А. Г. Уймин[1], В. С. Греков[1]

[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация

ОПЫТ ПРЕПОДАВАНИЯ ПРОДУКТОВЫХ КУРСОВ SIEM И NAD В ЛОГИКЕ ИНТЕГРИРОВАННОЙ ПРОФОРИЕНТАЦИИ: ОТ ПЕРВОГО КУРСА СПЕЦИАЛИТЕТА К СЕРТИФИКАЦИИ ВЫПУСКНИКОВ УКРУПНЁННОЙ ГРУППЫ 10.00.00

Аннотация. В статье представлен опыт реализации продуктовых курсов вендора Positive Technologies — PT-SIEM-CS (Certified Specialist по MaxPatrol SIEM) и PT-NAD-CS (Certified Specialist по PT Network Attack Discovery) — в образовательной траектории высшего образования, охватывающей два сечения подготовки: первый курс специалитета по направлениям укрупнённой группы 10.00.00 «Информационная безопасность» в рамках профильного (специального) предмета и старшие курсы (4–5) того же специалитета в рамках дисциплин «Безопасность сетей ЭВМ» и «Безопасность информационно-аналитических систем». Раскрыта педагогическая логика выведения студентов первого курса специалитета на независимую вендорскую сертификацию: эта практика рассмотрена как элемент интегрированной профориентации, обеспечивающий ранний и предметно-укоренённый контакт обучающегося с реальной профессиональной деятельностью, формирование мотивационно-ценностного и когнитивного компонентов профессиональной компетенции и закрепление выбора профессии через успех в нормативно признанной процедуре оценки. Подробно описаны педагогические технологии профориентации, использованные в учебном процессе: профессиональные пробы, контекстное обучение, кейс-метод, проектная технология, технология учебной симуляции на промышленном полигоне, технология наставничества, портфолио-технология и технология рефлексивной фиксации. Описаны содержательные и процессуальные условия реализации: интеграция вендорских материалов портала Positive Technologies, открытых данных Palo Alto, ресурса malware-traffic-analysis.net, вендоронезависимых фреймворков Sigma и Suricata, развёртывание лабораторной инфраструктуры на базе Яндекс Облака. Приведены количественные результаты: для блока SIEM из 14 студентов курс успешно завершили 11, для блока NAD все 29 студентов, приступивших к работе, успешно прошли курс и сертификацию с прокторингом. Показано, что интегрированная профориентация, опирающаяся на ранний выход на сертификацию, согласуется с положениями отечественной школы профессиональной педагогики (С. Я. Батышев, А. М. Новиков, В. С. Леднев, Т. Ю. Ломакина, А. А. Вербицкий, Е. А. Климов, Э. Ф. Зеер) и поддерживается современными зарубежными исследованиями.

Ключевые слова: профессиональная компетенция, высшее образование, информационная безопасность, профориентация, сертификация, контекстное обучение, SIEM/NAD.

Введение

Подготовка специалистов в области информационной безопасности относится к числу образовательных направлений, где разрыв между темпом развития профессиональной сферы и темпом обновления нормативно закреплённого содержания обучения проявляется особенно остро. Образовательные организации высшего образования сталкиваются с противоречием: ФГОС высшего образования по направлениям укрупнённой группы 10.00.00 «Информационная безопасность» формулируют требования к результатам подготовки на уровне видов профессиональной деятельности и универсальных, общепрофессиональных и профессиональных компетенций, тогда как реальная практика работодателей и профессиональные стандарты в области информационной безопасности предъявляют к выпускнику конкретные трудовые функции, соотносимые с владением промышленными платформами класса SIEM (Security Information and Event Management) и NTA/NDR (Network Traffic Analysis / Network Detection and Response). Между этими двумя нормативно-деятельностными плоскостями располагается зона, в которой образовательная организация обязана самостоятельно выстраивать содержание, средства и процессуальную развёртку подготовки.

Одним из инструментов снятия указанного противоречия является интеграция вендорских продуктовых курсов в учебный процесс с выходом обучающегося на независимую сертификацию. Подобная практика реализуется авторами на двух сечениях образовательной траектории высшего образования: на первом курсе специалитета по направлениям укрупнённой группы 10.00.00 в рамках профильного (специального) предмета и на старших курсах (4–5) того же специалитета в рамках дисциплин «Безопасность сетей ЭВМ» и «Безопасность информационно-аналитических систем». Цель настоящей статьи — обобщить опыт преподавания продуктовых курсов PT-SIEM-CS и PT-NAD-CS, теоретически обосновать раннее (первый

курс специалитета) выведение обучающегося на сертификационную процедуру как элемент интегрированной профориентации, развёрнуто описать педагогические технологии, обеспечивающие эту профориентацию, и сформулировать рекомендации по тиражированию практики.

Актуальность исследования определяется тем, что современная политика подготовки кадров для отраслей цифровой экономики прямо ориентирует образовательные организации высшего образования на сокращение «эффективного срока» вхождения выпускника в профессию, на сближение образовательной и производственной сред, на интеграцию работодателя в проектирование результатов и средств подготовки. В этой логике ранний выход обучающегося на нормативно признанную сертификацию у вендора-работодателя становится не периферийным «бонусом», а ядерным педагогическим средством, обеспечивающим связь между мотивационно-ценностным становлением обучающегося, нормативной картиной квалификаций и реальной профессиональной деятельностью. Особое значение этот тезис приобретает на фоне формирующегося в зарубежной литературе тренда на структурированные точки входа в профессию кибербезопасности через картографирование сертификаций, ролей и компетенций [12], а также на фоне исследований, фиксирующих устойчивую недостаточность кадрового предложения в кибербезопасности и необходимость более ранних и более структурированных карьерных интервенций в системе профессионального образования [13; 14].

В дополнение к этому, в современной образовательной литературе подчёркивается роль профессиональной идентичности обучающегося как ключевого фактора качества подготовки в условиях цифровизации и платформизации учебного процесса [15]. Это означает, что включение продуктового вендорского курса в первый год обучения должно рассматриваться не только как технологическая, но и как идентификационная процедура: обучающийся через работу с реальным промышленным продуктом отвечает себе на вопрос «кем я становлюсь», а не только «что я умею».

Материалы и методы

Исследование выполнено в логике опытно-педагогической работы с элементами педагогического проектирования и обобщения опыта. В работе использованы: анализ нормативной базы (ФГОС ВО по направлениям УГСН 10.00.00); содержательный анализ профессионально-педагогической литературы по проблемам компетентностной подготовки и профессиональной ориентации; анализ зарубежных исследований по проблемам киберобразования, лабораторной подготовки и карьерного консультирования в системе профессионального образования; метод педагогического наблюдения; анализ результатов внешней (вендорской) сертификации обучающихся; обобщение собственного педагогического опыта авторов в части преподавания дисциплин информационной безопасности на двух сечениях траектории высшего образования.

Базой исследования выступили обучающиеся ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», осваивающие программы специалитета по направлениям укрупнённой группы 10.00.00. Учебная нагрузка по продуктовым курсам распределена следующим образом: PT NAD — лабораторные работы 34 часа, семинары 16 часов, лекции 16 часов; MaxPatrol SIEM — лабораторные работы 34 часа, семинары 16 часов, лекции 16 часов. Лабораторная инфраструктура развёрнута на базе сервиса Яндекс Облако в рамках пилотного взаимодействия с вузами; ресурсное обеспечение каждого учебного стенда приведено в таблице 1.

Таблица 1 – Ресурсное обеспечение учебных стендов

Ресурс	ВМ, шт	vCPU, шт	RAM, Гб	HDD, Гб
SIEM	12	12	64	256
АРМ	2	2	4	64
NAD	1	24	72	192

При построении лабораторных работ использовалась технологическая логика обработки трафика в PT NAD: от захвата копии сетевого трафика до обогащения метаданных и работы оператора с ними через интерфейс продукта (рис. 1). Такая схема задавала структуру учебных кейсов и позволяла студентам связывать отдельные операции в единую цепочку расследования инцидента.

Рис. 1. Технологическая схема обработки сетевого трафика в PT NAD (по материалам [34])

Эмпирическую базу составили данные двух учебных циклов: цикла по блоку SIEM (контингент — студенты 5 курса специалитета по направлению «Информационно-аналитические системы безопасности», в рамках дисциплины «Безопасность информационно-аналитических систем», N = 14) и цикла по блоку NAD (контингент — студенты 4 курса специалитета по направлению «Информационная безопасность автоматизированных систем критически важных объектов», в рамках дисциплины «Безопасность сетей ЭВМ», N = 29). Дополнительно использованы данные о выведении на сертификацию обучающихся первого курса специалитета по направлениям УГСН 10.00.00 в рамках профильного предмета.

