DOI 10.37882/2223-2966.2025.09.20

# ОРГАНИЗАЦИЯ ЛАБОРАТОРНОГО ПРАКТИКУМА ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ РАСШИРЕННЫХ ВОЗМОЖНОСТЕЙ ГИБРИДНЫХ ВИРТУАЛЬНЫХ ЛАБОРАТОРНЫХ СРЕД

## ENHANCING THE LAB PRACTICUM FOR TRAINING OF INFORMATION SECURITY SPECIALISTS WITH THE HYBRID VIRTUAL LAB ENVIRONMENTS

***Mansurov A.***
***Minakova N.***
***Salita D.***
***Dmitriev A.***
***Zhuravleva V.***

*Summary*. The paper analyzes the approaches for deployment of the «PNETLAB» and «EVE-NG» hybrid virtual lab environments and successful development of lab training courses and practicums for training of information security specialists in higher education institutions and colleges. Ways of combining the virtual lab schemas with the real lab network and information security solutions and equipment are discussed and possible advantages and disadvantages are outlined. It is stated that the proposed hybrid virtual lab environments help design effective models of corporate infrastructure for various purposes. The education process this way can be greatly enhanced by using specific pedagogical approaches and techniques. It helps produce unique and effective lab work schemas and stimulates the process of obtaining new knowledge and skills.

*Keywords*: virtual lab environment, individual educational trajectory, network security, information security, information system security, cybersecurity education.

***Мансуров Александр Валерьевич***
*канд. техн. наук, ФГБОУ ВО «Алтайский государственный университет», г. Барнаул*
*mansurov.alex@gmail.com*
***Минакова Наталья Николаевна***
*доктор физ.-мат. наук, ФГБОУ ВО «Алтайский государственный университет», г. Барнаул*
*minakova@phys.asu.ru*
***Салита Даниил Сергеевич***
*канд. физ.-мат. наук, ФГБОУ ВО «Алтайский государственный университет», г. Барнаул*
*d.s.salita@gmail.com*
***Дмитриев Александр Александрович***
*канд. физ.-мат. наук, ФГБОУ ВО «Алтайский государственный университет», г. Барнаул*
*dmitriev@asu.ru*
***Журавлева Виктория Владимировна***
*Преподаватель, ФГБОУ ВО «Алтайский государственный университет», г. Барнаул*
*torinka8@gmail.com*

*Аннотация*. В статье проведен анализ способов организации виртуальных лабораторных сред на базе «PNETLAB» и «EVE-NG» и успешное формирование на их основе лабораторных занятий и практикумов, необходимых для подготовки специалистов по защите информации в высших учебных заведениях и колледжах. Детально поясняется механизм сопряжения виртуальных лабораторных схем и реального лабораторного сетевого оборудования и программно-аппаратных средств защиты информации, что позволяет создавать эффективные модели корпоративной инфраструктуры для проведения практико-ориентированного обучения. Отмечены высокий потенциал к расширению подходов к обучению студентов в ходе лабораторных практикумов, использующих дополнительный ряд педагогических техник и методов.

*Ключевые слова*: виртуальная лабораторная среда, индивидуальная образовательная траектория, сетевая безопасность, защита информации, безопасность информационных систем, обучение кибербезопасности.

## Введение

Подготовка технического специалиста, который обладает современными компетенциями, знаниями и умениями, является сложной, комплексной и дорогостоящей задачей, предполагающей большой объем теоретических знаний и развитую лабораторную базу. Особенно важным является наличие не только достаточного количества актуальных средств и решений, но и продвинутых подходов к обучению, чтобы будущие специалисты могли знать и комфортно применять возможные действенные сценарии и алгоритмы использо-

вания и работы с теми самыми решениями в различных случаях. В работах [1–4] неоднократно в ходе дискуссий отмечалось и подчеркивалось, что в настоящее время таким требованиям в полной мере отвечают виртуальные лабораторные среды, которые позволяют сократить финансовые затраты на организацию лабораторных практикумов, а также легко адаптировать лабораторные занятия под изменяющиеся обстоятельства реальности с учетом особенности изучаемых средств и методик защиты информации и применяемых для этого специфических решений.

