УДК 378

КИБЕРУЧЕНИЯ ВУЗОВ РОССИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК МЕТОД ПРАКТИЧЕСКОЙ ОЦЕНКИ КАЧЕСТВА ОБУЧЕНИЯ СПЕЦИАЛИСТОВ ПО РАССЛЕДОВАНИЮ КИБЕРИНЦИДЕНТОВ

Красов А.В., Казанцев А.А.
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича, Санкт-Петербург
e-mail: krasov@inbox.ru, farvest.ax@yandex.ru

Аннотация. *Статья посвящена анализу киберучений как метода оценки практической подготовки специалистов по информационной безопасности в российских ВУЗах. Центральное внимание уделено уникальному формату соревнований, разработанному кафедрой Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), который максимально приближен к реальным условиям работы экспертов по расследованию киберинцидентов. В статье рассматриваются этапы проведения киберучений, их организация, контингент участников, а также задания, которые охватывают широкий спектр тем, связанных с анализом кибератак и расследованием инцидентов.*
Ключевые слова: *Киберучения, подготовка кадров в области информационной безопасности, оценка качества образования, практическая подготовка*

Современные вызовы в области информационной безопасности требуют принципиально новых подходов к подготовке и оценке квалификации специалистов. В условиях стремительной цифровой трансформации и усложнения киберугроз традиционные методы обучения демонстрируют свою ограниченность, создавая потребность в практико-ориентированных форматах оценки профессиональных компетенций.

Киберучения возникли как ответ на эти вызовы, предложив принципиально новую модель оценки навыков будущих специалистов. В отличие от традиционных экзаменов и тестирований они позволяют:

- Моделировать реальные условия профессиональной деятельности.
- Оценивать не только теоретические знания, но и практические навыки.
- Тестировать способность работать в команде и принимать решения в условиях неопределенности.

С 2021 года в рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» организуются и проводятся Всероссийские киберучения для студентов ВУЗов, обучающихся по программам в области информационной безопасности. Реализация проходит под руководством Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации при методическом и организационном сопровождении и поддержке Федерального учебно-методического объединения в системе высшего образования по укрупнённой группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ). Площадкой для проведения данного мероприятия ежегодно становится кафедра Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича.

Киберучения представляют собой эффективный механизм комплексной оценки профессиональной подготовки студентов, выходящий за рамки традиционной проверки теоретических знаний. Их ключевая ценность заключается в создании реалистичной среды, моделирующей условия настоящих кибератак, где участники демонстрируют способность анализировать сложные ситуации, оперативно принимать решения и эффективно применять полученные знания на практике.

Федеральный проект "Информационная безопасность" как основа развития киберучений

Федеральный проект "Информационная безопасность" в рамках национальной программы "Цифровая экономика" представляет собой масштабную инициативу, направленную на системное развитие кадрового потенциала страны в сфере защиты информации. Современный формат проекта был утвержден в 2019 году как ответ на растущие вызовы в области кибербезопасности и необходимость создания устойчивой системы подготовки квалифицированных кадров.

Основными цели проекта являются:

1. ***Защита критической информационной инфраструктуры (КИИ):*** Обеспечение безопасности объектов, которые имеют ключевое значение для функционирования экономики, государства и общества.
2. ***Развитие отечественных технологий:*** Стимулирование разработки и внедрения российских решений в области информационной безопасности.
3. ***Повышение уровня подготовки специалистов:*** Подготовка кадров в сфере кибербезопасности и повышение квалификации существующих специалистов.
4. ***Создание нормативной базы:*** Разработка и совершенствование законодательства в области информационной безопасности.
5. ***Защита персональных данных:*** Обеспечение безопасности данных граждан и организаций.

