

DOI: 10.32517/2221-1993-2025-24-2-48-58

**А. В. Четверов***Школа № 1520 им. Капцовых, г. Москва, Россия;
Московский городской педагогический университет, г. Москва, Россия***Е. А. Алефиренко***Московский городской педагогический университет, г. Москва, Россия*

ТРЕНАЖЕР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК СРЕДСТВО ФОРМИРОВАНИЯ ПРЕДПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ В РАМКАХ КУРСА «ВВЕДЕНИЕ В ИТ-СПЕЦИАЛЬНОСТЬ»

Аннотация

В статье обсуждаются проблемы, связанные с недостаточной подготовкой школьников в области информационной безопасности. На основе анализа научно-педагогической литературы и существующей образовательной практики показано, что современные школьники испытывают недостаток знаний и практических навыков в области информационной безопасности. Рассмотрена роль информационной безопасности в структуре современных учебных программ по информатике. Для решения проблемы недостаточной практической подготовки обучающихся в области информационной безопасности предлагается комплексный подход, основанный на использовании современных интерактивных технологий и лабораторных работ, структурированных в рамках курса «Введение в ИТ-специальность». Рассмотрены интерактивные приложения для лабораторных работ, направленных на обучение основам информационной безопасности на уровне среднего общего образования (в X—XI классах). Приведены примеры лабораторных работ. Описаны преимущества внедрения интерактивных технологий для формирования предпрофессиональных компетенций.

Ключевые слова: информационная безопасность, предпрофессиональная подготовка, интерактивное обучение, цифровая грамотность, цифровые компетенции.

Информация об авторах

Четверов Алексей Владимирович, учитель информатики, школа № 1520 им. Капцовых, г. Москва, Россия; эксперт, Институт развития профильного обучения, Московский городской педагогический университет, г. Москва, Россия; *e-mail:* alexu-che@yandex.ru

Алефиренко Евгения Александровна, старший методист, Институт развития профильного обучения, Московский городской педагогический университет, г. Москва, Россия; *e-mail:* alefirenkoea@mgpu.ru

A. V. Chetverov*School 1520, Moscow, Russia;
Moscow City University, Moscow, Russia***E. A. Alefirenko***Moscow City University, Moscow, Russia*

INFORMATION SECURITY SIMULATOR AS A MEANS FOR FORMING PRE-PROFESSIONAL COMPETENCIES IN THE COURSE "INTRODUCTION TO THE IT SPECIALTY"

Abstract

The article discusses the problems associated with the insufficient training of schoolchildren in the field of information security. Based on the analysis of scientific and pedagogical literature and existing educational practice, it is shown that modern schoolchildren lack knowledge and practical skills in the field of information security. The role of information security in the structure of modern educational programs in informatics is considered. To solve the problem of insufficient practical training of students in the field of information security, an integrated approach is proposed based on the use of modern interactive technologies and laboratory works structured within the course "Introduction to the IT specialty". Interactive applications for laboratory works aimed at teaching the basics of information security at the level of secondary general education (in grades 10–11) are considered. Examples of laboratory works are given. The advantages of introducing interactive technologies for forming pre-professional competencies are described.

Keywords: information security, pre-professional training, interactive learning, digital literacy, digital competencies.

Information about the authors

Aleksey V. Chetverov, Informatics Teacher, School 1520, Moscow, Russia; Expert, Institute for Development of Profile Education, Moscow City University, Moscow, Russia; *e-mail:* alexu-che@yandex.ru

Evgeniya A. Alefirenko, Senior Methodologist, Institute for Development of Profile Education, Moscow City University, Moscow, Russia; *e-mail:* alefirenkoea@mgpu.ru

1. Введение

Современное информационное общество предъявляет высокие требования к навыкам работы с цифровыми данными.

Основным законом об информации в России является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [29]. Он определяет ключевые термины и понятия, регулирует отношения при осуществлении права на поиск, получение, передачу и распространение информации и устанавливает требования к защите информации.

Вторым документом, создающим правовую основу обращения с персональными данными физических лиц и обеспечивающим защиту прав на неприкосновенность частной жизни, личную и семейную тайну, является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [30].

Информация становится одним из основных ресурсов, а ее защита — важнейшей задачей для общества.

На фоне осуществляемого перехода общества от индустриального к информационному повышается значимость умения ориентироваться в постоянно возрастающем потоке информации, эффективно работая с ней [24].

Одновременно с увеличением роли информации повышается и важность ее защиты, обеспечивающейся посредством инструментов информационной безопасности [31].

Сущность информационной безопасности заключается в формировании активной защиты в отношении приоритетных интересов, связанных с использованием информационных ресурсов, направленной на создание условий для нормального развития общества и экономики [3, 14, 15].

В условиях цифровой экономики информация выступает ключевым фактором производства, обладая уникальными свойствами, отличающими ее от традиционных ресурсов. В отличие от материальных товаров, информация не исчезает при потреблении и может использоваться многократно [7]. Она служит основой для создания знаний, инноваций и повышения конкурентоспособности предприятий [4].

В связи с необходимостью защиты информации возникает потребность в квалифицированных специалистах в этой области. К сожалению, уровень знаний школьников в области информационной безопасности остается недостаточным [5]. Это может стать источником рисков в информационной безопасности и послужить причиной возникновения пробелов в знаниях будущих специалистов в этой области.

В данной статье мы постараемся дать краткое обоснование необходимости внедрения интерактивных тренажеров и лабораторных работ по информационной безопасности в школьную программу для формирования предпрофессиональных компетенций в данной области знаний.

Компетенции в области информационной безопасности можно отнести к группе цифровых компетенций [17–19].