При подготовке специалистов по информационной безопасности виртуальные лабораторные среды активно используются уже в течение нескольких лет [2-4]. Это позволило эффективно решить озвученные ранее проблемные моменты и получить единую лабораторную среду с возможностью мультиплицирования типовых лабораторных схем и стендов для минимизации затрат учебного времени на изучение рабочего места и подготовки лабораторных схем [3]. Отдельно в [4] отмечаются широкие перспективы и возможности, которые открываются при гибридизации виртуальных лабораторных схем включением реального сетевого оборудования и специализированных программно-аппаратных средств защиты информации, которые имеются в наличии в учебных лабораториях.

Эти факты позволяют по-новому взглянуть на возможности гибридных сред и на процесс разработки лабораторного практикума с использованием многократно дублируемых виртуальных лабораторных схем с возможностью подключать существующее реальное оборудование учебных лабораторий. В данной статье рассматриваются особенности построения и эксплуатации гибридных лабораторных сред с изменениями сценариев организации и проведения лабораторного практикума с использованием новых подходов к организации учебного процесса.

## Развертывание гибридной виртуальной лабораторной среды и ее особенности

Лабораторные практикумы по специальным дисциплинам направления подготовки организуются на базе родственных друг для друга лабораторных средах «EVE-NG» (Emulated Virtual Environment — Next Generation) [5] и «PNETLAB» (Packet Network Emulator Tool Lab) [6]. Виртуальная среда «PNETLAB» является основной средой для организации лабораторных занятий, поскольку обеспечивает многопользовательский режим работы с поддержкой независимых для каждого активного пользователя лабораторных сессий. Это дает возможность поддерживать одновременную работу нескольких отдельных лабораторных схем и конфигураций в рамках одной виртуальной лабораторной среды.

Серверы DEPO Storm 3450E2 (2 x Intel Xeon Gold 6133 (20 ядер, 2.5 ГГц), 128 Гб RAM, 2 ТВ HDD) под управлением гипервизора VMWare ESXi версии 8.0.2 [7] являются основной аппаратной платформой для поддержки работы нескольких серверных платформ виртуальной лабораторной среды «PNETLAB» с заранее подготовленным циклом лабораторных работ для конкретной учебной дисциплины. При этом с помощью гипервизора VMWare ESXi для каждой серверной платформы можно задать необходимое число виртуальных процессоров (до 80) и объем требуемой оперативной памяти (до 120 Гб). Каждая серверная платформа лабораторной среды использует основной сетевой интерфейс для доступа и работы с лабораторными схемами. Дополнительно (помимо основного сетевого интерфейса) доступны до 10 сетевых интерфейсов, которые схематично ассоциированы с «облаками связи» (Cloud) в виртуальных лабораторных схемах. Они включаются в отдельные VLAN со своими идентификаторами с помощью встроенного в гипервизор VMWare ESXi виртуального Ethernet-коммутатора vSwitch, который связан с реальным сетевым интерфейсом физического сервера, на котором работает гипервизор [4]. Далее, с использованием технологии 802.1Q VLAN организуется транковый канал к реальному сетевому оборудованию учебных лабораторий (к коммутаторам Ethernet), к которому уже можно подключать любое другое реальное оборудование или программно-аппаратное решение.

Виртуальная лабораторная среда «EVE-NG» инсталлируется и запускается в виде отдельной виртуальной машины на индивидуальных рабочих станциях лабораторий. Это позволяет организовать индивидуальное рабочее место с обособленной лабораторной средой, содержащей свой собственный заранее подготовленный цикл лабораторных работ. Рабочие станции учебных лабораторий оснащены многоядерными производительными процессорами Intel и AMD, а также имеют достаточный объем оперативной памяти (16–32 Гб ОЗУ), что позволяет свободно эксплуатировать виртуальные лабораторные среды «EVE-NG» в отдельных комплектациях, предназначенных для индивидуальной работы. Аналогично виртуальной среде «PNETLAB», среда «EVE-NG» также поддерживает включение дополнительных сетевых интерфейсов рабочей станции в свою работу.