Киберучения в рамках проекта выполняют три взаимосвязанные функции. Во-первых, они служат объективным инструментом оценки практических навыков студентов, используя стандартизированные методики проверки. Во-вторых, выступают как образовательная платформа, где задания разрабатываются на основе реальных кейсов ведущих компаний отрасли. В-третьих, создают уникальную среду для взаимодействия между академическим сообществом и потенциальными работодателями. [1]

Методическое сопровождение проекта обеспечивает Федеральное учебно-методическое объединение по направлению "Информационная безопасность". ФУМО не только унифицирует требования к содержанию соревнований, но и интегрирует их результаты в образовательные стандарты, обеспечивая постоянное обновление учебных программ в соответствии с актуальными вызовами.

Участники и география киберучений

Организационная структура киберучений в масштабах всей страны предусматривает распределение ВУЗов-участников по укрупненным федеральным округам на базе ведущих технических ВУЗов, подведомственных Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации:

- МТУСИ (Центральный округ) охватывает 55 ВУЗов, реализующих программы в области Информационной безопасности;
- СПбГУТ (Северо-Западный округ) – 22 ВУЗа;
- ПГУТИ (Приволжский, Северо-Кавказский и Южный округа) – 29 ВУЗов;
- СибГУТИ (Сибирский, Уральский и Дальневосточный округа) – 27 вузов.

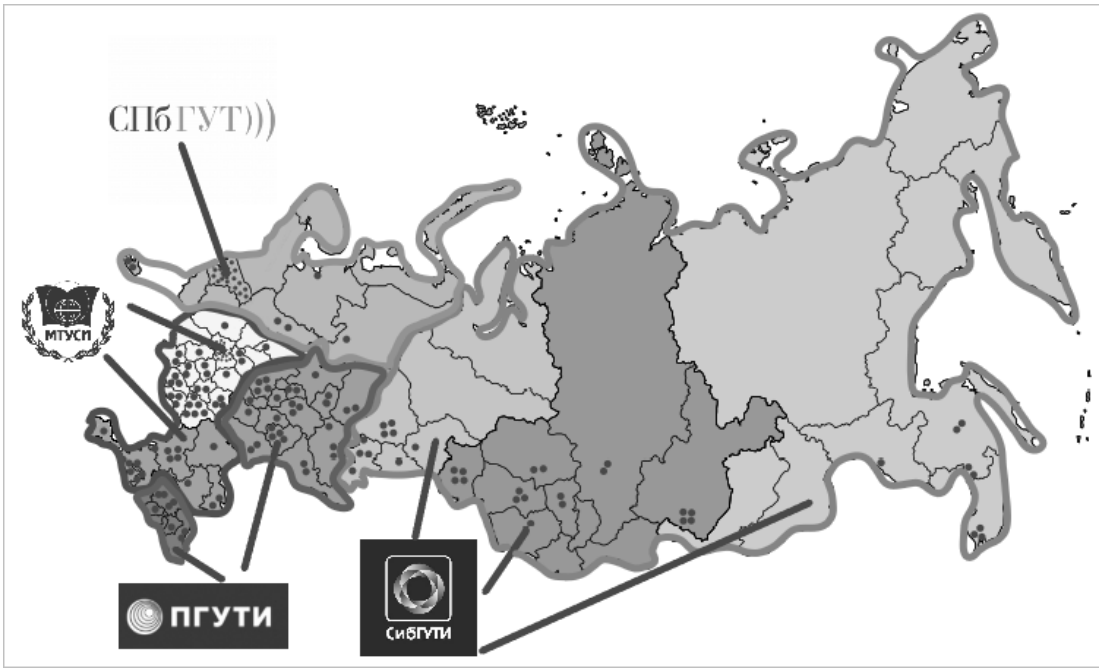

Рисунок 1 – Распределение федеральных округов по ВУЗам

За последние три года наблюдается устойчивая положительная динамика развития киберучений. Количество участвующих вузов увеличилось на 20%, при этом географический охват расширился за счет включения новых регионов. Особенно заметен рост активности в Северо-Западном и Сибирском федеральных округах, где к традиционным участникам из крупных университетских центров добавились команды из региональных вузов. Такое расширение свидетельствует о возрастающем признании ценности киберучений как инструмента оценки качества подготовки специалистов в области информационной безопасности.