Теоретико-методологической рамкой обоснования предлагаемой практики выступают положения отечественной школы профессиональной педагогики (С. Я. Батышев, А. М. Новиков, В. С. Леднев, Т. Ю. Ломакина), теории контекстного обучения А. А. Вербицкого, а также классические работы по теории профессиональной ориентации и профессионального становления личности (Е. А. Климов, Э. Ф. Зеер, Н. С. Пряжников, С. Н. Чистякова). На этой рамке выстраивается понимание профессиональной компетенции как интегративного образования, включающего знания, умения, навыки, практический опыт и профессионально значимые личностные качества, и понимание профессиональной ориентации не как разового мероприятия, а как непрерывного, встроенного в основной учебный процесс педагогического сопровождения профессионального самоопределения обучающегося.

Зарубежная рамка исследования опирается на работы, фиксирующие необходимость практико-ориентированного и лабораторно-укоренённого формата киберподготовки [1; 4; 5], значимость явного картирования карьерных траекторий в кибербезопасности, сертификационных шкал как точек входа в профессию и согласования содержания подготовки с отраслевыми профилями [12–14], а также на исследования профессиональной идентичности обучающихся, в которых показано, что устойчивая профессиональная идентичность формируется через включение в подлинную профессиональную практику, а не через её имитации [15; 16].

Теоретическое обоснование

В центре предлагаемой модели — тезис о том, что выведение обучающегося первого курса специалитета на независимую вендорскую сертификацию в рамках профильного предмета является не «опережающим обучением» в его узко-академическом значении, а элементом интегрированной профориентации. Под интегрированной профориентацией в настоящей работе понимается такая организация образовательного процесса, при которой профориентационные задачи решаются не вне учебных дисциплин (через тестирования, экскурсии, агитационные мероприятия), а внутри них — через содержание, средства и процессуальную развёртку самой профессиональной подготовки. При этом сертификация трактуется как педагогическая

проба профессиональной деятельности — оформленное в нормативной процедуре столкновение обучающегося с предметом и инструментами будущей профессии.

Такое понимание опирается на ряд принципиальных положений отечественной педагогики.

Во-первых, на положение А. М. Новикова о принципе учения как осознанной деятельности: «Принцип учения как осознанной деятельности — это осознанность учеником, студентом всех компонентов учебной деятельности: осознание её предмета, средств, способов, своих действий, своих личностных качеств, проявляющихся в учебной деятельности, осознание своей роли в коллективной учебной деятельности». В ситуации, когда обучающийся первого курса с первых месяцев работает с реальной промышленной системой SIEM или NAD, разворачивает её, конфигурирует сбор событий и проходит сертификационное тестирование с прокторингом, перечисленные А. М. Новиковым компоненты учебной деятельности перестают быть абстрактной перспективой и оформляются в наблюдаемой профессиональной пробе. Учебная деятельность приобретает «второй слой» — она одновременно является деятельностью учебной и квазипрофессиональной.

Во-вторых, на ключевое для школы С. Я. Батышева положение о соединении обучения с производительным трудом. С. Я. Батышев писал: «Подготовка квалифицированных рабочих немыслима без соединения обучения с производительным трудом, без активного участия учащихся в создании материальных ценностей в процессе обучения». В подготовке специалистов информационной безопасности в высшей школе функционально-эквивалентным «производительному труду» оказывается работа обучающегося с промышленным программным обеспечением вендора в рамках лабораторного полигона: студент производит не «материальный продукт» в индустриальном смысле, а реальный результат профессиональной деятельности аналитика — правило корреляции, отчёт об инциденте, заключение о вредоносном трафике. Сертификация фиксирует факт такой работы в нормативно признанной форме. Этот же тезис в современной транскрипции подтверждается зарубежными исследованиями практической лабораторной подготовки в кибербезопасности, где показано, что наиболее устойчивые компетенции формируются не на лекционных занятиях, а в условиях работы с реальными сценариями атак и защиты [4; 5].

В-третьих, на положение В. С. Леднева о структуре содержания образования и о необходимости включения в содержание образовательного процесса всех существенных видов деятельности, типичных для соответствующей области профессиональной практики. Согласно В. С. Ледневу, содержание образования включает не только систему знаний, но и опыт осуществления способов деятельности, опыт творческой деятельности и опыт эмоционально-ценностного отношения к действительности. Сертификационный экзамен с прокторингом задействует все четыре компонента: знаниевый (теоретическая часть), деятельностный (практическая часть), творческий (нестандартные кейсы, отклонения от типового сценария) и эмоционально-ценностный (стрессовое испытание, требующее принятия профессиональной ответственности за результат).

В-четвёртых, на положение Т. Ю. Ломакиной о непрерывности профессионального образования. Т. Ю. Ломакина определяет непрерывное профессиональное образование как «процесс целостный, состоящий из последовательно следующих друг за другом и преемственно связанных ступеней специально организованной учёбы». Раннее выведение студентов первого курса специалитета на ту же сертификацию, на которую выходят студенты 4–5 курсов, и есть способ обеспечить продольную связность образовательной траектории внутри высшего образования: одна и та же нормативная точка фиксируется в двух разных пунктах траектории, что превращает её из локального события в опору профессионального становления.

В-пятых, на положения теории контекстного обучения А. А. Вербицкого. А. А. Вербицкий определяет контекстное обучение следующим образом: «Контекстным является такое обучение, в котором с помощью всей системы дидактических форм, методов и средств моделируется предметное и социальное содержание будущей профессиональной деятельности специалиста, а усвоение им абстрактных знаний как знаковых систем наложено на канву этой

деятельности». Лабораторный полигон SIEM/NAD на промышленном вендорском продукте — практически образцовая иллюстрация контекстного обучения: в нём моделируются и предметное содержание (реальная инфраструктура, реальные события, реальные атаки), и социальное содержание (роль аналитика, регламент работы дежурной смены, регламент эскалации инцидента, нормативная процедура сертификации). На первом курсе специалитета такое контекстное обучение играет роль «педагогической точки входа» в профессию.

В-шестых, на положения теории профессионального самоопределения. Е. А. Климов подчёркивает, что профессиональное самоопределение представляет собой длительный процесс согласования личностных потребностей обучающегося с требованиями избранной профессиональной деятельности и осуществляется через систему профессиональных проб. В этой логике сертификационный экзамен у вендора — практически идеальная профессиональная проба: процедура нормативна, оценка независима, результат значим за пределами учебного заведения, кейс соответствует реальной профессиональной задаче. Э. Ф. Зеер развивает этот тезис в логике профессионального становления: «Профессиональное становление — это формообразование личности, адекватное требованиям профессиональной деятельности». Иначе говоря, профессиональное становление невозможно без столкновения с самой профессиональной деятельностью, и чем раньше такое столкновение оформляется в педагогически организованной и социально признанной форме, тем устойчивее результат. С. Н. Чистякова, развивая теорию профессиональных проб в отечественной педагогике, прямо указывает: «Профессиональная проба — это профессиональное испытание, моделирующее элементы конкретного вида профессиональной деятельности, имеющее завершённый вид, способствующее сознательному, обоснованному выбору профессии». Сертификация по продукту, признанная вендором, отвечает всем перечисленным признакам.

Наконец, важно специально остановиться на сопоставлении профессиональной ориентации в её традиционном и интегрированном понимании. Н. С. Пряжников указывает, что профориентация представляет собой «систему мер, направленных на оказание помощи человеку в выборе профессии в соответствии с его способностями, склонностями и потребностями рынка труда». В традиционной практике эти меры реализуются как набор разрозненных мероприятий, организационно отделённых от учебного процесса (профориентационные тестирования, экскурсии, дни открытых дверей, встречи со специалистами). Интегрированная профориентация, в отличие от традиционной, размещает соответствующие меры внутри учебных дисциплин и пользуется их собственным дидактическим аппаратом. На первом курсе высшей школы, где обучающийся ещё проходит этап адаптации к выбранной специальности и часто колеблется в обоснованности своего выбора, такая интеграция оказывается особенно эффективной. Эта позиция согласуется с международными исследованиями карьерного консультирования, показывающими, что наиболее результативные карьерные интервенции — это те, которые интегрированы в основное содержание профессиональной подготовки [7; 10].

Педагогические технологии профориентации, применяемые в продуктовом курсе на первом курсе специалитета

Поскольку основная новизна описываемой практики состоит не в самом факте сертификации, а в способе её педагогической включённости в учебный процесс первого курса, центральным узлом статьи является развёрнутое описание используемых педагогических технологий профориентации. Технологии описаны в той последовательности, в которой они разворачиваются в учебном цикле.

1. Технология профессиональной пробы. Базовая, замыкающая технология всего курса. Понятие профессиональной пробы введено в отечественную педагогику С. Н. Чистяковой как испытание, моделирующее элементы конкретной профессиональной деятельности и завершающееся продуктом, который можно вынести и обсудить. В описываемом курсе пробы строятся по трёхтактному циклу: проба «по образцу» (студент повторяет действия преподавателя на учебном стенде), проба «по аналогии» (студент решает задачу из другого, но методически родственного сценария), проба «творческая» (студент действует в условиях изменённого/неполного входа). Финальной профессиональной пробой выступает сам сертификационный

экзамен с прокторингом: для первого курса это первое в их жизни профессиональное испытание, признанное за пределами образовательной организации.

