ПРОГРЕССИВНЫЕ ПОДХОДЫ К ОБУЧЕНИЮ СТУДЕНТОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ ЧЕРЕЗ ФАКУЛЬТАТИВНЫЕ ЗАНЯТИЯ

Ф.М.Мухтаров
Доцент кафедры “Информационная безопасность” Ферганского филиала Ташкентского университета имени Мухаммада аль-Хорезми
https://doi.org/10.5281/zenodo.10389464

Аннотация: В статье рассматриваются прогрессивные подходы к обучению студентов в области кибербезопасности через факультативные занятия. Выделены эффективные методы и технологии, такие как, проектные технологии, моделирование, решение проблемных задач и другие, которые позволяют эффективно развивать навыки и знания в области кибербезопасности, стимулируют активное участие студентов и способствуют формированию критического мышления и практического опыта в решении проблем кибербезопасности.

Ключевые слова: Прогрессивные подходы, кибербезопасность, критическое мышление, виртуальные лаборатории, информационные технологии, киберугрозы, информационная безопасность, Capture The Flag (CTF).

Annotation: The article discusses progressive approaches to teaching students in the field of cybersecurity through elective classes. Effective methods and technologies are highlighted, such as design technologies, modeling, problem solving and others, which allow you to effectively develop skills and knowledge in the field of cybersecurity, stimulate the active participation of students and contribute to the formation of critical thinking and practical experience in solving cybersecurity problems.

Key words: Progressive approaches, cybersecurity, critical thinking, virtual laboratories, information technology, cyber threats, information security, Capture The Flag (CTF).

В современном информационном обществе кибербезопасность становится все более важной и актуальной темой. Расширение цифровой сферы и увеличение угроз в онлайн-среде требуют эффективных мер по защите информационных систем и данных. Однако, для эффективной борьбы с киберугрозами, необходимы хорошо подготовленные специалисты в области кибербезопасности. В связи с этим, обучение студентов в данной области приобретает все большую значимость. Для

обучения студентов важно разработать методику, позволяющую получить необходимы знания и навыки в области обеспечения кибербезопасности, которая основана на принципах активного обучения и практико-ориентированного подхода.

Первым шагом в разработке прогрессивных подходов к обучению студентов в области кибербезопасности является оценка текущих подходов и методологий. Традиционно, обучение в данной области осуществлялось через формальные курсы и лекции, предоставляя теоретические знания о кибербезопасности. Однако, такой подход часто оказывается недостаточным для формирования практических навыков и развития критического мышления у студентов.

Прогрессивные подходы в обучении студентов в области кибербезопасности включают в себя использование факультативных занятий. Факультативы предоставляют возможность студентам самостоятельно выбирать дополнительные занятия по кибербезопасности, исходя из своих интересов и потребностей. Такой подход позволяет студентам глубже исследовать конкретные аспекты кибербезопасности, а также получать практические навыки через активное участие в учебных проектах и симуляциях.

Следует отметить, что вопросы кибербезопасности, являясь приоритетными направлениями современного образования. В процессе проведения занятий «предлагается использовать традиционные и инновационные методики и технологии». Так эффективным представляется использование методики определения статуса защищенности информации, а также решение ситуационных задач.

Для обучения бакалавров был разработан авторская учебная программа и учебный курс по преподаванию предмета «Основы кибербезопасности» в формате Реверсивного инжиниринга.

Данная инновационная методика преподавания основана на принципе "реверсивного инжиниринга" и предлагает студентам погрузиться в мир кибербезопасности через факультативные занятия. Она позволяет студентам развивать свои навыки и знания в области кибербезопасности, а также учиться мыслить, как хакеры для более эффективного обнаружения и предотвращения киберугроз.

Составленный учебный курс по этой методики разбит на четыре основных разделов.

1. Введение в реверсивный инжиниринг.

2. Практические занятия по анализу вредоносных программ.
3. Участие в соревнованиях Capture The Flag (CTF).
4. Обсуждение и анализ результатов.

В первом разделе студентам предоставляется вводное обучение по реверсивному инжинирингу, который является процессом анализа программного обеспечения для понимания его работы и выявления потенциальных уязвимостей. Объясняются основные концепции и инструменты, используемые в реверсивном инжиниринге.

Во втором разделе студентам предлагается учебный план, включающий практические занятия по анализу вредоносных программ. Они изучают различные типы вредоносного программного обеспечения, обнаруживают его скрытые функции и исследуют методы защиты от него. Для этого используются специализированные инструменты и среды разработки.

