ЯЗЫК. КУЛЬТУРА. ОБЩЕСТВО

УДК 811.111’276.6:004.056
doi 10.17072/2073-6681-2026-2-7-17
EDN OOIUQV
https://elibrary.ru/ooiuqv

Особенности англоязычных терминов семантического поля «Информационная безопасность»

Балашова Анна Юрьевна
Российский университет транспорта
Московский городской университет управления Правительства Москвы имени Ю. М. Лужкова
a.hatyushina@yandex.ru

Сорокина Эльвира Анатольевна
Российский университет транспорта
Государственный университет просвещения
ellasor@mail.ru

Аннотация. В условиях стремительного развития цифровых технологий и повышения геополитической значимости кибербезопасности возрастает потребность в системном лингвистическом описании специализированной терминологии, а также в обеспечении качества перевода англоязычных терминов в русскоязычное профессиональное поле. В статье проводится анализ структурных моделей, механизмов словообразования и проявлений полисемии в англоязычной терминологии информационной безопасности. Исследование основано на корпусе из 987 терминологических единиц, отобранных методом сплошной выборки из авторитетных источников (глоссарии Texas State University, NIST, Cybersecurity Handbook, Heimdalsecurity.com и др.). Применены количественный, описательный и аналитический методы. Установлено, что 66,9 % терминов – полилексемные (преимущественно двух- и трехкомпонентные), построенные по моделям N + N и Adj. + Noun. Среди монолексем (33,1 %) доминируют аббревиатуры (28,7 %) и сложные слова (23,8 %). Выявлены тенденции к номинализации и повышению точности за счет увеличения числа компонентов. Подтверждено наличие полисемии – радиальной (*bug*) и цепочечной (*key*), а также активное использование метафорического (*sandbox, honeypot, kill chain*) и метонимического (*bot, zero-day*) переноса, что опровергает традиционный тезис о моносемии термина. Терминология информационной безопасности представляет собой динамично развивающуюся систему, характеризующуюся высокой продуктивностью словообразовательных моделей и семантической пластичностью. Результаты могут быть использованы при преподавании английского языка для специальных целей (ESP), в переводоведении и при разработке терминографических баз данных.

Ключевые слова: информационная безопасность; терминология; лексико-семантические особенности; структура терминов; полисемия; словообразование; аббревиация; метафорический перенос.

Для цитирования
Балашова А. Ю., Сорокина Э. А. Особенности англоязычных терминов семантического поля «Информационная безопасность» // Вестник Пермского университета. Российская и зарубежная филология. 2026. Т. 18, вып. 2. С. 7–17. doi 10.17072/2073-6681-2026-2-7-17. EDN OOIUQV

Features of English-Language Terms in the Semantic Field “Information Security”

Anna Yu. Balashova
Russian University of Transport
Moscow Metropolitan Governance Yury Luzhkov University
a.hatyushina@yandex.ru

Elvira A. Sorokina
Russian University of Transport
The State University of Education
ellasor@mail.ru

Abstract. In the context of rapid digital transformation and the growing geopolitical significance of cybersecurity, there is an increasing demand for a systematic linguistic description of specialized terminology, as well as for ensuring the quality of translation of English-language terms into the Russian professional domain. This study aims to identify and analyze structural patterns, word-formation mechanisms, and manifestations of polysemy in English information security terminology. The research is based on a comprehensive corpus of 987 terminological units collected via continuous sampling from authoritative sources, including the Texas State University’s Information Security Glossary, NIST Cybersecurity Framework, Greece's Cybersecurity Handbook, and Heimdalsecurity.com. Quantitative, descriptive, and analytical methods were employed to examine the lexical and semantic features of the selected terms. The findings reveal that 66.9 % of the terms are polylexemic, predominantly two- and three-component constructions following N + N and Adj. + Noun models, which reflects a tendency toward increased terminological precision through multi-component structures. Among monolexemic terms (33.1 %), abbreviations (28.7 %) and compounds (23.8 %) prevail, demonstrating high productivity of abbreviation and compounding processes. The analysis confirms the presence of polysemy in both radial (e.g., bug) and chain (e.g., key) forms. Furthermore, metaphorical transfer (sandbox, honeypot, kill chain) and metonymy (bot, zero-day) are widely used, challenging the traditional assumption of terminological monosemy. Information security terminology represents a dynamic, evolving system characterized by high productivity in word formation and semantic flexibility. The results of this study can be applied in teaching English for Specific Purposes (ESP), translation studies, and the development of terminographic databases, contributing to improved cross-linguistic communication in the field of cybersecurity.

Keywords: information security; terminology; lexical and semantic features; term structure; polysemy; word formation; abbreviation; metaphorical transfer.

For citation
Balashova A. Yu., Sorokina E. A. Features of English-Language Terms in the Semantic Field “Information Security”. *Perm University Herald. Russian and Foreign Philology*, 2026, vol. 18, issue 2, pp. 7–17. doi 10.17072/2073-6681-2026-2-7-17. EDN OOIUQV (In Russ.)

Введение

Известно, что специальная лексика является важнейшим компонентом научно-технического дискурса, обеспечивая точность, однозначность и эффективность коммуникации в профессиональной среде. В условиях стремительного развития цифровых технологий и усиления геополитических вызовов в сфере киберпространства терминология информационной безопасности (*information security*) приобретает всё большее значение как объект лингвистического исследования.

