Мир науки. Социология, филология, культурология https://sfk-mn.ru
World of Science. Series: Sociology, Philology, Cultural Studies

2026, Том 17, № 2 / 2026, Vol. 17, Iss. 2 https://sfk-mn.ru/issue-2-2026.html

URL статьи: https://sfk-mn.ru/PDF/44FLSK226.pdf

DOI: 10.15862/44FLSK226 (https://doi.org/10.15862/44FLSK226)

5.9.6. Языки народов зарубежных стран (с указанием конкретного языка или группы языков) (филологические науки)

Ссылка для цитирования этой статьи:
Хахалева, А. Ю. Особенности использования англицизмов в русском языке в сфере информационной безопасности / А. Ю. Хахалева, М. В. Романова // Мир науки. Социология, филология, культурология. — 2026. — Т. 17. — № 2. — URL: https://sfk-mn.ru/PDF/44FLSK226.pdf. DOI: 10.15862/44FLSK226.

For citation:
Khakhaleva A.Yu., Romanova M.V. Peculiarities of using anglicisms in the Russian language in the field of information security. *World of Science. Series: Sociology, Philology, Cultural Studies*. 2026;17(2): 44FLSK226. Available at: https://sfk-mn.ru/PDF/44FLSK226.pdf. DOI: 10.15862/44FLSK226. (In Russ., abstract in Eng.).

УДК 81'25, 81'373.45

Хахалева Анастасия Юрьевна
ФГБОУ ВО «Московский государственный лингвистический университет», Москва, Россия
Институт информационных наук
Доцент кафедры «Лингвистики и профессиональной коммуникации в области информационных наук»
Кандидат филологических наук
E-mail: mglu04@mail.ru
ORCID: https://orcid.org/0000-0002-1699-4252
РИНЦ: https://elibrary.ru/author_profile.asp?id=766259

Романова Мария Валерьевна
ФГБОУ ВО «Московский государственный лингвистический университет», Москва, Россия
Заведующий кафедрой «Лингвистики и профессиональной коммуникации в области информационных наук»
Кандидат педагогических наук, доцент
E-mail: rmw80@mail.ru
ORCID: https://orcid.org/0000-0002-5192-5009
РИНЦ: https://elibrary.ru/author_profile.asp?id=665008

Особенности использования англицизмов в русском языке в сфере информационной безопасности

Аннотация. Целью исследования является изучение особенностей использования терминов в формате заимствований в дискурсе информационной безопасности. В работе использованы методы сплошной выборки и контекстуального анализа. Материалом исследования являются профессиональные публикации по теме информационной безопасности и тексты выступлений в рамках профессиональных видеоконференций. В статье подчеркивается, что особая значимость вопроса использования терминологии при переводе научных и технических текстов в узкоспециализированных областях обусловлена тем, что точность передачи терминов определяет корректность передачи смысла, а неверное использование термина может привести к ошибкам в интерпретации научных данных и результатов. Авторами рассматриваются основные способы передачи англицизмов в русском языке (транскрибция, транслитерация, калька и т. д.), а также пути проникновения терминов в смежные области дискурса, что приводит к закреплению терминов в виде англицизмов в русскоязычной традиции. В результате исследования авторы приходят к выводу, что использование англицизмов в профессиональном дискурсе информационной безопасности может считаться нормой, так как служит удобству

профессионалов. Однако проникновение заимствований в смежные области институционального дискурса информационной безопасности может вызывать определенные сложности, например, связанные с благозвучностью термина, его ассимиляцией в русском языке, перегруженностью речи англицизмами и т. д., в связи с чем требуется введение унифицированных правил их употребления в данной сфере.

Ключевые слова: англицизм; заимствование; информационная безопасность; терминология; дискурс; калька; норма

Введение

Активное развитие технологий приводит к появлению в русском языке большого количества новых терминов из сферы цифровой трансформации, искусственного интеллекта, информационной безопасности (ИБ) и др. Функционирование данных терминов в русском языке вызывает широкий интерес исследователей, например, М. Р. Мироновой [1], О. В. Шурлиной [2], В. И. Велижаниной, С. В. Шешуковой [3] и др. В частности, возникает вопрос о целесообразности закрепления определенных вариантов, возникающих в языке для наименования реалий из данных областей, в том числе, в виде заимствований из английского языка как наиболее употребительных (в качестве нормы) в русскоязычной традиции.

Процесс перевода определяется как «трансформация текста на одном языке в текст на другом языке» [4, с. 5]. Особенности этого процесса определяются наличием у языковых единиц плана выражения и плана содержания, при этом у единиц из разных языков совпадение в плане содержания является частичным. При этом перевод подразумевает сохранение неизменного плана содержания, т. е. значения [4]. Отмечается, что «текст перевода никогда не может быть полным и абсолютным эквивалентом текста подлинника; задача переводчика заключается в том, чтобы сделать эту эквивалентность как можно более полной, то есть добиваться сведения потерь до минимума, но требовать «стопроцентного» совпадения значений, выражаемых в тексте подлинника и тексте перевода, было бы абсолютно нереальным» [4, с. 10–11].

