Рубрика 3. Методология и технология профессионального образования

УДК 004.056:378.147

Губина Т. Н.[1], Шмавонян С.А.[2], Уймин А. Г.[3]
[1]ООО «Базальт СПО», г. Москва, Российская Федерация
[2]ООО «Киберпротект», г. Москва, Российская Федерация
[3]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация

МЕТОДИЧЕСКАЯ СТРУКТУРА КУРСА ПО DLP-СИСТЕМАМ: КОМПЕТЕНТНОСТНЫЙ ПОДХОД К ФОРМИРОВАНИЮ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация. В статье обоснована методическая структура учебного курса, направленного на формирование профессиональных компетенций студентов в области корпоративной защиты от внутренних угроз информационной безопасности с использованием DLP-систем (Data Loss Prevention — предотвращение утечек данных). В качестве теоретической основы проектирования курса принят компетентностный подход, предполагающий единство знаний, умений, навыков, практического опыта и профессионально значимых личностных качеств обучающегося. Описана архитектура виртуального лабораторного стенда, включающего три узла: серверный (Windows Server 2025), клиентский на базе Windows 11 и клиентский на базе ОС Альт Рабочая станция 10.4 (разработчик — ООО «Базальт СПО»). Показано, что включение отечественной операционной системы в состав стенда не только соответствует контексту государственной политики импортозамещения, но и расширяет дидактические возможности курса: студенты получают практический опыт настройки и эксплуатации DLP-агента в гетерогенной среде, приближённой к реальным корпоративным условиям. Предложена трёхуровневая логика построения лабораторных работ (20 занятий, 72 академических часа): от освоения базовой инфраструктуры домена — к конфигурированию политик безопасности и далее к анализу инцидентов и цифровой криминалистике. Сформулированы педагогические условия реализации курса (содержательные, процессуальные, организационные, кадровые, нормативно-методические, технологические). Результаты апробации в двух технических вузах указывают на эффективность предложенной методики для формирования у обучающихся комплекса компетенций в области DLP-технологий.

Ключевые слова: DLP-система, информационная безопасность, компетентностный подход, лабораторный практикум, виртуальный стенд, ОС «Альт», инсайдерская угроза.

Введение

Цифровизация российской экономики и последовательный курс государства на технологический суверенитет формируют новые требования к подготовке специалистов в области информационной безопасности. Исследования по выявлению и прогнозированию внутренних угроз показывают устойчивую значимость инсайдерского фактора для корпоративной безопасности [1, 2]. В этих условиях системы предотвращения утечек данных (Data Loss Prevention, DLP) становятся одним из ключевых элементов защиты информации на предприятиях, в органах государственного управления и в инфраструктурах, обрабатывающих данные ограниченного доступа.

Между тем анализ требований работодателей показывает устойчивую потребность в специалистах, способных не только эксплуатировать DLP-решения, но и проектировать политики защиты, настраивать правила контентного анализа, расследовать инциденты и выявлять источники нарушений. Существующие образовательные программы по направлениям «Информационная безопасность» (10.05.03, 10.05.04) и «Компьютерная безопасность» (10.05.01) нередко ограничиваются теоретическим ознакомлением с классом DLP-решений и не всегда предлагают студентам систематизированный практикум на реальном программном обеспечении в условиях, приближённых к корпоративной среде.

Дополнительный вызов связан с переходом российских организаций с зарубежного системного программного обеспечения на отечественные альтернативы. Указ Президента Российской Федерации от 30 марта 2022 г. № 166 и ограничения на закупку иностранного программного обеспечения для государственных нужд задают нормативный контекст, в котором владение отечественными программными платформами становится значимым профессиональным требованием. Поэтому выпускник должен уметь работать с DLP-системами не

только в среде Microsoft Windows, но и в гетерогенной инфраструктуре, включающей Linux-дистрибутивы отечественного производства.

Цель настоящей статьи — обосновать методическую структуру курса практической подготовки по DLP-технологиям, в котором применение отечественной ОС «Альт Рабочая станция» (разработчик — ООО «Базальт СПО») встроено в учебный процесс как средство формирования профессиональных компетенций, а не как самоцель импортозамещения. Теоретической основой проектирования курса служит компетентностный подход, последовательно разработанный в трудах И.А. Зимней [3], Э.Ф. Зеера [4], В.А. Болотова и В.В. Серикова [5].

1. Теоретические основы проектирования курса

1.1. DLP-системы: понятие, архитектура, классификация

Термин Data Loss Prevention (DLP) обозначает класс программных решений, предназначенных для обнаружения, мониторинга и предотвращения несанкционированного использования, хранения и передачи конфиденциальной информации [6]. В прикладной литературе DLP-система рассматривается как продукт, который на основе централизованных политик идентифицирует, отслеживает и защищает данные в состоянии хранения, движения и использования посредством глубокого анализа содержимого [6]. Принципиально важно, что объектом защиты выступают именно данные в трёх состояниях: data at rest (хранящиеся), data in motion (передаваемые по сети) и data in use (обрабатываемые на рабочей станции).