2. Технология контекстного обучения по А. А. Вербицкому. На занятиях моделируется не учебная, а квазипрофессиональная ситуация: первокурсник работает не «над лабораторной работой», а в роли «младшего аналитика SOC», получает не «задание», а «инцидент с тикетом», оформляет не «отчёт по лабораторной», а «карточку инцидента». На лекциях вводятся понятия и нормативные рамки, но они немедленно «опрокидываются» в практику — в учебно-профессиональную задачу, выполняемую на промышленном полигоне. По А. А. Вербицкому, такая дидактическая конструкция обеспечивает переход от учебной деятельности академического типа к квазипрофессиональной и далее — к собственно профессиональной деятельности.

3. Кейс-метод (case study). Каждая лабораторная работа собрана как кейс — нарратив, описывающий конкретный инцидент или конкретное состояние инфраструктуры (с источником данных, со временем, с контекстом). Студент первого курса не «изучает интерфейс», а расследует инцидент. Кейсы построены на трёх типах источников: тренировочные кейсы вендора (Positive Technologies), открытые исследования Palo Alto Networks (отчёты об APT-кампаниях), публичные дампы malware-traffic-analysis.net. Кейс-метод в применении к продуктовому курсу решает важную профориентационную задачу: с первых занятий студент видит свою профессию «изнутри», как последовательность сделанных аналитиком решений, а не как набор книжных глав.

4. Проектная технология. Поверх кейсов разворачивается мини-проект: студент (или малая группа) принимает «инфраструктуру условного заказчика», ставит SIEM/NAD, обосновывает выбор источников, формирует базовый набор правил корреляции, готовит итоговый отчёт. Проект — это интегральный продукт курса, в котором сходятся знания, умения и навыки. Сертификация в конце цикла валидирует индивидуальный уровень обучающегося, а проект — его способность складывать частные действия в целое решение.

5. Технология учебной симуляции на промышленном полигоне. Существенный элемент дидактической архитектуры — отказ от «учебных аналогов» в пользу промышленного ПО, развёрнутого в облачной среде. Студент первого курса работает не с упрощённой моделью, а с тем же продуктом, который установлен в коммерческих SOC. Симуляция при этом сохраняется на уровне инфраструктуры (учебный сегмент, генератор событий, контролируемые цели), но не на уровне инструмента. Эта технология решает профориентационную задачу: исключает у обучающегося иллюзию «учебности» и переносит его в реальную предметную область с первых занятий.

6. Технология наставничества и сопровождения (mentoring). Курс ведут преподаватели, имеющие действующий или недавний опыт работы в индустрии. Их роль в первом курсе — не столько «лектор», сколько наставник, демонстрирующий профессию через собственное профессиональное поведение: как читает события, как ставит гипотезу, как сомневается, как ищет источник, как фиксирует вывод. Эта технология опирается на положение А. М. Новикова о роли личностного образца в профессиональном становлении и на международные исследования наставничества в киберобразовании, фиксирующие наставничество как один из ключевых факторов закрепления студента в профессии [5].

7. Портфолио-технология. Каждый студент с первого курса ведёт профессиональное портфолио, в которое последовательно собираются: сданные кейсы, выполненный проект, сертификат вендора, рефлексивные записи по итогам каждого блока. Портфолио формируется не как «бюрократический архив», а как «доказательная история профессионального становления»: в конце первого курса студент имеет внешне валидируемое подтверждение своего входа в профессию. Эта технология напрямую решает мотивационно-ценностную задачу профориентации.

8. Технология рефлексивной фиксации. По завершении каждого крупного блока обучающемуся предлагается короткая рефлексивная процедура: «что я сейчас узнал о профессии, что я узнал о себе как о будущем профессионале, какие сомнения у меня возникли, какой

следующий шаг». Рефлексия проводится не в форме «эссе ради эссе», а как педагогический инструмент управления профессиональным самоопределением. С позиции Э. Ф. Зеера рефлексия — необходимый компонент профессионального становления; без неё профессиональная проба теряет свой ориентационный смысл.

9. Технология ранней погружённой стажировки (соглашения с индустрией). В рамках курса первого года предусмотрены договорные встречи с действующими аналитиками SOC, разбор реальных (анонимизированных) инцидентов из практики работодателей, посещение площадок индустриальных партнёров. Эта технология достраивает контекстное обучение «снаружи»: студент первого курса встречает не только своего преподавателя, но и взрослого профессионала «в роли», что усиливает профессиональную идентификацию.

10. Технология независимой сертификации как венца цикла. Сертификация PT-NAD-CS / PT-SIEM-CS в конце цикла собирает все предыдущие технологии в один нормативный результат. Это не «контрольная работа», а первое профессиональное испытание обучающегося. Именно соединение перечисленных технологий с этим венцом и составляет содержание термина «интегрированная профориентация» в авторской трактовке.

Все десять технологий применяются не последовательно, а параллельно: курс собран как сеть технологий, каждая из которых вытягивает свою грань профессионального становления — мотивационную, когнитивную, деятельностную, рефлексивную и идентификационную.

Содержание и реализация продуктовых курсов

Содержательное ядро обоих продуктовых курсов сформировано на основе материалов портала обучения Positive Technologies. Курс по MaxPatrol SIEM раскрывает архитектуру современной SIEM-системы, управление активами и уязвимостями, управление журналами (сбор событий из источников, таксономия событий, потоки данных), работу с базой событий, создание дашбордов и отчётов, управление инцидентами и уведомлениями, мониторинг источников. Курс по PT Network Attack Discovery раскрывает технологии сетевой разведки и первоначального доступа, методы выполнения и закрепления в системе, повышения привилегий, предотвращения обнаружения, получения учётных данных, перемещения внутри периметра, эксфильтрации данных. Содержание курсов спроектировано в логике матрицы MITRE ATT&CK, что обеспечивает педагогическую прозрачность связки «учебная задача — реальный тактико-технический приём злоумышленника — средство обнаружения». Использование MITRE ATT&CK как педагогической метаструктуры согласуется с современными исследованиями применения этого фреймворка для смягчения киберугроз и систематизации учебных программ [3].

Для лабораторных работ по NAD дополнительно используются материалы открытых исследований Palo Alto Networks и публичный набор сетевых дампов с сайта malware-traffic-analysis.net. Это позволило сформировать учебно-профессиональные задачи на анализе реальных индикаторов компрометации, выявлении вредоносного трафика и расследовании инцидентов информационной безопасности с использованием языка Suricata. Такой подход соответствует современным методикам анализа сетевого трафика, основанным на обнаружении вторжений и тонкой обработке признаков [2]. Для лабораторных работ по SIEM в перспективе планируется внедрение вендоронезависимого фреймворка Sigma для написания правил корреляции и использование событий, предоставленных сообществом Security Experts Community (репозиторий open-xp-rules). Сочетание вендорских и открытых средств обеспечивает выполнение требования вариативности средств обучения и не привязывает результат подготовки к конкретному поставщику. Это особенно важно в свете последних работ по масштабированию SIEM-корреляции и снижению среднего времени реакции на инцидент в условиях городских и инфраструктурных систем [6].

Процессуально курс построен в трёхчастной структуре: лекционный блок (16 часов) — семинарский блок (16 часов) — лабораторный блок (34 часа). Лекции вводят понятийный аппарат и нормативно-методические рамки. Семинары обеспечивают переход от теории к инструментарию: разбираются стек протоколов TCP/IP, принципы работы сетевых сканеров (nmap), сканеры безопасности ОС, базовые навыки работы с операционными системами

Windows и Linux на уровне администратора, редактирование конфигурационных файлов и перезапуск служб в Linux, написание регулярных выражений, повышение привилегий в UNIX (sudo/su), настройка syslog. Лабораторные работы организованы вокруг типовых трудовых функций — установка продукта и его архитектура, управление активами и уязвимостями средствами MaxPatrol SIEM, управление журналами, работа с базой событий, база знаний и работа с ложными срабатываниями, создание отчётов, управление инцидентами и уведомлениями, решение проблем и мониторинг источников, сбор журналов и импорт/экспорт активов и событий. Для блока NAD аналогичные лабораторные работы покрывают весь цикл атаки: начальная настройка NAD (базовые и расширенные технологии), контроль попыток первоначального доступа, детектирование повышения привилегий, детектирование использования техник закрепления, детектирование исследования системы, детектирование сканирования сети, детектирование перемещения внутри периметра, инструменты эксфильтрации данных и PT NAD.

Начальный блок лабораторных работ по NAD был связан с установкой и настройкой продукта, включая выбор сетевых интерфейсов для захвата копии сетевого трафика (рис. 2). Такой материал позволял студентам увидеть, что аналитическая работа в NTA/NDR-системе начинается не с интерфейса расследования, а с корректного получения и подготовки сетевых данных.