При соответствующей настройке лабораторного сетевого оборудования сетевую связность и обмен данными может быть организована не только между лабораторными схемами внутри виртуальных лабораторных сред и каким-либо реальным программно-аппаратным решением или иным реальным оборудованием в лаборатории, но и с другими лабораторными схемами, работающими внутри других виртуальных лабораторных сред на других серверных платформах или рабочих станциях лабораторий. Таким образом, такой гибридный

принцип организации и работы виртуальных лабораторных сред открывает дополнительные возможности по переходу к распределенным лабораторным схемам работ и практикумов, а также к эффективной децентрализации контроля и управления фрагментами таких распределенных лабораторных схем при сохранении сетевой связности и обмена данными между фрагментами в рамках единой сложной лабораторной работы или практического задания.

## Подходы к разработке и организации лабораторных практикумов

С 2020 года виртуальные лабораторные среды полноценно используются в учебном процессе для проведения циклов лабораторных работ по нескольким специальным дисциплинам подготовки будущих специалистов по защите информации [3]. Применение виртуальных лабораторных сред позволяет организовать лабораторный практикум в виде серии работ, которые включают в себя группу базовых и расширенных заданий. Все группы работ имеют заранее сформированные и преднастроенные (если это необходимо в рамках выполнения задания) лабораторные схемы, что избавляет студентов от необходимости тратить учебное время на сборку лабораторного стенда или схемы, а также конкурировать с другими студентами за ограниченное количество реального лабораторного оборудования. Расширенные и дополнительные задания в цикле лабораторных работ дают возможность студентам повысить свои аттестационные баллы, формировать расширенные и дополнительные профессиональные компетенции, получить больший объем знаний и умений. Сами лабораторные схемы могут «переходить» из одной работы в другую или являться частями более сложных лабораторных работ. Студент при этом продолжает находиться в привычном для него окружении лабораторной среды с однотипным интерфейсом, а часть лабораторной схемы уже может быть преднастроена ранее в ходе выполнения предыдущих лабораторных работ.

Традиционный вариант формирования методических рекомендаций по выполнению лабораторных работ включает в себя предоставление студентам необходимого для выполнения работы набора теоретических знаний, инструкции по работе с применяющимся в лабораторной схеме оборудованием, поэтапные задания для выполнения и контрольные вопросы. Этот вариант подходит, если студенту необходимо сформировать некоторый «фундамент» из практических знаний и умений, что требует методичной и последовательной проработки выполняемых заданий с фиксированием и анализом получаемых на каждом шаге результатов. Однако, в ряде специализированных дисциплин направления подготовки, таких как «Безопасность вычислительных сетей», «Практикум по защите информационных систем», «Программно-аппаратные средства защиты информации», современные реалии требуют внесения специфических корректив в способы подготовки будущих специалистов по информационной безопасности. Особенно это связано с необходимостью учиться командной работе в коллективе (поскольку сольная деятельность специалиста по защите информации на современных предприятиях не является эффективной), а также учиться выполнять и отрабатывать ряд действий в рамках весьма специфичных мероприятий по защите информации, как, например, «пен-тестинг», или «тестирование на проникновение».

Под «пен-тестингом» обычно понимается проверка защищенности и поиск критичных уязвимости корпоративной инфраструктуры и информационных систем (ИС), в ходе которых моделируется реальная атака условного нарушителя или хакера [8–10]. Проведение пен-тестинга подразумевает достаточно большое количество вариантов и сценариев действий, среди которых следует выделить несколько классических подходов и алгоритмов [8]:

1) организация атакующих действий, имитирующих действия нарушителя (Red Team)
2) обнаружение и анализ атакующих действий на стороне корпоративной инфраструктуры с выстраиванием динамического противодействия (Blue Team)
3) проверка защищенности корпоративной инфраструктуры из точки за пределами корпоративной инфраструктуры (внешнее пен-тестирование)
4) проверка защищенности корпоративной инфраструктуры путем непосредственного подключения к корпоративной инфраструктуре (внутреннее пен-тестирование)