Рис. 1. Обобщённая схема работы DLP-системы

В зависимости от точки контроля DLP-системы традиционно классифицируют на три архитектурных типа: хостовые (Endpoint DLP), сетевые (Network/Gateway DLP) и гибридные [7, 8]. Хостовый DLP-агент устанавливается непосредственно на рабочую станцию пользователя и контролирует операции с данными на уровне операционной системы: перехватывает системные вызовы, отслеживает обращения к буферу обмена, съёмным носителям, принтерам, мессенджерам и веб-браузерам. Сетевой DLP-компонент анализирует трафик на уровне шлюза, выявляя попытки передачи конфиденциальных данных по почте, в облачные хранилища и через иные сетевые каналы. Гибридные решения объединяют оба подхода, обеспечивая комплексную защиту периметра [9].

Для идентификации конфиденциальных данных современные DLP-системы используют несколько методов контентного анализа: регулярные выражения и словари, цифровые отпечатки документов (document fingerprinting), статистический анализ, методы машинного обучения [10]. Цифровой отпечаток формируется на основе математического преобразования эталонного документа и позволяет обнаружить его копию или модифицированную версию даже при частичном изменении содержимого.

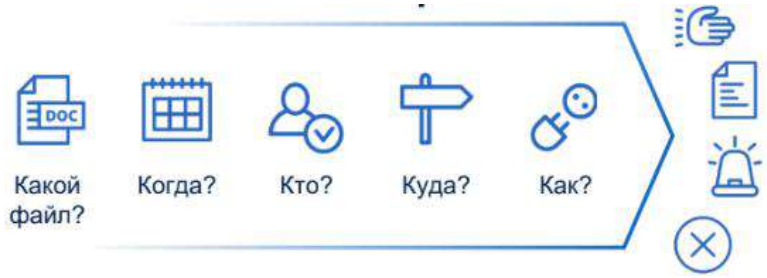

Рис. 2. Контекстный контроль в DLP-системе

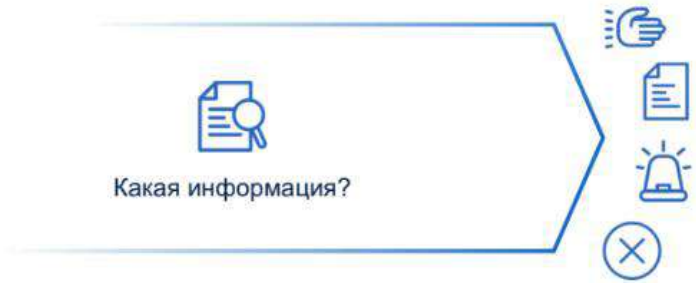

Рис. 3. Контентно-зависимый контроль в DLP-системе

Таблица 1 – Классификация DLP-систем по архитектурному принципу

Хостовый (Endpoint DLP)	Сетевой (Network/Gateway DLP)	Гибридный (Hybrid DLP)
Агент на рабочей станции	Шлюз/прокси на периметре	Агент + шлюз
Контроль операций ОС	Анализ сетевого трафика	Комплексная защита
Съёмные носители, печать, буфер обмена	E-mail, HTTP/S, FTP, мессенджеры	Все каналы одновременно
Пример: Кибер Протего (агентский модуль)	Пример: шлюзовой модуль перехвата почты	Пример: Кибер Протего v11.0 (полное развёртывание)

1.2. Компетентностный подход в подготовке специалистов по информационной безопасности

Компетентностный подход, сложившийся в российской педагогике на рубеже XX–XXI вв. в трудах И.А. Зимней, Э.Ф. Зеера, В.А. Болотова, В.И. Байденко и других учёных, постулирует, что образовательный результат должен выражаться не в объёме усвоенных знаний, а в готовности и способности применять их для решения реальных профессиональных задач [3, 4, 5]. Применительно к подготовке специалистов по информационной безопасности это означает, что выпускник должен не просто знать устройство DLP-системы, но уметь самостоятельно развернуть её, настроить политики под конкретный профиль угроз и провести расследование инцидента.

В структуре профессиональной компетенции специалиста по DLP-технологиям выделяются пять обязательных компонентов [3, 4, 11]:

– знания: понятийный аппарат информационной безопасности, принципы работы DLP-агентов, методы контентного анализа, протоколы сетевого взаимодействия, требования регуляторов (ФСТЭК, ФСБ, ГОСТ Р 57580);
– умения: развёртывать и конфигурировать DLP-систему в доменной среде, разрабатывать правила обнаружения конфиденциальных данных, настраивать каналы перехвата, анализировать журналы событий и отчёты системы;
– навыки: устойчивое выполнение типовых операций — добавление агентов в консоль управления, настройка групповых политик, экспорт теневых копий;
– практический опыт: применение знаний, умений и навыков в нестандартных ситуациях — выявление скрытых каналов утечки, расследование инцидентов по неполным данным, восстановление работоспособности DLP-компонентов и проверка целостности журналов событий;
– профессионально значимые личностные качества: аккуратность и методичность при работе с конфиденциальной информацией, стрессоустойчивость при анализе инцидентов, ответственность за принятые решения по блокировке действий пользователей.

Дополнительно в составе профессиональной компетенции специалиста ИБ необходимо учитывать гибкость и адаптивность — способность применять освоенные методы защиты в условиях смены технологического стека, включая переход с зарубежных платформ на отечественные. Именно это качество оказывается наиболее востребованным в условиях политики импортозамещения.