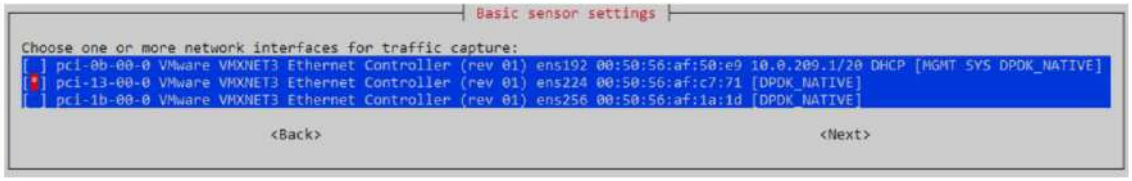

Рис. 2. Выбор интерфейсов для захвата трафика при настройке PT NAD (по материалам [36])

Основной акцент в обучении сделан на подготовке аналитика, а не администратора. Студенты изучают основы установки и настройки систем, однако более глубокий акцент сделан на анализе данных и работе с событиями. Такой подход обусловлен тем, что понимание базовых принципов установки системы является необходимым, но не достаточным условием эффективного анализа и расследования инцидентов; продуктивная деятельность аналитика опирается прежде всего на способность интерпретировать совокупность событий в контексте модели угроз. Современные исследования киберобразования подтверждают этот выбор: устойчивые навыки формируются именно через работу с реальными или приближёнными к реальным наборами данных и сценариев [4; 5].

Сопоставление учебных действий с разделами продукта и методическими материалами PT NAD представлено в таблице 2. Эта таблица была добавлена в статью как связующее звено между содержанием курса, интерфейсными сценариями и профориентационным результатом обучения.

Таблица 2 – Сопоставление учебных действий с материалами PT NAD

Учебный блок	Разделы PT NAD	Материалы руководств	Профориентационный результат
Начальная настройка и подготовка стенда	Установка продукта, мастер настройки, выбор интерфейсов захвата	Руководство по установке на один сервер: разделы 7-8	Понимание инфраструктурной основы работы аналитика и зависимости качества расследования от корректного захвата трафика
Ориентация в интерфейсе и первичный обзор	Дашборды, диаграмма интенсивности трафика, панель фильтрации	Руководство оператора: разделы 6, 11	Формирование первичного навыка чтения состояния сети и выделения зоны внимания
Анализ сетевых сессий	Список сессий, карточка сессии, экспорт PCAP и метаданных	Руководство оператора: раздел 9	Переход от наблюдения отдельных событий к реконструкции сетевого взаимодействия

Рубрика 3. Методология и технология профессионального образования

Анализ атак	Список атак, карточка атаки, причина срабатывания, ложные срабатывания	Руководство оператора: раздел 10	Освоение логики расследования: от сработавшего правила к выводу о характере инцидента
Работа с активностями, узлами и связями	Лента активностей, узлы, сетевые связи	Руководство оператора: разделы 12, 14, 15	Развитие способности видеть инцидент в контексте инфраструктуры, а не как изолированную запись
Правила, репутационные списки и исключения	Правила для атак и активностей, репутационные списки, исключения	Руководство оператора: раздел 20	Понимание границы между типовым обнаружением, настройкой продукта и аналитическим решением

Для визуализации состояния трафика и первичной ориентации в данных использовались дашборды и виджеты PT NAD (рис. 3). На этом этапе студент учился связывать отдельные числовые показатели, географические распределения и протокольную структуру трафика с возможными гипотезами расследования.

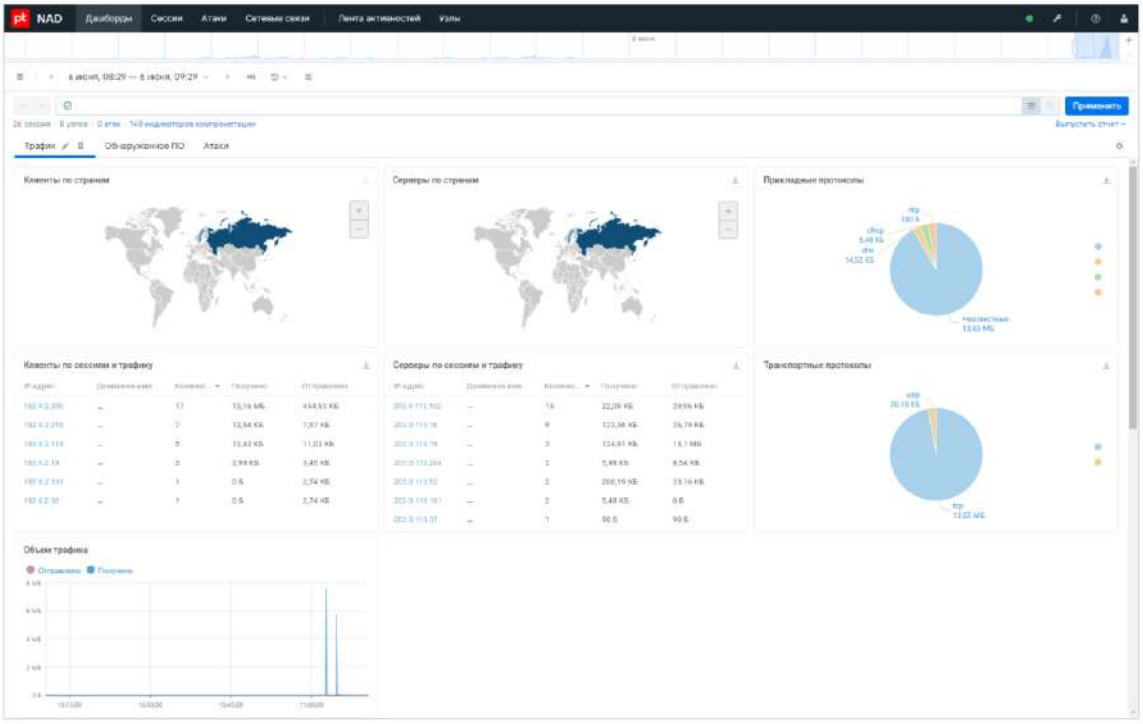

Рис. 3. Дашборд PT NAD для просмотра статистических данных о трафике (по материалам [35])

Переход к расследованию строился от общего списка атак и временной диаграммы срабатываний к карточке конкретной атаки (рис. 4–5). Такая последовательность соответствует логике профессиональной пробы: обучающийся сначала видит общий поток событий, затем выделяет значимое срабатывание и только после этого анализирует правило, сессию, атакующий и атакуемый узлы.

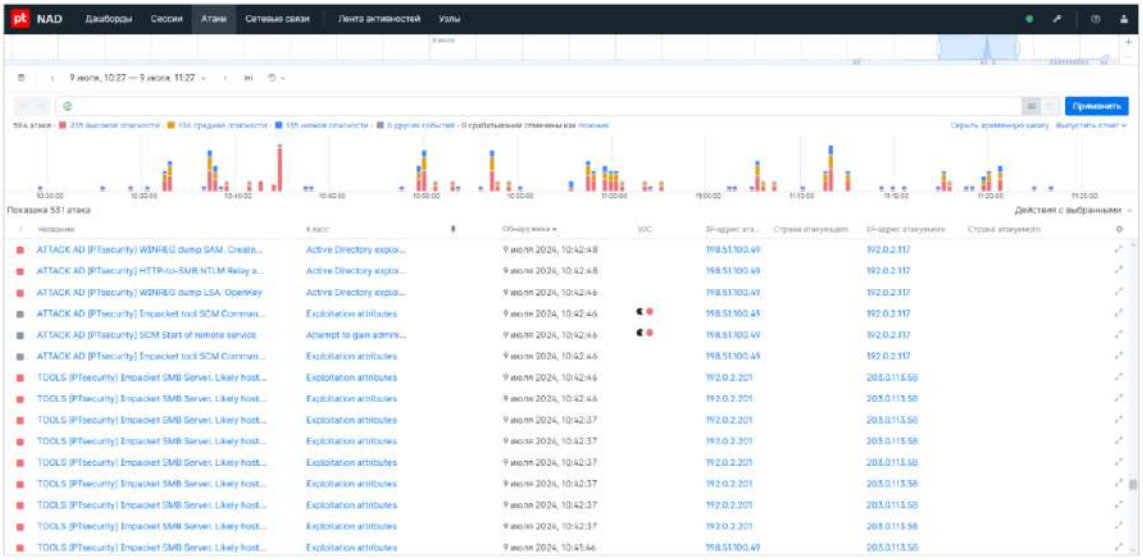

Рис. 4. Список атак и временная диаграмма срабатываний в PT NAD (по материалам [35])