2. Проблемы подготовки школьников в области информационной безопасности

2.1. Информационная безопасность — больше, чем просто цифровая грамотность

Еще в 2003 году в своей диссертации «Информационная безопасность школьников в образовательном учреждении» Н. И. Саттарова писала, что школьники сталкиваются с радикальными изменениями в цифровой среде, но образовательная система не успевает адаптироваться к этим вызовам [22]. Более того, несовершенство школьной программы приводит к отсутствию базовых знаний по информационной безопасности.

Но и спустя более двадцати лет проблема остается актуальной. В статье Е. О. Лежавы, С. С. Абанеевой «Информационная безопасность школьников в сети Интернет: проблемы и пути решения» [12] подчеркивается, что учащиеся сталкиваются с угрозами в интернете, такими как кибербуллинг, фишинг и груминг. Авторы отмечают, что образовательные учреждения недостаточно оснащены программами, направленными на формирование навыков безопасного поведения в сети, а существующие меры защиты часто ограничиваются техническими средствами, без должного внимания к образовательным аспектам.

В 2023 году в России были предприняты значительные шаги для повышения уровня знаний школьников в области информационной безопасности (ИБ). Например, правительство утвердило Концепцию информационной безопасности детей [11], направленную на защиту детей от информационных угроз и рисков в цифровой среде, согласно которой **для решения проблемы недостаточного уровня знаний школьников в области информационной безопасности предлагаются следующие меры:**

- *введение образовательных программ* (создание уроков и курсов по информационной безопасности и цифровой грамотности, интегрированных в школьные программы);
- *повышение информированности родителей* (проведение регулярных информационных кампаний, направленных на обучение родителей использованию инструментов защиты, таких как «Родительский контроль»);
- *разработка позитивного контента* (поддержка создания безопасных интернет-ресурсов и продвижение контента, направленного на укрепление традиционных ценностей);
- *мониторинг и предотвращение угроз* (усовершенствование механизмов выявления деструктивной информации и вовлечения детей в противозаконные действия через сеть Интернет);
- *обучение педагогов* (повышение квалификации учителей для эффективного внедрения тематики информационной безопасности в образовательный процесс);
- *межведомственное взаимодействие* (усиление координации между государственными органами, образовательными учреждениями и общественными организациями для комплексного подхода к решению задач).

Подтверждая существование проблемы недостаточной подготовки старшеклассников в области информационной безопасности и обозначая некоторые пути ее устранения, Концепция в то же время не предлагает конкретные материалы и пособия для этой подготовки.

На сегодняшний день пособий, которые бы развивали необходимые практические навыки в сфере информационной безопасности подростка, практически нет, за малым исключением выпущенных небольшим тиражом экземпляров, а также общих теоретических пособий с общими рекомендациями безопасности жизнедеятельности, в содержательной части относящихся больше к понятию цифровой грамотности и кибергиgiene [10].

Развитие навыков и компетенций в области информационной безопасности влияет на формирование должного поведения обучающихся в современной цифровой среде, необходимого для комфортной жизни в условиях всепроникающего информационного пространства. Но по-прежнему во многих образовательных практиках главное внимание сосредоточено на теоретическом материале без отработки практических навыков.

В соответствии с Федеральным государственным образовательным стандартом среднего общего образования [28], углубленное изучение информатики в X—XI классах направлено на формирование у учащихся глубоких знаний и *практических навыков* в области информационных технологий, программирования и алгоритмизации. Для углубленного изучения курса информатики в X—XI классах в рамках ФГОС предлагаются следующие основные разделы: «Цифровая грамотность», «Теоретические основы информатики», «Алгоритмы и программирование», «Информационные технологии». В ФГОС предлагается формирование практических навыков только для работы с текстовыми, графическими редакторами, системами управления базами данных и интегрированными средами разработки, для раздела информационной безопасности остается практика по созданию безопасных паролей и своевременному обновлению программного обеспечения.

Например, для практического изучения следующего предметного содержания, предлагаемого при реализации Федеральной рабочей программы (ФРП) среднего общего образования на углубленном уровне изучения курса информатики по теме «Информационная безопасность» [27, с. 26–27], можно реализовать практические занятия:

1. В рамках предложенной в ФРП практической работы по применению средств защиты информации [там же, с. 27] рассмотреть работу с антивирусным ПО и брандмауэрами:
 - Вредоносное программное обеспечение и способы борьбы с ним.
 - Использование антивирусных программ как одного из основных средств защиты информации.
 - Настройка брандмауэров и фильтров.
2. В рамках предложенной в ФРП практической работы по предотвращению несанкционированного доступа к личной конфиденциальной информации [там же, с. 27] изучить предотвращение несанкционированного доступа к информации:
 - Организация безопасного соединения (SSL/TLS, VPN), в том числе посредством совре-

менных методов шифрования данных, включая использование SSL/TLS-протоколов.

- Использование защищенных сетей.

При этом первый пункт возможно рассмотреть лишь теоретически, используя инструкции и презентации, и де-факто использование HTTPS (TLS/SSL) является стандартом, в котором любой браузер всеми способами оповещает пользователя о работе в незащищенном режиме. Получение сертификата безопасности SSL для HTTPS сводится лишь к сообщению в удостоверяющий центр адреса электронной почты [16].

В качестве практических работ предлагаются: «Антивирусные программы», «Шифрование данных» без конкретных рекомендаций и примеров практических работ [27, с. 27].

Также стоит добавить, что практические работы, разрабатываемые в рамках системы основного образования, преимущественно охватывают *базовые правила цифровой грамотности* в области информационной безопасности [6] и направлены на «формирование цифровой грамотности обучающихся», что не включает:

- отработку навыков разработки безопасного программного обеспечения;
- использование практических инструментов для шифрования и защиты информации;
- проверку файлов по хеш-суммам;
- навыки работы с удаленными системами и их защиты и т. д.

