

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ В УЧРЕЖДЕНИЯХ ВОЕННОГО ОБРАЗОВАНИЯ

Юнчиц Е.И., Пилипенко А.О., Игнатенко А.А.

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, egorynchic2007@gmail.com

Abstract. The paper analyzes current problems of training cybersecurity specialists in military higher education institutions. Five interrelated directions of modernization are considered: transition from classical programming training to training operators of artificial intelligence tools, systematic practice outside the educational institution, crediting the results of cybersecurity competitions within the curriculum, integration of students into the professional information community, and detailed analysis of real cyber incidents following the full cycle of reconnaissance, attack, defense and consequences. Implementation of these directions allows bringing military education closer to the requirements of modern cyber confrontation while preserving the systematic nature of state educational standards.

Государственный образовательный стандарт обеспечивает надежный фундамент подготовки, который целесообразно дополнить актуальными практиками для полного соответствия динамике современных киберугроз. В статье рассматриваются несколько направлений интеграции передового опыта в учебный процесс без нарушения системности базовой программы.

Традиционная модель подготовки опирается на фундаментальные дисциплины: программирование, архитектуру вычислительных систем, основы сетей и криптографии. Эта база сохраняет значение, однако она уже не исчерпывает содержание профессии. Современные атаки всё в большей степени генерируются нейросетевыми инструментами: автоматически создаются убедительные фишинговые сообщения, синтезируются поддельные аудио- и видеоматериалы, формируются полиморфные вредоносные образцы, автоматизируется поиск уязвимостей [1, 2]. Деятельность защитника соответственно приобретает характер управления искусственным интеллектом: анализ потока событий обрабатывается также и интеллектуальным агентом, а человек ставит им задачи, проверяет корректность выдаваемых результатов и принимает решения на их основе. Отсюда новые требования к подготовке: навыки постановки задач для моделей (промпт-инжиниринг), понимание принципов и границ применимости машинного обучения, умение вскрывать сгенерированный противником контент. Важно подчеркнуть, что операторская модель не отменяет фундаментальной подготовки: обоснованно доверять или не доверять результату модели способен лишь специалист, свободно владеющий классическими основами дисциплины.

Образовательный процесс запаздывает с реакцией: искусственный интеллект чаще рассматривается как объект изучения отдельных курсов, а не как полноценный субъект кибервойны, действующий и на стороне атакующего, и на стороне защитника. Усугубляет проблему скептицизм части преподавательского состава: опасения академической недобросовестности обучающихся и недоверие к результатам моделей приводят к запретам вместо обучения грамотному и контролируруемому применению инструментов. Разрешается противоречие последова-

тельной интеграцией ИИ в учебный процесс: введением дисциплин об основах машинного обучения и противоборстве в интеллектуальной среде, включением заданий, предполагающих работу с ИИ-ассистентами и обязательную верификацию их результатов, а также чёткой регламентацией допустимого использования таких инструментов.

Также необходимо поднять тему практики за пределами учебного заведения. Лабораторные стенды образовательной организации, даже самые современные, воспроизводят реальную инфраструктуру лишь частично: они лишены производственного масштаба, действующих регламентов и живого противодействия. Поэтому значимой составляющей подготовки должна стать систематическая практика в органах и организациях, непосредственно осуществляющих деятельность по обеспечению информационной безопасности: подразделениях мониторинга и реагирования на инциденты, испытательных лабораториях, эксплуатирующих организациях. Стажировки дают курсантам знакомство с находящимися в эксплуатации новейшими программно-аппаратными комплексами, реальными технологическими процессами и служебной документацией, а также опыт работы в коллективе.

Необходимым условием является регулярное повышение квалификации и преподавательского состава. Организационными механизмами выступают долгосрочные соглашения о сотрудничестве, совместные учебные центры, взаимные стажировки и привлечение практикующих специалистов к проведению отдельных занятий. Особенности военного образования – режимные ограничения и требования защиты информации – не отменяют, а уточняют эти формы: они реализуются на обезличенных материалах, типовых стендах и неконфиденциальных фрагментах процессов. Целесообразно также чередовать типы практики: краткосрочные ознакомительные стажировки на младших курсах и продолжительное участие в производственных процессах на старших, когда обучающийся уже владеет базовыми навыками. Эффективной формой является и совместное участие обучающихся и преподавателей в одних и тех же мероприятиях по повышению квалификации: общее актуальное поле знаний существенно упрощает последующую аудиторную работу.

