Лекция 2

Вклад лингвистов-переводчиков в безопасность глобального информационного пространства

Перевод
это репрезентация текста в новой языковой форме с сохранением эквивалентного содержания и такого же коммуникативного эффекта на рецептора переводного текста (ПТ), какой производит на своего рецептора исходный текст (ИТ).

Участники перевода

Автор = источник сообщения

Оригинал = исходный текст

Переводчик

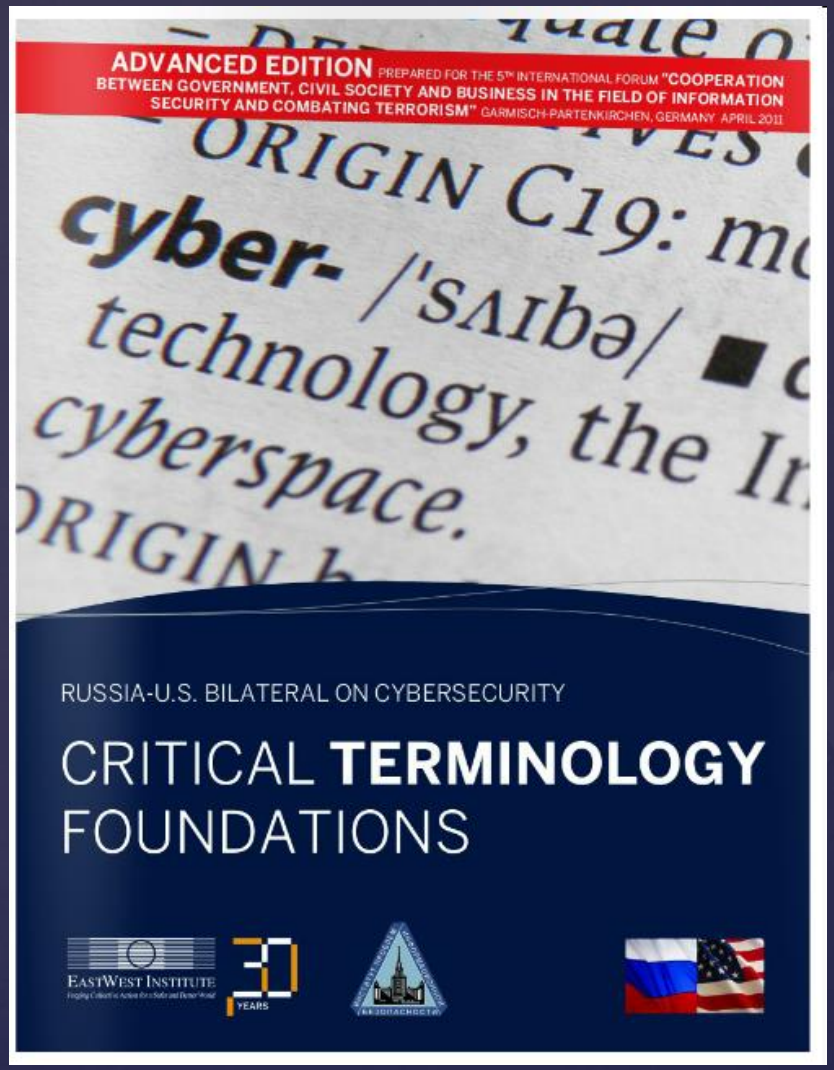
Переводной текст = целевой текст

Рецептор = реципиент = адресат

Заказчик (теория Скопос)

"Адекватный перевод включает определенную степень эквивалентности, но эквивалентный перевод может и не быть адекватным".

[Комиссаров В.Н. Современное переводоведение. - М.: ЭТС, 2001, с. 113].


ADVANCED EDITION PREPARED FOR THE 5TH INTERNATIONAL FORUM "COOPERATION BETWEEN GOVERNMENT, CIVIL SOCIETY AND BUSINESS IN THE FIELD OF INFORMATION SECURITY AND COMBATING TERRORISM" GARMISCH-PARTENKIRCHEN, GERMANY APRIL 2011
ORIGIN C19: m
cyber- /'saɪbə/
technology, the In
cyberspace.
RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS
EastWest Institute
30 YEARS


EastWest INSTITUTE
Critical Terminology Foundations 2
Russia-U.S. Bilateral on Cybersecurity
POLICY REPORT
2/2014

Консенсусные термины Российско-американского проекта по созданию терминологии в области информационной/кибер безопасности

Киберпространство
Киберинфраструктура
Киберсервисы (услуги, службы)
Критически важное киберпространство
Критически важная киберинфраструктура
Критически важные киберсервисы (услуги, службы)
Информационное пространство
Киберобъект
Кибератив
Киберсилы
Кибербоец

Консенсусные термины Российско-американского проекта по созданию терминологии в области информационной/кибер безопасности

Боевые действия в киберпространстве
Кибератака
Киберконтратака
Оборонительные средства противодействия в киберпространстве
Кибероборона
Оборонительные возможности в киберпространстве
Наступательные возможности в киберпространстве
Использование преимуществ в киберпространстве
Средства киберсдерживания
Информационное превосходство
Информационная операция
Доминирование в информационных операциях
Информационная безопасность
Кибероружие
Киберуязвимость
Киберразведка

Консенсусные термины Российско-американского проекта по созданию терминологии в области информационной/кибер безопасности

Киберпространство
Киберинфраструктура
Киберсервисы (услуги, службы)
Критически важное киберпространство
Критически важная киберинфраструктура
Критически важные киберсервисы (услуги, службы)
Информационное пространство
Киберобъект
Кибератив
Киберсилы
Кибербоец

Безопасность информации ≠ информационная безопасность

2.19 **Information security**: preservation of confidentiality (2.9), integrity (2.25) and availability (2.7) of information. Note 1 to entry: In addition, other properties, such as authenticity (2.6), accountability (2.2), non-repudiation (2.27), and reliability (2.33) can also be involved.

ISO/IEC 27000:2009(en)

2.19 **Информационная безопасность**: сохранение конфиденциальности (2.9), целостности (2.25) и доступности (2.7) информации. Примечание — Также сюда могут быть включены другие свойства, такие как подлинность (2.6), подотчетность (2.2), неотказуемость (2.27) и достоверность (2.33)

ГОСТ Р ИСО/МЭК 27000-2012

Способность обеспечить безопасность или защитить использование киберпространства

(глобальная сфера, находящаяся в информационной среде и состоящая из взаимозависимых сетевых инфраструктур информационных систем, в том числе Интернета, телекоммуникационных сетей, компьютерных систем и встраиваемых процессоров и контроллеров)

от кибератак

(атак, осуществляемых через киберпространство, объектом нападения которых является использование киберпространства предприятиями, а целью – нарушение, отключение, разрушение или злонамеренное управление вычислительной средой/инфраструктурой, или нарушение целостности данных или кража контролируемой информации).

NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*

Доктрина информационной безопасности Российской Федерации

2000г

состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства

Доктрина информационной безопасности Российской Федерации 2016г

the state of protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity and sustainable socio-economic development of the Russian Federation, as well as defence and security of the State.

состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года

2013г

«состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры»


Безопасность информации
Компьютерная безопасность
Сетевая безопасность
Кибербезопасность
Информационная безопасность

Спасибо за внимание