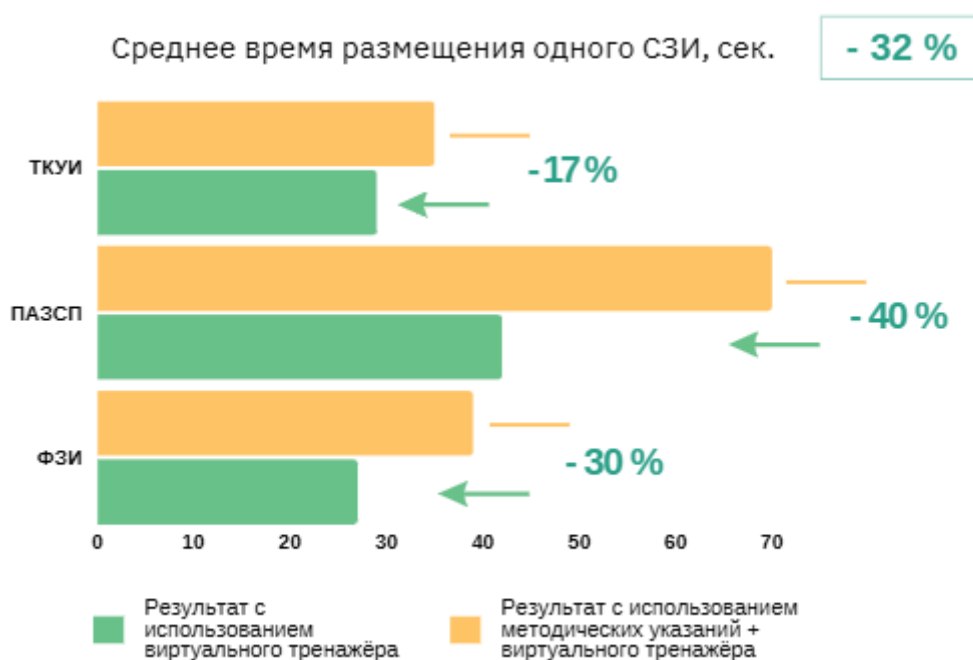


Рис. 9. Гистограмма распределения среднего времени размещения одного средства защиты информации

Fig. 9. Histogram of the distribution of the average placement time of one information protection tool

В рамках апробации были получены статистические данные среднего количества корректно установленных средств защиты информации при каждой попытке отдельно в каждой виртуальной комнате. По полученным данным можно сделать вывод о том, что виртуальный тре-

нажер является эффективным инструментом для обучения студентов. Гистограмма показывает улучшение результатов обучающихся с каждой попыткой выполнения практического задания. На рис. 10 представлена гистограмма распределения среднего количества корректно установленных средств защиты информации при каждой попытке.



Рис. 10. Гистограмма распределения среднего количества верно установленных средств защиты информации при каждой попытке
 Fig. 10. Histogram of the distribution of the average number of correctly installed information protection tools for each attempt

Результат эксперимента показал, что выполнение практических работ с использованием только виртуальной лаборатории обеспечивает высокий процент количества верно размещенных средств защиты информации на объекте информатизации за все использованные попытки. Представленные результаты демонстрируют динамику среднего количества верно установленных средств защиты информации (СЗИ) по каждой попытке выполнения лабораторных работ в трех виртуальных комнатах: «Защита информации от утечки по техническим каналам» (ТКУИ), «Программно-аппаратная защита сетевого периметра» (ПАЭСП) и «Физическая защита информации» (ФЗИ).

В группе, использовавшей только виртуальный тренажер (без методических указаний), наблюдается более выраженная положительная динамика. В комнате ТКУИ количество верно установленных СЗИ увеличилось на 450 % (с 12 до 66), в ПАЭСП – на 206 % (с 18 до 55), в ФЗИ – на 175 % (с 20 до 55). В группе, использовавшей традиционные методические указания совместно с тренажером, прирост составил: в ТКУИ – 32 % (с 40 до 53), в ПАЭСП – 124 % (с 21 до 47), в ФЗИ – 122 % (с 23 до 51).

Таким образом, использование виртуальной лаборатории способствует более интенсивному усвоению материала и позволяет обучающимся быстрее достигать высоких результатов за счет активного взаимодействия с иммерсивной средой. Полученные данные подтверждают эффективность разработанной виртуальной лаборатории как инструмента формирования профессиональных компетенций в области защиты информации.

На рис. 11 представлена диаграмма распределения среднего количества верно установленных средств защиты информации по каждой виртуальной комнате.