Вопрос использования терминологии при переводе научных и технических текстов в узкоспециализированных областях представляет особую значимость, поскольку точность передачи терминов определяет корректность передачи смысла, а неверное использование термина может привести к ошибкам в интерпретации данных и результатов исследований и, как следствие, к практическим ошибкам в работе специалистов [5]. В этой связи данный аспект критически важен в отношении определения терминологического минимума для специалистов в области информационной безопасности, изучающих английский язык в качестве инструмента международной профессиональной коммуникации. Системный подход с точным определением нормы перевода того или иного термина на родной язык пользователя является неотъемлемым условием формирования терминологической базы при обучении иностранному языку для специальных целей [6]. Д. С. Лотте отмечал, что термин не должен рассматриваться как простое наименование какого-либо научно-технического понятия, должен обладать определенными систематизирующими свойствами [7]. О. С. Ахманова также выделяла категорию системности, подчеркивая необходимость соотнесенности терминологической системы с системой научных понятий. По ее мнению, терминология конкретной научной области представляет собой не простую совокупность терминов, а семиологическое выражение определенной системы понятий, которая отражает соответствующее научное мировоззрение [8].

Таким образом, вопрос определения терминологического минимума и установления нормативных соответствий между иноязычным термином и его эквивалентом на родном языке непосредственно связан с проблемой переводческой эквивалентности.

Если терминология профессиональной области представляет собой системно организованную совокупность понятий, отражающую специфику научного знания, то ее передача на другой язык требует учета не только формы языковой единицы, но и сохраняемого содержания. В этой связи особую значимость приобретает перевод как процесс межъязыковой трансформации, предполагающий максимально полное сохранение значения при неизбежной неполноте соответствия между единицами разных языков.

Целью данного исследования является изучение особенностей технической терминологии, существующей в дискурсе информационной безопасности в формате англицизмов, а также возможностей регулирования использования заимствованных вариантов в данном виде дискурса при помощи различных механизмов, в том числе через систему образования.

Специфика функционирования англоязычных заимствований в русскоязычном дискурсе информационной безопасности

Учитывая актуальность проблем ИБ в свете развития технологий и стремительного увеличения количества разнообразных угроз информации, функционирование терминологического аппарата в данной сфере в русском языке заслуживает особого внимания. Многие термины, обозначающие названия угроз, а также тактик, техник и процедур защиты от них, употребляются в русском языке в форме англицизмов[1] (например, транскрибции или кальки с английского языка): *аутентификация — authentication, авторизация — authorization, бэкап — backup, вирус — virus, пентест — pentest, фишинг — phishing, инцидент — incident* и т. д.

Основными **способами вхождения англицизмов** в русскоязычный дискурс информационной безопасности можно назвать:

1. Транскрибция — передача звучания слова: *фаервол (*от англ. *firewall), бэкап (backup), апдейт (update), опенсорс (opensource).*
2. Транслитерация — передача графической формы слова без учета фонетической формы: *троян (trojan), патч (patch).*
3. Тансформация — изменение англоязычного заимствования в первую очередь для удобства произношения: *логиниться (to log in).*
4. Калькирование — буквальный перевод слова: *социальная инженерия (social engineering), уязвимость (vulnerability), песочница (sandbox), отказоустойчивость* (*fault tolerance*).
5. Трансплантация — интегрирование англицизмов в их оригинальном виде в письменную речь: *3D.*
6. Комбинированные англицизмы — сочетание нескольких из вышеперечисленных способов заимствования в одном термине: *кибебуллинг* (*cyberbulling:* транслитерация + транскрибция), *флеш-память* (*flash-memory*: транскрибция + калька) [9].

Причиной заимствования терминов могут являться отсутствие термина в русском языке, например, в случае его заимствования вместе с называемой им технологией для удобства коммуникации профессионалов и быстроты интеграции технологий в деятельность специалистов (*контейнер*[2]), стремление к экономии языковых средств (*решения*[3] — калька термина *solutions,*

[1] Англицизм — это «единица любого языкового уровня, перенесенная в русский язык, прошедшая определенную трансформацию или оставшаяся в своем оригинальном облике» [9, с. 73].

[2] Контейнер — это изолированная среда для запуска одного приложения, создаваемая средствами на уровне ядра ОС [https://www.kaspersky.ru/blog/container-security/36087/?ysclid=mnj1dtnh1q386772599] (дата обращения 15.05.2026).