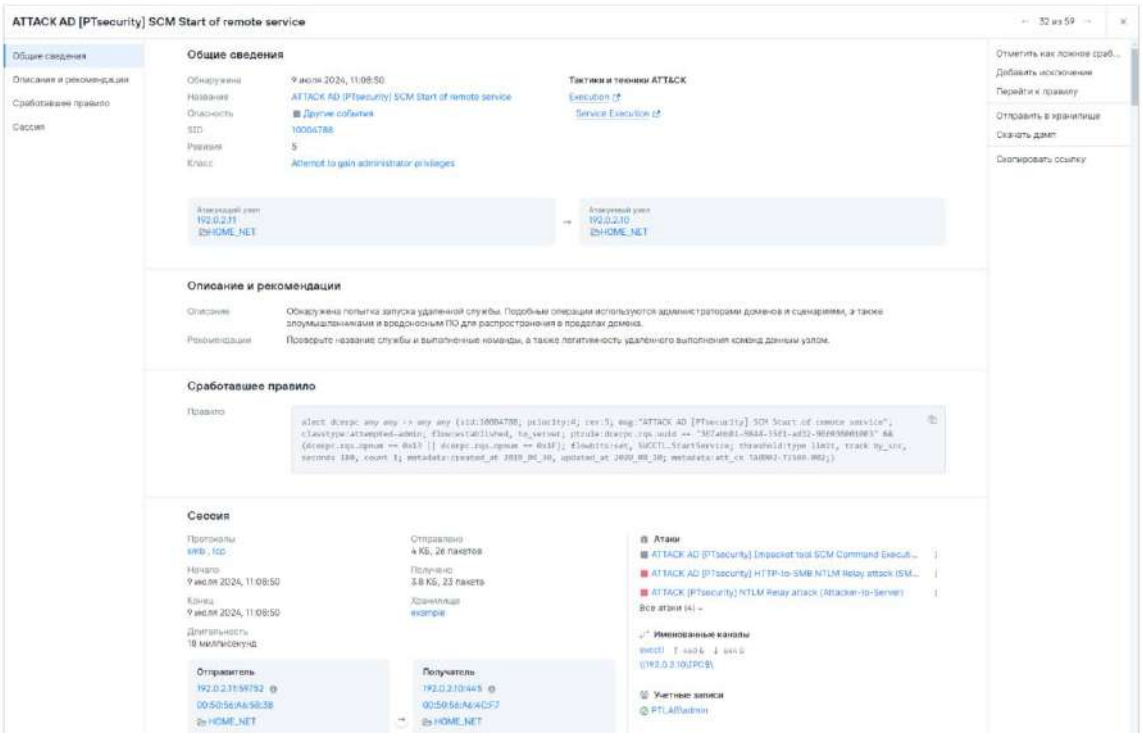

Рис. 5. Карточка атаки в PT NAD как элемент учебного кейса расследования (по материалам [35])

Раннее выведение на сертификацию в первом курсе специалитета как элемент интегрированной профориентации

Принципиальная особенность описываемой практики состоит в том, что аналогичные сертификационные процедуры, к которым приходят студенты 4–5 курсов специалитета по завершении дисциплин «Безопасность сетей ЭВМ» и «Безопасность информационно-аналитических систем», организуются и в рамках профильного предмета первого курса специалитета. Указанное решение вызывает обоснованные вопросы: насколько целесообразно нагружать первокурсника, который только что перешёл со ступени общего образования, нормативно признанной вендорской сертификацией взрослого профессионального уровня? Не противоречит ли это принципу доступности обучения и не оборачивается ли формальным «натаскиванием» на тест?

Развёрнутый ответ на эти вопросы возможен только в логике интегрированной профориентации. Сертификация на первом курсе не подменяет собой обучение и не является самоцелью; она является педагогическим средством решения профориентационной задачи и

одновременно — диагностическим средством оценки начального уровня сформированности компонентов профессиональной компетенции. С позиции отечественной школы профессиональной педагогики такая постановка непротиворечива и обеспечивается следующей системой педагогических аргументов.

1. Снятие «эффекта отложенной профессии». Е. А. Климов прямо отмечал: «Профессиональное самоопределение — это не одномоментный акт выбора, а длительный, многоэтапный процесс выработки человеком собственного отношения к профессионально-трудовой сфере». В традиционной системе высшего образования студент первого курса нередко получает преимущественно общетеоретическое содержание и фактически отложенно сталкивается с профессией только на втором-третьем курсе, при появлении первых профильных дисциплин. Это удлиняет «период неопределённости» и повышает риск отказа от выбранной специальности. Раннее выведение на продуктовый курс и сертификацию решает эту проблему: обучающийся уже в первый учебный год получает опыт профессиональной пробы в её нормативно оформленной версии. Этот вывод корреспондирует с современными исследованиями, фиксирующими, что отсутствие раннего и предметного карьерного сопровождения значимо снижает способность к планированию карьеры и устойчивость карьерного выбора [8; 9].

2. Формирование мотивационно-ценностного компонента компетенции. Согласно А. М. Новикову, мотивация учения существенно усиливается, когда учебная деятельность воспринимается обучающимся как имеющая смысл за пределами самой учебной ситуации: «Мотивация учебной деятельности тесно связана с осознанием её социального и личностного смысла». Сертификат вендора — материальный носитель такого смысла: его можно предъявить за пределами образовательной организации, он значим для работодателя, он связывает учебный успех со взрослым профессиональным статусом. В этом смысле сертификация даёт первокурснику то, чего практически невозможно добиться внутренней зачётно-экзаменационной системой образовательной организации: внешне валидированный знак профессиональной состоятельности.

3. Согласование с принципом природосообразности и принципом ведущей деятельности. Раннее (на первом курсе) включение обучающегося в продуктовую среду промышленного класса согласуется с положением Л. С. Выготского о зоне ближайшего развития: «То, что ребёнок сегодня может сделать в сотрудничестве и под руководством, завтра он становится способен выполнять самостоятельно». Промышленная среда SIEM/NAD на этапе первого курса лежит в зоне ближайшего развития обучающегося только при условии методически выстроенного педагогического сопровождения, которое и обеспечивается аудиторными часами курса, инструкциями лабораторного полигона и фигурой преподавателя-наставника. Сертификация фиксирует переход содержания из зоны ближайшего развития в актуальный уровень развития обучающегося.

4. Продольная связность образовательной траектории. Т. Ю. Ломакина указывает, что «непрерывное профессиональное образование выступает важнейшим условием формирования всесторонне развитой, профессионально мобильной личности». В авторской практике на одну и ту же сертификацию (PT-NAD-CS, PT-SIEM-CS) выходят обучающиеся двух сечений траектории высшего образования: первый курс специалитета и старшие курсы того же специалитета. Этим обеспечивается прямая нормативная связность: студент проходит через одну и ту же шкалу профессиональной оценки на разных этапах своей траектории, что облегчает педагогическое управление его профессиональным развитием. Структурированное картирование сертификаций как точек входа в профессию кибербезопасности рассматривается в современных международных исследованиях как один из основных инструментов снижения дефицита кадров и закрепления молодёжи в профессии [12].

5. Содержательное укрепление профильного предмета. Включение продуктового курса в специальный предмет первого курса переводит этот предмет из разряда «общеподготовительных» в разряд предметов, непосредственно встроенных в профессиональную деятельность. По выражению А. М. Новикова, «учебный предмет в профессиональном образовании имеет смысл лишь постольку, поскольку он работает на профессиональную деятельность

будущего специалиста». Сертификация, привязанная к специальному предмету первого курса, делает эту работу очевидной для обучающегося, его родителей, работодателя и педагогического коллектива.

6. Диагностическая функция. С. Я. Батышев писал: «Контроль и оценка не сводятся к констатации результата, они выступают средством управления процессом подготовки квалифицированного рабочего». Внешняя сертификация даёт педагогу диагностический материал, не зависящий от внутренней зачётно-экзаменационной системы: видно, какие именно содержательные блоки оказались усвоены недостаточно, и видно, какие именно компоненты профессиональной компетенции (знания, умения, навыки, практический опыт, личностные качества) у конкретного обучающегося уже сформированы. Современные исследования цифровой трансформации оценки компетенций показывают, что внешние нормативные процедуры с прокторингом обеспечивают существенно более высокую достоверность диагностического заключения, чем внутренние формы контроля [17].

7. Формирование профессиональной идентичности. Зарубежные исследования профессиональной идентичности обучающихся показывают, что устойчивая профессиональная идентичность не возникает в результате чисто учебных событий; её источником служит включение обучающегося в подлинную профессиональную практику с признанным сообществом профессионалов [15; 16]. Сертификация вендора — это вход в такое сообщество: сертифицированный обучающийся становится частью внешнего профессионального реестра, признанного работодателем, и тем самым обретает основу для устойчивой профессиональной идентификации.

Таким образом, ранний выход обучающегося первого курса специалитета на сертификацию у вендора рассматривается не как опережающее «взрослое» обучение, а как педагогически оправданная профессиональная проба, размещённая внутри специального предмета и решающая одновременно задачи профориентации, мотивации, диагностики, формирования компонентов профессиональной компетенции, обеспечения продольной связности траектории высшего образования и закрепления профессиональной идентичности.

Критерии и уровни сформированности компетенции в условиях ранней сертификации

Поскольку сертификация в авторской практике выполняет двойную функцию (педагогическая проба и диагностический инструмент), необходимо специально оговорить критерии и уровни, по которым оценивается результат подготовки.

В работе используется четырёхкритериальная модель, объединяющая отечественную и зарубежную традиции: мотивационно-ценностный критерий (готовность и желание профессионально действовать в области информационной безопасности, отношение к профессии, устойчивость профессионального выбора); когнитивный критерий (владение понятийным аппаратом, моделью угроз, архитектурой SIEM/NAD, нормативной базой); деятельностный критерий (способность выполнять типовые профессиональные действия — установка и конфигурация продукта, нормализация и обогащение событий, написание правил корреляции, расследование инцидента); рефлексивный критерий (способность анализировать собственные действия, обнаруживать ошибки, корректировать профессиональное поведение в нестандартной ситуации).