Исследования в области компетентностной подготовки специалистов по кибербезопасности подтверждают, что формирование устойчивых компетенций требует обязательного включения практических лабораторных занятий, воспроизводящих реальную корпоративную среду [11, 12]. A. Alammari и соавторы показали, что компетентностная оценка в области кибербезопасности должна охватывать три измерения KSA (knowledge, skills, abilities — знания, навыки, способности) и быть привязана к конкретным профессиональным задачам [11]. V.R. Kebande отмечает, что использование виртуальных лабораторий повышает вовлечённость студентов и активность обучения при дистанционном изучении кибербезопасности [12].

2. Методическая структура курса

2.1. Концепция курса и целевые компетенции

Разработанный курс «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий» ориентирован на обучающихся старших курсов специалитета по направлениям подготовки 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.04 «Информационно-аналитические системы безопасности», а также на студентов СПО по специальностям 10.02.04 и 10.02.05. Объём курса составляет 72 академических часа, реализованных в форме 20 лабораторных работ [19]. Лекционная составляющая встроена в лабораторный формат в виде вводных теоретических блоков к каждой работе.

Курс направлен на формирование следующих профессиональных компетенций ФГОС ВО: ОПК-12 (способность применять средства защиты информации от несанкционированного доступа), ОПК-13 (способность осуществлять контроль и мониторинг защищённости информационных систем), ОПК-14 (способность проводить анализ и оценку угроз информационной безопасности) и ОПК-15 (способность разрабатывать политики и регламенты информационной безопасности). Перечисленные компетенции раскрываются через пятикомпонентный состав (знания, умения, навыки, практический опыт, личностные качества), описанный в разделе 1.2.

2.2. Виртуальный лабораторный стенд

Центральным педагогическим средством курса является виртуальный лабораторный стенд, развёрнутый на гипервизоре Альт Виртуализация. Выбор платформы виртуализации обусловлен её открытостью, доступностью для образовательных учреждений и возможностью развёртывания в типовой серверной конфигурации учебных вычислительных центров. Использование виртуальных лабораторий в обучении информационной безопасности обосновано в ряде исследований [12, 13, 14]: они обеспечивают изолированную среду для проведения экспериментов, снижают риск повреждения реальной инфраструктуры и позволяют воспроизводить разнообразные сценарии угроз.

Стенд включает три виртуальные машины (рис. 4, табл. 2–3):

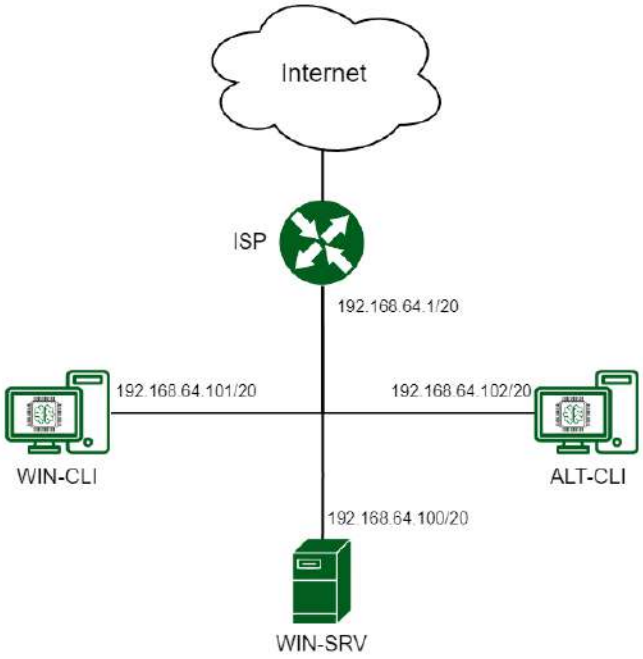

Рис. 4. Топология виртуального лабораторного стенда

Таблица 2 – Состав и назначение узлов лабораторного стенда

Узел	ОС / Роль	IP-адрес	Компоненты DLP
WIN-SRV	Windows Server 2025 Контроллер домена AD DS/AD CS Сервер управления DLP	192.168.64.100	Management Server Search & Discovery Server Group Policy Manager
WIN-CLI	Windows 11 Клиентская рабочая станция (член домена)	192.168.64.101	DLP-агент (Endpoint) Agent Settings Editor Central Management Console
ALT-CLI	ОС Альт Рабочая станция 10.4 (Базальт СПО) Клиентская рабочая станция	192.168.64.102	DLP-агент для Linux Web Console (управление агентом через браузер)

Таблица 3 – Минимальные ресурсы виртуальных машин лабораторного стенда

Наименование	HDD, ГБ	RAM, ГБ	CPU, ядер	Операционная система
WIN-CLI	80	4	2	Windows 11
WIN-SRV	80	4	2	Windows Server 2025
ALT-CLI	50	2	1	Альт Рабочая станция 10.4

Архитектурное решение с двумя клиентскими узлами на разных операционных системах воспроизводит типовую гетерогенную корпоративную среду, в которой наряду с рабочими станциями Windows присутствуют Linux-машины разработчиков, серверы и специализированные АРМ. Такая конфигурация особенно актуальна для организаций, находящихся в процессе перехода на отечественное программное обеспечение.

