Ковальчук Богдан Олегович
студент
Паршуков Марк Артурович
студент
Келеш Степан
студент
Научный руководитель
Врублевский Юрий Олегович
старший преподаватель
ФГБОУ ВО «МИРЭА – Российский технологический университет»
г. Москва

ИНТЕГРАЦИЯ АНГЛИЙСКОЙ ТЕРМИНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОГРАММЫ ОБУЧЕНИЯ ДЛЯ БУДУЩИХ IT-СПЕЦИАЛИСТОВ

Аннотация*: в условиях интернационализации отрасли и преобладания англоязычных первоисточников в сфере информационной безопасности (ИБ) владение профессиональной английской терминологией следует рассматривать как обязательный компонент подготовки будущих IT-специалистов. Цель статьи заключается в обосновании необходимости системной интеграции англоязычного лексикона ИБ (в частности, vulnerability, patch, encryption, SQL injection) в образовательные программы СПО и высшего образования, а также в предложении организационно-методической модели внедрения терминологии в учебные дисциплины и практико-ориентированные модули. Рассматриваются принципы отбора терминов, их соотнесение с профессиональными компетенциями и трудовыми функциями, а также инструменты контроля результатов обучения: глоссарии, кейс-задания, лабораторные работы и проектная документация с опорой на материалы OWASP. Показано, что максимальный эффект достигается при междисциплинарном подходе, при котором терминология*

осваивается в контексте реальных процессов обеспечения ИБ: управления уязвимостями, обновлениями, криптографической защиты, мониторинга и реагирования на инциденты, а также безопасной разработки.

***Ключевые слова**: информационная безопасность, профессиональная терминология, английский язык для IT, vulnerability, patch, encryption, SQL injection, OWASP, компетентностный подход.*

Введение

Современная практика обеспечения информационной безопасности опирается на постоянное обращение к англоязычным источникам: описаниям уязвимостей и идентификаторам CVE, рекомендациям поставщиков (security advisory), технической документации, руководствам по внедрению контролей, материалам профессиональных сообществ и отраслевым базам знаний. При этом значительная часть инструментов ИБ (сканеры уязвимостей, средства мониторинга, EDR/SIEM, платформы управления инцидентами) использует англоязычные интерфейсы и терминологию «по умолчанию».

Указанные обстоятельства формируют практическую потребность в том, чтобы будущий специалист уверенно понимал и корректно употреблял ключевые английские термины не только в рамках учебного курса иностранного языка, но и при выполнении профильных задач. В противном случае возникает разрыв между формально освоенными теоретическими сведениями и реальными требованиями рабочей среды, где решающим фактором нередко выступает скорость интерпретации англоязычной информации (impact, mitigation, remediation steps) и точность профессиональной коммуникации.

Задачи исследования:

– определить значимость владения англоязычной терминологией ИБ для профессиональной деятельности будущих IT-специалистов и учебных результатов программ СПО/вузов;

– соотнести терминологический компонент подготовки с трудовыми функциями и требованиями профессионального стандарта «Специалист по информационной безопасности»;

– сформировать и обосновать базовое терминологическое ядро (в т.ч. vulnerability, patch, encryption, SQL injection) и принципы его отбора;

– разработать междисциплинарную модель поэтапной интеграции терминологии в профильные дисциплины и практико-ориентированные форматы с опорой на OWASP-материалы.

Определить инструменты и критерии оценивания сформированности терминологической компетентности (уровни «знание – применение – продуктивность»).

1. Компетентностное обоснование интеграции терминологии.

Профессиональный стандарт «Специалист по информационной безопасности» закрепляет ориентацию подготовки на выполнение трудовых функций, связанных с анализом угроз и рисков, внедрением и сопровождением мер защиты, мониторингом, реагированием на инциденты и контролем соблюдения требований. Практически каждая из указанных функций предполагает работу с регламентами, техническими описаниями, отчетностью и доказательной базой, значительная часть которой представлена на английском языке либо включает англоязычные термины как элементы общепринятого профессионального дискурса.

Владение англоязычной терминологией ИБ целесообразно рассматривать как компонент профессиональной грамотности по следующим основаниям:

– ряд терминов обладает высокой семантической емкостью и не имеет полного эквивалента без искажения смысла (например, patch, mitigation, hardening);

– англоязычные термины встроены в международный контекст: стандарты, руководства, сообщества практиков, документация поставщиков;

– точность терминов влияет на качество инженерных решений (например, различение encryption и hashing, authentication и authorization) и снижает вероятность ошибочной интерпретации задач.

2. Классификация базовой терминологии и принципы отбора.

Для образовательной программы методически оправдано формирование не «максимального» словаря, а ядра терминов, которое последовательно расширяется и закрепляется через практику. В качестве принципов отбора целесообразно использовать: частотность встречаемости в профессиональной документации, прикладную проверяемость через лабораторные задания, актуальность в контексте современных угроз, а также соответствие требованиям профессиональной подготовки.