Уровни сформированности задаются в трёхкомпонентной шкале «базовый — практический — продвинутый». На базовом уровне обучающийся способен воспроизвести типовые операции с инструкцией; на практическом — выполнить полный учебно-профессиональный сценарий самостоятельно, в том числе в условиях прокторинга; на продвинутом — действовать в нестандартной ситуации (изменённый трафик, отсутствие части данных, противоречивые индикаторы) и предлагать собственное решение.

Сертификация PT-NAD-CS / PT-SIEM-CS относительно этой шкалы фиксирует достижение практического уровня. Продвинутый уровень требует дополнительной работы (стажировки в SOC, участие в Capture the Flag, разработка собственных правил Sigma); базовый уровень обнаруживается у тех обучающихся, кто завершил курс, но не вышел на сертификацию.

Результаты

Внедрение продуктовых курсов SIEM и NAD в учебный процесс продемонстрировало высокую педагогическую результативность.

По блоку SIEM: из 14 студентов, приступивших к курсу, успешно завершили его и прошли сертификацию 11 человек (78,6 %).

По блоку NAD: из 29 студентов, приступивших к курсу, успешно завершили его и прошли сертификацию все 29 (100 %).

Сертификационный экзамен проводился у вендора Positive Technologies в формате тестирования с прокторингом. Независимая оценка, проводимая внешней организацией, подтверждает объективность результатов и квалификацию студентов, успешно сдавших экзамен. Несмотря на стрессовый характер испытания и страх провала, типичный для процедуры с прокторингом, большинство студентов справились с задачей, что свидетельствует о достаточном уровне подготовки. Студенты, успешно сдавшие экзамен, получили не только подтверждение своих профессиональных навыков, но и конкурентное преимущество на рынке труда.

Иллюстративный фрагмент результатов прохождения сертификации представлен на рисунке 6. Для соблюдения требований к защите персональных данных сведения, позволяющие идентифицировать обучающихся и номера сертификатов, в изображении обезличены.

Рис. 6. Примеры сертификатов PT-NAD-CS, полученных по итогам курса (персональные данные обучающихся обезличены)

Помимо достижения основных целей курса, у студентов сформированы навыки работы с реальными промышленными инструментами, что существенно повысило их конкурентоспособность на рынке труда. Внедрение вендоронезависимых фреймворков, таких как Sigma и

Suricata, позволило студентам глубже понять принципы работы с различными SIEM и NTA-системами и снизить зависимость от конкретного поставщика. На уровне первого курса специалитета подтверждено, что выведение обучающихся на сертификацию в рамках профильного предмета не приводит к «вымыванию» мотивации, а напротив, формирует у обучающихся устойчивое профессиональное самоопределение и закрепляет выбор направления УГСН 10.00.00.

Для успешного внедрения курсов была проведена тщательная подготовка, включающая разработку курсов и лабораторных работ, подготовку инфраструктуры и обучение преподавателей (см. Приложение 1). Таймлайн включал следующие ключевые этапы: разработка курсов и лабораторных работ — 2 месяца; подготовка инфраструктуры — 1 месяц; обучение преподавателей и старт курса — 1 месяц; проведение лабораторных работ и итоговая оценка — 2 месяца. В процессе реализации возникли технические сложности, связанные с интеграцией различных инструментов, а также необходимость постоянного обновления учебных материалов в соответствии с актуальной картиной угроз.

Качественные эффекты, отмеченные в ходе наблюдения за первокурсниками, включают: рост вовлечённости в профильный предмет, появление инициативных запросов обучающихся на дополнительные лабораторные работы, формирование «студенческого сообщества» вокруг продуктового курса, рост числа обучающихся, демонстрирующих устойчивое намерение продолжать обучение по выбранному направлению и заниматься профильной научно-исследовательской работой со второго курса.

Обсуждение

Полученные результаты позволяют обсудить четыре принципиальных вопроса.

Первый вопрос — о соотношении вендорской зависимости и содержательной самостоятельности подготовки. Использование исключительно вендорских материалов несёт риск формирования у обучающегося так называемого «продуктового» взгляда на профессию, при котором за конкретным интерфейсом теряются стоящие за ним фундаментальные понятия и принципы. Авторский подход к снятию этого риска состоит в параллельном включении в учебный процесс вендоронезависимых фреймворков (Sigma для правил корреляции, Suricata для сетевого анализа), отраслевой матрицы MITRE ATT&CK как метаструктуры описания тактик и техник, открытых исследовательских материалов Palo Alto Networks и публичных наборов данных malware-traffic-analysis.net. В этой конструкции вендорский курс выступает носителем актуального технологического стандарта, а вендоронезависимые средства — носителем теоретической инвариантной части содержания. Этот баланс согласуется с международной практикой проектирования киберобразовательных программ, где сертификации играют роль «карты местности», а не «единственного маршрута» [12].

Второй вопрос — о применимости описанной практики в системе высшего образования по направлениям УГСН 10.00.00. Современная политика подготовки кадров для отраслей цифровой экономики предполагает усиление связки с работодателем, переход от лекционно-репродуктивной к деятельностной педагогической логике. В этом контексте раннее выведение первокурсника на сертификацию у вендора-работодателя оказывается органичным элементом архитектуры программы специалитета: сертификация фиксирует переход обучающегося в категорию признанного работодателем носителя профессиональных навыков и тем самым выполняет именно ту функцию интеграции с производственной сферой, которая закладывается в современных образовательных программах высшей школы.

Третий вопрос — о месте описанной практики в системе педагогических условий формирования профессиональных компетенций. В терминах школы В. С. Леднева — Т. Ю. Ломакиной выделяются шесть видов педагогических условий: содержательные, процессуальные, организационные, кадровые, нормативно-методические, технологические. Применительно к описанной практике:

– содержательные условия обеспечиваются интеграцией вендорских материалов Positive Technologies, открытых исследований Palo Alto, дампов malware-traffic-analysis.net, вендоронезависимых фреймворков Sigma и Suricata;

– процессуальные условия — последовательной развёрткой «лекция — семинар — лабораторная работа — сертификация», обеспечивающей переход от понятийного к деятельностному уровню освоения, и сетью педагогических технологий профориентации, описанных в отдельном разделе;

– организационные условия — развёртыванием цифровой образовательной среды на базе Яндекс Облака, обеспечением доступа к промышленному ПО и моделированию реальной производственной среды;

– кадровые условия — наличием преподавателей с актуальным опытом работы в области информационной безопасности;

– нормативно-методические условия — соответствием содержания требованиям ФГОС ВО по направлениям УГСН 10.00.00 и согласованием с актуальной картиной профессиональных задач индустрии;

– технологические условия — выбором цифровых инструментов моделирования производственной среды (промышленные SIEM/NAD, виртуальные аналоги оборудования, облачные стенды).

Системность педагогических условий означает, что описанная практика опирается не на единственное «удачное» средство, а на согласованную сеть условий, каждое из которых играет свою роль в формировании профессиональной компетенции.

Четвёртый вопрос — об ограничениях исследования. Объём эмпирической базы (14 студентов в блоке SIEM, 29 в блоке NAD, пилотные группы первого курса) не позволяет сделать строго статистически обоснованные обобщения; данные собраны на одной образовательной организации; долгосрочные эффекты ранней сертификации (закрепление выпускников в профессии, академическая успешность на последующих курсах) пока не прослежены. Эти ограничения определяют направление дальнейшей работы.

Заключение

Опыт реализации продуктовых курсов PT-SIEM-CS и PT-NAD-CS на двух сечениях образовательной траектории высшего образования — первом курсе специалитета и старших курсах того же специалитета по направлениям укрупнённой группы 10.00.00 — позволяет сформулировать следующие выводы.

Во-первых, продуктовые курсы вендора при соответствующем педагогическом сопровождении встраиваются в программу специалитета по направлениям УГСН 10.00.00 и обеспечивают продольную связность результатов подготовки через единую внешнюю сертификационную шкалу.

Во-вторых, раннее (на первом курсе специалитета) выведение обучающегося на сертификацию у вендора педагогически оправдано в логике интегрированной профориентации: оно решает задачи раннего профессионального самоопределения обучающегося, формирования мотивационно-ценностного и когнитивного компонентов профессиональной компетенции, диагностики начального уровня подготовки и закрепления выбора направления, а также формирования профессиональной идентичности обучающегося как члена признанного профессионального сообщества.

В-третьих, интегрированная профориентация в курсе первого года реализуется через сеть взаимосвязанных педагогических технологий: технологию профессиональной пробы, контекстное обучение, кейс-метод, проектную технологию, технологию учебной симуляции на промышленном полигоне, технологию наставничества, портфолио-технологию, технологию рефлексивной фиксации, технологию ранней погружённой стажировки и технологию независимой сертификации как венца цикла.