Киберучения 2024 года продемонстрировали значительный рост интереса со стороны высших учебных заведений России. В Северо-Западном федеральном округе в соревнованиях приняла участие 21 команда из ведущих технических и военных ВУЗов региона

Важной особенностью современного этапа развития киберучений стало формирование устойчивых связей между вузами разных регионов. Университеты-лидеры, такие как СПбГУТ и МТУСИ, активно передают опыт организации соревнований своим коллегам из других городов, что способствует выравниванию уровня подготовки участников. Регулярно проводятся методические семинары и вебинары, на которых обсуждаются лучшие практики проведения киберучений. Этот обмен опытом особенно важен для вузов, только начинающих развивать направления подготовки в области информационной безопасности [2].

Организация и методика проведения киберучений

Современная система проведения киберучений в российских вузах представляет собой многоуровневый процесс, разработанный с учетом отечественных образовательных стандартов. Организационная структура включает три последовательных этапа, каждый из которых имеет четко определенные цели и методическое обеспечение.

Отборочный дистанционный этап служит важным фильтром, позволяющим оценить базовые навыки участников в области анализа киберугроз. В ходе этого этапа командам предоставляются файлы сетевого трафика в формате PCAP, содержащие следы смоделированных атак. Участники должны идентифицировать различные типы компьютерных атак, включая сканирование сетей, эксплуатацию уязвимостей и несанкционированный доступ. Особое внимание уделяется способности студентов не просто обнаружить факт атаки, но и проанализировать ее последствия, определить используемые злоумышленником техники и тактики [3]. Отчеты участников оцениваются по строгим

критериям, включающим точность определения временных меток, корректность классификации атак и полноту анализа последствий.

Региональный финальный этап проводится в очном формате на специализированных площадках базовых вузов. Этот этап отличается значительно более сложными заданиями, максимально приближенными к реальным условиям работы специалистов по информационной безопасности. Участники работают с образами виртуальных машин, содержащими артефакты киберинцидентов. В их задачи входит проведение полного цикла расследования: от сбора и анализа цифровых доказательств до реконструкции цепочки компрометации. Для выполнения заданий команды используют профессиональный инструментарий, включающий как классические средства анализа (Wireshark, Volatility), так и современные платформы для киберразведки (Timesketch, Brim). Особенностью этого этапа является ограничение времени на выполнение заданий (6 астрономических часов), что моделирует условия реального инцидента, когда специалистам приходится работать в условиях жестких временных ограничений.

Всероссийский финал представляет собой кульминацию всего цикла киберучений. На этом этапе встречаются сильнейшие команды из всех федеральных округов, что создает уникальную среду для профессионального роста и обмена опытом. Задания для финала разрабатываются с привлечением ведущих экспертов отрасли и часто включают элементы новейших киберугроз, с которыми сталкиваются российские компании. Особенностью финальных заданий является их комплексный характер - участникам приходится одновременно анализировать сетевой трафик, исследовать компрометированные системы, восстановление хронологии событий и разработку мер по предотвращению подобных атак в будущем. Такой подход позволяет наиболее объективно оценить способность будущих специалистов работать в условиях реального киберинцидента [4].

Методическое обеспечение киберучений включает несколько ключевых компонентов. Во-первых, это система оценивания, разработанная с учетом международных стандартов в области кибербезопасности. Каждое задание имеет четкие критерии оценки и весовые коэффициенты для различных аспектов решения. Во-вторых, важную роль играет система проверки и валидации заданий, которая осуществляется как академическими экспертами, так и представителями индустрии. В-третьих, организаторы уделяют особое внимание постсоревновательному анализу, проводя подробные разборы решений и публикуя методические рекомендации для преподавателей.