2.3. Трёхуровневая структура лабораторных работ

Двадцать лабораторных работ курса организованы в три последовательных уровня, каждый из которых соответствует определённому этапу формирования компетенции. Логика построения опирается на принцип восходящей сложности: каждый последующий уровень предполагает не только новые знания, но и опору на навыки, сформированные на предыдущем [15, 16].

Таблица 4 – Трёхуровневая структура лабораторных работ курса

Уровень / ЛР	Тематика	Формируемые компоненты	Педагогические средства
I. Инфраструктура (ЛР 1–5) 10 ч.	Установка и настройка ОС. Развёртывание AD DS, AD CS. Настройка ОС Альт, вступление в домен.	Знания: архитектура домена, роли сервера. Умения: развёртывать доменную среду.	Инструктивная карта; пошаговый лабораторный практикум; самопроверка.
II. Установка и конфигурация DLP (ЛР 6–14) 36 ч.	Развёртывание компонентов Кибер Протего v11.0. Настройка агентов на Windows и ОС Альт. Правила и политики DLP.	Умения: конфигурировать DLP-систему. Навыки: работа с консолью управления. Опыт: гетерогенная среда.	Ситуационные задачи; работа с реальным ПО; групповое обсуждение; отчёт по результатам.
III. Политики, инциденты, форензика (ЛР 15–20) 26 ч.	Контентный анализ, цифровые отпечатки. Анализ инцидентов. Досье пользователя. Теневое копирование.	Практический опыт: расследование инцидентов. Личностные качества: ответственность, аккуратность.	Кейс-метод; ролевая игра «следователь / нарушитель»; портфолио отчётов; защита результатов.

Первый уровень (ЛР 1–5) посвящён развёртыванию базовой доменной инфраструктуры: установке и начальной настройке операционных систем на всех трёх узлах стенда, развёртыванию служб Active Directory Domain Services (AD DS) и Active Directory Certificate Services (AD CS), вступлению клиентских машин в домен, включая ОС Альт через механизм SSSD/Kerberos. На этом уровне у студентов формируются знания об архитектуре доменной среды и базовые умения её развёртывания.

Второй уровень (ЛР 6–14) — центральный и наиболее объёмный (36 часов). Студенты последовательно устанавливают и настраивают компоненты DLP-системы Кибер Протего v11.0 (разработчик — ООО «Киберпротект»): сервер управления (Management Server), поисковый сервер (Search and Discovery Server), агент на Windows-клиенте, агент на ОС «Альт» с управлением через веб-консоль. Особое внимание уделяется конфигурированию политик контроля, аудита и перехвата: настройке правил для каналов e-mail, USB-носителей, буфера обмена, печати и мессенджеров. На этом уровне формируются умения и навыки работы с DLP-консолью, а также практический опыт эксплуатации системы в гетерогенной среде.

Рис. 5. Каналы контроля DLP-политик в Кибер Протего

Третий уровень (ЛР 15–20) ориентирован на формирование практического опыта анализа инцидентов и цифровой криминалистики. Студенты создают базу цифровых отпечатков конфиденциальных документов, настраивают правила контентного анализа, моделируют сценарии утечки данных и проводят их расследование с использованием досье пользователя, теневых копий и журналов событий. Применение кейс-метода и ролевых игр на этом уровне обеспечивает формирование профессионально значимых личностных качеств: аккуратности, ответственности и способности работать в условиях неполноты данных.

3. Роль отечественной операционной системы в дидактической структуре курса

3.1. Импортозамещение как педагогический контекст

Включение ОС «Альт Рабочая станция» 10.4 в состав лабораторного стенда продиктовано не только нормативным контекстом, но и педагогической логикой. Начиная с 2022 года переход на отечественное системное программное обеспечение приобрёл характер государственной задачи. Указ Президента РФ от 30 марта 2022 г. № 166 и Постановление Правительства РФ от 16 ноября 2015 г. № 1236 с последующими изменениями ограничивают использование иностранного программного обеспечения в ряде государственных и критически значимых контуров. В образовательном процессе это означает необходимость готовить выпускников к работе в смешанных инфраструктурах, где отечественные ОС сосуществуют с Windows-решениями.

Бурняшов в своём исследовании показал, что переход российских вузов на отечественное программное обеспечение в учебном процессе сопряжён с рядом системных трудностей: дефицитом методических материалов, необходимостью переподготовки преподавательского состава и сопротивлением со стороны студентов, привыкших к зарубежным платформам [17]. Разработанный курс решает эту проблему иначе: ОС «Альт» вводится не как замена Windows, а как органичная часть профессионального контекста — корпоративной среды, в которой сосуществуют разные платформы, и специалист по ИБ обязан уметь работать с каждой из них.

Продуктовая линейка Базальт СПО — ОС «Альт Рабочая станция», ОС «Альт Сервер»— представлена в реестре отечественного программного обеспечения Минцифры России и применяется в государственных, образовательных и корпоративных организациях. Использование этого дистрибутива в учебном курсе повышает соответствие практической подготовки будущей профессиональной деятельности выпускников [18].