[3] Решения — комплекс мер, технологий, инструментов или подходов направленных на защиту информации. Такие решения могут включать технические, организационные, правовые и другие меры.

44FLSK226
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

CI/CD pipeline — CI/CD пайплайн — вместо *конвейер непрерывной интеграции и доставки*), стремление конкретизировать / уточнить термин [10] (*фишинг* — вместо *мошенничество* — от англ. *phishing*[4]; *экосистема кибербезопасности* — вместо *компоненты системы кибербезопасности* — от англ. *cybersecurity ecosystem, вендор* — вместо *поставщик* — от англ. *vendor*).

С одной стороны, большинство таких терминов являются понятными для профессионалов и могут свободно использоваться в рамках профессионального дискурса информационной безопасности (общение специалистов на темы из общей сферы профессиональной деятельности), например, *даркнет*, *аккаунт*, *антивирус*, *прокси-сервер* и т. д. Однако из-за актуальности вопросов защиты информации такие термины неизбежно проникают в смежные области институционального дискурса информационной безопасности, в рамках которого говорящие выступают в роли представителей социальных институтов, например, в следующих ситуациях:

1. Общение в академическом контексте: конференции, круглые столы, обучение студентов по направлениям, связанным с ИБ, научные публикации (научные статьи, ВКР) и т. д.
2. Общение между специалистами в сфере ИБ и сотрудниками организации (менеджерами, руководителями и т. д.).
3. Общение между специалистами ИБ и конечными пользователями технологий (рядовые сотрудники компаний, обычные пользователи и т. д.).
4. Коммуникация представителей сферы ИБ (производители программного обеспечения, вендоры и т. д.) с клиентами (частные лица, представители организаций и т. д.).

Процесс проникновения англицизмов из профессионального дискурса специалистов ИБ в смежные области дискурса способствует закреплению терминов в виде англицизмов в русскоязычной традиции, после чего скорректировать сложившиеся правила употребления термина и укоренившийся вариант его перевода становится более сложным. При этом вариант перевода с использованием англицизмов не всегда является благозвучным, а его склонение не всегда соответствует принципам, принятым в языке (*vendor*: *вендор* (*им. п., ед. ч.*) — *ве́ндоры* или *вендора́* (*им. п., мн. ч.*), *API*: [эйпиАй] или [Апи]), при его употреблении возникают сложности с ассимиляцией, при чрезмерном насыщении речи заимствованиями может наступать ее перегруженность англицизмами, обилие терминов, заимствованных из английского языка, может осложнять деятельность неспециалистов, которые взаимодействуют с профессионалами в сфере ИБ в рабочих контекстах, переводчиков, вызывать недопонимание, осложнять вхождение в профессию молодых специалистов и т. д.

Кроме того, с 1 марта 2026 года в РФ (ФЗ № 168-ФЗ, поправки к ФЗ «О государственном языке») вводится строгий запрет на использование англицизмов и иностранных слов в рекламе, вывесках и информации для потребителей при наличии русских аналогов. Иностранные слова могут использоваться только в том случае, если они отсутствуют в русском языке, написаны кириллицей или зарегистрированы как товарные знаки. За нарушение предусмотрены штрафы.[5]

На материале профессиональных публикаций в сети интернет (блоги по информационной безопасности), а также текстов видеоконференций нами были проанализированы случаи употребления англицизмов в русском языке в профессиональном контексте ИБ. В таблице 1

[4] Фишинг — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей [https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/] (дата обращения 15.05.2026).

[5] Федеральный закон от 24.06.2025 N 168-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации". URL: https://base.garant.ru/412211046/ (дата обращения:10.03.2026).

приведены примеры англицизмов в профессиональном дискурсе ИБ: представлены следующие варианты: (1) употребление слова/выражения (термина) в речи в русскоязычном профессиональном контексте ИБ; (2) альтернативный вариант, адаптированный к русскому языку; (3) слово/ выражение на английском языке; (4) формат заимствования.

Таблица 1()

Примеры англицизмов в сфере информационной безопасности

Вариант употребления слова / термина в русском языке (англицизм)	Альтернативный вариант (адаптированный к русскому языку)	Вариант слова / предложения на английском языке (оригинал)	Формат заимствования
1. Решения из коробки	Готовые/стандартные решения	Out-of-the-box solutions	Калька
2. Фолс позитИв	Ложное/ложноположительное срабатывание	False positive	Транслитерация
3. Ханипот	Сервер для привлечения злоумышленников / приманка	Honeypot	Транскрибция
4. Оупенсорс, оупенсорсные решения	С открытым кодом (решения)	Open-source	Транслитерация
5. Кубер	Платформа для оркестрации контейнеризированных приложений	Kuber (Kubernetes)	Транлитерация
6. Докер	Платформа для контейнеризации	Docker	Транслитерация
7. EDR [идиАр]	Обнаружение угроз и реагирование на конечных точках	EDR	Транскрибция
8. SIEM [сийЭм]	Система управления информацией о безопасности и событиями безопасности	SIEM	Транслитерация
9. Mean-Time-to-Respond [Мин тайм ту респонд]	Минимальное время на реагирование	Mean time to respond	Транскрибция
10. Асэт менеджмент	Управление активами	Asset management	Транслитерация
11. Форензик(а)	Криминалистика	Forensics	Транскрибция + Трансформация (Комбинированный англицизм)
12. Методология комплайэнса	Методология обеспечения соответствия (деятельности организации) требованиям	Compliance	Транскрибция
13. Песочница	Изолированная виртуальная среда	Sandbox	Калька
14. Черный список	Список подозрительных / небезопасных ресурсов	Black list	Калька