В-четвёртых, успешность практики обеспечивается комплексом педагогических условий — содержательных, процессуальных, организационных, кадровых, нормативно-методических и технологических, — каждое из которых должно быть спроектировано отдельно и согласовано с остальными.

В-пятых, использование вендоронезависимых средств (Sigma, Suricata, MITRE ATT&CK, открытые исследования и дампы) параллельно с вендорскими курсами обеспечивает теоретическую инвариантность подготовки и снимает риск «продуктовой» зависимости.

Перспективным направлением дальнейшей работы является расширение курсов за счёт новых лабораторных работ, включающих использование дополнительных вендоронезависимых инструментов и фреймворков, а также эмпирическое исследование долгосрочных эффектов ранней сертификации: устойчивости профессионального выбора, академической успешности на последующих курсах и трудоустройства выпускников по профилю подготовки.

Библиографический список

1. Lazarov, W. Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education / W. Lazarov, T. Schafeitel-Tähtinen, J. Squillace [et al.] // Technology, Knowledge and Learning. — 2025. — DOI: 10.1007/s10758-025-09840-y.
2. Ghosh, S. Network traffic analysis based on cybersecurity intrusion detection through an effective statistical features selection and supervised learning classifier / S. Ghosh // Applied Soft Computing. — 2025. — DOI: 10.1016/j.asoc.2024.112603.
3. The Application of MITRE ATT&CK Framework in Mitigating Cybersecurity Threats // Issues in Information Systems. — 2024. — DOI: 10.48009/3_iis_2024_106.
4. Lippi, G. Practical strategies for laboratory cybersecurity / G. Lippi // Ukrainian Journal of Laboratory Medicine. — 2025. — DOI: 10.62151/2786-9288.3.4.2025.11.
5. Dincelli, E. Exploring the Agentic Metaverse's Potential for Transforming Cybersecurity Workforce Development / E. Dincelli, H. Jafarian // MIS Quarterly Executive. — 2025. — DOI: 10.17705/2msqe.00122.
6. Chernikov, P. Cyber defense of urban digital systems: Scaling SIEM correlation to reduce incident response time / P. Chernikov // Cybersecurity: Education, Science, Technique. — 2025. — DOI: 10.28925/2663-4023.2025.31.1066.
7. Zelloth, H. Career guidance for Vocational Education and Training (VET) / H. Zelloth // Journal of the National Institute for Career Education and Counselling. — 2025. — DOI: 10.20856/jnicec.3308.
8. Chang, F. The impact of lack of parental career engagement on the career planning ability of vocational students / F. Chang, P. Wang // International Journal for Educational and Vocational Guidance. — 2025. — DOI: 10.1007/s10775-025-09755-1.
9. Dayag, R. P. Strengthening career readiness through structured career guidance services of graduating students / R. P. Dayag, J. J. Picajas // Global Journal of Guidance and Counselling in Schools. — 2025. — DOI: 10.18844/gjgc.v15i2.9758.
10. Barigye, D. Technical Vocational Education and Training in Uganda: Career guidance and practice / D. Barigye // African Journal of Career Development. — 2024. — DOI: 10.4102/ajcd.v6i1.100.
11. Mathur, A. Navigating the Future: How Career Guidance Programs Prepare Secondary Students for the Future / A. Mathur, A. Mishra // International Journal of Science and Research. — 2024. — DOI: 10.21275/sr241210140511.
12. Kovalev, A. Skill-Driven Certification Pathways: Measuring Industry Training Impact on Graduate Employability / A. Kovalev, N. Stefanac, M.-A. Rizoiu // arXiv. — 2025. — arXiv:2506.04588. — URL: https://arxiv.org/abs/2506.04588.
13. Maennel, K. Human Aspects of Cyber Security for Computing Higher Education: Current Status and Future Directions / K. Maennel, O. Maennel // ACM Transactions on Computing Education. — 2025. — Vol. 25, No. 3. — Art. 27. — P. 1–30. — DOI: 10.1145/3733839.
14. Wang, H. Study on the Types of Career Decision-Making Difficulties of Chinese Higher Vocational College Students and the Influence of Parental Career Intervention Behaviors / H. Wang, L. Chen, S. Xu, X. Gu // Journal of Higher Education Management. — 2025. — Vol. 19, No. 2. — P. 86–100. — DOI: 10.13316/j.cnki.jhem.20250122.008.

Рубрика 3. Методология и технология профессионального образования

15. Kryger, M. Conceptualizing and Developing Vocational Identity: A Scoping Review of Research in Vocational Education and Training / M. Kryger, A. Qvortrup // Vocations and Learning. — 2025. — Vol. 18. — Art. 15. — DOI: 10.1007/s12186-025-09371-8.
16. Bükki, E. Teacher, Professional or Both? A Mixed Method Study of the Professional Identity / E. Bükki, A. Fehérvári // International Journal for Research in Vocational Education and Training. — 2024. — DOI: 10.13152/ijrvet.11.3.4.
17. Kharchenko, O. The digital transformation of competency assessment: Challenges and future of integrity / O. Kharchenko, D. Bondarenko // Cybersecurity: Education, Science, Technique. — 2025. — DOI: 10.28925/2663-4023.2025.30.917.
18. Pleshakova, A. Yu. Defining the concept of identity of national vocational education system / A. Yu. Pleshakova // Professional education in the modern world. — 2024. — DOI: 10.20913/2618-7515-2023-4-8.
19. Smirnov, D. Methodology for Collecting Data on the Activity of Malware for Windows OS / D. Smirnov, O. Evsutin // Informatics and Automation. — 2024. — DOI: 10.15622/ia.23.3.2.
20. Partyka, O. Integrated approach to detecting Bluetooth threats using Wireshark and Splunk SIEM / O. Partyka, B. Fihol, T. Nakonechnyi // Cybersecurity: Education, Science, Technique. — 2024. — DOI: 10.28925/2663-4023.2024.26.684.
21. Pidhornyi, P. Analytical review of models and systems for network traffic classification / P. Pidhornyi // Cybersecurity: Education, Science, Technique. — 2024. — DOI: 10.28925/2663-4023.2024.26.639.
22. Батышев, С. Я. Профессиональная педагогика : учебник для студентов, обучающихся по педагогическим специальностям и направлениям / С. Я. Батышев, А. М. Новиков ; под ред. С. Я. Батышева, А. М. Новикова. — 3-е изд., перераб. — Москва : Из-во ЭГВЕС, 2010. — 456 с.
23. Новиков, А. М. Основания педагогики : пособие для авторов учебников и преподавателей / А. М. Новиков. — Москва : Из-во ЭГВЕС, 2010. — 208 с.
24. Леднев, В. С. Содержание образования: сущность, структура, перспективы / В. С. Леднев. — 2-е изд., перераб. — Москва : Высшая школа, 1991. — 224 с.
25. Ломакина, Т. Ю. Современный принцип развития непрерывного образования / Т. Ю. Ломакина. — Москва : Наука, 2006. — 221 с.
26. Вербицкий, А. А. Активное обучение в высшей школе: контекстный подход / А. А. Вербицкий. — Москва : Высшая школа, 1991. — 207 с.
27. Климов, Е. А. Психология профессионального самоопределения : учебное пособие для студентов высших учебных заведений / Е. А. Климов. — 4-е изд., стер. — Москва : Академия, 2010. — 304 с.
28. Зеер, Э. Ф. Психология профессий : учебное пособие для студентов вузов / Э. Ф. Зеер. — 5-е изд., перераб. и доп. — Москва : Академический Проект; Фонд «Мир», 2008. — 336 с.
29. Пряжников, Н. С. Профессиональное самоопределение: теория и практика : учебное пособие / Н. С. Пряжников. — Москва : Академия, 2008. — 320 с.
30. Чистякова, С. Н. Педагогическое сопровождение самоопределения школьников: методическое пособие для профильной и профессиональной ориентации и профильного обучения / С. Н. Чистякова. — Москва : Академия, 2007. — 128 с.
31. Выготский, Л. С. Педагогическая психология / Л. С. Выготский ; под ред. В. В. Давыдова. — Москва : АСТ : Астрель, 2010. — 671 с.
32. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. — 2025. — № 11(628). — С. 58–62. — EDN DMHQJU.
33. Греков, В. С. Перспективы кибербезопасности в нефтегазовой отрасли / В. С. Греков, А. Г. Уймин // Губкинский университет в решении вопросов нефтегазовой отрасли России : Тезисы докладов VI Региональной научно-технической конференции, Москва, 19–21

сентября 2022 года. — Москва : РГУ нефти и газа (НИУ) имени И. М. Губкина, 2022. — С. 1108–1109.
34. Positive Technologies Network Attack Discovery. Версия 12.2 : руководство администратора. — Positive Technologies, 2025. — 181 с. — Дата редакции: 19.03.2025.
35. Positive Technologies Network Attack Discovery. Версия 12.2 : руководство оператора. — Positive Technologies, 2025. — 256 с. — Дата редакции: 19.03.2025.
36. Positive Technologies Network Attack Discovery. Версия 12.2 : руководство по установке на один сервер. — Positive Technologies, 2025. — 53 с. — Дата редакции: 19.03.2025.