3.2. Дидактические преимущества гетерогенной среды

Ключевой дидактический эффект от включения ОС «Альт» в состав стенда состоит в формировании у студентов более глубокого понимания механизмов работы DLP-системы. Если установка и настройка DLP-агента в Windows-среде во многом сводится к запуску установочного пакета и выбору параметров в графическом интерфейсе, то настройка агента в ОС «Альт» требует работы с командной строкой, понимания структуры файловой системы Linux, механизмов systemd, правил SELinux/AppArmor и процедур аутентификации через SSSD/Kerberos.

Таким образом, Linux-клиент выполняет в курсе двойную дидактическую функцию: во-первых, он является объектом практики по освоению отечественной ОС; во-вторых, он помогает явно раскрыть архитектурные особенности DLP-системы, которые остаются менее заметными при работе исключительно в среде Windows. Студент, успешно настроивший DLP-агент под управлением веб-консоли на ОС «Альт», демонстрирует более глубокое понимание серверно-клиентского взаимодействия в DLP-системе, чем студент, ограничившийся только Windows-агентом.

Опыт апробации курса показал, что задания, связанные с ОС «Альт» (ввод машины в домен, развёртывание Linux-агента, настройка веб-консоли и применение политики к Linux-клиенту), оказались наиболее значимыми с точки зрения диагностики реального уровня профессиональной компетентности. Студенты, демонстрировавшие поверхностные знания в Windows-ориентированных работах, чаще всего обнаруживали пробелы именно при переходе к Linux-среде.

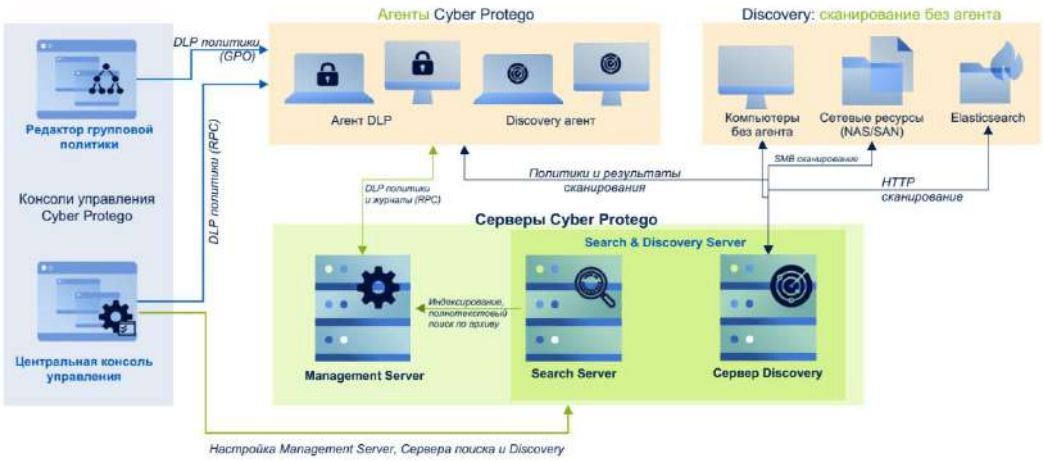

Рис. 6. Состав и взаимодействие компонентов Кибер Протего

Таблица 5 – Функциональное распределение компонентов Кибер Протего на узлах лабораторного стенда

Узел стенда	Операционная система и роль	Компоненты Кибер Протего	Основные взаимодействия
WIN-SRV (192.168.64.100)	Windows Server 2025; контроллер домена AD DS/AD CS; серверный узел DLP	Management Server; Search & Discovery Server; Group Policy Manager	Распространение политик, сбор агентских отчётов, хранение журналов и теневых копий
WIN-CLI (192.168.64.101)	Windows 11; клиентская рабочая станция, член домена	Endpoint Agent; Agent Settings Editor; Central Management Console	Получение политик, контроль локальных каналов, отправка событий на сервер управления
ALT-CLI (192.168.64.102)	ОС «Альт Рабочая станция» 10.4; Linux-клиент	Linux Agent; Web Console для управления агентом	Работа через HTTPS-веб-консоль, получение политик, передача агентских отчётов

4. Педагогические условия реализации курса

Эффективность курса обеспечивается совокупностью педагогических условий, которые охватывают все аспекты образовательного процесса: от содержания учебного материала до нормативной базы и технологического оснащения. В соответствии с устоявшейся традицией профессиональной педагогики выделяется шесть видов педагогических условий [3, 4].

1. Содержательные условия

Содержание курса структурировано на основе реальных профессиональных задач специалиста по защите информации от инсайдерских угроз. Каждая лабораторная работа имеет чёткую профессиональную направленность: студент не «изучает систему ради системы», а решает конкретную учебно-профессиональную задачу — развернуть защищённую доменную среду, расследовать инцидент утечки, создать базу цифровых отпечатков конфиденциальных документов. Включение учебно-профессиональных задач разной степени сложности — от типовых до нестандартных — обеспечивает формирование всех пяти компонентов профессиональной компетенции.

2. Процессуальные условия

Процесс формирования компетенций разворачивается в определённой последовательности: диагностическое тестирование входного уровня → вводный теоретический блок → выполнение лабораторной работы → защита отчёта → рефлексивное обсуждение. Диагностика уровня сформированности компетенции осуществляется на трёх срезах: после первого уровня (ЛР 1–5), после второго уровня (ЛР 6–14) и по завершении курса (ЛР 15–20). Инструменты диагностики — практические задания в виде сценариев-инцидентов, которые студент должен воспроизвести и расследовать на стенде в ограниченное время.