Составлена авторами

В результате анализа в первую очередь была отмечена высокая частотность заимствований аббревиатур в сфере ИБ из английского языка в оригинальной форме с написанием латиницей: *SOC, DevSecOps, SaaS, HTML, MSSP*. Это касается не только письменного, но и устного дискурса. В устном дискурсе заимствование происходит как с сохранением англоязычного произношения (*API* [Эй пи ай]), так и с изменением / ассимиляцией в русском языке (*SIEM* [сИйэм]). Исследования подтверждают, что аббревиация англоязычных терминов в русском языке является более продуктивной, чем аббревиация русскоязычных терминов. Это может быть связано с большим количеством аббревиатур, встречающихся в документации и других текстах в сфере информационной безопасности, и необходимостью их частого использования [11].

Кроме того, нами было отмечено, что в большинстве проанализированных примеров при отсутствии русскоязычного аналога термина возможно подобрать краткий описательный вариант перевода. Очевидно, что выбор варианта перевода должен осуществляться с учетом контекста, в том числе ситуативного (экстралингвистических факторов, влияющих на процесс перевода) [12].

44FLSK226
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

При переводе важно выбирать наиболее адекватный вариант, соответствующий цели перевода, нормам принимающего языка, а также сохраняющий прагматику оригинала [13]. Однако зафиксированы случаи, когда употребление англицизма можно считать более уместным, например:

1. Русскоязычный аналог не может передать всё содержание англоязычного термина. Это может быть вызвано отсутствием самого явления/технологии в виде реалии в русскоязычной традиции, необходимостью точной и полной передачи технических характеристик/особенностей термина, чтобы избежать ошибок:

- *Вендор* — от англ. *vendor* — вместо *продавец.*
- *Архитектура приложения*[6] — от англ. *application architecture*: данный термин является ёмким, не имеет аналогов в русском языке, описательный вариант перевода в данном случае представляется громоздким.
- *Мы взяли фидЫ от других компаний*: (TI-)фиды (*threat intelligence feed*) — любые данные, которые так или иначе описывают киберугрозы или указывают на следы хакеров. В простейшем случае это индикаторы компрометации: IP-адреса, домены, ссылки на фишинговые страницы, файловые хеши.[7]
- *Атака на цепочку поставок* — от англ. *supply chain attack* — вместо *атака на систему снабжения / атака через систему поставщиков*. Метафора «цепочки поставок» передает устройство системы поставок и ее уязвимость, вызванную такой организацией.

2. Стремлением к краткости и экономии усилий, особенно при общении с профессионалами той же сферы:

- *Решения* — от англ. *solutions* — вместо *инструменты обеспечения безопасности*. Описательный перевод также не всегда является лучшим вариантом представления слова в переводящем языке (ПЯ) [12]. В данном случае термин *решения* закрепился в речи и активно используется в профессиональном контексте.

При этом каждый случай должен быть рассмотрен отдельно для адекватного выбора варианта перевода. Проанализируем примеры употребления англицизмов в контексте:

Пример 1: *При грамотном использовании **экосистемы** продуктов повышается уровень **детекта**. Просто потому что у нас есть разные продукты, которые вместе вот эти все **синергии**... У нас есть много разных продуктов. Они были от разных **вендоров** и мы решили в какой-то момент это объединить. Почему стало лучше? Потому что часто **вендора** предоставляют ещё **нативные интеграции**. Это не какие-то **костыли**. У нас сразу один продукт отправляет в другой продукт. При этом есть тот **контент**, который нужен для **детекта**. То есть тут всё не упирается в **аналитика**, который смог или не смог написать тот или иной **контент**. Это делается **by design вендором**, который понимает, зачем тот продукт существует и что он может **задетектить**. Т. е. у нас **аналитика** всё это видит. При этом **аналитик** все это понимает, потому что у нас есть **обогащение** со всей этой **инфраструктуры экосистемы**. И мы сразу видим большее количество данных. И опять же, **аналитик** сразу может понять: это что-то плохое или не что-то плохое. Это **инцидент** или мы можем дальше смотреть в **интерфейс*** (текст отрывка из видеоконференции профессионалов ИБ).