Понятие «информационная безопасность» традиционно трактуется как защита информации от несанкционированного доступа, использования, раскрытия, нарушения целостности или отказа в обслуживании. В Российской Федерации концепция информационной безопасности закреплена в Доктрине 2024 г. как защита национальных интересов в информационной сфере [Доктрина информационной безопасности… 2024]. По мнению Г. Г. Феоктистова, она предполагает возможность получения сведений о действиях конкурентов при минимальной утечке

собственной информации [Феоктистов 1996: 211]. В то же время А. Д. Урсул определяет ее как состояние защищенности ключевых сфер жизнедеятельности от вредоносных информационных воздействий [Урсул 2006: 7]. Развитие вычислительной техники, особенно в военной и коммерческой сферах, потребовало создания новых механизмов защиты данных. Как заметили исследователи, если в 1940-х гг. шифровальная машина «Энигма» стала символом криптографии, то с 1980-х гг. рост числа персональных компьютеров и сетей привел к эскалации киберугроз – от кибершпионажа до кибертерроризма [Кураков Л. П., Кураков В. Л. 2024: 607].

Будучи синонимом термину «информационная безопасность», термин «кибербезопасность» (*cybersecurity*) вошел в широкое употребление в конце XX в. [Филонов 2022: 131]. Интересным фактом является то, что корень *cyber-*, восходящий к греческому *kybernetes* («кормчий»), был использован Норбертом Винером в 1948 г. для создания названия новой науки – *кибернетики*. За очень короткое время данный корень стал функционировать в качестве префиксоида во многих терминах: *cyberspace* (1982), *cyberpunk* (1986). К 1994 г. в английском языке уже насчитывалось более 100 слов с этим префиксом [Online Etymology Dictionary].

Следует заметить, что термины «кибербезопасность» и «информационная безопасность» характеризуются одновременно и семантической близостью, что делает их синонимами, и наличием отличительных семантических смыслов, что отделяет их друг от друга. Решение вопроса о предпочтительности одного из терминов (в русском языке «кибербезопасность» или «информационная безопасность», в английском языке – *cybersecurity* или *information security*) зависит от контекста: научного, нормативно-правового, технического или повседневного употребления.

Считаем, что термин *Information Security (InfoSec)* обозначает более широкое понятие, охватывающее все аспекты защиты информации, независимо от ее формы: бумажные документы; устная информация; данные на цифровых носителях, что согласуется со стандартом ISO/IEC 27000: *Preservation of confidentiality, integrity and availability of information* (Сохранение конфиденциальности, целостности и доступности информации) [Macak 2020]. *Cybersecurity* – подмножество *InfoSec*, относится исключительно к защите цифровой информации, передаваемой или хранимой в компьютерных системах и сетях. По определению NIST (National Institute of Standards and Technology): *The ability to protect or defend the use of cyberspace from cyberattacks* (Способность защищать или обеспечивать защиту использования киберпространства от кибератак) [Global Knowledge. Skillsoft 2025]. Следовательно, термин *Information Security* может считаться центром (ядром, ядерным термином) лексико-семантического поля «информационная безопасность» (родовым термином, гиперонимом), а термин *Cybersecurity* функционирует в названном поле в качестве гипонима.

Объектом нашего исследования является формирующаяся терминосистема «информационная безопасность» (*Information Security*) в английском языке.

Предметом анализа послужили лексико-семантические и формально-структурные особенности терминов, включая процессы морфологического и неморфологического словообразования, а также типы семантической многозначности.

Цель работы – выявление и анализ структурных моделей, механизмов словообразования и проявлений полисемии в англоязычной терминологии информационной безопасности.

Заметим, что в современной лингвистике (в частности, в переводоведении и терминоведении) наблюдается повышенный интерес к терминологиям новых наук, к появлению и закреплению новых терминов (в том числе заимствованных), остро ощущается потребность в системном анализе семантического объема и валентностных свойств англоязычных терминов. Как отмечают Л. Я. Долгоновская [Долгоновская 2023] и М. Р. Миронова [Миронова 2021], терминосистемы динамично развивающихся областей демонстрируют уникальные словообразовательные и семантические паттерны, требующие детального описания.

Этим и определяется степень **актуальности** проводимого исследования, поскольку анализ терминов кибербезопасности обусловлен необходимостью лингвистического осмысления процессов формирования и функционирования терминологической системы информационной безопасности.

В качестве рабочего инструмента использованы такие методы, как сплошная выборка (сбор всех терминов, соответствующих тематике, из заранее определенных источников), количественный анализ (подсчет частотности структурных типов и способов образования), описательный метод (характеристика словообразовательных моделей и семантических трансформаций), аналитический метод (интерпретация данных с опорой на теорию терминоведения и лексической семантики).

Новизна исследования состоит в применении комплексного подхода к анализу терминологии кибербезопасности: языковым материалом послужили 987 английских слов, функционирую-

щих в сфере информационной безопасности в английской лингвокультуре; впервые проведен анализ структуры лексем и дана количественная оценка соотношения монолексемных и полилексемных единиц; впервые предпринята попытка систематизирования словообразовательных моделей терминов-неологизмов; при использовании этимологических словарей (OED, Etymonline) и корпусных данных впервые осуществлен анализ семантических отношений английских терминов, относящихся к молодой английской терминологии «информационная безопасность», являющейся еще не вполне сформировавшейся.