Студенты получают задание анализировать конкретную вредоносную программу, предоставленную преподавателем. Они проводят исследование структуры программы, изучают используемые алгоритмы и выявляют скрытые функции, такие как сбор информации о пользователях или уязвимости в системе. Затем студенты разрабатывают контрмеры для предотвращения атак и создают отчет о своих находках и рекомендациях.

В третьем разделе для практического применения полученных знаний и навыков студенты участвуют в соревнованиях Capture The Flag (CTF).

CTF - это соревновательная платформа, где команды соревнуются в решении задач по кибербезопасности, включая анализ вредоносных программ, поиск уязвимостей и защиту системы. Это позволяет студентам применять свои знания на практике и развивать командную работу.

Студенты формируют команды и принимают участие в онлайн-соревновании CTF. Им предлагаются различные задачи, от анализа вредоносных программ до решения криптографических головоломок. Студенты соревнуются в решении задач и получают баллы за каждое успешное решение. Победитель определяется по общему количеству набранных баллов.

Наконец-то в последнем разделе после соревнования CTF студенты проводят групповое обсуждение, где каждая команда представляет свои находки и рассказывает о своем опыте. Они обсуждают сложности, с которыми столкнулись, и делятся своими стратегиями решения задач.

Преподаватель проводит анализ результатов и обсуждает с командами возможные улучшения в области кибербезопасности.

Преимущества методики.

✓ Методика акцентирует внимание на практическом обучении, что помогает студентам развить реальные навыки в области кибербезопасности.

✓ Участие в реверсивном инжиниринге позволяет студентам мыслить, как хакеры, что помогает им лучше понимать уязвимости и находить эффективные методы защиты.

✓ Участие в соревнованиях CTF стимулирует студентов к активной работе, развивает командную работу и способствует повышению мотивации.

✓ Методика предлагает использование современных инструментов и технологий, которые актуальны в индустрии кибербезопасности.

✓ Групповые обсуждения и анализ результатов способствуют обмену опытом между студентами и преподавателем, а также развитию коллаборации в области кибербезопасности.

Эта методика преподавания позволяет студентам активно участвовать в процессе обучения, развивать реальные навыки и мышление хакера, а также применять полученные знания на практике через участие в соревнованиях CTF. Она способствует формированию компетентных специалистов в области кибербезопасности, готовых к решению сложных задач и защите информационных систем.

Заключение: Прогрессивные подходы к обучению студентов в области кибербезопасности через факультативные занятия предоставляют студентам возможность развития практических навыков, критического мышления и самостоятельности. Они позволяют более эффективно подготовить специалистов, способных эффективно бороться с киберугрозами и защищать информационные системы. Дальнейшее развитие и применение таких подходов в образовательных учреждениях будет способствовать повышению уровня кибербезопасности и обеспечению безопасной цифровой среды для всех пользователей.

Список литературы:

1. Ganiyeva Shakhrizod Nurmakhamadovna. (2023). PROSPECTS FOR MODERNIZING EDUCATIONAL PROCESSES USING INTERACTIVE METHODS OF BLENDED LEARNING. JournalNX - A Multidisciplinary Peer Reviewed Journal, 9(11), 57–62.

2. Mirzayev, J. (2023). TA'LIM SIFATINI OSHIRISHDA ELEKTRON MULTIMEDIYALI RESURLAR AHAMIYATI. Engineering problems and innovations.
3. Хусанова, М., & Рахматов, Р. (2023, October). ИССЛЕДОВАНИЕ ПРОТОКОЛОВ МОНИТОРИНГА И ОБНАРУЖЕНИЯ МОБИЛЬНЫХ УГРОЗ. In Conference on Digital Innovation:" Modern Problems and Solutions".
4. Мирзаев, Ж., Умаров, А., & Худайназаров, У. (2023, October). KIBERXAVFSIZLIK ASOSLARI FANINI O'QITISHDA VR (VIRTUAL REALLIK) ASOSIDA ISHLOVCHI DASTURDAN FOYDALANISH METODIKASI. In Conference on Digital Innovation:" Modern Problems and Solutions".
5. Raxmatov, R. (2023). ELEKTR ENERGIYASINI SAQLASHDA MEXANIK USULLARDAN FOYDALANISH. Engineering problems and innovations, 113-114.
6. Boymurodovich, M. J. (2021). MASOFAVIY TA'LIMNI RIVOJLANTIRISHDA COURSELAB DASTURI ASOSIDA ELEKTRON O 'QUV RESURSLARINI YARATISH TEXNOLOGIYASI. FAN, TA'LIM VA AMALIYOTNING INTEGRASIYASI, 2(4), 90-100.