Техническая инфраструктура киберучений за последние годы претерпела значительные изменения. Если раньше соревнования проводились на базе стандартных компьютерных классов, то сейчас используются специализированные киберполигоны, позволяющие моделировать сложные сетевые топологии и реалистичные сценарии атак. Такие полигоны, как, например, развернутый в СПбГУТ, обеспечивают изолированную среду для проведения соревнований, одновременно позволяя участникам работать с реальными инструментами и технологиями [5, 6].

Особого внимания заслуживает эволюция формата заданий. В отличие от ранних лет, когда основное внимание уделялось отдельным аспектам информационной безопасности, современные киберучения предлагают комплексные сценарии, охватывающие весь жизненный цикл киберинцидента. Типичное задание может включать элементы сетевого анализа, исследование вредоносного ПО, цифровую криминалистику и реагирование на инциденты. При этом организаторы сознательно усложняют задания, вводя элементы обфускации, использование нестандартных протоколов и техник уклонения от обнаружения, что соответствует современным реалиям кибербезопасности.

Важной методической инновацией последних лет стало внедрение системы динамического оценивания, когда баллы начисляются не только за конечный результат, но и за применяемые методы решения. Такой подход стимулирует участников к использованию наиболее эффективных и профессиональных методик работы, а не просто к поиску

"правильного ответа". Кроме того, это позволяет оценить не только технические навыки участников, но и их способность к системному мышлению и работе в команде. [7]

Пример задания для финала регионального этапа киберучений

Выбор задания регионального этапа для анализа обусловлен его репрезентативностью и ориентацией на фундаментальные компетенции. В отличие от финальных заданий всероссийского этапа, которые часто включают узкоспециализированные и экспериментальные сценарии, региональные задания разрабатываются с учетом среднего уровня подготовки участников из различных вузов.

Типичное задание финального тура регионального этапа предполагало реконструкцию многоэтапной атаки на корпоративную инфраструктуру. Участникам необходимо было проанализировать действия злоумышленника, последовательно компрометировавшего различные сегменты сети.

Схема атаки отражена на Рисунке 2, где показаны все этапы проникновения и перемещения атакующего по сети, начиная с WAN (10.0.0.0/24) через DMZ (172.16.1.0/24) и заканчивая LAN (192.168.1.0/24).