Считаем, что некоторые наблюдения и результаты анализа могут рассматриваться как определенный вклад в дополнение и расширение имеющихся в современном терминоведении знаний о молодых развивающихся терминологиях, чем может быть определена ***теоретическая значимость*** проведенного исследования.

Практическая значимость заключается в том, что теоретические материалы и результаты анализа языкового материала могут быть востребованы в вузовской деятельности (особенно в технических вузах) для создания учебных материалов по английскому языку для специальных целей (ESP), а также в усовершенствовании описаний заимствованных из английского языка терминов в современной русской терминографии.

Методология исследования

Языковым материалом для исследования послужили терминологические единицы, отобранные из следующих источников:

– Texas State University Information Security Glossary – официальный глоссарий университета, содержащий стандартизированные определения [Information Security Glossary: Texas State University];

– Cybersecurity Handbook (Ministry of Digital Governance, Greece, 2021) – национальное руководство по защите информационных систем [Ministry of Digital Governance, Hellenic Republic. Cybersecurity Handbook];

– Heimdalsecurity.com – аналитические материалы по киберугрозам и защите [Heimdalsecurity. Unified Cybersecurity];

– Globalknowledge.com – образовательные ресурсы по IT-безопасности [Global Knowledge. Skillsoft];

– NIST Cybersecurity Framework – стандарты США по управлению киберрисками [NIST Cybersecurity Framework].

Поскольку терминология *Information Security (InfoSec)* в настоящее время стремительно развивается, считаем важным подчеркнуть временные рамки, когда производился отбор: все термины, относящиеся к сфере информационной безопасности, фиксировались в течение трех месяцев (март–май 2025 г.). В результате отбора получено 987 терминологических единиц.

Для проверки адекватности перевода и эквивалентов использовались источники:

– Парошин А. А. Информационная безопасность: стандартизированные термины и понятия [Парошин 2010];

– Пройдаков Е. М., Теплицкий Ю. А. Англо-русский толковый словарь по информационной безопасности [Пройдаков, Теплицкий 2022];

– roskiber.ru – платформа Роскибербезопасности [Роскибербезопасность].

Анализ структуры терминов

На начальном этапе исследований новых терминологий традиционно проводится анализ структуры терминов. Весь массив (987 лексем) собранного языкового материала был расклассифицирован на монолексемные (327 монолексемных, что составляет 33,1 % от общего количества) и полилексемные (660 полилексемных терминов, что составляет 66,9 % от общего количества).

Анализ 327 монолексемных терминов информационной безопасности выявил доминирующие способы словообразования. Результаты представлены в табл. 1.

При анализе словообразовательных процессов, участвовавших в создании терминов *Information Security (InfoSec)*, и полученных количественных показателей можно сделать вывод о том, что преобладают процессы сокращения языковых средств и процессы сложения: более половины всех терминов (172 из 327 монолексемных единиц) составляют аббревиатуры и сложные слова-термины, что может свидетельствовать в пользу стремления к краткости и экспрессивности создаваемого термина. Анализ монолексемных терминов показал, что основными способами словообразования являются морфологические, включая суффиксальный, префиксальный, префиксально-суффиксальный, основосложение, аббревиацию и конверсию.

Таблица 1 / Table 1

Морфологические способы словообразования

Morphological means of word formation

Способ словообразования	Примеры терминов	Перевод/толкование	Общее количество
Аббревиация	VPN (Virtual Private Network); AES (Advanced Encryption Standard); TLS (Transport Layer Security); IoT (Internet of Things); CA (Certificate Authority); EoP (Exchange Online Protection); FDE (Full Disk Encryption); HSM (Hardware Security Module); IPSec (Internet Protocol Security); KMS (Key Management Service)	Виртуальная частная сеть; Стандарт расширенного шифрования; Безопасность на транспортном уровне; Интернет вещей; Удостоверяющий центр; Защита Exchange Online; Полное шифрование диска; Аппаратный модуль безопасности; Протокол безопасности IP; Служба управления ключами	**94 (28.7%)**
Основосложение	Firewall; Spyware; Malware; Honeypot; Botnet; Sandbox; Phishing; Backdoor; Zero-day; Kill chain	Брандмауэр; Шпионское ПО; Вредоносное ПО; Ловушка для хакеров; Ботнет; Песочница; Фишинг; Бэкдор; Уязвимость «в день ноль», то есть отсутствие информации о сбое в работе программного обеспечения; Цепочка кибератак	**78 (23,8 %)**
Префиксально-суффиксальный	Cybersecurity; Unpatched; Reauthenticated; Misconfigured; Overwrite; Underprotected	Кибербезопасность; Необновлённый; Повторно аутентифицированный; Неправильно настроенный; Перезапись; Недостаточно защищенный	**62 (18,9 %)**
Суффиксальный	Phishing; Encryption; Authenticator; Logging; Detection; Monitoring	Фишинг; Шифрование; Устройство аутентификации; Ведение логов; Обнаружение; Мониторинг	**48 (14,7 %)**
Префиксальный	Cyberspace; Metadata; Overwrite; Subdomain Pre-authentication	Киберпространство; Метаданные; Перезапись; Поддомен; Предварительная аутентификация	**35 (10,7 %)**
Конверсия	Log (n.) → to log (v.); Spam (n.) → to spam (v.); Patch (n.) → to patch (v.)	Запись → регистрировать; Спам → рассылать спам; Патч → обновлять	**10 (3,1 %)**

Лексико-семантический и морфолого-синтксический способы терминообразования проявили себя в создании 70 терминов. Известно, что конверсия представляет собой морфолого-синтаксический способ создания новых лексических единиц путем перехода слова из одной части речи в другую, например, слово *log* может функционировать в качестве имени существительного в значении «регистрация» и в качестве глагола в значении действия («регистрироваться»).