References

1. Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P., & Fujdiak, R. (2025). Lessons learned from using cyber range to teach cybersecurity at different levels of education. Technology, Knowledge and Learning. https://doi.org/10.1007/s10758-025-09840-y
2. Ghosh, S. (2025). Network traffic analysis based on cybersecurity intrusion detection through an effective statistical features selection and supervised learning classifier. Applied Soft Computing. https://doi.org/10.1016/j.asoc.2024.112603
3. The application of MITRE ATT&CK framework in mitigating cybersecurity threats. (2024). Issues in Information Systems. https://doi.org/10.48009/3_iis_2024_106
4. Lippi, G. (2025). Practical strategies for laboratory cybersecurity. Ukrainian Journal of Laboratory Medicine. https://doi.org/10.62151/2786-9288.3.4.2025.11
5. Dincelli, E., & Jafarian, H. (2025). Exploring the agentic metaverse's potential for transforming cybersecurity workforce development. MIS Quarterly Executive. https://doi.org/10.17705/2msqe.00122
6. Chernikov, P. (2025). Cyber defense of urban digital systems: Scaling SIEM correlation to reduce incident response time. Cybersecurity: Education, Science, Technique. https://doi.org/10.28925/2663-4023.2025.31.1066
7. Zelloth, H. (2025). Career guidance for Vocational Education and Training (VET). Journal of the National Institute for Career Education and Counselling. https://doi.org/10.20856/jnicec.3308
8. Chang, F., & Wang, P. (2025). The impact of lack of parental career engagement on the career planning ability of vocational students. International Journal for Educational and Vocational Guidance. https://doi.org/10.1007/s10775-025-09755-1
9. Dayag, R. P., & Picajas, J. J. (2025). Strengthening career readiness through structured career guidance services of graduating students. Global Journal of Guidance and Counselling in Schools. https://doi.org/10.18844/gjgc.v15i2.9758
10. Barigye, D. (2024). Technical vocational education and training in Uganda: Career guidance and practice. African Journal of Career Development. https://doi.org/10.4102/ajcd.v6i1.100
11. Mathur, A., & Mishra, A. (2024). Navigating the future: How career guidance programs prepare secondary students for the future. International Journal of Science and Research. https://doi.org/10.21275/sr241210140511
12. Kovalev, A., Stefanac, N., & Rizoiu, M.-A. (2025). Skill-driven certification pathways: Measuring industry training impact on graduate employability. arXiv. https://arxiv.org/abs/2506.04588
13. Maennel, K., & Maennel, O. (2025). Human aspects of cyber security for computing higher education: Current status and future directions. ACM Transactions on Computing Education, 25(3), Article 27, 1–30. https://doi.org/10.1145/3733839
14. Wang, H., Chen, L., Xu, S., & Gu, X. (2025). Study on the types of career decision-making difficulties of Chinese higher vocational college students and the influence of parental career intervention behaviors. Journal of Higher Education Management, 19(2), 86–100. https://doi.org/10.13316/j.cnki.jhem.20250122.008
15. Kryger, M., & Qvortrup, A. (2025). Conceptualizing and developing vocational identity: A scoping review of research in vocational education and training. Vocations and Learning, 18, Article 15. https://doi.org/10.1007/s12186-025-09371-8

16. Bükki, E., & Fehérvári, A. (2024). Teacher, professional or both? A mixed method study of the professional identity. International Journal for Research in Vocational Education and Training. https://doi.org/10.13152/ijrvet.11.3.4
17. Kharchenko, O., & Bondarenko, D. (2025). The digital transformation of competency assessment: Challenges and future of integrity. Cybersecurity: Education, Science, Technique. https://doi.org/10.28925/2663-4023.2025.30.917
18. Pleshakova, A. Yu. (2024). Defining the concept of identity of national vocational education system. Professional Education in the Modern World. https://doi.org/10.20913/2618-7515-2023-4-8
19. Smirnov, D., & Evsutin, O. (2024). Methodology for collecting data on the activity of malware for Windows OS. Informatics and Automation. https://doi.org/10.15622/ia.23.3.2
20. Partyka, O., Fihol, B., & Nakonechnyi, T. (2024). Integrated approach to detecting Bluetooth threats using Wireshark and Splunk SIEM. Cybersecurity: Education, Science, Technique. https://doi.org/10.28925/2663-4023.2024.26.684
21. Pidhornyi, P. (2024). Analytical review of models and systems for network traffic classification. Cybersecurity: Education, Science, Technique. https://doi.org/10.28925/2663-4023.2024.26.639
22. Batyshev, S. Ya., & Novikov, A. M. (Eds.). (2010). Professional pedagogy (3rd ed., revised). EGVES.
23. Novikov, A. M. (2010). Foundations of pedagogy. EGVES.
24. Lednev, V. S. (1991). Content of education: Essence, structure, prospects (2nd ed., revised). Vysshaya Shkola.
25. Lomakina, T. Yu. (2006). The modern principle of the development of lifelong education. Nauka.
26. Verbitsky, A. A. (1991). Active learning in higher education: Contextual approach. Vysshaya Shkola.
27. Klimov, E. A. (2010). Psychology of professional self-determination (4th ed.). Akademia.
28. Zeer, E. F. (2008). Psychology of professions (5th ed., revised and expanded). Academic Project; Mir Foundation.
29. Pryazhnikov, N. S. (2008). Professional self-determination: Theory and practice. Akademia.
30. Chistyakova, S. N. (2007). Pedagogical support of self-determination of schoolchildren. Akademia.
31. Vygotsky, L. S. (2010). Pedagogical psychology (V. V. Davydov, Ed.). AST; Astrel.
32. Uymin, A. G., & Tolmachev, I. M. (2025). Application of domestic network equipment Eltex and EcoRouter within the specialty 09.02.06 «Network and System Administration». Automation and Informatization of the Fuel and Energy Complex, (11), 58–62.
33. Grekov, V. S., & Uymin, A. G. (2022). Prospects of cybersecurity in the oil and gas industry. In Gubkin University in solving issues of the oil and gas industry of Russia (pp. 1108–1109). Gubkin Russian State University of Oil and Gas.
34. Positive Technologies. (2025). Positive Technologies Network Attack Discovery, version 12.2: Administrator guide. Positive Technologies.
35. Positive Technologies. (2025). Positive Technologies Network Attack Discovery, version 12.2: Operator guide. Positive Technologies.
36. Positive Technologies. (2025). Positive Technologies Network Attack Discovery, version 12.2: Single-server installation guide. Positive Technologies.

Информация об авторах

Уймин Антон Григорьевич — старший преподаватель кафедры безопасности информационных технологий, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, e-mail: au-mail@ya.ru

Греков Владимир Сергеевич — ассистент кафедры безопасности информационных технологий, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, e-mail: grekov.vs.work@gmail.com

EXPERIENCE OF TEACHING PRODUCT-BASED COURSES IN SIEM AND NAD IN THE LOGIC OF INTEGRATED CAREER GUIDANCE: FROM THE FIRST YEAR OF

SPECIALIST DEGREE PROGRAMMES TO THE CERTIFICATION OF GRADUATES IN THE EXTENDED GROUP 10.00.00

Uymin A. G.1, Grekov V. S.1

1National University of Oil and Gas «Gubkin University»

Abstract. The paper presents the experience of implementing vendor product-based courses by Positive Technologies — PT-SIEM-CS (Certified Specialist in MaxPatrol SIEM) and PT-NAD-CS (Certified Specialist in PT Network Attack Discovery) — within a higher education trajectory covering two cross-sections of training: the first year of the specialist degree programme in the extended group of fields 10.00.00 «Information Security» within a profile subject and senior years (4–5) of the same specialist degree programme. The pedagogical rationale for taking first-year students to an independent vendor certification within a profile subject is unfolded: this practice is considered as an element of integrated career guidance ensuring early and subject-rooted contact of the learner with real professional activity, the formation of motivational-axiological and cognitive components of professional competence, and the consolidation of the professional choice through success in a normatively recognised assessment procedure. The pedagogical technologies of career guidance applied in the course are described in detail: professional probe, contextual learning, case study, project-based learning, simulation on an industrial training ground, mentoring, portfolio technology, reflective fixation, early embedded internship and independent certification as the culmination of the cycle. Quantitative results: 11 out of 14 students completed the SIEM block; all 29 students completed the NAD block and passed the proctored certification. The findings are consistent with the positions of the Russian school of professional pedagogy (S. Ya. Batyshev, A. M. Novikov, V. S. Lednev, T. Yu. Lomakina, A. A. Verbitsky, E. A. Klimov, E. F. Zeer) and recent international research on cybersecurity education and structured career pathways.

Keywords: professional competence, higher education, information security, career guidance, certification, contextual learning, SIEM/NAD.

Information about the authors

Uymin Anton Grigorievich — Senior Lecturer of the Department of Information Technology Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: au-mail@ya.ru

Grekov Vladimir Sergeevich — Assistant of the Department of Information Technology Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: grekov.vs.work@gmail.com