Рис. 11. Диаграмма распределения среднего количества верно установленных средств защиты информации по каждой виртуальной комнате

Fig. 11. Distribution chart of the average number of correctly installed information security tools for each virtual room

Экспериментальное исследование подтвердило эффективность разработки: среднее количество верно установленных средств защиты информации при использовании только виртуальной лаборатории составило на 6 % больше, чем при использовании комбинированного подхода (виртуальная лаборатория совместно с методическими указаниями). Таким образом, экспериментальное исследование подтверждает эффективность виртуальной лаборатории в учебном процессе. Иммерсивная среда обеспечивает безопасное, наглядное и интерактивное моделирование реальных условий защиты информации, что особенно актуально в условиях ограниченной материально-технической базы учебных заведений и высокой стоимости реальных технических средств защиты. Полученные данные имеют практическую ценность разработанного программного продукта как инструмента подготовки квалифицированных специалистов в области информационной безопасности.

Заключение

Результаты проведенного исследования свидетельствуют о том, что разработанная виртуальная лаборатория по защите информации на объекте информатизации, включающая технические, программно-аппаратные и физические средства защиты, обеспечивает более глубокое усвоение учебного материала по сравнению с традиционными методами обучения. Апробация данной лаборатории в образовательном процессе показала, что обучающиеся успешно трансформируют теоретические знания в практические навыки и компетенции в условиях, максимально приближенных к реальным профессиональным задачам в области информационной безопасности. В работе основное внимание уделено корректности выбора типа и места установки средства защиты, что является базовым навыком для начинающих специалистов. В дальнейшем планируется дополнить лабораторию модулем конфигурирования, в котором обучающемуся потребуется не только установить, но и настроить устройство (например, задать политику межсетевого экрана или определить зону обнаружения датчика).

Список литературы

1. Дудырев Ф. Ф., Максименкова О. В. Симуляторы и тренажеры в профессиональном образовании: педагогические и технологические аспекты // Вопросы образования. 2020. № 3. С. 255–276. DOI 10.17323/1814-9545-2020-3-255-276
2. Вольнов М. М., Китов А. А., Горячкин Б. С. Виртуальная реальность: виды, структура, особенности, перспективы развития // Информационные технологии. 2023.

3. Виртуальный тренажер «Технология VPN» [Электронный ресурс] // Портал учебного оборудования. URL: <https://labstand.ru/catalog/virtualnye-trenazhery-i-emulyatory-zashhita-informaczii/virtualnyj-trenazher-tehnologiya-vpn> (дата обращения: 13.11.2025).
4. Виртуальный учебник «Кибербезопасность: Управление и реагирование на инциденты безопасности» // Портал учебного оборудования. URL: <https://labstand.ru/catalog/virtualnye-trenazhery-i-emulyatory-zashhita-informaczii/virtualnyj-uchebnik-kiberbezopasnost-upravlenie-i-reagirovanie-na-inczidenty-bezopasnosti> (дата обращения: 13.11.2025).
5. Демонстрационная виртуальная среда «Монтаж средств ТЗИ» // DOKISAN. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/demonstracionnaya-virtualnaya-sreda-montazh-sredstv-tzi> (дата обращения: 13.11.2025).
6. Виртуальный тренажер «Системы видеонаблюдения» // DOKISAN. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/virtualnyj-trenazhior-sistemy-videonabljudeniya> (дата обращения: 13.11.2025).
7. Виртуальный тренажер «Монтаж и сервисное обслуживание систем охраны» (МССО) // DOKISAN. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/mssso> (дата обращения: 13.11.2025).
8. Виртуальный тренажер «Защита объекта от утечек информации по техническим каналам» // DOKISAN. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/defend-exam> (дата обращения: 13.11.2025).
9. Виртуальный тренажер «Обнаружение закладных устройств и скрытых видеокамер» // DOKISAN. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/ozu> (дата обращения: 13.11.2025).
10. Виртуальный тренажер «Основы квантовой криптографии» // DOKISAN. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/virtualnyj-trenazhior-osnovy-kvantovoj-kriptografii> (дата обращения: 13.11.2025).
11. **Шарилов Р. Р., Макаров С. П., Кассирова А. А.** Разработка программного комплекса потокового шифра RC4 для обучающихся по дисциплине «криптография». Международный научно-исследовательский журнал. 2024. № 9(147). С. 1–8. DOI 10.60797/IRJ.2024.147.15
12. **Хаерова Э. И., Гарифуллин Р. Ф., Тумбинская М. В.** VR-тренажер по обработке конфиденциальных данных на физическом носителе // Информатизация образования и науки. 2024. № 2 (62). С. 62–76.
13. **Гибадуллин Р. Ф., Лекомцев Д. В., Перухин М. Ю.** Анализ параметров промышленных сетей с применением нейросетевой обработки // Искусственный интеллект и принятие решений. 2020. № 1. С. 80–87.
14. **Гизатуллин З. М., Гизатуллин Р. М., Мубаракوف Р. Р.** Моделирование помех в электронном устройстве при воздействии импульсного магнитного поля с использованием искусственной нейронной сети // Журнал радиоэлектроники. 2024. № 5. С. 1–15.
15. **Гизатуллин З. М., Мубаракوف Р. Р.** Прогнозирование помех электростатического разряда в электронном устройстве с использованием искусственной нейронной сети // Журнал радиоэлектроники. 2024. № 8. С. 1–18.