Примером лексико-семантического преобразования слова может служить термин *exploit*, первоначальным значением которого было «подвиг, деяние», а с развитием информационных технологий данное слово стало употребляться злоумышленниками и приобрело значение «программа или код для совершения нелегитимных действий, связанных с кражей информации».

Полилексемные термины

Из 660 полилексемных терминов наиболее распространены двух- и трехкомпонентные конструкции. Результаты их анализа представлены в табл. 2.

Таблица 2 / Table 2

Классификация полилексемных терминов по количеству компонентов, входящих в их состав

Classification of polylexemic terms by the number of components they contain

Количество элементов	Примеры	Общее количество
2	Threat Actor (Лицо или группа, ответственные за кибератаки) Data Breach (Утечка данных) Zero Trust (Модель нулевого доверия) Attack Surface (Поверхность атаки) Shadow IT (Теневой IT (теневые информационные технологии))	**48,5 %**
3	Secure Operating System (Безопасная операционная система) Multi-Factor Authentication (Многофакторная аутентификация) Public Key Infrastructure (Инфраструктура открытых ключей) Real-time Monitoring (Мониторинг в реальном времени) File Integrity Check (Проверка целостности файлов)	**35,6 %**
4+	Cyber Information Sharing and Collaboration Program (Программа обмена информацией и сотрудничества в области кибербезопасности) Advanced Persistent Threat Actor (Атакующий с продвинутыми постоянными угрозами (продвинутая постоянно действующая угроза)) Encrypted File Transfer Protocol (Протокол зашифрованной передачи файлов)	**15,9 %**

Доминирующие структурные модели:

Noun + Noun:

– *data breach* – несанкционированный доступ к конфиденциальной информации, приводящий к ее раскрытию или краже;

– *threat actor* – субъект угрозы, лицо или группа (например, хакер, киберпреступная организация, государственный актор), которая инициирует кибератаку;

– *security audit* – аудит безопасности. Систематическая проверка мер защиты информационных систем для оценки их эффективности и соответствия стандартам;

– *identity provider (IdP)* – поставщик удостоверяющих данных / провайдер идентификации. Сервис или система, которая подтверждает личность пользователя при входе в приложения (например, Google, Microsoft в рамках SSO);

– *network access control (Data breach)* – утечка данных;

– *Network access control (NAC)* – контроль сетевого доступа. Технология, позволяющая ограничивать доступ к корпоративной сети на основе политик безопасности, например, типа устройства или статуса его обновлений.

Adjective + Noun:

– *Secure system – безопасная система.* Система, защищенная от несанкционированного доступа, атак и уязвимостей., encrypted data, digital footprint, untrusted source, critical infrastructure;

– *encrypted data – зашифрованные данные*. Данные, преобразованные с помощью криптографических методов для обеспечения конфиденциальности;

– *digital footprint* – цифровой след. Совокупность данных, оставляемых пользователем в ин-

тернете и цифровых системах (история поиска, публикации, метаданные и т. д.);

– *untrusted source* – недоверенный источник. Источник информации, программного обеспечения или подключения, которому система или пользователь не доверяют из соображений безопасности;

– *critical infrastructure* – критическая инфраструктура. Объекты и системы жизненной важности (например, энергетика, связь, здравоохранение), отказ которых может повлечь серьезные последствия для общества и государства [Information Security Glossary 2025].

Исследование полилексемных терминов информационной безопасности подтверждает тенденцию к номинализации – преобразованию синтаксических конструкций в именные группы, характерному для научного стиля.

К вопросу о полисемии в терминологии

Вопрос о полисемии термина является предметом дискуссий среди лингвистов. Ранее одним из наиболее важных признаков терминологической единицы рассматривалась ее моносемия; так, Н. В. Васильева отмечает стремление термина к однозначности [Васильева 2020]. Однако большинство исследователей говорят о полисемии в терминологии как об одном из неотъемлемых признаков современного термина [Польщикова 2022: 2330]. Б. Н. Головин указывает, что невозможно требовать от термина однозначности, поскольку большинство функционирующих терминологий не отвечают требованиям моносемии [Головин 1987].

