УДК 004.056

**Проблемы русификации специализированных ресурсов информационной безопасности**

**Д.О. Корягин**, студент гр. БИ-20Э1;

Федеральное государственное бюджетное образовательное учреждение высшего

образования «Сибирский государственный автомобильно-дорожный университет

(СибАДИ)», Омск, Россия

**Аннотация.** В статье рассмотрена проблема использования специализированных англоязычных источников информации и баз данных в сфере информационной безопасности. Автором отображены результаты проведённого исследования, которое позволило выявить имеющийся у пользователей уровень владения иностранным языком и популярность онлайн-переводчиков, что обосновывает актуальность создания специализированного сервиса по переводу текста. В исследовании выполнено моделирование идеального клиента такого сервиса на основе изучения потребительского интереса.

**Ключевые слова:** *онлайн-переводчик, информационная безопасность, моделирование, англоязычные ресурсы.*

**Problems of russification of specialized information security resources**

**D.O. Koryagin**, student gr. BI-20E1

Federal State Budget Educational Institution of Higher Education

«The Siberian State Automobile and Highway University», Omsk, Russia

**Abstract**. *The article considers the problem of using specialized English-language information sources and databases in the field of information security. The author displays the results of the conducted research, which revealed the level of foreign language proficiency available to users and the popularity of online translators, which justifies the relevance of creating a specialized text translation service. In the study, the modeling of the ideal client of such a service was carried out based on the study of consumer interest.*

**Keywords**: *online translator, information security, modeling, English-language resources.*

**Введение**

В настоящее время вопрос обеспечения информационной безопасности является актуальной задачей. Связанно это с процессами цифровизации, которые наблюдаются практически во всех сферах деятельности человека [1]. Всё больше разнообразных информационных систем используются на предприятиях и в организациях, соответственно всё больше информации обрабатывается с их помощью. В связи с этим, наравне с ростом использования информационных технологий, растет и число нарушений в информационном пространстве. Проблема киберпреступности имеет глобальный характер и требует эффективных мер по противодействию атакам злоумышленников [2]. Важное значение в системе защиты информации имеют превентивные меры, позволяющие предотвратить кибератаки. Для этого необходимо изучать тактики, техники и процедуры доступные нарушителям и моделировать возможные сценарии атак. Процесс моделирования угроз и/или кибератак является сложной творческой задачей, при этом чем больше используется источников данных, тем выше уровень достоверности сценариев.

В открытом доступе существует множество специализированных баз описания уязвимостей, угроз и шаблонов атак, пользующихся заслуженным признанием в среде специалистов по кибербезопасности. Однако многие из таких ресурсов являются англоязычными, для их применения специалист должен обладать определёнными уровнем владения английским языком или пользоваться специализированным переводчиком.

**Основная часть**

Моделирование атак позволяет понять используемые злоумышленником методы, приемы и инструменты, что позволяет своевременно предпринять меры по противодействию возможным нарушениям. Как отмечалось выше, процесс моделирования является творческой задачей, причём сложность заключается в том, что сценарий моделирует специалист по безопасности, рассуждая от лица злоумышленника как можно действовать, а реальный нарушитель может использовать совсем другие тактики и техники, процедуры [3]. Чтобы сценарии угроз были более адекватными специалисту необходимо использовать сведения из различных источников, таких как базы знаний (Mitre ATT&CK), шаблоны описания атак (CAPEC), базы описания уязвимостей (CWE, CVE) и другие. Подавляющее большинство таких ресурсов являются международными, то есть предоставляются на английском языке. Кроме этого, профессионал в сфере информационной безопасности должен использовать специализированные порталы, сайты, научные публикации, инструкции, руководства для средств защиты информации и другие ресурсы, в том числе и международные.

Однако, как показывает практика, довольно большое количество практических специалистов, либо не обладают достаточным уровнем владения английским языком, либо ранее не сталкивались с той или иной англоязычной терминологией. Для того, чтобы решить данную проблему, многие обращаются к онлайн-переводчикам. Вместе с тем, как неоднократно отмечалось специалистами, данный вид переводчиков не способен в полной мере произвести корректный перевод узконаправленных текстов. В связи с этим создание специализированного онлайн-переводчика является актуальным вариантом решения данной проблемы.

Востребованность онлайн-переводчика тематической направленности подтверждается проведенным исследованием среди студентов выпускных групп УГСН 10.00.00 – Информационная безопасность.

Основная масса респондентов (68%) оценивает свой уровень владения английским языком как базовый (рисунок 1).



Рисунок 1 - Статистика уровня владения английским языком

Использование программ переводчиков при работе с англоязычными ресурсами отмечают 65% респондентов (рисунок 2).

****

Рисунок 2 - Статистика предпочтений пользователей при изучении с англоязычными источниками

Предпочтения по вспомогательным средствам распределились следующим образом: на первом месте - программы-переводчики (26%), на втором месте - словари (8%) (рисунок3).



Рисунок 3 - Статистика использования инструментов перевода

По мнению участников опроса, корректность перевода онлайн-переводчиками оценивается как средняя (6,3 балла из 10 возможных) (рисунок 4).



Рисунок 4 - Уровень корректности онлайн-переводчиков по мнению пользователей

Причём если перевод текстов общего характера вполне приемлемый, то перевод специализированных, профессиональных текстов оставляет желать лучшего (рисунок 5) [4].



Рисунок 5 - Пример некорректного перевода онлайн-переводчиком

В процессе исследования потребительского интереса к разрабатываемому продукту было выполнено моделирование идеального клиента (потребителя). В результате получено подробное описание нескольких сегментов идеального клиента (таблица 1).