[6] Архитектура приложения — структура, в которой собраны все компоненты, а также описание их взаимодействия между собой, способов управления данными и пользовательским интерфейсом [https://practicum.yandex.ru/blog/arhitektura-mobilnogo-prilozheniya/?ysclid=mnj0qhy4ka4738078] (дата обращения 20.03.2026).

[7] Парадокс пилота: развенчиваем мифы о фидах Threat Intelligence и проверяем их качество. URL: https://habr.com/ru/companies/solarsecurity/articles/1021456/ (дата обращения 23.04.2026).

В данном отрывке из видеоинтервью встречаются англицизмы *детект* (от англ. *to detect*), *контент* (англ. *content*) — 2 случая в тексте, *инцидент*, *интерфейс*, *вендора, экосистема, синергии, костыли* (*workaround*), *обогащение* (*enrichment*), *инфраструктура, интерфейс, аналитик/аналитика*, а также словосочетания *нативные интеграции*, *by design*. Использование такого количества англицизмов можно объяснить тем, что общение осуществляется в профессиональном контексте (между профессионалами в сфере информационной безопасности, которым понятен смысл всех терминов), а также тем, что видеоконференция в данном случае имеет достаточно неформальный характер и не является научным мероприятием (это подтверждается внешним видом участников, стилем их одежды).

Однако при анализе содержания данного высказывания представляется возможным заменить некоторые из использованных терминов на русскоязычные (в т. ч. описательные) аналоги. Так, слово *детект*, а также однокоренное *задетектить* (англ. *to detect*) может быть без потери смысла заменено на термин *обнаружение/обнаружить*; слово *инцидент* также возможно заменить словом *атака* или *нарушение безопасности*. Это позволит избежать перегруженности высказывания англоязычными заимствованиями.

При этом в данном контексте слово *контент* подразумевает *данные, которые необходимо проанализировать для обнаружения угроз (файлы, трафик, логи, сообщения и т. д.)*. Данный англицизм можно считать более подходящим вариантом, поскольку он является емким и содержательным. То же можно сказать относительно словосочетания *нативные интеграции*.[8]

Анализ данного примера указывает на то, что необходимо находить баланс между удобством использования термина и его благозвучием в русском зыке.

Пример 2: *Для чего же всё-таки нужны **honeypot'ы**? Гайд по установке T-pot.*

*Цель **honeypot** в работе ЦМР — навлечь на себя атаку или несанкционированное исследование. Такое средство позволяет изучить стратегию злоумышленника и определить, каким образом могут быть нанесены удары по реально существующим объектам безопасности.*

*«Лаборатория Касперского» в 2018 году запустила систему из 50 **ханипотов** для анализа атак злоумышленников. За час сеть из **ловушек** регистрировала около 80 тыс. зараженный сессий. Помимо обычных **ханипотов**, прослушивающих конкретные порты, они также создали многопортовый **ханипот**, который получил название **uberpot**. Идея проста: **ханипот** прослушивает все порты TCP и UDP, принимает подключения и протоколирует полученные данные и метаинформацию*[9] (статья на сайте Habr).

В приведенном выше примере отмечается отсутствие единообразия в использовании заимствованного термина. Слово *honeypot* встречается (1) с написанием латиницей без склонения (*honeypot,* производное *uberpot*), (2) с написанием латиницей и использованием окончания множественного числа *ы* после апострофа (*honeypot'ы*), (3) с написанием кириллицей транскрибированного заимствования, склоняемого по правилам русского языка (*ханипот — ханипотов*), (4) в формате русскоязычного аналога — *ловушка*. Представляется, что наиболее удачным в данном контексте будет выбор единого варианта употребления заимствованного термина.

[8] Нативная интеграция — это метод, позволяющий различным приложениям и системам взаимодействовать друг с другом естественным образом без необходимости использования дополнительных надстроек или посредников [https://tobiz.net/support/klyuchevye-aspekty-nativnoy-integracii/] (дата обращения: 15.05.2026).

[9] Для чего же всё таки нужны honeypot'ы? Гайд по установке T-pot. URL: https://habr.com/ru/articles/597871/ (дата обращения: 16.05.2026).

Рекомендации по результатам анализа англицизмов в русскоязычном дискурсе ИБ

В результате исследования мы пришли к выводу о том, что вопрос употребления англицизмов в русском языке требует контроля и принятия определенных мер, в частности:

1. Установление единых правил в отношении употребления отдельных видов терминов, например, закрепить правило употребления аббревиатур в письменной речи с написанием на латинице с сохранением англоязычной формы: *SOAR, SIEM, XDR, IP-адрес* и т. д.