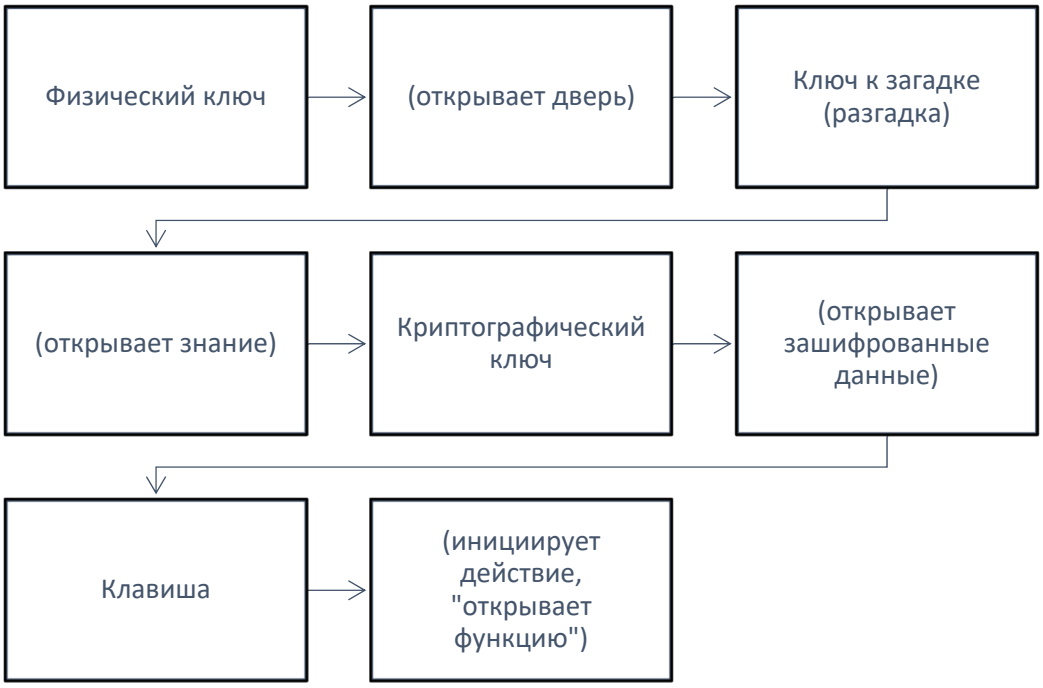
При рассмотрении полисемии в терминологии считаем необходимым отметить, что Ю. Д. Апресян выделяет радиальную (при которой все производные значения берут начало от одного исходного) и цепочечную (когда каждое новое значение формируется на основе предыдущего) разновидности полисемии. Кроме этого, ученый классифицирует еще несколько разновидностей полисемии, базирующихся на способах переноса значения (метонимическая и метафорическая разновидности полисемии) [Апресян 1995: 104].

В качестве иллюстративного примера присутствия *радиальной полисемии* в английской терминологии *Information Security (InfoSec)* рассмотрим особенности семантики термина *bug*. Первое основное значение данной лексемы «жук», однако существуют и другие (*микроб, инфекционное заболевание, потайной микрофон* и *ошибка/сбой в программе*). Термин ***bug:***

– жук (биология);
– микроб, инфекция (мед.);
– скрытый микрофон (жарг.);
– ошибка в программе (IT).

Все значения исходят от одного ядра – «что-то маленькое и нежелательное», что характерно, по Ю. Д. Апресяну, для радиального типа [там же: 95].

Примером *цепочечной полисемии* может выступать термин *key* со значением «ключ», «разгадка», «символ», «клавиша». Термин ***key:*** физический ключ →ключ доступа →разгадка проблемы →символ шифрования →клавиша на клавиатуре. Для обоснования такого семантического развития можно предложить логическую схему:



Заметим, что каждое последующее значение основано на предыдущем.

Собранный языковой материал и результаты его семантического анализа позволяют утверждать, что метафорический перенос активно используется в английской терминологии информационной безопасности. В качестве иллюстративного подтверждения можно привести термин *honeypot*: дословно «горшочек с медом». А в результате терминологизации слово *honeypot* становится языковым знаком того, что на самом деле означает ловушку, то есть сервер или систему, спроектированную так, чтобы привлечь хакеров с целью изучения стратегии злоумышленников.

Слово *sandbox* («песочница») в результате специализации (или *терминологизации*) становится профессиональным термином, обозначающим систему, которая позволяет запускать ненадежные программные приложения в строго контролируемой среде с ограниченными правами доступа. В частности, приложению в «песочнице» (специально смоделированному безопасному приложению) обычно запрещен доступ к файловой системе или сети [Фадеева, Плеханов, Лопатин 2024: 609].

Также в качестве примера можно назвать словосочетание *heat map* (тепловая карта атак – визуализация интенсивности угроз, в которой значения отображаются с помощью цветовой интенсивности), что представляет собой так называемую сенсорную метафору восприятия [Разумкова 2022: 30].

В рассматриваемой английской терминологии *Information Security (InfoSec)* присутствуют термины, образованные на основе зооморфной метафоры, действием которой является перенос названия признаков животных на технические или абстрактные явления: *web crawler* («паук»), *worm* («червь»), *zombie computer* («зомби», зараженное устройство). Результатом действия географо-топологической метафоры (при которой осуществляется перенос пространственных понятий [Тиден 2019: 27]) можно считать термин *firewall* – брандмауэр: буквально «огненная стена», «защитная граница» между сетями.

Известно, что метафорические переносы упрощают понимание сложных концепций, помогая мышлению ассоциативно представить сходства далеких друг от друга предметов, действий, признаков, понятий. Вероятно, даже непрофессионалы могут представить, что такое *honeypot* или *sandbox* терминологии *Information Security (InfoSec)*, зная изначальное (или исконное) значение этих английских слов.

Присутствие разных видов метафорического переноса в терминологии подчеркивает сравнительную молодость отрасли знания и принадлежащего этой отрасли языкового словарного состава. Виды метафоры способны участвовать в формировании единого профессионального дискурса, поскольку отражают динамику развития науки: новые технологии требуют новых слов, а метафора – самый быстрый способ их создания.

Часто в общем языкознании (и в теории перевода) метонимические переносы рассматриваются как элементы проявления метафоры вообще. В нашем исследовании мы предпочли учитывать некоторые различия в понятиях «метафора» и «метонимия», поэтому и метонимические переносы рассмотрим отдельно.