3. Организационные условия

Курс реализуется в условиях цифровой образовательной среды учебного вычислительного центра, оснащённого серверным оборудованием, достаточным для одновременного функционирования лабораторных стендов для всей учебной группы. Обязательным организационным условием является обеспечение изолированности сетевой среды каждого стенда во избежание взаимного влияния лабораторных работ разных студентов. Привлечение представителей работодателей (компаний в сфере ИБ) к разработке сценариев инцидентов третьего уровня повышает профессиональную значимость учебных задач.

4. Кадровые условия

Преподаватель курса должен обладать актуальным практическим опытом работы с корпоративными DLP-системами и знанием как Windows-экосистемы, так и Linux. Рекомендуется прохождение дополнительной профессиональной подготовки по программам сертификации продукта (ООО «Киберпротект») и повышение квалификации не реже одного раза в три года с учётом обновлений версий используемого программного обеспечения. Желательно наличие у преподавателя опыта работы в корпоративных службах информационной безопасности.

5. Нормативно-методические условия

Курс разработан в соответствии с требованиями ФГОС ВО по направлениям 10.05.03 и 10.05.04, а также ФГОС СПО 10.02.04 и 10.02.05. Тематика лабораторных работ согласована с приказами ФСТЭК России, регламентирующими требования к средствам защиты от несанкционированного доступа и мониторинга информационной безопасности. Локальная нормативная база включает рабочую программу дисциплины, методические указания к каждой лабораторной работе и фонд оценочных средств, охватывающий все заявленные компетенции.

6. Технологические условия

Виртуализация на платформе Альт Виртуализация обеспечивает воспроизводимость учебной среды: перед началом каждого занятия стенд восстанавливается из эталонного снапшота, что гарантирует одинаковые стартовые условия для всех студентов. Использование ОС «Альт Рабочая станция» 10.4 соответствует контексту государственной политики импортозамещения и обеспечивает доступность лицензионного программного обеспечения для образовательных учреждений. DLP-система Кибер Протего v11.0 включена в единый реестр российских программ для ЭВМ и баз данных Минцифры России, что подтверждает возможность её использования в государственных образовательных организациях.

5. Результаты апробации

Курс прошёл апробацию в двух технических университетах. Апробация проводилась в формате опытно-экспериментальной работы с выделением контрольной и экспериментальной групп. Контрольная группа изучала тематику DLP-систем в традиционном формате (лекции + единичные лабораторные работы на демонстрационном стенде преподавателя). Экспериментальная группа проходила полный курс из 20 лабораторных работ на индивидуальных виртуальных стендах.

Диагностика уровня сформированности компетенций проводилась по четырём критериям: мотивационно-ценностному (отношение к задачам профессиональной защиты информации), когнитивному (знание архитектуры и принципов работы DLP-систем), деятельностному (способность самостоятельно выполнить типовую задачу на стенде) и рефлексивному (способность оценить результат и скорректировать действия). Уровни сформированности: базовый, практический, продвинутый.

По результатам итоговой диагностики в экспериментальной группе доля студентов, достигших практического и продвинутого уровней, составила 78 %, в контрольной — 31 %; по когнитивному компоненту приведены 82 % и 61 %. Авторы рассматривают эти показатели как описательные результаты пилотной апробации, а не как доказательство причинного эффекта, поскольку размеры групп, абсолютные значения, диагностический инструмент и статистическая обработка в исходных материалах не приведены.

Включение ОС «Альт» в состав стенда первоначально вызвало затруднения у части студентов, однако после выполнения заданий по доменному подключению, развёртыванию

Linux-агента и настройке веб-консоли понимание архитектуры DLP-системы заметно улучшалось. В анкетах студенты отмечали, что именно работа с Linux-клиентом помогла им понять, как DLP-агент взаимодействует с операционной системой на уровне ниже графического интерфейса.

Заключение

В статье обоснована методическая структура курса практической подготовки специалистов по DLP-технологиям, отличительными чертами которого являются: компетентностная ориентированность (единство знаний, умений, навыков, практического опыта и личностных качеств), практикоориентированность (20 лабораторных работ на индивидуальном виртуальном стенде), трёхуровневая прогрессия сложности и гетерогенная программно-аппаратная среда, включающая отечественную операционную систему ОС «Альт».

Показано, что применение ОС «Альт Рабочая станция» 10.4 в учебном стенде выполняет двойную функцию: нормативную (соответствие требованиям государственной политики импортозамещения) и дидактическую (углублённое понимание архитектурных механизмов DLP-системы через практику в Linux-среде). Именно сочетание этих двух функций отличает предложенный подход от простого «замещения» одной платформы другой.

Результаты апробации в двух технических университетах показывают выраженные различия в уровне сформированности деятельностного компонента профессиональной компетенции между экспериментальной и контрольной группами. Перспективы дальнейших исследований связаны с разработкой методики оценки рефлексивного компонента компетенции, масштабированием курса на программы СПО и адаптацией сценариев инцидентов к отраслевой специфике предприятий — потенциальных работодателей.

