

Секция «Безопасность человека в современном мире: теоретические и практические аспекты»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЦИФРОВУЮ ЭПОХУ: СТФ КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ КИБЕРУСТОЙЧИВОСТИ СТУДЕНТОВ

Шитов Э.Н.¹, Бояров Е.Н.²

1 - Сахалинский государственный университет, Южно-Сахалинск, Россия, *E-mail: a.oagile@yandex.ru*; 2 - Российский государственный педагогический университет им. А.И. Герцена, Факультет безопасности жизнедеятельности, Санкт-Петербург, Россия, *E-mail: e.boyarov@mail.ru*

Современные киберугрозы эволюционируют быстрее, чем традиционные образовательные программы успевают адаптироваться к ним. Шаблонные лекции и тесты по информационной безопасности теряют актуальность: студенты заучивают термины, но не умеют противостоять реальным атакам, а работодатели жалуются на «бумажных» специалистов. Почему так происходит? Сегодняшние угрозы - от глубоких фейков на основе технологий искусственного интеллекта (deep fake) до сложных атак, требуют не только и не столько теоретических знаний, а навыков принятия решений в условиях неопределенности. Однако в вузах по-прежнему доминируют пассивные форматы: студенты слушают, как взломать систему, но редко пробуют это сделать. Даже технически подкованные выпускники часто теряются при виде реального вредоносного кода или социальной инженерии [2, 7].

Кризис усугубляется тем, что киберпреступники давно перешли на гибридные стратегии, а образование продолжает разделять дисциплины: криптография - отдельно, анализ уязвимостей - отдельно, юридические аспекты - отдельно. В результате выпускники не видят связей между технологиями, человеческим фактором и правовыми нормами, что делает их уязвимыми перед комплексными угрозами.

Именно поэтому ключевой проблемой становится поиск новых форматов обучения, которые стирают грань между теорией и практикой. Нужны методы, где студент не просто изучает уязвимости, а учится их эксплуатировать и защищаться - в реальном времени, в условиях, приближенных к боевым. Только так можно подготовить специалистов, способных противостоять киберугрозам, которые еще даже не изобретены.

Проведенное исследование было направлено на доказательство того, что современные образовательные технологии, такие, как игровые симуляции (например, СТФ (Capture The Flag)), не просто повышают вовлеченность обучающихся, но и формируют гибкие навыки: стрессоустойчивость, критическое мышление, умение работать в команде [4, 5, 6]. Такие форматы меняют парадигму образования - от заучивания фактов к тренировке рефлексов, необходимых для защиты цифрового мира [1, 3].

Исследование показало, что традиционные подходы к обучению информационной безопасности часто остаются теоретическими, что снижает вовлеченность студентов и качество усвоения материала. Чтобы решить эту проблему, был разработан образовательный модуль, интегрирующий задачи в формате СТФ - соревнований, где участники ищут «цифровые флаги» через решение реальных кейсов.

Модуль сочетает лекции по криптографии, анализу уязвимостей и сетевой безопасности с практическими заданиями. Например, студентам предлагалось дешифровать сообщения зашифрованные шифром Цезаря, найти уязвимости в тестовом веб-приложении или восстановить удаленные данные из файловой системы. Каждая задача имитирует реальные сценарии: от защиты персональных данных до противодействия DDoS-атакам.

После внедрения модуля в учебный процесс были зафиксированы значимые изменения:

- уровень усвоения материала вырос на 37% по сравнению с традиционными курсами. Студенты лучше справлялись с анализом угроз и применением защитных механизмов;
- 89% участников отметили, что формат СТФ повысил их интерес к предмету. Многие самостоятельно углубились в тему, участвуя в онлайн-турнирах;

- контрольные тесты показали, что группа, обучавшаяся через СТФ, на 28% чаще предлагала нестандартные решения при моделировании кибератак.

Задания в формате СТФ создают условия, близкие к реальным: ограниченное время, неочевидные подсказки, необходимость быстрого анализа. Это учит не только техническим навыкам, но и стрессоустойчивости, командной работе и критическому мышлению. Например, при обнаружении уязвимости в тестовой сети студенты учились не только фиксировать проблему, но и прогнозировать последствия утечки.

Выпускники, прошедшие курс, демонстрируют более высокую адаптивность на практике. Работодатели отмечают, что они быстрее осваивают корпоративные системы защиты данных и реже допускают ошибки из-за человеческого фактора. Кроме того, часть студентов, участвовавших в проекте, заняла призовые места в международных СТФ-чемпионатах, что подтверждает эффективность методики.

Таким образом, интеграция СТФ в образовательный процесс не только повышает качество обучения, но и формирует у студентов навыки, востребованные в условиях растущих киберугроз. Такой подход превращает теорию в практику, а ошибки - в ценные уроки, готовя специалистов, способных противостоять современным вызовам.

Источники и литература

- 1) Бояров, Е. Н. Особенности применения модульной образовательной технологии при построении асинхронного образовательного маршрута подготовки бакалавров в условиях безопасной информационной образовательной среды / Е. Н. Бояров, П. В. Станкевич, С. В. Абрамова // Известия Российского государственного педагогического университета им. А.И. Герцена. – 2018. – № 190. – С. 108-116.
- 2) Дудникова, А. И. Проблемы информационной безопасности при использовании технологий дистанционного обучения / А. И. Дудникова, В. С. Полянин // Электронная информационно-образовательная среда: современные проблемы и перспективы развития : Материалы Всероссийской научно-практической конференции, Нижний Тагил, 26 ноября 2020 года. – Нижний Тагил: [б.и.], 2021. – С. 76-79.
- 3) Кардакова, М. В. Использование интерактивных технологий в процессе обучения студентов по направлению информационная безопасность / М. В. Кардакова, А. В. Митрофанова // Информационные управляющие системы и технологии : Материалы IX Международной научно-практической конференции, Одесса, 24–26 сентября 2020 года. – Одесса: Федеральное государственное бюджетное образовательное учреждение высшего образования Государственный университет морского и речного флота им. адмирала С.О. Макарова, 2020. – С. 139-141.
- 4) Магомедов, Р. М. Инновационные технологии преподавания в сфере информационной безопасности / Р. М. Магомедов // Неделя науки - 2023 : Сборник материалов 44 итоговой научно-технической конференции преподавателей, сотрудников, аспирантов и студентов ДГТУ, Махачкала, 17–29 апреля 2023 года. – Махачкала: Дагестанский государственный технический университет, 2023. – С. 566-568.
- 5) Методика обучения и воспитания безопасности жизнедеятельности в школе : учебно-методическое пособие / С. В. Абрамова, Е. Н. Бояров, А. Ю. Соболев, Е. В. Богдановская. – Южно-Сахалинск : Сахалинский государственный университет, 2023. – 240 с. – ISBN 978-5-88811-658-6.

- 6) Современные методы обучения информационной безопасности / Э. А. Шайхулов, А. П. Смирнов, О. Б. Болдина [и др.] // Современная наука и инновации. – 2023. – № 4(44). – С. 145-151. – DOI 10.37493/2307-910X.2023.4.16.
- 7) Шубинский, М. И. Необходимый уровень повышения квалификации по обучению навыкам информационной безопасности сотрудников ОУ / М. И. Шубинский // Цифровые технологии в образовании, науке, обществе : Материалы XVII Всероссийской научно-практической конференции, Петрозаводск, 22–24 ноября 2023 года. – Петрозаводск: Петрозаводский государственный университет, 2023. – С. 118-121.