2. Закрепление, в т. ч. в словарях, грамматических справочниках, особенностей употребления, в частности, склонения терминов в русском языке: *хостЫ (host)*: например, «Англо-русский толковый словарь по информационной безопасности» Э. М. Пройдаков, Л. А. Теплицкий, 2020 г.[10] и др.:

hacking — 1. неавторизованный доступ [к компьютерным данным], проникновение [в систему], взлом программ, *разг.* хакерство # один из рисков ИБ — требует разнообразных мер защиты и обеспечения безопасности систем и данных (см. также *attack, cybersecurity risks, data security, hacker, hacking spike, hacking techniques, hacking tool, threat*); 2. *проф.* хакинг, хакерство;

blacklist (*также* **black list**) — чёрный список;

blacklisting — технология «чёрных списков» # в ИБ — *1*. определение списка ресурсов, объектов, систем, хостов, приложений, которые считаются подозрительными, непроверенными и небезопасными для общения, обмена данными, сообщениями и др. Одно из средств борьбы со спамом заключается в составлении и ведении списков *DNS* подозрительных серверов (*DNSBL*), почта от которых блокируется. Метод не эффективен, так как спам в настоящее время чаще всего рассылается с «зомбированных» компьютеров, находящихся в самых разных частях планеты; *2*. обнаружение, идентификация и перечисление программ, не авторизованных для выполнения на данной компьютерной системе; *3*. выявление опасных веб-сайтов (см. также *blacklist, greylisting, whitelisting*);

false positive (**FP**) — 1. ошибочный допуск [к системе]; ложно положительная [аутентификация, идентификация] # в ИБ — ситуация, когда средства биометрической аутентификации (биометрические, двухфакторные или иные) идентифицируют атакующего, злоумышленника или просто случайного человека как зарегистрированного пользователя и ошибочно разрешают ему доступ к ресурсам и данным компьютерной системы и сети, что является серьёзным нарушением информационной безопасности (ср. *false negative*; см. также *authentication, biometric identification, FAR, identification system*); 2. ложно положительный # ошибочный результат работы программы (приложения, системы), воспринимаемый как правильный. Например, false positive alerts — ложные положительные предупреждения (см. также *false-positive result*).

file sandboxing — проверка файла (файлов) в песочнице # в ИБ — анализ поведения неизвестных (подозрительных) файлов с соблюдением максимальных мер безопасности в изолированной защищённой среде (см. также *sandbox*).

3. Предпочтение (в словарях и справочниках) русскоязычному ассимилированному варианту при наличии равнозначных русскоязычных вариантов: *точки входа / портЫ, ложноположительное срабатывание / фолспозитив, обращение в службу поддержки / тикеты, ошибка в системе (программе) / баг, менеджмент активов / áсэт менеджмен, методология соответствия требованиям регуляторов / методология комплайенса*;

[10]Фрагмент первого издания «Англо-русского толкового словаря по информационной безопасности» Э. М. Пройдаков, Л. А. Теплицкий, 2020 г. URL: https://www.infosystems.ru/library/glossary/slovar-terminov-po-informatsionnoy-bezopasnosti/ (дата обращения: 16.05.2026).

4. Использование различных онлайн и офлайн мероприятий, в том числе конференций, круглых столов, а также официальных публикаций и форумов, для того чтобы дать участникам, особенно молодым специалистам, представление о приоритетном способе употребления терминов: формулировать основные требования к докладам, тезисам, научным статьям, сообщениям и презентациям в отношении употребления в них англоязычных терминов, выступать в качестве примера, образца для подражания (во время приветственного слова, выступления руководителей на пленарном заседании) и т. д.

5. Выявленная специфика функционирования англоязычных заимствований в русскоязычном дискурсе информационной безопасности закономерно актуализирует вопрос о формировании терминологической и переводческой компетенции специалистов, изучающих иностранный язык специальности. Поскольку в данной профессиональной сфере значительная часть понятий репрезентируется посредством англицизмов, транскрибированных, транслитерированных или подвергнутых различным видам адаптации, будущий специалист должен обладать не только знанием соответствующих лексических единиц, но и способностью адекватно соотносить их форму, значение и коммуникативную функцию. Это означает, что работа с терминологией в сфере информационной безопасности требует развития переводческой компетенции на нескольких взаимосвязанных уровнях, каждый из которых предполагает различную степень глубины владения материалом. В частности, на *базовом уровне* необходимо сформировать умение распознавать англоязычные заимствования в профессиональном тексте, устанавливать их связь с исходной единицей и понимать механизм их вхождения в русский язык [14]. Данный уровень включает знание основных способов адаптации терминов, таких как транскрипция, транслитерация и семантическая трансформация, а также понимание того, что одна и та же единица может функционировать в разных графических и морфологических вариантах. Для специалиста это особенно важно, поскольку в текстах по информационной безопасности заимствованные термины нередко выступают в форме, максимально приближенной к английскому оригиналу, и их корректная интерпретация непосредственно влияет на точность профессионального понимания [15].