Очевидно, что такие особенности проведения пентестирования, как, например, разделение на две команды (Red Team/Атака и Blue Team/Защита) со своими специфическими действиями в ходе работы, большое количество действий по работе с сетевым оборудованием и средствами защиты информации лабораторных схем и стендов вынуждают перестраивать традиционный формат выполнения работы и формирования учебно-методических материалов. Сам лабораторный практикум целесообразно реорганизовать с учетом следующих особенностей:

1) весь объем единой лабораторной работы разделяется на отдельные группы работ пен-тестера (Red Team) и группы работ по анализу и защите модельной корпоративной инфраструктуры
2) задания отдельных лабораторных работ разных групп синхронизуются друг с другом в рамках единого цикла или объединяющей лабораторной работы с общей «легендой» и постановкой задания для отдельных лабораторных работ
3) организуются групповая (2–3 обучающегося) и командная (в соответствии с группами задач) работы над заданиями лабораторных работ

4) традиционные последовательные задания обычной лабораторной работы преобразуются в проблемно-ориентированные задачи с выстраиванием алгоритмов решения поставленных задач до получения требуемого результата

Аналогичным образом можно реорганизовать лабораторный практикум по другим специализированным учебным дисциплинам, где изучаются вопросы развертывания, настройки и эксплуатации современных комплексов программно-аппаратных средств защиты информации и защищенных информационных систем. Поскольку современные средства и решения для защиты информации зачастую сложны в настройке и последующей эксплуатации, это приводит к переизбытку необходимого для выполнения работы объема учебной и методической информации, а также инструкций и задач и является невозможным для освоения одним студентом в отведенные для этого учебные часы. Переход же к командной работе с формированием малых учебных групп, сегментации фронта деятельности и проблемно-ориентированным задачам позволит не только уменьшить «стрессовость» учебного процесса для студентов, но и формировать у них навыки командной и коллективной работы над конкретной проблемой, учиться выстраивать рабочее взаимодействие с коллегами и повышать эффективность обучения путем «погружения» в рабочую атмосферу и ситуацию.

Применение рассмотренных ранее гибридной виртуальной лабораторной среды и ее возможностей позволяет реализовать предлагаемую трансформацию лабораторного практикума. Сложная и комплексная лабораторная схема отлично децентрализуется на мелкие фрагменты с сохранением сетевой связности и обмена данными между ними. Возможность независимого контроля и управления каждым фрагментом сложной лабораторной схемы позволяет разбивать участие студентов в выполнении такой работы на отдельные команды. Специфичность каждого фрагмента даст возможность формировать обособленные проблемно-ориентированные задачи, акцентирующиеся на особенности применения решений отдельных лабораторных фрагментов и объединяющиеся глобальной целью всего комплекса связанных лабораторных работ. На рис. 1 представлен схематичный вариант организации такого лабораторного практикума в гибридной виртуальной лабораторной среде с разделением на отдельные группы задач и командную форму работы.

Схематическая конфигурация лабораторной работы, представленной на рис. 1 демонстрирует возможность разбиения большой комплексной схемы на отдельные фрагменты, которые поддерживаются виртуальными лабораторными средами «PNETLAB» и “EVE-NG». Между фрагментами лабораторной схемы обеспечивается сетевая связность с использованием сетевого оборудования учебных лабораторий. С каждым фрагментом происходит независимое взаимодействие, что позволяет разделить сформированные в рамках общей проблемы задачи на отдельные группы, определить разные задачи для разных команд, изолировать друг от друга рабочее окружение каждой из команды и сохранить возможность групповой работы нескольких обучающихся над одной и той же лабораторной схемой (для виртуальной лабораторной среды «PNETLAB”). При этом лабораторная схема каждой из команд, работающих вместе, соответствует отдельным схемам отдельных лабораторных работ, ориентированных на свою собственную группу заданий и составляющих вместе единый цикл. На рис. 1 показано, что «команда 2» при выполнении своей части лабораторного практикума имела возможность сформировать модельный вариант сегмента корпоративной сети с применением реальных программно-аппаратных средств защиты информации учебной лаборатории, интегрировав их в лабораторную схему виртуальной среды. Автономность действия команд также вносит разнообразие в возможные сценарии выполнения командных лабораторных работ, например, уведомлять о деталях своего сформированного фрагмента глобальной лабораторной схемы остальных участников (метод White-box) или нет (Black-box), если речь идет о практикуме по тестированию на проникновение.