Государственный учебный план обеспечивает системность, полноту и законность подготовки, однако его содержание обновляется медленнее, чем меняется практика противоборства. При этом значительная часть актуальных знаний и умений, востребованных в кибербезопасности, формируется вне аудиторных занятий – прежде всего в ходе соревнований формата capture the flag, олимпиад и турниров по информационной безопасности [3]. Немалая часть обучающихся участвует в таких мероприятиях самостоятельно, однако подавляющее большинство выпускается без подобного опыта: участие не поддержано учебным планом ни организационно, ни мотивационно.

Разрешение противоречия видится в дополнении государственного учебного плана механизмами зачёта знаний, полученных в турнирной деятельности: признание результатов выступлений основанием для поощрения и учёта при промежуточной аттестации, введение внутривузовских турниров с закреплённой учебной нагрузкой, формирование и планомерная подготовка сборных команд учреждения. Это переводит стихийное участие в соревнованиях в управляемый образовательный процесс, охватывает им большинство обучающихся и создаёт устойчивую мотивацию к повышению уровня подготовки: соревновательная деятельность становится признаваемой и поддерживаемой учреждением образования траекторией развития, а не личной инициативой отдельных курсантов. Учёт турнирной активности может также использоваться при определении индивидуальных траекторий подготовки и назначении поощрений. При этом зачёт не должен носить формального характера: результат турнира признаётся в той мере, в какой он подтверждает освоение соответствующих разделов программы, а личный вклад обучающегося проверяется в ходе защитного собеседования. Такой подход исключает замещение учебной деятельности соревновательной и сохраняет за учебным планом роль системообразующего документа.

Академическая база формирует фундамент профессии, но не обеспечивает постоянного присутствия в живом профессиональном контексте. Отрасль развивается настолько быстро, что свежие техники атак и защиты обсуждаются в профессиональных сообществах задолго до того, как попадают в официальные методические издания. Выпускник, не включённый в это информационное поле, остаётся в информационном вакууме: его знания соответствуют моменту поступления, а не моменту выпуска.

Проблема усугубляется тем, что часть актуальных знаний в принципе не успевает пройти полный цикл методической переработки: от появления новой техники атаки до её описания в утверждённом пособии проходят годы.

Задача учреждения образования – сделать вовлечение в профессиональное сообщество системным: рекомендовать проверенные каналы и источники актуальной информации, организовывать участие обучающихся в профильных конференциях и

встречах, обеспечивать плотное взаимодействие с опытными специалистами – от приглашённых экспертов до наставников из числа выпускников. Отдельного внимания требует культура информационной безопасности самого общения: курсанты должны усвоить правила поведения в профессиональных чатах и каналах, границы допустимого обсуждения и требования по защите сведений. Поскольку не вся информация в открытых сообществах достоверна, отдельной задачей становится обучение критической оценке источников и перепроверке сведений.

Изучение теоретических моделей угроз формирует понятийный аппарат, но само по себе не создаёт системного мышления. Абстрактные примеры вида «атакующий эксплуатирует уязвимость» скрывают причинно-следственные связи реального инцидента: почему результаты разведки оказались успешными, какие тактические ошибки допустила защита, как развивались последствия. В результате обучающийся знает отдельные приёмы, но не понимает логику противоборства как целого и не умеет выделять узлы, в которых исход противостояния мог быть изменён. Учебный план целесообразно расширить детальным разбором состоявшихся киберинцидентов по полному циклу «разведка – атака – защита – последствия». Методически это реализуется как поэтапное воспроизведение инцидента на учебном стенде: курсанты последовательно проходят путь атакующего, анализируют решения защитников на каждом этапе, фиксируют допущенные ошибки и оценивают итоговые последствия, после чего формулируют, какие организационные и технические меры могли бы изменить исход. Источниками материала служат обезличенные отчёты о реально произошедших инцидентах и сводные исследования угроз [1].

Такая работа развивает навыки чтения первичной информации, критического анализа и принятия решений в условиях неполных данных. Формой итогового контроля по теме может служить командный разбор инцидента с защитой предложенных мер перед преподавателем и товарищами.

Предложенные меры позволяют гармонично объединить прочность академической базы с гибкостью реальных профессиональных требований. Такой синтез гарантирует выпускникам высокую конкурентоспособность и готовность к решению сложных задач в сфере национальной безопасности.

Литература

1. ENISA Threat Landscape 2023 [Электронный ресурс] // ENISA. – Режим доступа: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>. – Дата доступа: 07.09.2026.
2. MITRE ATLAS: Adversarial Threat Landscape for Artificial Intelligence Systems [Электронный ресурс] // MITRE. – Режим доступа: <https://atlas.mitre.org/>. – Дата доступа: 07.09.2026.
3. Werther J., Zhivich M., Lekakis T., Zeldovich N. Experiences Teaching Security Using CTF Competitions // login: – 2011. – Vol. 36, № 3.