Заключение

В русскоязычном дискурсе информационной безопасности присутствует большое количество терминов, заимствованных из английского языка. Они позволяют экономить усилия, а также дают возможность конкретизировать термин в профессиональном контексте. Однако в случае проникновения терминов из дискурса профессионального общения в другие сферы дискурса, закрепление данных терминов в языке может иметь негативные последствия. Для защиты и сохранения чистоты русского языка необходимо принимать определенные меры, в том числе пояснять обучающимся направлений ИБ принципы правильного использования англоязычных терминов в речи. Важно, чтобы обучающиеся понимали, что использование кальки / транскрибции / транслитерации англоязычного термина в русском языке не всегда является маркером профессионализма специалиста. Корректное употребление терминов способствует формированию образа профессионала в своей сфере деятельности.

Вместе с тем формирование терминологической компетенции у специалистов, изучающих иностранный язык специальности, должно строиться как поэтапный процесс, направленный на развитие умения распознавать, интерпретировать, переводить и нормативно использовать англоязычные термины в профессиональном дискурсе. Такая компетенция предполагает не только знание лексики, но и владение переводческими стратегиями, обеспечивающими точность, адекватность и функциональную целесообразность терминологического выбора.

Именно поэтому обучение иностранному языку в профессионально ориентированном контексте должно быть нацелено на формирование глубокой терминологической осведомленности и устойчивых навыков работы с англоязычными заимствованиями в области информационной безопасности.

Перспективы дальнейшего исследования могут быть связаны с расширением эмпирической базы за счет анализа не только профессиональных интернет-публикаций и видеоконференций, но и нормативных документов, учебных материалов, форумов специалистов, а также устной коммуникации в рабочей среде. В дальнейшем представляется актуальной работа по систематизации и классификации словарных единиц, заимствованных из других языков, а также изучение динамики закрепления англоязычных заимствований в русском языке информационной безопасности, выявив, какие из них постепенно переходят из профессионального жаргона в общеупотребительную лексику. Особый интерес представляет разработка практических рекомендаций для переводчиков, преподавателей и специалистов по информационной безопасности, направленных на унификацию терминологии, выбор нормативных вариантов и формирование устойчивой переводческой компетенции.

ЛИТЕРАТУРА

1. Миронова, М. Р. Структурные модели терминов по информационной безопасности / М. Р. Миронова // Известия Волгоградского государственного педагогического университета. — 2021. — № 1(154). — С. 160–164. — EDN MDVBIO.
2. Шурлина, О. В. Английские и русские термины сферы информационных технологий: сопоставительный аспект (на материале терминологической базы данных компании «Майкрософт») / О. В. Шурлина // Исследования языка и современное гуманитарное знание. — 2024. — Т. 6, № 1. — С. 45–53. — DOI 10.33910/2686-830X-2024-6-1-45-53. — EDN XFMWGS.
3. Велижанина, В. И. Проблема перевода терминов сферы информационных технологий с английского языка на русский / В. И. Велижанина, С. В. Шешукова // Проблемы инженерного и социально-экономического образования в техническом вузе в условиях модернизации высшего образования: Материалы Международной научно-практической конференции, Тюмень, 20–21 мая 2021 года. — Тюмень: Тюменский индустриальный университет, 2021. — С. 165–169. — EDN TNLLSR.
4. Бархударов, Л. С. Язык и перевод. М.: Международные отношения. — 1975. — 240 с. — URL: https://search.rsl.ru/ru/record/01006908474.
5. Волгина, М. Ю. Перевод терминов как ключевых единиц специального текста / М. Ю. Волгина // Перспективы науки и образования. — 2013. — № 6. — С. 170–175. — URL: https://cyberleninka.ru/article/n/perevod-terminov-kak-klyuchevyh-edinits-spetsialnogo-teksta (дата обращения: 23.06.2026).
6. Анисимова, А. Г. Методология отбора терминов при обучении языку для специальных целей / А. Г. Анисимова // Известия ВУЗов. Поволжский регион. Гуманитарные науки. — 2011. — № 2. — С. 98–108. — URL: https://cyberleninka.ru/article/n/metodologiya-otbora-terminov-pri-obuchenii-yazyku-dlya-spetsialnyh-tseley (дата обращения: 14.06.2026).
7. Лотте, Д. С. Вопросы заимствования и упорядочения иноязычных терминов и терминоэлементов / Д. С. Лотте; [Предисл. Т. Л. Канделаки, С. В. Гринева]. — Москва: Наука, 1982. — 149 с. — URL: https://search.rsl.ru/ru/record/01001111712.