Одним из самых распространенных примеров *метонимической полисемии* в английской терминологии *Information Security (InfoSec)* является термин *bot*, произведенный от *robot*. Метонимический перенос здесь основан на близости понятий, на смежности обозначаемых явлений. Изначально словом *bot* называли программу-робот, а в современном понимании термином *bot* обозначаются программы, которые автоматически выполняют задачи по указанию создателя заразившей их программы.

Более сложная ассоциативная смысловая связь присутствует в семантике таких терминов, как *zero-day* и *Patch Tuesday*, где *zero* («ноль, пустота») и *zero-day* ← день обнаружения уязвимости → сама уязвимость; *patch* («заплатка») *Tuesday* («вторник») и *Patch Tuesday* ← день выпуска обновлений → сам процесс регулярного обновления.

Полилексемный двухкомпонентный термин *kill chain* («цепочка убийств») в английской терминологии *Information Security (InfoSec)* имеет значение «последовательная череда кибератак».

Следует согласиться с мнением С. В. Гринева-Гриневича и Э. А. Сорокиной в том, что явление полисемии, присутствующей в той или иной степени в отраслевых профессиональных терминологиях, имеет свои специфические черты, способные отделять ее от полисемии в общеупотребительном языке [Гринев-Гриневич, Сорокина 2015: 62].

Заключение

Проведенное исследование позволило выявить ключевые закономерности формирования англоязычной терминологии информационной безопасности. Установлено, что преобладают полилексемные термины (66,9 %), особенно двух- и трехкомпонентные, построенные по моделям N + N и Adj. + Noun. Данная закономерность приводит к номинализации синтаксических структур, то есть к преобразованию исходных терминологических сочетаний в более сложные именные конструкции, объединяющие их с определяемым существительным [Караулин 1987: 176].

Отмечается, что увеличение длины полилексемных терминов определяется стремлением к конкретности и точности передачи информации, а также к целенаправленной однозначности, поскольку с увеличением количества элементов в терминологической единице уменьшается вероятность ее многозначности [Гринев-Гриневич 2008: 144]. Для научного стиля характерно описание понятий в рамках уже известных и разработанных концепций за счет увеличения атрибутивных элементов. Как результат наблюдается повышение частоты употребления терминологических словосочетаний и более точное отражение особенностей научного мышления в текстах тематической направленности [Чернышова, Черникова, Балашова 2025].

Результаты исследования подчеркивают то, что, как и в других терминологических системах, подавляющее большинство (86 %) полилексемных терминов состоят из стержневых слов с двух- и трехкомпонентными атрибутивными группами [Балашова 2024: 20]. Среди монолексемных терминов лидируют аббревиатуры (28,7 %) и сложные слова (23,8 %), что связано с потребностью в краткости и емкости. Наблюдается активное использование различных видов метафорического переноса (*sandbox, honeypot, kill chain*) и метонимии (*bot, zero-day, Patch Tuesday*). Подтверждается наличие полисемии, представленной в виде радиальной (*bug*) и цепочечной (*key*) моделей, что противоречит традиционному представлению о моносемии термина [Macak 2020]. Процессы номинализации и аббревиации отражают специфику научно-технического дискурса, направленного на повышение точности и эффективности коммуникации.

Следовательно, английская терминология *Information Security (InfoSec)*, являясь молодой отраслью научного знания, находится в стадии активного формирования и требует дальнейшего лингвистического изучения. Собранный языковой материал и результаты его анализа могут быть дополнением к уже имеющимся в отечественной литературе сведениям о кибербезопасности. Полученные результаты нашего научного исследования могут быть использованы в переводоведении и в преподавании английского языка, могут быть востребованными в терминографии и в разработке лингвистических учебных ресурсов.

Список литературы

Апресян Ю. Д. Избранные труды. Т. I. Лексическая семантика. М.: Восточная литература, 1995. 104 с.

Балашова А. Ю. Особенности терминологий новых наук: автореф. дис. ... канд. филол. наук. М., 2024. 24 с.

Васильева Н. В. Терминология лингвистическая // Русский язык: Энциклопедия. М.: АСТ-Пресс Школа, 2020. С. 211–216.

Головин Б. Н. Лингвистические основы учения о терминах. М.: Высшая школа, 1987. 224 с.

Гринев-Гриневич С. В. Терминоведение: учеб. пособие для студ. высш. учеб. заведений. М.: Академия, 2008. 304 с.

Гринев-Гриневич С. В., Сорокина Э. А. Полисемия в общеупотребительной и специальной лексике // Вестник Московского государственного областного университета. 2015. № 4. С. 51–64.

Долгоновская Л. Я. Сопоставительный анализ терминополя «защита» в сфере информационной безопасности (на материале английского и русского языков) // Актуальные вопросы англистики и методики преподавания русского языка как иностранного: сб. науч. ст. М., 2023. Вып. 2. С. 189–196.

Доктрина информационной безопасности Российской Федерации. Официальный интернет-портал правовой информации. 2024. URL: https://pravo.gov.ru (дата обращения: 30.11.2025).

Кураков Л. П., Кураков В. Л. Экономика и право: словарь-справочник. 2024. URL: https://dic.academic.ru (дата обращения: 30.11.2025).