При этом наблюдается разрыв в методах подготовки специалистов в области информационной безопасности не только в рамках рассматриваемого среднего общего образования, но и на высших ступенях образования, указывающий в том числе и на недостаточную практическую подготовку, с обучением без практических работ и без формирования навыков, необходимых для эффективной работы. Это также связано с тем, что традиционные образовательные программы часто фокусируются на теоретических аспектах, не предоставляя достаточного количества практических занятий [21].

Информационная безопасность изучается на уровне среднего общего образования в рамках учебного предмета «Информатика» как часть раздела «Цифровая грамотность» [27, с. 5]. Также она может изучаться в других предметах («Основы безопасности и защиты Родины» — при знакомстве с практиками социальной инженерии, «Иностранный язык» — при ознакомлении с приемами безопасного взаимодействия в интернете, «История» [28] и др.). Целью данного изучения является формирование компетенций учащихся в современном информационном обществе и достижение ими метапредметных результатов обучения — безопасной работы с информацией, соблюдения норм информационной безопасности [28]. Однако изучение информационной безопасности обычно осуществляется без знакомства с практиками защиты информации в предпрофессиональной и профессиональной деятельности.

Раздел «Информационная безопасность» упоминается в нескольких документах, связанных со средним общим образованием.

В ФГОС СОО информационная безопасность упоминается в следующих контекстах [28]:

- в требованиях к метапредметным результатам освоения основной образовательной программы: учащиеся должны уметь использовать средства ИКТ, соблюдая нормы информационной безопасности;
- в требованиях к предметным результатам на углубленном уровне изучения информатики: обучающиеся должны понимать принципы обеспечения информационной безопасности, способы и средства обеспечения надежного функционирования средств ИКТ.

В Федеральной рабочей программе по информатике для X–XI классов (углубленный уровень) тема «Информационная безопасность» выделена в разделе «Цифровая грамотность» и представлена следующим содержанием [27]:

- угрозы, связанные с использованием информационных технологий;
- общие проблемы защиты информации;
- средства защиты информации;
- правовое обеспечение информационной безопасности;
- предотвращение несанкционированного доступа к информации;
- вредоносное программное обеспечение и способы борьбы с ним;
- использование антивирусных программ;
- резервное копирование;
- шифры и шифрование данных.

Перечисленное выше содержание имеет большее отношение к безопасности жизнедеятельности, нежели к профессиональной сфере защиты информации.

В профессиональной литературе отмечается, что доля внутренних нарушений в области информационной безопасности, вызванных действиями или бездействием сотрудников, в последнее время фиксируется реже [26]. Однако доля инцидентов, связанных с информационной безопасностью, имеет тенденцию к росту, что в числе прочего может быть связано с низкой квалификацией разработчиков и недостатком практических навыков в области защиты информации и информационной безопасности, даже таких простых базовых навыков, как безопасная обработка входных данных, защита от SQL-инъекций, правильная работа с хешированием паролей и использование специализированных библиотек для работы с криптографией [1].

Можно сделать вывод, что, несмотря на предпринимаемые шаги по совершенствованию образовательных программ, **существует необходимость в разработке практико-ориентированных заданий и создании методических разработок для обучения информационной безопасности, которые бы выходили за рамки базовой цифровой грамотности, с включением освоения реальных практических навыков защиты информации.**

2.2. Отсутствие практических занятий

Как указывается в статье М. П. Тулохоновой «Интерактивные технологии обучения как средство развития информационного иммунитета школьников» [25], роль интерактивных тренажеров и систем с быстрой обратной связью в условиях повышения роли информационных

технологий в жизни общества и экономики становится все более важной. Автор отмечает, что традиционные методы обучения не позволяют эффективно сформировать у школьников навыки информационной безопасности, поскольку эти методы направлены преимущественно на теоретическое усвоение материала, а не на формирование навыков через практические упражнения.

Проблематика использования традиционных подходов:

- *Недостаточная вовлеченность учащихся.* Одной из ключевых проблем предпрофессионального и профессионального обучения является слабая вовлеченность учеников в процесс изучения материала. При отсутствии интерактивных и практических заданий материал воспринимается как абстрактный и плохо связанный с реальными ситуациями [2, 13].
- *Сложность практического применения.* Многие учебные курсы и материалы оказываются малоприменимыми в реальной жизни и быстро забываются, что опять же обусловлено преобладанием теоретического материала без достаточного практического закрепления [23]. Например, школьники редко сталкиваются с файрволами, антивирусами или механизмами фильтрации трафика в DDoS-атаках, и отсутствие практических упражнений делает эти концепции трудными для понимания и применения.

Таким образом, **отсутствие практических упражнений в школьном обучении информационной безопасности затрудняет понимание и применение обучающимися ключевых концепций информационной безопасности, что снижает эффективность подготовки школьников к реальным вызовам цифрового мира.**

3. Предлагаемое решение

Для решения обозначенной проблемы недостаточной подготовки старшеклассников в области информационной безопасности предлагается **комплексный подход**, основанный на использовании следующих **онлайн-сервисов**:

- 1) Отработка навыков двухфакторной аутентификации: <https://lesson1311.kasperstudent.ru/>
- 2) Тестовые задания в нескольких частях по теме кодирования и шифрования <https://lesson13134.kasperstudent.ru/>
- 3) Практическая учебная тренировка на отработку понимания принципов работы брандмауэров и антивирусов: <https://lesson132.kasperstudent.ru/>
- 4) Практическая учебная тренировка на отработку понимания принципов работы DDoS-фильтрации трафика: <https://lesson212.kasperstudent.ru/>
- 5) Практическая учебная тренировка на отработку понимания принципов запросов к базе данных на языке SQL и уязвимостей связанных с инъекцией SQL команд: <https://lesson213.kasperstudent.ru/>
- 6) Интерактивный блокнот Jupiter Notebook с инструментами и комментариями по моделям обнаружения вирусов с помощью машинного обучения: <https://lesson215.kasperstudent.ru/>

Также используется **графический сетевой эмулятор GNS3** (GPLv3, <https://www.gns3.com/>), позволяющий моделировать реальные сетевые устройства и обрабатывать топологии без физического оборудования виртуальной среды.