Таблица 1 – Описание сегментов идеального клиента

|  | **Сегмент 1** | **Сегмент 2** | **Сегмент 3** |
| --- | --- | --- | --- |
| **Название сегмента** | Студенты 2 курса и выше. | Люди, которые только завершили обучение. Не имеют профессионального опыта. К этой группе относятся начинающие работники, стажёры, практиканты, начинающие специалисты. | Люди, проходящие профессиональная переподготовку. |
| **Целевой рынок (отрасль/ниша)** | Рынок технологий машинного перевода. | Рынок технологий машинного перевода. | Рынок технологий машинного перевода. |
| **Должности ЛПР / ЛВР в сегменте** | Студент | Работники, стажёры, практиканты, начинающие специалисты. | Человек, проходящий профессиональная переподготовку. |
| **Специфические характеристики сегмента** | Учащийся среднего профессионального либо высшего учебного заведения. | Молодой работник, который только начинает свой профессиональный путь. Развивающийся специалист, который работает в компании в течение короткого времени, чтобы получить опыт начального уровня и знания в определенной области карьеры. Рабочий, служащий, с целью обученья, получения практических знаний прикомандированный к какому-нибудь учреждению, делу. | Человек проходящий программу профессиональной переподготовки, освоения исключительно профессиональных компетенций. |
| **Боли/задачи сегмента** | Возникает проблема с пониманием, усваиванием информации, увеличивается затрачиваемое время на выполнение работы. |
| **Гипотеза ценности для этого сегмента** | Из-за отсутствия специализированных переводчиков ориентированных на сферу ИБ пользователям приходиться использовать онлайн-переводчики, которые допускают множество ошибок разного характера. Для того, чтобы пользователи могли избежать проблем с ошибочным переводом англоязычных ресурсов предлагаем воспользоваться нашим специализированным продуктом, который предоставит корректный перевод в сфере ИБ.  |
| **Ценностное предложение для идеального клиента** | Наше программное решение в виде специализированного переводчик в сфере информационной безопасности, призвано выдавать корректный перевод англоязычных терминов и словосочетаний в данной сфере. |
| **Возможные варианты/пути маркетинга** | Реклама продукта через сообщества, научные конференции, связанные с областью информационной безопасности. |

Одним из наиболее востребованных англоязычных ресурсов является открытая база знаний: «Mitre ATT&CK», представляющая собой набор матриц, в которых представлены техники нарушителей, используемых на различных этапах атаки (рисунок 6). Матрицы составлены на основе анализа реальных инцидентов.



Рисунок 6 – Фрагмент матрицы MITRE ATT&CK

С помощью информации, представленной в базе знаний Mitre Att&ck, специалисты по информационной безопасности могут решать следующие задачи:

1. Анализ существующей защиты на предмет соответствия реальным угрозам и повышение безопасности инфраструктуры компании;
2. Своевременное реагирование на инциденты;
3. Расследование киберинцидентов;
4. Атрибуция атак;
5. Анализ деятельности киберпреступников;
6. Обмен информацией с коллегами.

Востребованность тематических англоязычных ресурсов подтверждают и результаты проведённого опроса, так 88,5% респондентов отмечают, что используют Mitre ATT&CK, 76,9% применяют CAPEC, 73% обращаются к базе описания уязвимостей программных продуктов CVE (рисунок7).



Рисунок 7 - Рейтинг наиболее используемых ресурсов по ИБ

Популярность ресурса Mitre ATT&CK среди специалистов подтверждает и тот факт, что предпринимаются попытки перевода матриц на русский язык. Так в настоящее время широко известны следующие проекты:

1. перевод матрицы от Positive Technologies (<https://mitre.ptsecurity.com/ru-RU/techniques/product/pt-nad>, <https://mitre.ptsecurity.com/ru-RU/techniques/product/mp-siem>);
2. перевод часто задаваемых вопросов от ряда исследователей в рамках проекта «attack\_community» (<https://habr.com/ru/articles/658293/>);
3. перевод и соотнесение Mitre ATT&CK с техниками по версии ФСТЭК России от Алексея Лукацкого (<https://lukatsky.ru/mapping-attack-to-fstek>).

Однако следует отметить, что вышеуказанные переводы включают только часть данных, содержащихся в матрицах Mitre ATT&CK, и не позволяют получить быстрый адаптированный перевод, как это принято на онлайн-сервисах.

**Заключение**

Таким образом, можно заключить, что англоязычные источники в сфере информационной безопасности являются востребованными. В связи с этим существует необходимость в переводе, соответствующим терминологическим особенностям сферы информационной безопасности. Использование онлайн-переводчиков является удобным способом быстрого получения русскоязычного текста. Исходя из проведенного опроса потенциальных пользователей, и анализа существующих решений следует, что создание специализированного онлайн-переводчика является актуальным.

**Библиографический список**

1. Цифровая экономика РФ // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. – сайт – URL : <https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fdigital.gov.ru%2fru%2factivity%2fdirections%2f858%2f> (дата обращения: 9.10.2023 )
2. Кибербезопасность в 2022–2023. Тренды и прогнозы // Positive Technologies. Исследования. – сайт – URL : <https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/> (дата обращения: 9.10.2023)
3. Моделирование угроз на основе сценариев или Как Cyber Kill Chain и ATT&CK помогаютанализировать угрозы ИБ // Интернет-портал по информационной безопасности в сети. – сайт – URL : <https://safe-surf.ru/specialists/article/5247/626649/> (дата обращения: 9.10.2023 )
4. Enterprise Matrix // Mitre ATT&CK. – сайт – URL : <https://attack.mitre.org/matrices/enterprise/> (дата обращения: 9.10.2023)

Научные руководители– З.В. Семенова, д.пед.н, профессор кафедры Информационная безопасность, А.Г. Анацкая, к.пед.н., доцент кафедры Информационная безопасность