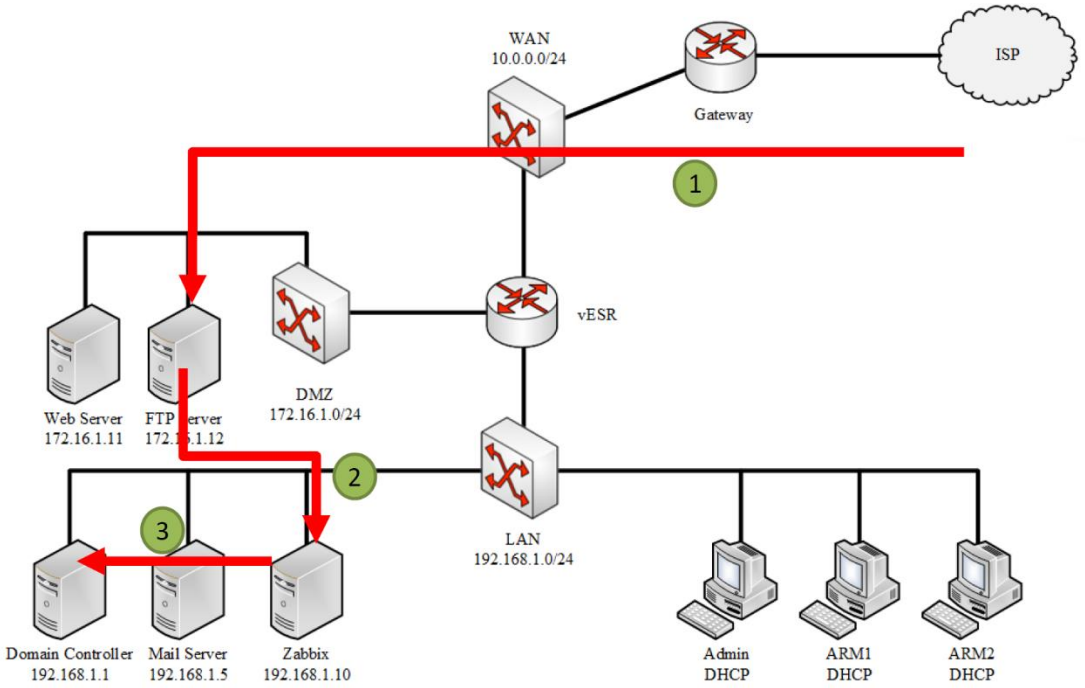

Рисунок 2 – Схема атаки злоумышленника в задании

Атака началась с попытки подбора пароля к веб-интерфейсу WordPress, но поскольку защита оказалась достаточно надежной, злоумышленник переключился на другой вектор атаки. Он сфокусировался на сервисе SNMP, где благодаря слабой парольной политике смог подобрать учетные данные. Получив доступ, атакующий воспользовался известной уязвимостью CVE-2020-15862, позволяющей выполнить произвольный код, и с помощью утилиты busybox установил реверс-шелл, получив тем самым контроль над системой.

Дальнейшие действия злоумышленника были направлены на расширение своего присутствия в сети. Через скомпрометированную систему он загрузил вредоносный агент на FTP-сервер (172.16.1.12), расположенный в демилитаризованной зоне (DMZ) (172.16.1.0/24). Это позволило ему закрепиться в сети и продолжить разведку. Следующей целью стал Zabbix-сервер (192.168.1.10), к которому злоумышленник успешно подобрал пароль. Получив доступ к веб-интерфейсу Zabbix, он эксплуатировал уязвимости для повышения привилегий и загрузил дополнительный агент, усилив свой контроль над системой.

Используя возможности Zabbix, атакующий перешел к атаке на критически важные внутренние ресурсы [6]. Он скомпрометировал контроллер домена (192.168.1.1), получил права администратора и завершил атаку шифрованием файлов с паролями. Это действие не

только заблокировало доступ легитимным пользователям, но и позволило злоумышленнику сохранить контроль над всей внутренней сетью (LAN, 192.168.1.0/24).

Результаты и анализ эффективности киберучений

Анализ результатов всероссийских киберучений за последние три года позволяет проследить динамику развития соревнований и выявить лидирующие вузы в области подготовки специалистов по информационной безопасности.

2022 год стал знаковым в истории киберучений - впервые финальные соревнования проводились на базе нового Национального киберполигона СПбГУТ. В финале приняли участие 12 команд, при этом разрыв между лидерами и остальными командами был минимальным (не более 5 баллов), что свидетельствовало о высокой конкуренции.

1 место – команда «ITMO)))», Национальный исследовательский университет ИТМО (Санкт-Петербург).

2 место – команда «Test Team Please Ignore», Северный (Арктический) федеральный университет имени М. В. Ломоносова (Архангельск).

3 место – команда «Datapoison», Казанский национальный исследовательский технический университет имени А. Н. Туполева (Казань).

2023 год отметился расширением географии и усложнением заданий. Впервые в соревнованиях приняли участие представители новых вузов - Уральского федерального университета и Дальневосточного федерального университета.

1 место – команда «АпельсиновыйSOC», Тихоокеанский государственный университет (Хабаровск).

2 место – команда «Datapoison», Казанский национальный исследовательский технический университет имени А. Н. Туполева (Казань).

3 место – команда «UnsafeTeam», Самарский государственный технический университет (Самара).

2024 год установил новые рекорды по уровню сложности и количеству участников. В отборочных этапах приняли участие более 130 команд из 45 вузов страны, что на 25% больше, чем в 2023 году.