Профессиональная платформа CyberED Labs предлагает виртуальные лабораторные работы для выполнения индивидуальных заданий, что позволяет изучить на практике реалистичные сценарии киберугроз. При этом практика исключает необходимость сложной настройки оборудования и дает возможность сосредоточиться на изучении ключевых концепций, таких как защита сети с помощью файрволов или предотвращение DDoS-атак.

Кроме того, геймификация образовательного процесса (например, моделирование кибератак, требующих решения здесь и сейчас, изменяющихся в зависимости от действий учащегося) стимулирует обучающихся к активному участию в решении практических задач, симуляциях по информационной безопасности и к закреплению знаний. Исследования показывают, что такие упражнения повышают уровень усвоения материала почти в пять раз, предоставляя учащимся возможность «опробовать на практике» принципы работы антивирусов, системы обнаружения угроз или сетевых фильтров [9]. Подобные методы существенно увеличивают понимание информационных угроз и готовность учащихся к реальной работе с ними, доказывая важность внедрения практико-ориентированных подходов в школьное образование, особенно в темах, связанных с информационной безопасностью [8].

3.1. Предлагаемые интерактивные образовательные приложения по информационной безопасности (базовым правилам цифровой грамотности)

На основе материалов курса «Введение в ИТ-специальность», являющегося частью проекта предпрофессионального образования «ИТ-класс в московской школе», одним из авторов данной статьи А. В. Четверовым при поддержке «Лаборатории Касперского» разработаны шесть перечисленных выше онлайн-приложений, расположенных на домене второго уровня kasperstudent.ru (<https://github.com/chetTEst/CyberSecuLab>), распространяемых по лицензии Apache 2.0 [32]. Приложения включают отработку практических навыков, например, отработку двухфакторной аутентификации (<https://lesson1311.kasperstudent.ru/>), чтобы учащиеся смогли понять принципы и преимущества многофакторной защиты; в этом приложении также рассматриваются понятия нарушений в области конфиденциальности, доступности и целостности.

Проект «ИТ-класс в московской школе» учрежден Департаментом образования и науки города Москвы в сотрудничестве с вузами города Москвы (МИФИ, МИРЭА, ВШЭ, МГТУ им. Н. Э. Баумана, СТАНКИН, МЭИ, МТУСИ, МИСИС), которые готовят будущих ИТ-специалистов, и крупными ИТ-компаниями («1С», «Яндекс», «ВКонтакте», Ростелеком, «Лаборатория Касперского»).

На рисунке 1 представлен скриншот интерфейса панели учителя.

Рис. 1. Страница сессии тренировки

Рис. 2. Начало тренировки

Рис. 3. Ввод логина и пароля обучающимся

В предлагаемых онлайн-сервисах преподавателю необходимо запустить тренировку, указав количество учащихся в классе (рис. 2), и далее подключить к тренировке обучающихся, раздав каждому из них логин и пароль, предлагаемый сервисом (см. рис. 1), которые нужно ввести по ссылке сессии тренировки (рис. 3), например, <https://lesson1311.kasperstudent.ru/session392/login>, где 392 является номером сессии тренировки. Ссылку можно сократить через сервис clck.ru.

Для работы в приложении ученик должен войти в аккаунт (рис. 4) и подключить двухфакторную аутентификацию по технологии TOTP (Time-based One-time Password Algorithm — алгоритм создания одноразовых паролей для защищенной аутентификации), нажав на кнопку «Двухфакторная аутентификация» (рис. 5).

На странице подключения двухфакторной аутентификации (рис. 6) через стандартное приложение, например Яндекс.Ключ, необходимо просканировать предлагаемый QR-код и ввести в текстовое поле сервиса «Введите код из приложения» сгенерированный приложением код (рис. 7).

После указанных выше действий ученику необходимо выйти из сервиса, нажав на кнопку «Выйти», как изображено на рисунке 8.

После процедуры выхода обучающийся снова увидит интерфейс входа, показанный на рисунке 3. В текстовые поля необходимо заново ввести выданные ранее логин и пароль и нажать на кнопку «Войти» (см. рис. 4).

Рис. 4. Логин и пароль для сессии 392, выданные учащемуся

Рис. 5. Кнопка «Двухфакторная аутентификация» в интерфейсе сервиса

Рис. 6. Ввод кода из приложения

Рис. 7. One-time password от сервиса Яндекс.Ключ

Рис. 8. Отображение в интерфейсе подключенной двухфакторной аутентификации

Рис. 9. Элементы интерфейса для ввода второго кода

Рис. 10. Панель учителя при прохождении задания обучающимися

При этом сервис запросит код подтверждения, генерируемый стандартным приложением, например, Яндекс.Ключ (рис. 9).

На панели учителя (см. рис. 1) при этом отображаются этапы прохождения учащимся практического задания (рис. 10).

В набор авторских приложений также входит приложение симуляции настройки и работы брандмауэров и антивирусных систем (<https://lesson132.kasperstudent.ru/>), что способствует практическому закреплению учащимся теоретических знаний об инструментах защиты, пониманию терминов «порт» и «хеш-сумма».

Интерфейс панели ученика в данном тренировочном задании показан на рисунке 11. На рисунке 12 представлена рабочая панель обучающегося в приложении на отработку навыков отражения DDoS-атак (<https://lesson212.kasperstudent.ru/>).