Таблица 1

Базовые группы англоязычных терминов ИБ и варианты их учебного освоения

Группа терминов	*Примеры терминов* (*EN*)	*Типичные учебные контексты*	*Проверяемый результат*
Управление уязвимостями и обновлениями	vulnerability, exploit, PoC, patch, update, mitigation, remediation, severity, impact	анализ advisory; разбор CVE-описания; оформление заявки на обновление	студент формулирует описание уязвимости и обоснование установки patch на английском (кратко и корректно)
Криптография и защита данных	encryption, decryption, hashing, signature, certificate, key management, TLS	лабораторные по TLS; разбор схем обмена ключами; анализ ошибок конфигурации	студент различает encryption и hashing; объясняет назначение certificate и последствия key compromise
Веб-безопасность и безопасная разработка	SQL injection, XSS, CSRF, input validation, authentication, authorization, session	OWASP-материалы; лабораторные на уязвимых стендах; код-ревью фрагментов	студент описывает механизм SQL injection и корректные меры исправления (parameterized queries, validation)
Мониторинг и реагирование на инциденты	incident, alert, detection, triage, containment, eradication, IOC, forensic	разбор кейса инцидента; построение timeline; формирование отчета	студент составляет краткий incident report: what happened, indicators, containment actions
Риски и контрмеры	risk, threat, control, safeguard, compliance, policy, baseline, audit	моделирование угроз; оценка рисков; сопоставление контролей	студент формирует связку threat-control и обосновывает residual risk

3. Модель внедрения: междисциплинарная интеграция.

Опыт реализации учебных программ показывает, что изолированное изучение терминов в рамках дисциплины «Иностранный язык» не обеспечивает устой-

чивого переноса в профессиональную деятельность. В связи с этим целесообразна междисциплинарная модель, при которой терминология включается в содержание профильных дисциплин и используется как инструмент выполнения практических задач.

Предлагается трехуровневый подход.

3.1. Этап «встраивание» (базовый уровень).

На данном этапе формируется первичное терминологическое ядро и корректные смысловые связи. Эффективными средствами выступают двуязычные мини-глоссарии к лабораторным работам, карточки терминов с контекстом употребления, а также задания на сопоставление термина с определением, сформулированным на английском языке в упрощенной форме.

3.2. Этап «закрепление» (основной цикл обучения).

Целью является развитие навыков чтения англоязычных первоисточников и применения терминологии в решении задач. Наиболее результативны:

– анализ кратких фрагментов из профильных учебных материалов (в т. ч. Cambridge English for IT) с последующей терминологической интерпретацией;

– практические задания по разбору advisory (affected versions, impact, mitigation);

– лабораторные работы по веб-безопасности с использованием материалов OWASP и обязательным включением англоязычных фрагментов в отчет (например, vulnerability description, steps to reproduce, remediation).

3.3. Этап «производство» (проектная и выпускная деятельность).

На завершающем этапе студент демонстрирует способность создавать профессиональные тексты и артефакты с корректным употреблением терминологии. К целесообразным форматам относятся:

– командные проекты по анализу архитектуры и моделированию угроз, где часть документации оформляется на английском;

– отчеты по аудиту/тестированию на проникновение с двуязычной структурой: краткое резюме на русском и технические детали на английском;

– защита проекта с использованием терминов при объяснении attack vector, impact, mitigation plan и критериев приемки исправлений.

4. Методические приемы формирования устойчивого лексикона.

Терминологическая компетентность формируется эффективнее при опоре на действие и контекст.

Контекстные определения вместо механического перевода: термин фиксируется в типовом профессиональном употреблении (например, apply a patch, disclose a vulnerability, encrypt data at rest).

Работа с коллокациями: освоение устойчивых словосочетаний снижает риск кальки и повышает точность формулировок.

Кейс-метод и микросценарии: студент принимает решение (например, установить patch немедленно либо применить mitigation) и оформляет его в виде краткого англоязычного текста (тикет, фрагмент отчета).

Терминологические карты (concept maps): визуальная фиксация связей vulnerability → exploit → mitigation → patch → verification способствует системному усвоению.

5. Оценивание результатов обучения.

Контроль целесообразно строить по трем уровням: знание, применение, продуктивность.

Знание: тестирование различий ключевых понятий (encryption vs hashing; authentication vs authorization) и понимания дефиниций.

Применение: выполнение лабораторных работ и оформление отчета с обязательными англоязычными разделами.

Продуктивность: подготовка краткого incident report или vulnerability report с ограничением по объему и обязательным использованием заданного набора терминов и коллокаций.

Заключение

Интеграция англоязычной терминологии информационной безопасности в образовательные программы подготовки будущих IT-специалистов является ме-

тодически обоснованной и практически необходимой, поскольку профессиональная деятельность в ИБ напрямую связана с англоязычными источниками, инструментами и формами коммуникации. Наиболее результативным представляется междисциплинарный подход, при котором терминология осваивается в логике реальных процессов обеспечения ИБ и закрепляется через лабораторные работы, кейсы и проектную деятельность. Реализация предложенной модели способствует повышению готовности выпускников к чтению первоисточников, корректному оформлению технической документации и эффективному взаимодействию в профессиональной среде.

Список литературы

1. Профессиональный стандарт «Специалист по информационной безопасности»: утв. приказом Министерства труда и социальной защиты РФ от 18.11.2013 г. № 679н. – М., 2013.

2. Zemach S., Edwards S. Cambridge English for IT. Cambridge: Cambridge University Press, 2011. 112 p. ISBN 978-0-521-72438-6.

3. Марвани М. Английский язык для IT-специалистов: учебное пособие / М. Марвани. – СПб.: Питер, 2022. – 192 с. – ISBN 978-5-4461-1985-9.

4. Kohnke A., Shoemaker D., Sigler K. The Complete Guide to Cybersecurity Risks and Controls. Boca Raton: CRC Press, 2016. 325 p. ISBN 978-1-4987-3042-6 (hbk.).

5. OWASP Foundation (Open Web Application Security Project). Официальная документация и проекты [Электронный ресурс]. – Режим доступа: https://owasp.org (дата обращения: 18.12.2025).