1 место – команда «monKEYz», Дальневосточный государственный университет путей сообщения (Хабаровск).

2 место – команда «HisWoo», Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича (Санкт-Петербург).

3 место – команда «RedCadets», Военно-космическая академия им. А. Ф. Можайского (Санкт-Петербург).

Сравнительный анализ результатов за три года позволяет выявить несколько устойчивых тенденций:

1. Рост уровня подготовки - средний балл участников последовательно увеличивается, при этом сложность заданий ежегодно возрастает на 15-20%.
2. Расширение географии – соревнования позволяют охватывать все федеральные округа.
3. Повышение качества методического обеспечения - анализ результатов позволяет организаторам корректировать систему оценки и оптимизировать форматы заданий. На основе выявленных типичных затруднений участников многие вузы вводят дополнительные практические курсы, что способствует повышению качества подготовки специалистов.
4. Усиление практической направленности - доля команд, успешно справившихся с комплексными заданиями, увеличилась с 45% в 2022 году до 68% в 2024.
5. Развитие кадрового потенциала - 85% победителей и призеров киберучений последних трех лет сейчас работают в ведущих российских компаниях в области информационной безопасности.

Изменения отражают эволюцию киберугроз и соответствуют реальным вызовам, с которыми сталкиваются специалисты по информационной безопасности. Акцент сместился на

подготовку к работе с усложняющимися методами сокрытия вредоносной активности, что особенно актуально в условиях роста числа целевых атак.

Особого внимания заслуживает анализ типичных ошибок участников:

- В 2022 году основные сложности возникали с анализом зашифрованного трафика (справились лишь 30% команд).
- В 2023 году проблемной зоной стало исследование цепочек косвенных доказательств и анализ сложных многоэтапных атак.
- В 2024 году наибольшие трудности вызвали задания по выявлению и анализу современных техник уклонения от обнаружения.

Эти данные активно используются организаторами для совершенствования учебных программ и методики подготовки студентов.

Заключение

Анализ всероссийских киберучений, проводимых в СПбГУТ, позволяет утверждать, что данный формат стал важнейшим элементом системы подготовки специалистов по информационной безопасности в России. Киберучения выполняют комплексную функцию, сочетая в себе элементы оценки, обучения и профессиональной ориентации.

Ключевым достижением проекта стало создание объективной системы оценки профессиональных компетенций будущих специалистов. В ходе соревнований участники демонстрируют:

- Способность к комплексному анализу киберинцидентов, включая выявление векторов атаки, анализ компрометированных систем и восстановление хронологии событий.
- Навыки работы с профессиональным инструментарием в условиях, максимально приближенных к реальным.
- Умение оперативно принимать решения в условиях неполной информации и временных ограничений.
- Командную работу и распределение ролей при решении сложных многоэтапных задач.
- Способность документировать и презентовать результаты расследования.

Особую ценность представляет практико-ориентированный характер соревнований. Разрабатывая задания, организаторы ориентируются на актуальные вызовы, с которыми сталкиваются специалисты по информационной безопасности. Это обеспечивает высокую релевантность формируемых компетенций требованиям работодателей.

Национальный киберполигон СПбГУТ стал важнейшим элементом этой системы, предоставляя участникам доступ к профессиональной инфраструктуре. Его развитие позволяет постоянно повышать уровень реалистичности моделируемых сценариев, что особенно важно для формирования практических навыков.

Перспективы развития киберучений видятся в следующих направлениях:

- Углубление интеграции с профессиональным сообществом.
- Разработка специализированных треков для различных направлений ИБ.
- Создание системы непрерывного профессионального роста участников.
- Расширение международного сотрудничества в этом формате.