8. Ахманова, О. С. О принципах и методах лингвистического исследования / О. С. Ахманова, Л. Н. Натан, А. И. Полторацкий, В. И. Фатющенко; Под ред. О. С. Ахмановой. — М.: МГУ. — 1966. — 184 с. — URL: https://search.rsl.ru/ru/record/01005427655.
9. Дьяков, А. И. Англицизмы: заимствование или словообразование / А. И. Дьяков // Филологические науки. Вопросы теории и практики. — 2012. — № (16). — С. 72–75. — URL: http://www.gramota.net/materials/2/2012/5/17.html (дата обращения: 10.06.2026).
10. Кочарян Ю. Г., Забусова П. А. Анализ заимствований и адаптации англицизмов в русскоязычной IT-терминологии / Ю. Г. Кочарян // Международный журнал гуманитарных и естественных наук. — 2025. — № 4-1(103). — С. 279–283. — URL: https://cyberleninka.ru/article/n/analiz-zaimstvovaniy-i-adaptatsii-anglitsizmov-v-russkoyazychnoy-it-terminologii (дата обращения: 23.06.2026).
11. Апалько, И. Ю. Продуктивность аббревиации в терминопроизводстве предметной области «Защита информации» / И. Ю. Апалько // Вестник ЧелГУ. — 2008. — № 36. — С. 9–12. — EDN KTNXNV.
12. Комиссаров, В. Н. Слово о переводе. / В. Н. Комиссаров. — М.: Международные отношения. — 1973. — 215 с.
13. Березина, Я. Н. Переводческие трансформации при переводе терминов в сфере кибербезопасности / Я. Н. Березина // Вестник ПНИПУ. –Проблемы языкознания и педагогики. — 2022. — № 1. — С. 59–67. — URL: https://cyberleninka.ru/article/n/perevodcheskie-transformatsii-pri-perevode-terminov-v-sfere-kiberbezopasnosti/viewer (дата обращения: 17.06.2026).
14. Московкин, Л. В. Теоретические источники концепции речевых навыков и умений С. Ф. Шатилова. / Л. В. Московкин // Известия Российского государственного педагогического университета имени А. И. Герцена. — 2020. — № 198. — с. 7–16. — URL: https://cyberleninka.ru/article/n/teoreticheskie-istochniki-kontseptsii-rechevyh-navykov-i-umeniy-s-f-shatilova (дата обращения: 14.06.2026).
15. Труфанова, Н. О. Лингводидактические основы формирования рецептивной терминологической компетенции на материале предметной области цифровой криминалистики / Н. О. Труфанова, К.М. Иноземцева // Гуманитарный вестник. — 2024. — № 4(108). — URL: https://cyberleninka.ru/article/n/lingvodidakticheskie-osnovy-formirovaniya-retseptivnoy-terminologicheskoy-kompetentsii-na-materiale-predmetnoy-oblasti-tsifrovoy (дата обращения: 14.06.2026).

Khakhaleva Anastasiya Yurjevna
Moscow State Linguistic University, Moscow, Russia
Institute of Information Sciences
E-mail: mglu04@mail.ru
ORCID: https://orcid.org/0000-0002-1699-4252
RSCI: https://elibrary.ru/author_profile.asp?id=766259

Romanova Maria Valerievna
Moscow State Linguistic University, Moscow, Russia
E-mail: rmw80@mail.ru
ORCID: https://orcid.org/0000-0002-5192-5009
RSCI: https://elibrary.ru/author_profile.asp?id=665008

Peculiarities of using anglicisms in the Russian language in the field of information security

Abstract. The aim of the research is to examine the features of terminology usage in the form of borrowings in the discourse of information security. The paper employs a comprehensive sampling method and contextual analysis. The material for the research consists of professional publications on the topic of information security and transcripts of speeches delivered during professional video conferences. The article emphasizes that the particular importance of the issue of using terminology when translating scientific and technical texts in highly specialized fields is due to the fact that the accuracy of the translation of terms determines the correctness of the transfer of meaning, and incorrect use of a term can lead to errors in the interpretation of scientific data and results. The authors examine the main ways of transmitting Anglicisms in English (transcription, transliteration, tracing, etc.), as well as ways of penetration of terms into the adjacent areas of discourse, which, in turn, leads to the consolidation of terms in the form of anglicisms in the Russian-language tradition. As a result of the study, the authors conclude that the use of anglicisms in the professional discourse of information security can be considered normative, as it facilitates the work of professionals. However, the penetration of borrowings into the related areas of the institutional discourse of information security may pose certain challenges, connected to the the euphony of the term, its assimilation in the Russian language, the overload of speech with anglicisms, etc., necessitating the introduction of standardized rules for their usage in this field.

Keywords: anglicism; borrowing; information security; terminology; discourse; calque; norm