Миронова М. Р. Структурные модели терминов по информационной безопасности // Известия Волгоградского государственного педагогического университета. 2021. № 1 (154). С. 160–164.

Парошин А. А. Информационная безопасность: стандартизированные термины и понятия. Владивосток: Изд-во Владивост. ун-та, 2010. 216 с.

Польщикова О. Н. Полисемия в терминологии компьютерной лингвистики // Филологические науки. Вопросы теории и практики. 2022. № 5 (7). С. 2328–2332. doi 10.30853/phil20220385

Пройдаков Е. М., Теплицкий Ю. А. Англо-русский толковый словарь по информационной безопасности. 2022. URL: https://infosystems.ru (дата обращения: 30.11.2025).

Разумкова Н. В. Лексические репрезентации сенсорных образов в лирике Осипа Мандельштама // Вестник Тюменского государственного университета. Гуманитарные исследования. Humanitates. 2022. Т. 8, № 3 (31). С. 23–44. doi 10.21684/2411-197X-2022-8-3-23-44

Роскибербезопасность. URL: https://roskiber.ru (дата обращения: 30.11.2025).

Тиден Е. В. Термины-метафоры в научной речи // Личность – Язык – Культура: материалы VII Всерос. науч.-практ. конф. Саратов: Наука, 2019. С. 129–134.

Урсул А. Д. Информационная стратегия и безопасность в концепции устойчивого развития // Научно-техническая информация. 1996. № 1. С. 7–12.

Фадеева А. А., Плеханов М. С., Лопатин Д. В. Анализ использования англоязычных терминов в области кибербезопасности // Образование и право. 2024. № 5. С. 606–611.

Феоктистов Г. Г. Информационная безопасность общества // Социально-политический журнал. 1996. № 5. С. 211–216.

Филонов А. А. Теоретические и исторические аспекты защиты информации // Вестник национального института бизнеса. 2022. № 1 (45). С. 130–140.

Чернышова Л. А., Черникова Е. О., Балашова А. Ю. Специфика формальной структуры терминологических словосочетаний в английском и немецком языках сферы высокоскоростных железнодорожных магистралей // Филологические науки. Вопросы теории и практики. 2025. № 18 (3). С. 1045–1052. doi 10.30853/phil20250151

Global Knowledge. Skillsoft. 2025. URL: https://www.globalknowledge.com (дата обращения: 30.11.2025).

Heimdalsecurity. Unified Cybersecurity Platform. 2025. URL: https://heimdalsecurity.com (дата обращения: 30.11.2025).

Information Security Office at Texas State University. Information Security Glossary.2025. URL: https://infosecurity.txst.edu/work/information-security-glossary.html (дата обращения: 30.11.2025).

Macak K. Towards a Taxonomy of Cyber Attacks // IEEE Communications Surveys & Tutorials. 2020. Vol. 22, № 2. P. 1356–1384.

Ministry of Digital Governance, Hellenic Republic. Cybersecurity Handbook. 2021. URL: https://cyber.gov.gr/wp-content/uploads/2025/03/Cybersecurity-Handbook-English-version-compressed.pdf (дата обращения: 30.11.2025).

Online Etymology Dictionary. Cyber. 2025. URL: https://www.etymonline.com (дата обращения: 30.11.2025).

NIST Cybersecurity Framework. 2025. URL: https://www.nist.gov/cyberframework (дата обращения: 30.11.2025).

References

Apresyan Yu. D. *Selected Works. Vol. I. Lexical Semantics.* Moscow, Vostochnaya literatura Publ., 1995. 104 p. (In Russ.)

Balashova A. Yu. *Specific features of terminologies of emerging sciences*. Abstract of Cand. philol. sci. diss. Moscow, 2024. 24 p. (In Russ.)

Vasil'eva N. V. Linguistic terminology. *Russian Language: An Encyclopedia*. Moscow, AST-PRESS SHKOLA Publ., 2020, pp. 211–216. (In Russ.)

Golovin B. N. *Linguistic Foundations of Terminology Studies*. Moscow, Vysshaya shkola Publ., 1987. 224 p. (In Russ.)

Grinev-Grinevich S. V. *Terminology.* Moscow, Akademiya Publ., 2008. 304 p. (In Russ.)

Grinev-Grinevich S. V., Sorokina E. A. Polysemy in general and specialized vocabulary. *Moscow Region State University Herald*, 2015, issue 4, pp. 51–64. (In Russ.)

Dolgonovskaya L. Ya. Comparative analysis of the term field 'protection' in information security (based on the material of the English and Russian languages). *Current Issues in English Studies and Methodology of Teaching Russian as a Foreign Language: A collection of scientific articles.* Moscow, 2023, issue 2, pp. 189–196. (In Russ.)

Doctrine of Information Security of the Russian Federation. *Official Internet portal of legal information*. 2024. Available at: https://pravo.gov.ru (accessed 30 Nov 2025). (In Eng.)

Kurakov L. P., Kurakov V. L. *Economics and Law: A reference dictionary.* 2024. Available at: https://dic.academic.ru (accessed 30 Nov 2025). (In Russ.)

Mironova M. R. Structural models of the terms of the cyber security *Izvestia of the Volgograd State Pedagogical University*, 2021, issue 1(154), pp. 160–164. (In Russ.)

Paroshin A. A. *Information Security: Standardized Terms and Concepts.* Vladivostok, 2010. 216 p. (In Russ.)