Отдельное преимущество гибридной лабораторной среды можно продемонстрировать, моделируя работу защитных решений класса EDR (Endpoint Detection and Response), таких как MaxPatrol EDR [11] (рис. 2). Здесь распределенная корпоративная инфраструктура моделируется силами трех команд, одна из которых формирует и администрирует сегмент центрального офиса, а две других команды отвечают за свои «филиальные» сегменты сети. Единое решение по обнаружению и выявлению эксплуатируемых уязвимостей на оконечных устройствах распределенной корпоративной сети MaxPatrol EDR подразумевает централизованный сервис контроля и управления, а также сбор всех данных с филиальных устройств путем инсталляции агентов, которые не только передают телеметрию на центральный сервер EDR, но и способны осуществлять базовую реакцию на события в соответствии с получаемыми от центра командами. Базовая защита филиальной корпоративной инфраструктуры здесь обеспечивается путем анализа поступающей телеметрии и формирования блокирующих действий установленными EDR-агентами путем получения команд от центрального EDR-сервера. Усиленные меры по обеспечению защиты филиальных элементов корпоративной сети обеспечиваются персоналом филиала на местах с использованием локально установленных средств защиты информации. Подобная организация лабораторной работы позволяет учиться работе по организации защиты информации в рас-

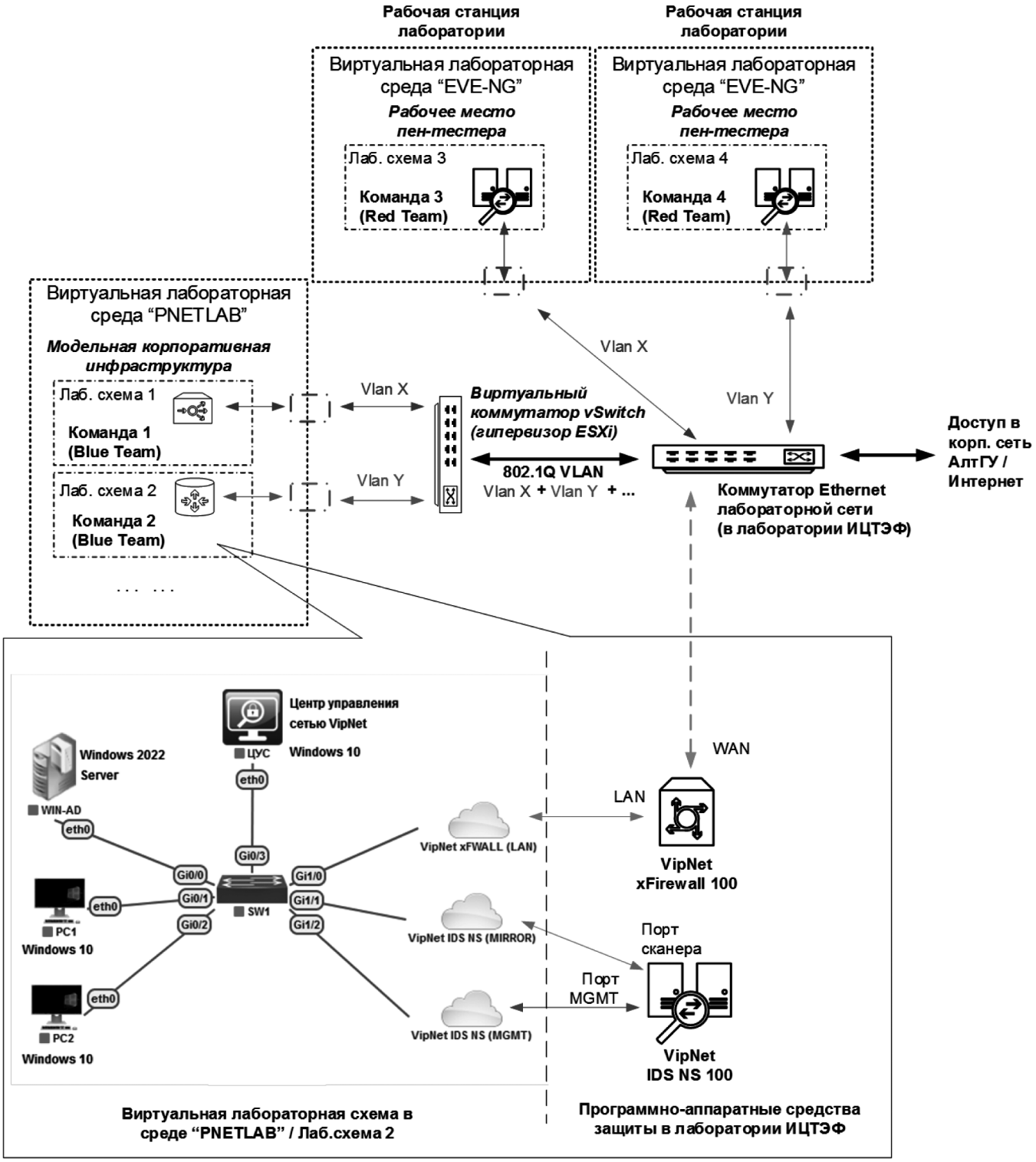


Рис. 1. Пример схемы организации лабораторного практикума с использованием возможностей гибридных виртуальных лабораторных сред для командной работы над заданиями

пределенной корпоративной среде с единым центром управления, тренировать реакцию персонала в филиалах на атаки и синхронизировать свои действия с действиями корпоративного «центра», вырабатывая таким образом единый алгоритм взаимодействия для обнаружения и отражения активных атак команд «Red Team» на более уязвимые филиальные сегменты корпоративной сети. При такой организации практикума студенты не только учатся использовать штатные централизованные решения вендоров (таких как MaxPatrol EDR), но и формировать свои локальные алгоритмы действий для повышения эффективности отражения поступающих