Рабочая панель взвода Антивирусов			
Пользователь: Миша Киша			
Имя фала	Скачать для анализа	Это вирус?	Проверка файла
Угроза_безопасности.docx	Скачать	☐	Проверить hash на Virustotal
avoid.exe	Скачать	☐	Проверить hash на Virustotal
DOSBox0.74.exe	Скачать	☐	Проверить hash на Virustotal
Bowling.exe	Скачать	☐	Проверить hash на Virustotal
IconDance.exe	Скачать	☐	Проверить hash на Virustotal
vi4a.apk	Скачать	☐	Проверить hash на Virustotal
porup.exe	Скачать	☐	Проверить hash на Virustotal
Аутентификация.docx	Скачать	☐	Проверить hash на Virustotal

Рис. 11 Рабочая панель антивирусной проверки файлов

Рабочая панель «Системного администратора»			
IP адрес	Нагрузка	CAPTCHA	Выбрать действие
71.82.43.57		☐	Выбрать действие ▾
168.141.152.69		☐	Выбрать действие ▾
157.40.44.125		☐	Выбрать действие ▾
98.98.63.21		☐	Выбрать действие ▾
161.20.155.161		☐	Выбрать действие ▾
159.87.147.35		☐	Выбрать действие ▾
109.111.156.73		☐	Выбрать действие ▾
30.92.118.144		☐	Выбрать действие ▾

Рис. 12. Рабочая панель обучающегося в приложении на отработку навыков отражения DDoS-атак

3.2. Предлагаемые интерактивные образовательные приложения по дополнительным навыкам информационной безопасности

Для понимания работы SQL-запросов и защиты от SQL-инъекций предлагается использование упрощенного языка запросов Запросик (рис. 13), адаптированного для школьников, в котором необходимо сначала научиться взаимодействовать с базой данных, а уже после этого изучить работу механизмов SQL-инъекций.

Напишите запрос, который **ВЫБЕРЕТ** записи 2022 года.
Структура запроса:

ЧТО СДЕЛАТЬ для_каких_полей ИЗ_какого_Хранилища Условие;

1 2 3 4 5

Ваш ответ

1 ВЫБРАТЬ * ИЗ Хранилища Деревья ГДЕ Урожай = 1000

Проверить Обновить значения Базы данных

Результат Вашего запроса:

2	'Вишня'	1	'Жуковская'	1000	2022
8	'Вишня'	1	'Молодежная'	1000	2022

1 2

Поисковый запрос. Какие деревья вы ищете?

ВЫБРАТЬ Тип, Съедобное, Плод, Урожай, Год ИЗ Хранилища Деревья; --

Это запрос к Базе данных.

1 ВЫБРАТЬ Тип, Съедобное, Плод, Урожай, Год
2 ИЗ Хранилища Деревья
3 ГДЕ Тип = '[ТЕКСТ_ЗАПРОСА]';

Проверить Обновить значения Базы данных

Выйти

Рис. 13. Применение языка запросов Запросик

Другим примером применения интерактивного образовательного приложения является изучение принципов DDoS-фильтрации и работы с трафиком (<https://lesson212.kasperstudent.ru/>, см. рис. 12), что позволяет лучше понять исходящие от кибератак угрозы и методы их минимизации.

3.3. Мотивация к предпрофессиональной подготовке

Курс по информационной безопасности нацелен не только на развитие технических навыков, но и на мотивацию старшеклассников к дальнейшему обучению в области ИТ через выполнение лабораторных работ.

Лабораторные работы выполняются с использованием GNS3 (Graphical Network Simulator — графический симулятор сети). GNS3 — это мощный инструмент

с графическим интерфейсом для моделирования сетей различного уровня через инструменты виртуализации, позволяющий создавать сложные сетевые топологии и тестировать их в виртуальной среде. Он поддерживает эмуляцию различных сетевых устройств, включая маршрутизаторы, коммутаторы и брандмауэры. GNS3 распространяется по лицензии GPLv3 [20], что делает его удобным инструментом, отвечающим задачам решения проблемы отсутствия практических работ.

Основные особенности GNS3:

- эмуляция реальных устройств: GNS3 позволяет запускать образы операционных систем сетевых устройств, таких как Cisco IOS, pfSense, OpenWRT и др.;
- гибкость в создании топологий: пользователи могут создавать и настраивать сложные сетевые схемы, комбинируя виртуальные и физические устройства.

GNS3 позволяет создавать виртуальные сети, где обучающиеся могут на практике:

- реализовать защиту с помощью брандмауэров;
- настроить трансляцию сетевых адресов (NAT);
- выполнить проброс портов;
- настроить виртуальные частные сети (VPN).

3.3.1. Лабораторная работа

«Настройка брандмауэра для контроля трафика»

Цели лабораторной работы:

- запретить пинг (ICMP) из внешней сети во внутреннюю;
- обеспечить доступ к веб-серверу по HTTP из внешней сети;
- настроить SSH-доступ только с определенного клиента.

Основные шаги выполнения лабораторной работы:

1. Настройка политики безопасности. Использование приложения iptables для управления входящим и исходящим трафиком:
 - разрешение HTTP-трафика на сервер;
 - запрет ICMP для минимизации разведывательных атак;
 - настройка правил для SSH-доступа.
2. Тестирование настроек. Проверка через команды ping, ssh и веб-браузер.

Результат выполнения заданий лабораторной работы представлен на рисунке 14.

3.3.2. Лабораторная работа

«Настройка NAT для скрытия внутренних IP-адресов»

Цели лабораторной работы:

- скрыть внутренние IP-адреса, используя NAT;
- настроить проброс портов для доступа к внутренним ресурсам.

Задачи лабораторной работы:

- настроить маршрутизатор с поддержкой NAT (например, OpenWrt);
- создать правила для преобразования внутреннего IP-адреса в публичный;
- организовать проброс портов для доступа к веб-серверу.