References

1. **Dudyrev F. F., Maksimenkova O. V.** Simulators and training devices in vocational education: pedagogical and technological aspects. *Voprosy obrazovaniya*, 2020, no. 3, pp. 255–276. DOI 10.17323/1814-9545-2020-3-255-276 (in Russ.)
2. **Volnov M. M., Kitov A. A., Goryachkin B. S.** Virtual reality: types, structure, features, development prospects. *Information technologies*, 2023, pp. 1–18. (in Russ.)

3. Virtual simulator “VPN Technology”. *Portal of educational equipment*. URL: <https://labstand.ru/catalog/virtualnye-trenazhery-i-emulyatory-zashhita-informaczii/virtualnyj-trenazher-tehnologiya-vpn> (date of access: 11/13/2025). (in Russ.)
4. Virtual textbook “Cybersecurity: Managing and responding to security incidents”. *Portal of educational equipment*. URL: <https://labstand.ru/catalog/virtualnye-trenazhery-i-emulyatory-zashhita-informaczii/virtualnyj-uchebnik-kiberbezopasnost-upravlenie-i-reagirovanie-na-inczidenty-bezopasnosti> (date of access: 11/13/2025). (in Russ.)
5. Demonstration virtual environment “Installation of TZI equipment”. *DOKISAN*. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/demonstracionnaya-virtualnaya-sreda-montazh-sredstv-tzi> (date of access: 11/13/2025). (in Russ.)
6. Virtual simulator “Video surveillance systems”. *DOKISAN*. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/virtualnyj-trenazh-jor-sistemy-videonabljudeniya> (date of access: 11/13/2025). (in Russ.)
7. Virtual simulator “Installation and maintenance of security systems” (MSSO). *DOKISAN*. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/mssso> (date of access: 11/13/2025). (in Russ.)
8. Virtual simulator “Protecting an object from information leaks through technical channels”. *DOKISAN*. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/defend-exam> (date of access: 11/13/2025). (in Russ.)
9. Virtual simulator “Detection of bugs and hidden video cameras”. *DOKISAN*. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/ozu> (date of access: 11/13/2025). (in Russ.)
10. Virtual simulator “Fundamentals of quantum cryptography”. *DOKISAN*. URL: <https://dokisan.com/catalog/virtualnye-trenazhery/virtualnyj-trenazh-jor-osnovy-kvantovoj-kriptografii> (date of access: 13.11.2025). (in Russ.)
11. **Sharipov R. R., Makarov S. P., Kassirova A. A.** Development of a software package for the RC4 stream cipher for students majoring in cryptography. *International Research Journal*, 2024, no. 9 (147), pp. 1–8. DOI 10.60797/IRJ.2024.147.15. (in Russ.)
12. **Khaerova E. I., Garifullin R. F., Tumbinskaya M. V.** VR simulator for processing confidential data on a physical medium. *Informatization of education and science*, 2024, no. 2 (62), pp. 62–76. (in Russ.)
13. **Gibadullin R. F., Lekomtsev D. V., Perukhin M. Yu.** Analysis of industrial network parameters using neural network processing. *Artificial Intelligence and Decision Making*, 2020, no. 1, pp. 80–87. (in Russ.)
14. **Gizatullin Z. M., Gizatullin R. M., Mubarakov R. R.** Modeling of interference in an electronic device exposed to a pulsed magnetic field using an artificial neural network. *Journal of Radio Electronics*, 2024, no. 5, pp. 1–15. (in Russ.)
15. **Gizatullin Z. M., Mubarakov R. R.** Prediction of electrostatic discharge interference in an electronic device using an artificial neural network. *Journal of Radio Electronics*, 2024, no. 8, pp. 1–18. (in Russ.)

Информация об авторах

Тумбинская Марина Владимировна, кандидат технических наук, доцент

Гатауллин Булат Ильнурович, студент

Хаерова Эндже Ильдаровна, магистрант

Information about the Authors

Marina V. Tumbinskaya, Candidate of Technical Sciences

Bulat I. Gataullin, Student

Endje I. Haerova, Master's Student

Статья поступила в редакцию 16.01.2026;

одобрена после рецензирования 23.03.2026; принята к публикации 30.03.2026

The article was submitted 16.01.2026;

approved after reviewing 23.03.2026; accepted for publication 30.03.2026