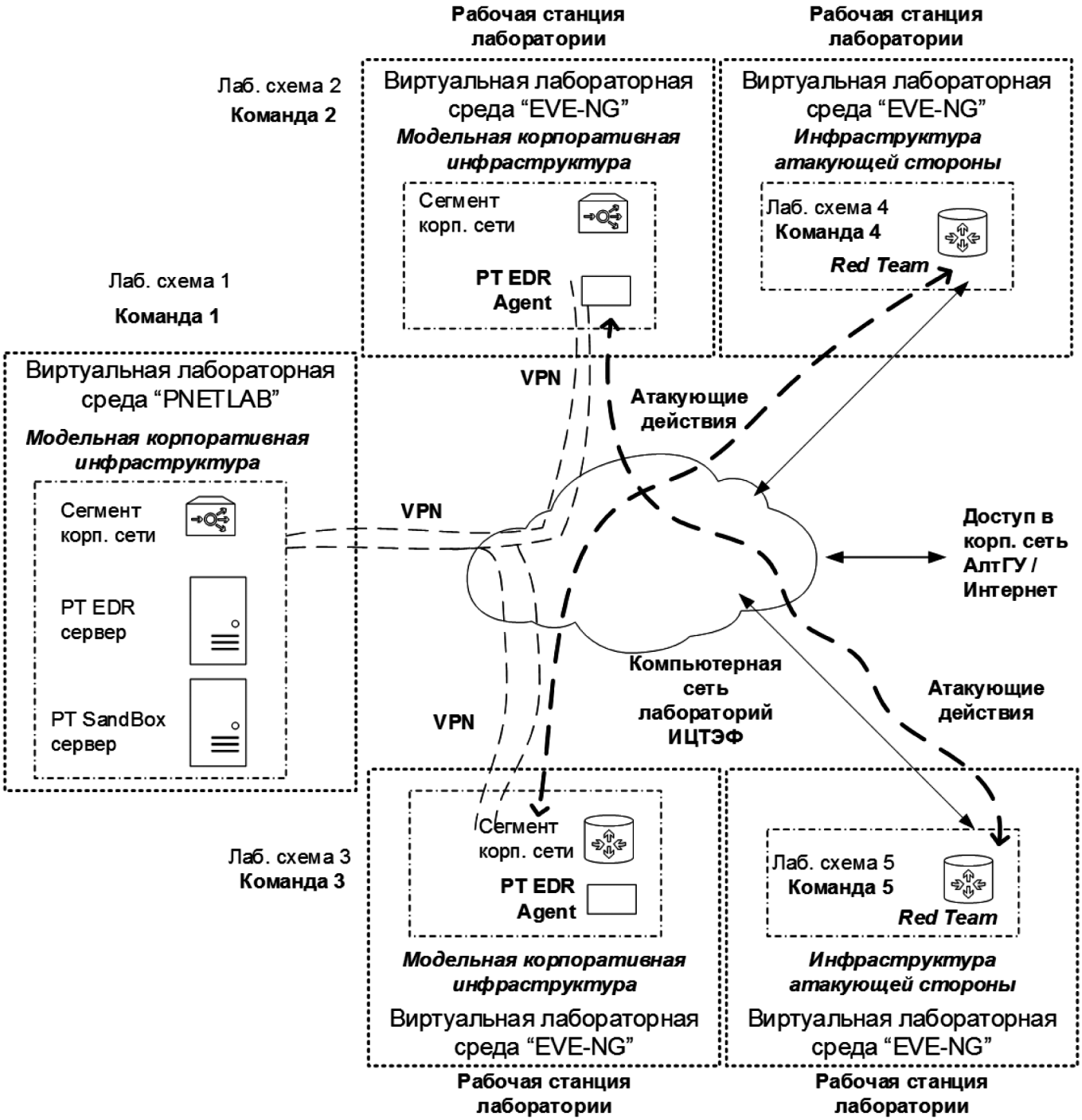


Рис. 2. Пример использования гибридной виртуальной лабораторной среды для моделирования распределенной корпоративной инфраструктуры с централизованными средствами защиты (MaxPatrol EDR)

атак. Гибридный подход к организации лабораторного практикума при этом обеспечивает независимость действий каждой группы (учебных «команд») специалистов по защите информации в центральном офисе и филиальных структурах.

Используя возможности гибридной виртуальной лабораторной среды всю работу с лабораторным практикумом можно попробовать организовать по принципу взаимодействия участников соревнований CTF (Capture the Flag) в режиме «Attack and Defense». Преимущества геймификации учебного процесса и проведения части практических занятий в стиле CTF-соревнований рассматривались в [12], где отмечалось, что это дает возможность более открыто формировать лабораторные задания, позволяет обучающимся получать в парал-

лельном режиме не только специфичные знания в области пен-тестирования, но и углублять и развивать свои навыки и умения в части администрирования операционных систем, скрипт-программированию на shell (Bash) и Python, а также использованию прикладного инструментария сетевого администратора, помимо особых навыков работы с проприетарными средствами защиты информации, используемыми в лабораторных схемах. Фрагменты лабораторных схем при подобной организации лабораторного практикума у команд могут или полностью дублироваться (вариант классического CTF «Attack and Defence») или отличаться друг от друга. Это открывает перед участниками такого практикума более широкие возможности как по поиску уязвимостей у других участвующих команд, так и по защите своего фрагмента лабораторной схемы (модельной корпоративной инфраструктуры).