Библиографический список

1. Sarhan, B. B. Insider Threat Detection Using Machine Learning Approach / B. B. Sarhan, N. Altwaijry // Applied Sciences. – 2022. – Vol. 13, № 1. – P. 259. – DOI: 10.3390/app13010259.
2. Gheyas, I. A. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis / I. A. Gheyas, A. E. Abdallah // Big Data Analytics. – 2016. – Vol. 1, № 1. – P. 6. – DOI: 10.1186/s41044-016-0006-0.
3. Зимняя, И. А. Ключевые компетенции — новая парадигма результата образования / И. А. Зимняя // Высшее образование сегодня. – 2003. – № 5. – С. 34–42.
4. Зеер, Э. Ф. Психология профессионального образования / Э. Ф. Зеер. – Москва : Академия, 2009. – 384 с.
5. Болотов, В. А. Компетентностная модель: от идеи к образовательной программе / В. А. Болотов, В. В. Сериков // Педагогика. – 2003. – № 10. – С. 8–14.
6. Liu, S. Data Loss Prevention / S. Liu, R. Kuhn // IT Professional. – 2010. – Vol. 12, № 2. – P. 10–13. – DOI: 10.1109/MITP.2010.52.
7. Alsuwaie, A. Data Leakage Prevention Adoption Model & DLP Maturity Level Assessment / A. Alsuwaie, B. Habibnia, P. Gladyshev // Proceedings of the International Symposium on Computer Science and Intelligent Controls. – IEEE, 2021. – P. 396–405.
8. Balinsky, H. System Call Interception Framework for Data Leak Prevention / H. Balinsky, D. Subiros Perez, S. J. Simske // Proceedings of the IEEE 15th International Enterprise Distributed Object Computing Conference. – IEEE, 2011. – P. 139–148. – DOI: 10.1109/EDOC.2011.25.
9. Data Loss Prevention Solution for Linux Endpoint Devices // Proceedings of the ACM Conference on Data and Application Security and Privacy. – ACM, 2023. – DOI: 10.1145/3600160.3605036.
10. Gupta, K. A Learning Oriented DLP System based on Classification Model / K. Gupta, A. Kush // arXiv preprint. – 2023. – arXiv:2312.13711.
11. Alammari, A. Developing and evaluating cybersecurity competencies for students in computing programs / A. Alammari, O. Sohaib, S. Younes // PeerJ Computer Science. – 2022. – Vol. 8. – e827. – DOI: 10.7717/peerj-cs.827.
12. Kebande, V. R. The Impact of Virtual Laboratories on Active Learning and Engagement in Cybersecurity Distance Education / V. R. Kebande // arXiv preprint. – 2024. – arXiv:2404.04952.

13. Willems, C. Online assessment for hands-on cyber security training in a virtual lab / C. Willems, C. Meinel // Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON). – IEEE, 2012. – DOI: 10.1109/EDUCON.2012.6201104.
14. Pirta-Dreimane, R. Application of intervention mapping in cybersecurity education design / R. Pirta-Dreimane [et al.] // Frontiers in Education. – 2022. – Vol. 7. – DOI: 10.3389/feduc.2022.998335.
15. Švábenský, V. Scalable Learning Environments for Teaching Cybersecurity Hands-on / V. Švábenský [et al.] // Proceedings of the 2021 IEEE Frontiers in Education Conference. – IEEE, 2021. – DOI: 10.1109/FIE49875.2021.9637180.
16. Alsmadi, I. Practical Information Security: A Competency-Based Education Course / I. Alsmadi. – Cham : Springer, 2018. – DOI: 10.1007/978-3-319-72119-4.
17. Бурняшов, Б. А. Импортозамещение программного обеспечения в образовательном процессе российских вузов / Б. А. Бурняшов // Информатика и образование. – 2022. – Т. 37, № 1. – С. 27–36. – DOI: 10.32517/0234-0453-2022-37-1-27-36.
18. Бурняшов, Б. А. Отечественные облачные пакеты офисных приложений в образовательном процессе вузов / Б. А. Бурняшов // Информатика и образование. – 2023. – Т. 38, № 2. – С. 5–15. – DOI: 10.32517/0234-0453-2023-38-2-5-15.
19. Уймин, А. Г. Практикум. Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий : учебное пособие / А. Г. Уймин. – Москва : РГУ нефти и газа (НИУ) имени И. М. Губкина, 2025.