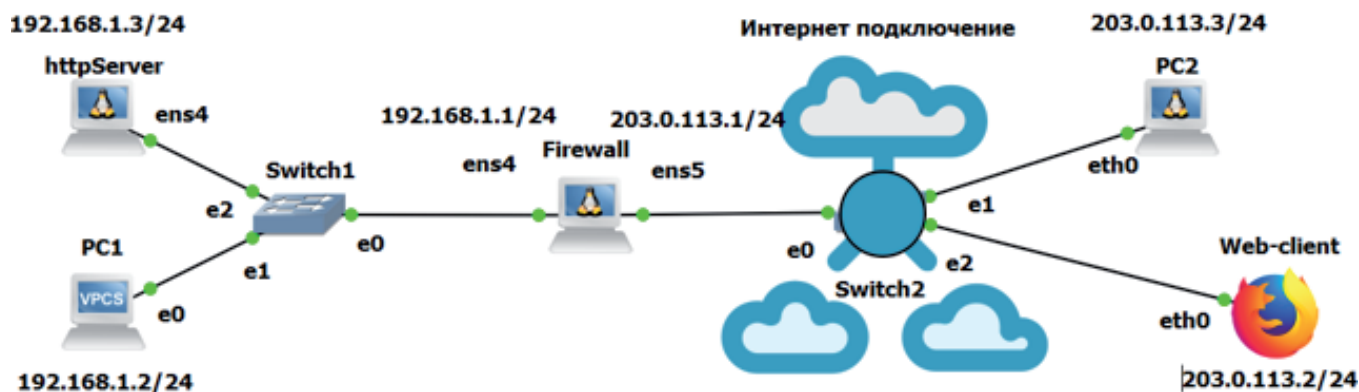


Рис. 14. Скриншот результатов выполнения заданий лабораторной работы по настройке брандмауэра

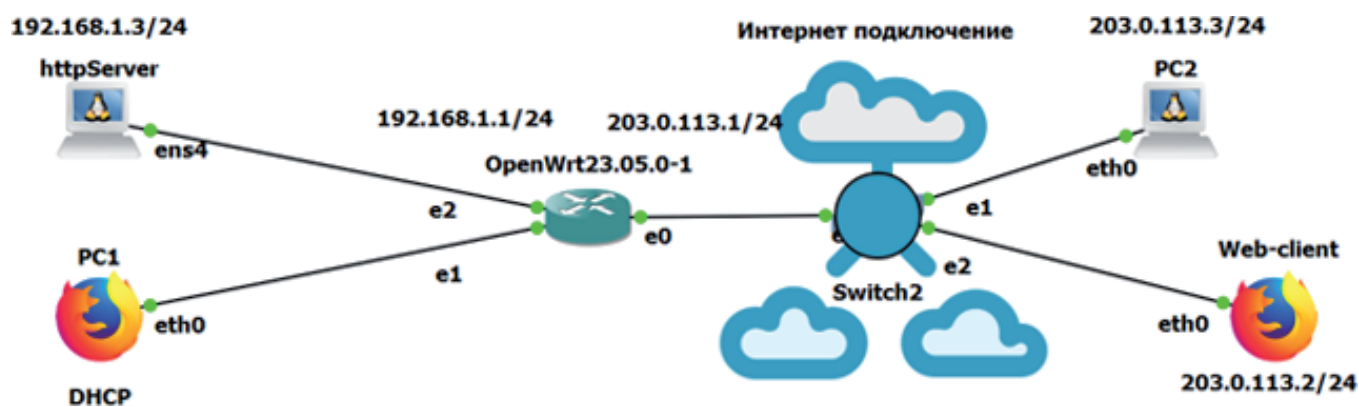


Рис. 15. Скриншот результатов выполнения заданий лабораторной работы по настройке NAT

Основные шаги выполнения лабораторной работы (выполняются в графическом интерфейсе открытой прошивки роутеров OpenWrt):

1. Подключение сети.
2. Конфигурация OpenWrt. Настройка интерфейсов WAN и LAN, добавление правил NAT и проброса портов.
3. Проверка настроек. Тестирование доступа к внутренним сервисам через внешний интерфейс.

Результат выполнения заданий лабораторной работы представлен на рисунке 15.

3.3.3. Лабораторная работа «Настройка VPN для безопасного доступа»

Цели лабораторной работы:

- создать защищенную сеть с помощью приложения WireGuard;
- настроить сервер и клиенты для доступа к внутренним ресурсам.

Основные шаги выполнения лабораторной работы:

1. Установка и настройка приложения WireGuard.
 - Генерация ключей для сервера и клиентов.
 - Настройка конфигурационных файлов с использованием VPN-туннеля.
 - Настройка IP-переадресации на сервере.
2. Подключение клиентов.
 - Добавление клиентов в конфигурацию сервера.
 - Настройка конфигурационных файлов клиентов.

3. Тестирование соединения.

- Проверка доступа к внутренним ресурсам через VPN.
- Убедитесь, что трафик защищен и маршрутизируется через VPN-туннель.

Результат выполнения заданий лабораторной работы представлен на рисунке 16.

3.3.4. Преимущества использования лабораторных работ перед только теоретическим освоением материала

- **Практическая ориентация:** учащиеся обучаются реальным сценариям настройки и управления сетями.
- **Безопасная среда:** использование виртуальных симуляторов исключает риски, связанные с ошибками.
- **Подготовка к профессиональной деятельности:** навыки, полученные в лабораторных работах, могут быть применены в будущей профессиональной практике.

Эти работы создают основу для глубокого понимания учащимися сетевой безопасности и формирования компетенций в области информационной безопасности.