Pol'shchikova O. N. Polysemy in computer linguistics terminology. *Philology. Theory & Practice*, 2022, issue 5 (7), pp. 2328–2332. doi 10.30853/phil20220385 (In Russ.)

Proydakov E. M., Teplitsky Yu. A. English-Russian Explanatory Dictionary on Information Security. 2022. Available at: https://infosystems.ru (accessed 30 Nov 2025). (In Russ.)

Razumkova N. V. Lexical representations of sensory images in Osip Mandelstam's lyrics. *Tyumen State University Herald. Humanities Research. Humanitates*, 2022, vol. 8, issue 3 (31), pp. 23–44. doi 10.21684/2411-197X-2022-8-3-23-44 (In Russ.)

Roskiberbezopasnost' = Russian cyber security [website]. 2025. Available at: https://roskiber.ru (accessed 30 Nov 2025). (In Russ.)

Tiden E. V. Metaphorical terms in scientific discourse. *Personality – Language – Culture:* Proc. VII All-Russ. Sci. Pract. Conf. Saratov, Nauka Publ., 2019, pp. 129–134. (In Russ.)

Ursul A. D. Information strategy and security... *Scientific and Technical Information*, 2006, issue 1, pp. 7–12. (In Russ.)

Fadeeva A. A., Plekhanov M. S., Lopatin D. V. Analysis of the use of English-language terms in the field of cyber security. *Education and Law*, 2024, issue 5, pp. 606–611. (In Russ.)

Feoktistov G. G. Information security of society. *Socio-Political Journal*, 1996, issue 5, pp. 211–216. (In Russ.)

Filonov A. A. Theoretical and historical aspects of information protection in the Russian Federation. *Bulletin of the National Institute of Business*, 2022, issue 1 (45), pp. 130–140. (In Russ.)

Chernyshova L. A., Chernikova E. O., Balashova A. Yu. Specificity of the formal structure of terminological collocations in the English and German languages of the sphere of high-speed railway lines. *Philology. Theory & Practice*, 2025, issue 18 (3), pp. 1045–1052. doi 10.30853/phil20250151 (In Russ.)

Global Knowledge. Skillsoft. Available at: https://www.globalknowledge.com (accessed 30 Nov 2025). (In Eng.)

Heimdalsecurity. Unified Cybersecurity Platform. Available at: https://heimdalsecurity.com (accessed 30 Nov 2025). (In Eng.)

Information Security Office at Texas State University. *Information Security Glossary.* Available at: https://infosecurity.txst.edu/work/information-security-glossary.html (accessed 30 Nov 2025). (In Eng.)

Macak K. Towards a taxonomy of cyber attacks. *IEEE Communications Surveys & Tutorials,* 2020, vol. 22, issue 2, pp. 1356–1384. (In Eng.)

Ministry of Digital Governance, Hellenic Republic. *Cybersecurity Handbook*. 2021. Available at: https://cyber.gov.gr/wp-content/uploads/2025/03/Cybersecurity-Handbook-English-version-compressed.pdf (accessed 30 Nov 2025). (In Eng.)

Online Etymology Dictionary. *Cyber.* Available at: https://www.etymonline.com (accessed 30 Nov 2025). (In Eng.)

NIST Cybersecurity Framework. Available at: https://www.nist.gov/cyberframework (accessed 30 Nov 2025). (In Eng.)

Информация об авторах

Балашова Анна Юрьевна
кандидат филологических наук,
доцент кафедры «Лингвистика»
Российский университет транспорта
127994, Россия, г. Москва, ул. Образцова, 9, стр. 9

a.hatyushina@yandex.ru

доцент кафедры иностранных языков
Московский городской университет управления
Правительства Москвы имени Ю. М. Лужкова
107045, Россия, г. Москва, ул. Сретенка, д. 28

SPIN-код: 7860-8314
ORCID: https://orcid.org/0009-0000-8628-5227

Сорокина Эльвира Анатольевна
доктор филологических наук,
профессор кафедры «Лингвистика»
Российский университет транспорта
127994, Россия, г. Москва, ул. Образцова, 9, стр. 9

ellasor@mail.ru

профессор кафедры английской филологии
Государственный университет просвещения
105005, г. Москва, ул. Радио, 10А, стр. 2

SPIN-код: 5678-9876
ORCID: https://orcid.org/0000-0002-4965-078X

Статья поступила в редакцию 14.01.2026; одобрена после рецензирования 30.01.2026; принята к публикации 09.02.2026

Information about the authors

Anna Yu. Balashova
Associate Professor in the Department of Linguistics
Russian University of Transport
9, bld. 9, Obraztsova st., Moscow, 127994, Russia

a.hatyushina@yandex.ru

Associate Professor in the Department
of Foreign Languages
Moscow Metropolitan Governance
Yury Luzhkov University
28, Sretenka st., Moscow, 107045, Russia

SPIN-code: 7860-8314
ORCID: https://orcid.org/0009-0000-8628-5227

Elvira A. Sorokina
Professor in the Department of Linguistics
Russian University of Transport
9, bld. 9, Obraztsova st., Moscow, 127994, Russia

ellasor@mail.ru

Professor in the Department of English Philology
State University of Education
10A, bld. 2, Radio st., Moscow, 105005, Russia

SPIN-code: 5678-9876
ORCID: https://orcid.org/0000-0002-4965-078X

Submitted 14 Jan 2026; revised 30 Jan 2026; accepted 09 Feb 2026