References

1. Sarhan, B. B., & Altwaijry, N. (2022). Insider threat detection using machine learning approach. Applied Sciences, 13(1), 259. https://doi.org/10.3390/app13010259
2. Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. Big Data Analytics, 1(1), 6. https://doi.org/10.1186/s41044-016-0006-0
3. Zimnyaya, I. A. (2003). Key competencies as a new paradigm of educational outcomes. Higher Education Today, (5), 34–42.
4. Zeer, E. F. (2009). Psychology of professional education. Akademiya.
5. Bolotov, V. A., & Serikov, V. V. (2003). Competency model: From idea to educational program. Pedagogy, (10), 8–14.
6. Liu, S., & Kuhn, R. (2010). Data loss prevention. IT Professional, 12(2), 10–13. https://doi.org/10.1109/MITP.2010.52
7. Alsuwaie, A., Habibnia, B., & Gladyshev, P. (2021). Data leakage prevention adoption model & DLP maturity level assessment. In Proceedings of the International Symposium on Computer Science and Intelligent Controls (pp. 396–405). IEEE.
8. Balinsky, H., Subiros Perez, D., & Simske, S. J. (2011). System call interception framework for data leak prevention. In Proceedings of the IEEE 15th International Enterprise Distributed Object Computing Conference (pp. 139–148). IEEE. https://doi.org/10.1109/EDOC.2011.25
9. Data loss prevention solution for Linux endpoint devices. (2023). In Proceedings of the ACM Conference on Data and Application Security and Privacy. ACM. https://doi.org/10.1145/3600160.3605036
10. Gupta, K., & Kush, A. (2023). A learning oriented DLP system based on classification model. arXiv. https://arxiv.org/abs/2312.13711
11. Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. PeerJ Computer Science, 8, e827. https://doi.org/10.7717/peerj-cs.827
12. Kebande, V. R. (2024). The impact of virtual laboratories on active learning and engagement in cybersecurity distance education. arXiv. https://arxiv.org/abs/2404.04952

13. Willems, C., & Meinel, C. (2012). Online assessment for hands-on cyber security training in a virtual lab. In Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON). IEEE. https://doi.org/10.1109/EDUCON.2012.6201104
14. Pirta-Dreimane, R., et al. (2022). Application of intervention mapping in cybersecurity education design. Frontiers in Education, 7. https://doi.org/10.3389/feduc.2022.998335
15. Švábenský, V., et al. (2021). Scalable learning environments for teaching cybersecurity hands-on. In Proceedings of the 2021 IEEE Frontiers in Education Conference. IEEE. https://doi.org/10.1109/FIE49875.2021.9637180
16. Alsmadi, I. (2018). Practical information security: A competency-based education course. Springer. https://doi.org/10.1007/978-3-319-72119-4
17. Burnyashov, B. A. (2022). Import substitution of software in the educational process of Russian universities. Informatics and Education, 37(1), 27–36. https://doi.org/10.32517/0234-0453-2022-37-1-27-36
18. Burnyashov, B. A. (2023). Domestic cloud office application suites in the educational process of universities. Informatics and Education, 38(2), 5–15. https://doi.org/10.32517/0234-0453-2023-38-2-5-15
19. Uymin, A. G. (2025). Practicum. Corporate protection against internal information security threats using modern DLP technologies: Textbook. Gubkin Russian State University of Oil and Gas.

Информация об авторах

Губина Татьяна Николаевна — кандидат педагогических наук, руководитель направления по работе с образовательными организациями, ООО «Базальт СПО», г. Москва, e-mail: gubina@basealt.ru.

Шмавонян Саркис Артушевич — руководитель группы по работе с образовательными организациями, ООО «Киберпротект», г. Москва, Российская Федерация, e-mail: Sarkis.Shmavonyan@cyberprotect.ru.

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.

METHODOLOGICAL STRUCTURE OF A COURSE ON DLP SYSTEMS: A COMPETENCY-BASED APPROACH TO DEVELOPING PROFESSIONAL COMPETENCIES IN INFORMATION SECURITY USING DOMESTIC SOFTWARE

Gubina T. N.[1], Shmavonyan S.A.[2], Uymin A. G.[3]

[1]BaseALT LLC, Moscow, Russian Federation
[2]Cyberprotect LLC, Moscow, Russian Federation
[3]Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation

Abstract. This paper presents the methodological structure of an academic course aimed at developing professional competencies in protection against insider threats to corporate information security using DLP (Data Loss Prevention) systems. A competency-based approach is adopted as the theoretical foundation for course design, encompassing the unity of knowledge, skills, practical abilities, professional experience, and professionally significant personal qualities of the learner. The architecture of a virtual laboratory stand is described, comprising three nodes: a server running Windows Server 2025, a client workstation running Windows 11, and a client workstation running Alt Workstation 10.4 (developed by BaseALT LLC). The paper shows that incorporating a domestic operating system into the stand not only corresponds to the state import-substitution policy context but also expands the didactic capabilities of the course: students gain practical experience in configuring and operating a DLP agent in a heterogeneous environment close to real corporate conditions. A three-level logic for constructing laboratory assignments is proposed (20 sessions, 72 academic hours): from mastering basic domain infrastructure to configuring security policies and then to incident analysis and digital forensics. Pedagogical conditions for implementing the course are formulated (content-related, procedural, organisational, personnel-related, regulatory-methodological, and technological). Pilot results from two technical universities indicate the effectiveness of the proposed methodology for developing students' competencies in DLP technologies.

Keywords: DLP system, information security, competency-based approach, laboratory practicum, virtual stand, Alt OS, insider threat.

Information about the authors

Gubina Tatiana Nikolaevna — Candidate of Pedagogical Sciences, Head of Educational Organizations Relations, BaseALT LLC, Moscow, e-mail: gubina@basealt.ru.

Shmavonyan Sarkis Artushevich — Head of the group for work with educational organizations, Cyberprotect LLC, Moscow, Russian Federation, e-mail: Sarkis.Shmavonyan@cyberprotect.ru.

Uymin Anton Grigorevich — 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.