4. Заключение

Рассмотренный подход к формированию предпрофессиональных компетенций в области информационной безопасности — за счет внедрения в школьную

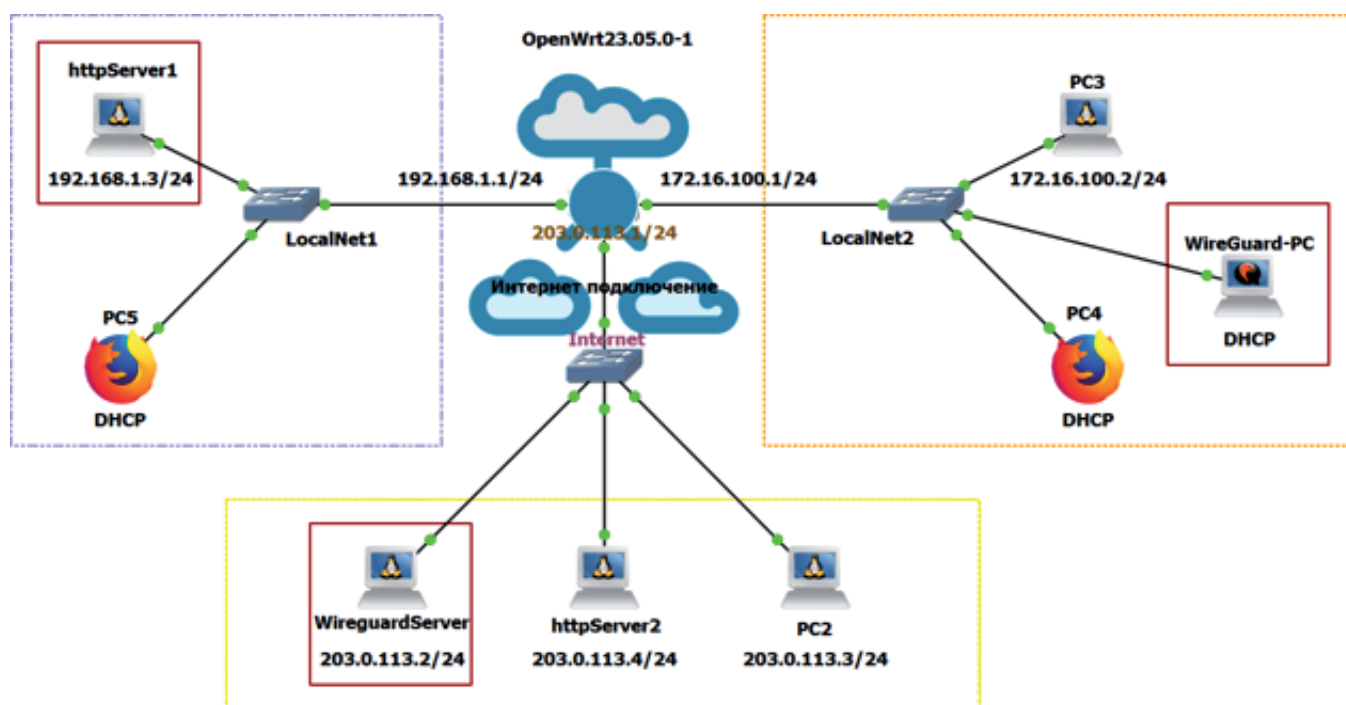


Рис. 16. Скриншот результатов выполнения заданий лабораторной работы по настройке VPN для безопасного доступа»

программу интерактивных тренажеров и практико-ориентированных заданий — отвечает растущим требованиям в области защиты информации и подготовки кадров. Приведенные в статье аргументы и примеры показывают, что традиционные теоретические формы обучения не способствуют развитию навыков, необходимых в реальной практике.

Практические задачи, моделирование сетевых настроек с помощью таких инструментов, как GNS3, отработка принципов двухфакторной аутентификации и настройка брандмауэров, а также понимание механизмов SQL-инъекций и реагирования на DDoS-атаки превращают процесс обучения из пассивного в активный. Такие занятия дают учащимся возможность самостоятельно изучить основы информационной безопасности, понять, как работают конкретные инструменты и технологии. Это не только повышает интерес и мотивацию к изучению информационной безопасности, но и обеспечивает закрепление практико-ориентированных знаний и практических умений и навыков.

Предложенные в статье решения формируют у школьников целостное представление о защите данных, рисках цифровой среды и эффективных методах их минимизации.

Разработка интерактивных тренажеров и их интеграция в образовательный процесс позволит не только закрыть существующие пробелы в подготовке, но и сформировать у учащихся фундамент для дальнейшего профессионального развития в ИТ-сфере и смежных областях, обеспечивая тем самым устойчивую основу для информационно безопасного будущего.

Список источников

1. Бирюков А. Безопасная разработка и уязвимости программного кода // Хабр. 7 апреля 2022. <https://habr.com/ru/companies/otus/articles/659575/>

2. Бороненко Т. А., Федотова В. С. Приемы создания и использования интерактивных учебных материалов в профессиональной деятельности учителя // Вестник педагогических инноваций. 2022. № 1 (65). С. 60–73. EDN: PXGGCB. DOI: 10.15293/1812-9463.2201.07.

3. Бudyко М. Ю., Миняев А. А. Метод оценки эффективности системы защиты персональных данных // Информатизация и связь. 2016. № 2. С. 85–87. EDN: VVGRBD.

4. Бучинская О. Н. Информация как ресурс в эпоху цифровой экономики // Вестник Удмуртского университета. Серия: Экономика и право. 2022. Т. 32. № 2. С. 209–215. EDN: CPBMDT. DOI: 10.35634/2412-9593-2022-32-2-209-215.

5. Давыдов А. В. Анализ уровня осведомленности школьников 9–11-х классов по вопросу информационной безопасности (на примере МБОУ СОШ № 86 г. Краснодара) // Актуальные задачи педагогики. Материалы X Международной научно-практической конференции (Санкт-Петербург, 20–23 января 2019 года). СПб.: Свое издательство, 2019. С. 40–42. EDN: YWCQBV.

6. Дубровина Н. Н. Развитие цифровой грамотности учащихся основной школы в условиях дистанционного обучения // Мир педагогики и психологии: Международный научно-практический журнал. 2023. № 12. С. 46–50. EDN: TTOWDU.

7. Евсеева А. О., Закирова М. И. Информация как ресурс экономики // Инновационная наука. 2017. № 2-1. С. 190–192. EDN: XVSKOD.