## Заключение

В работе выполнено рассмотрение особенностей применения виртуальных лабораторных сред «PNETLAB» и «EVE-NG» в учебном процессе подготовки специалистов по информационной безопасности в их расширенном гибридном варианте. Широкие функциональные возможности таких гибридных виртуальных лабораторных сред позволяют расширить стандартные комплексы лабораторных практикумов путем включения в них реального лабораторного сетевого оборудования и программно-аппаратных решений защиты информации. Кроме этого, отмечается большой потенциал для трансформирования стандартных лабораторных работ и выстраивания специализированных групп лабораторных работ, активно использующих для своего выполнения командную групповую работу студентов, децентрализацию и проблемно-ориентированное формирование лабораторных заданий. Это дает возможность строить лабораторный практикум с условиями его выполнения, более близкими к реальным рабочим условиям и ситуациям, с которыми могут столкнуться будущие специалисты по защите информации. Отдельно следует отметить потенциал к расширению традиционной парадигмы выполнения лабораторных работ в сторону увеличения элементов геймификации и переходу к практикумам в формате, близкому к формату популярных соревнований CTF.

ЛИТЕРАТУРА


1. Золотухин М.С., Кубанских О.В. Виртуальные лаборатории в преподавании и обучении // Современные научные исследования и инновации). 2019. №7. [Электронный ресурс] — Режим доступа — URL: https://web.snauka.ru/issues/2019/07/89984 (дата обращения 25.06.2025)
2. Мансуров А.В., Минакова Н.Н. Опыт успешного внедрения виртуальной лабораторной среды для лабораторных практикумов учебных дисциплин направления подготовки 10.03.01 Информационная безопасность // Высокопроизводительные вычислительные системы и технологии. — 2023. — Т. 7, № 1. — С. 139–146.
3. Мансуров А.В., Минакова Н.Н., Рудер Д.Д., Ладыгин П.С. Опыт внедрения виртуальных лабораторных сред «PNETLAB» и «EVE-NG» для организации лабораторных практикумов при подготовке специалистов по защите информации в АлтГУ // Современное профессиональное образование. — 2024. — №1. — С. 63–69.
4. Минакова Н.Н., Мансуров А.В. Успешная практика комбинирования лабораторных схем виртуальной лабораторной среды и реального лабораторного оборудования при подготовке специалистов по защите информации в АлтГУ // Высокопроизводительные вычислительные системы и технологии. — 2024. — Т. 8. — № 1. — С. 26–33.
5. EVE-NG. [Электронный ресурс] — Режим доступа — URL: https://www.eve-ng.net/ (дата обращения 25.06.2025)
6. PNETLab: Lab is Simple. [Электронный ресурс] — Режим доступа — URL: https://pnetlab.com/ (дата обращения 25.06.2025)
7. VMWare ESXi. [Электронный ресурс] — Режим доступа — URL: https://www.vmware.com/products/esxi-and-esx.html (дата обращения 25.06.2025)
8. Beheshti B.D., Shebli H. M. Z. A. A study on penetration testing process and tools. // 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2018. P. 1–7. DOI: 10.1109/LISAT.2018.8378035.
9. Kumar S. Critical Analysis of Penetration Testing Process and Tools. // EPRA International Journal of Research & Development (IJRD). 2021. Vol. 6. Issue 9. P. 228–235. DOI: 10.36713/epra2016.
10. Anand A., Kumar S.,Rana R.,Sakharkar A.N. A Comprehensive Review on Penetration Testing Tools with Emerging Technology. // Proceedings of the KILBY 100 7th International Conference on Computing Sci-ences 2023 (ICCS 2023). DOI: 10.2139/ssrn.4488188.
11. MaxPatrol EDR — защита конечных устройств от сложных и целевых атак. [Электронный ресурс] — Режим доступа — URL: https://www.ptsecurity.com/ru-ru/products/edr/ (дата обращения 25.06.2025)
12. Mansurov A. A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia. // Modern Applied Science. 2016. Vol. 10. No. 11. P. 159–166. DOI: 10.5539/mas.v10n11p159.


© Мансуров Александр Валерьевич (mansurov.alex@gmail.com); Минакова Наталья Николаевна (minakova@phys.asu.ru);
Салита Даниил Сергеевич (d.s.salita@gmail.com); Дмитриев Александр Александрович (dmitriev@asu.ru);
Журавлева Виктория Владимировна (torinka8@gmail.com)
Журнал «Современная наука: актуальные проблемы теории и практики»