Современные киберучения представляют собой качественно новый этап развития профессионального образования. Преодолев формат локальных студенческих состязаний, они стали действенным механизмом формирования национального кадрового резерва. Через систему конкурсных заданий, разработанных совместно с отраслевыми экспертами, происходит не только отбор наиболее перспективных специалистов, но и синхронизация образовательных программ различных вузов с актуальными требованиями рынка. Такая модель взаимодействия академической среды и профессионального сообщества создаёт устойчивую основу для развития отечественной школы информационной безопасности.

Список литературы

1. Ушаков, И. А. Организация Всероссийских киберучений с использованием киберполигона кафедры защищенных систем связи СПБГУТ / И. А. Ушаков, А. Ю. Цветков, М. А. Скорых // Прикладные процессы в области информационной безопасности. Тенденции развития методов защиты информации: Материалы научно-практических конференций, Самара, 19–20 октября 2023 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2023. – С. 47-49. – EDN INLZAA.
2. Красов, А. В. Опыт прохождения международной профессионально-общественной аккредитации на примере Санкт-Петербургского университета телекоммуникаций им. Проф. Бонч-Бруевича / А. В. Красов, А. А. Казанцев // Новые технологии оценки качества образования: Сборник материалов XVII Форума Гильдии экспертов в сфере профессионального образования, Йошкар-Ола, 11 ноября 2022 года / Под общей редакцией Г.Н. Мотовой. – Москва: Ассоциация "Гильдия экспертов в сфере профессионального образования", 2022. – С. 13-18.
3. Миняев, А. А. Анализ сетевого трафика при различных видах эксфильтрации данных / А. А. Миняев, В. М. Моисеев, М. А. Скорых // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): Сборник научных статей XII Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2023 года / Под редакцией С.И. Макаренк, сост. В.С. Елагин, Е.А. Аникевич. Том 4. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 669-676. – EDN WEBNMQ.
4. Красов, А. В. Магистерская программа нового поколения экспертов в информационной безопасности, признанная ЕС (ENGENSEC) / А. В. Красов, И. А. Ушаков, С. И. Штеренберг // Современное образование: содержание, технологии, качество. – 2015. – Т. 1. – С. 79-81. – EDN UBHKJR.
5. Ушаков, И. А. Методика обнаружения аномалий в сетевом трафике с использованием IPS на основе Security Onion / И. А. Ушаков, А. В. Красов, Д. Д. у. Мулладжанов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2022. – № 1. – С. 5-11. – DOI 10.46418/2079-8199_2022_1_1. – EDN DSQOHB.
6. Кибирев, М. П. Сравнительный анализ утилит для проведения атаки PTH / М. П. Кибирев, А. А. Миняев, М. А. Скорых // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): Сборник научных статей XII Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2023 года / Под редакцией С.И. Макаренк, сост. В.С. Елагин, Е.А. Аникевич. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 710-715. – EDN LBUYLS.
7. Красов, А. В. Подготовка специалистов в области информационной безопасности в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича / А. В. Красов, И. А. Ушаков // Инновации. – 2013. – № 7(177). – С. 92-97.

RUSSIAN UNIVERSITY CYBER EXERCISES IN INFORMATION SECURITY AS A PRACTICAL METHOD FOR ASSESSING THE TRAINING QUALITY OF DIGITAL FORENSICS SPECIALISTS

Krasov A.V., Kazantsev A.A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications, Saint-Petersburg
e-mail: krasov@inbox.ru, farvest.ax@yandex.ru

Abstract. *The article analyzes cyber exercises as a method for assessing the practical training of information security specialists in Russian universities. Special attention is given to the unique competition format developed by the Department of Secure Communication Systems at the Bonch-Bruevich Saint-Petersburg State University of Telecommunications (SPbSUT), which closely replicates real-world conditions for incident response experts. The article examines the stages of conducting cyber exercises, their organization, participant profiles, as well as tasks covering a wide range of topics related to cyberattack analysis and incident investigation.*
Keywords: *Cyber exercises, information security personnel training, education quality assessment, practical training*