8. Жаркевич А. Теории недостаточно: о важности практических навыков при обучении сотрудников кибербезопасности // Anti-Malware.ru — информационная безопасность для профессионалов. 21 января 2021. https://www.anti-malware.ru/analytics/Threats_Analysis/importance-of-practical-skills-in-cybersecurity-training

9. Жидков А. А., Гордеев К. С., Илюшина Е. С., Ермолаева Е. Л., Федосеева Л. А. Значение практического обучения для системы профессионального образования // Современные научные исследования и инновации. 2020. № 11 (115). С. 32. EDN: PPAVEA.

10. Козырева А. А. Определение термина «кибергигиена» и возможность его применения в правовом поле // Пробелы в российском законодательстве. 2018. № 7. С. 92–94. EDN: VQQTIA.

11. Концепция информационной безопасности детей в Российской Федерации (утв. распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р). https://rkn.gov.ru/docs/Koncepcija_informacionnoj_bezopasnosti_detej_14062023.pdf
12. Лежава Е. О., Абанеева С. С. Информационная безопасность школьников в сети Интернет: проблемы и пути решения // Теория и практика современной науки. 2019. № 12 (54). С. 233–236. EDN: QFXWNR.
13. Марат З. Д., Юсупова С. И., Исмаилова Р. Б. Эффективность использования интерактивных методов обучения // Молодой ученый. 2023. № 40 (487). С. 57–59. EDN: YXOCРХ.
14. Миняев А. А. Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем // Информатизация и связь. 2020. № 6. С. 29–36. EDN: ESJFSC.
15. Миняев А. А., Будько М. Ю. Метод оценки эффективности системы защиты информации территориально распределенных информационных систем // Информатизация и связь. 2017. № 3. С. 119–121. EDN: YMZNAF.
16. Панов М. А., Посохин А. Е. Сертификаты SSL // Научные междисциплинарные исследования. 2020. № 8-1. С. 83–89.
17. Попов В. С., Абросимова-Романова Л. А. Ключевые компетенции для обучения в течение всей жизни в контексте компетенций и компетентностей в области информационных технологий // Информатика: проблемы, методы, технологии. Сборник материалов XXIV Международной научно-практической конференции (Воронеж, 14–15 февраля 2024 года). Воронеж: Воронежский государственный университет, 2024. С. 1648–1657. EDN: LMNJAT.
18. Попов В. С., Абросимова-Романова Л. А. Трансформация ключевых компетенций модели Key competences for lifelong learning // Текущие вызовы в подготовке кадров. Обучение специалистов по современным направлениям информационных технологий, кибербезопасности и ИКТ-электроники, актуальным для экономики данных. Сборник научных трудов конференции «Преподавание информационных технологий в Российской Федерации» (Тверь, 16–17 мая 2024 года). Тверь: Тверской государственный университет, 2024. С. 474–477. EDN: QUFFBF.
19. Попов В. С., Алефиренко Е. А., Черницына Л. Ю. Компетентный подход в федеральных рабочих программах по информатике на уровне среднего общего образования // Текущие вызовы в подготовке кадров. Обучение специалистов по современным направлениям информационных технологий, кибербезопасности и ИКТ-электроники, актуальным для экономики данных. Сборник научных трудов конференции «Преподавание информационных технологий в Российской Федерации» (Тверь, 16–17 мая 2024 года). Тверь: Тверской государственный университет, 2024. С. 604–607. EDN: BUWEMV.
20. Савельев А. И. Лицензирование программного обеспечения в России: законодательство и практика: учебное пособие. М.: Infotropic Media, 2012. 432 с. EDN: SDTYOB.
21. Саматов К. Уровень образования специалиста и высокие требования к квалификации: кто кого? <https://www.itsec.ru/articles/uroven-obrazovaniya-spetsialista-i-vysokiye-trebovaniya-k-kvalifikatsii-kto-kogo>
22. Саттарова Н. И. Информационная безопасность школьников в образовательном учреждении: специальность 13.00.01 «Общая педагогика, история педагогики и образования»: дис. ... канд. пед. наук. СПб.: Санкт-Петербургская академия постдипломного педагогического образования, 2003. 215 с.
23. Сафонов Л. Практические навыки по информационной безопасности // Хабр. 24 августа 2017. <https://habr.com/ru/articles/336164/>
24. Сидельникова Н. В., Беседина Т. В. Информационная безопасность // Образование. Карьера. Общество. 2018. № 1 (56). С. 71–72. EDN: USNLHT.
25. Тулохонова М. П. Интерактивные технологии обучения как средство развития информационного иммунитета школьников // Сибирский педагогический журнал. 2011. № 3. С. 212–219. EDN: PEYMZJ.
26. Фатихова Я. Р., Дьячкова К. С. Киберпреступность: проблема утечки данных в сфере информационных технологий // Молодой ученый. 2023. № 15 (462). С. 247–249. EDN: WVHPJV.
27. Федеральная рабочая программа среднего общего образования. Информатика (углублённый уровень) (для 10–11 классов образовательных организаций). https://edsoo.ru/wp-content/uploads/2023/08/22_ФРП_Информатика-10-11-классы_угл.pdf
28. Федеральный государственный образовательный стандарт среднего общего образования. <https://base.garant.ru/70188902/8ef641d3b80ff01d34be16ce9bafc6e0/>
29. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». <http://www.kremlin.ru/acts/bank/24157>
30. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». <http://www.kremlin.ru/acts/bank/24154>
31. Чесноков А. Д. Информационная безопасность // StudNet. 2022. Т. 5. № 1. С. 478–489. EDN: IIPKSO.
32. Шинкарев А. А. Роль программного обеспечения с открытым исходным кодом в современной разработке корпоративных информационных систем // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2021. Т. 21. № 2. С. 16–22. EDN: OTHPNG. DOI: 10.14529/ctcr210202.