ОЦЕНКА АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ ТРАНСФОРМЕРОВ

Васильев В.И.[1], Вульфин А.М.[2], Кучкарова Н.В.[3]

Цель исследования: *повышение эффективности оценки актуальных угроз безопасности программного обеспечения (ПО) промышленных автоматизированных систем и потенциальных сценариев их реализации на основе технологий Text Mining и моделей трансформеров.*

Метод исследования: *сопоставление множества выявленных уязвимостей ПО, соответствующих им тактик, техник и релевантных угроз безопасности информации путем оценки метрик семантической близости их текстовых описаний с использованием технологии Text Mining на основе моделей трансформеров. Применяются методы предобработки проблемно-ориентированного корпуса текстовых данных, подготовки и формализации текстовых описаний с помощью нейросетевых моделей векторных вложений на уровне слов, предложений и фрагментов текста.*

Полученные результаты: *разработаны алгоритм и прототип программного обеспечения для оценки актуальных угроз безопасности ПО, позволяющие сопоставить и ранжировать угрозы нарушения информационной и кибербезопасности для выявленного перечня уязвимостей ПО из Банка данных угроз безопасности информации ФСТЭК России, автоматизировать подбор техник и тактик для построения потенциальных сценариев реализации угроз. Применение предложенного подхода позволяет упростить процедуру оценки релевантных угроз на основе перечня выявленных уязвимостей, а также автоматизировать процесс построения возможных сценариев (тактик и техник) их реализации, сокращая временные затраты на проведение анализа более чем в три раза.*

Ключевые слова: *уязвимости программного обеспечения, угрозы информационной безопасности, Text Mining, векторное представление текстов, модели трансформеры, семантическая близость.*

DOI:10.21681/2311-3456-2022-2-27-38

Введение

Одним из ключевых направлений в области обеспечения информационной безопасности (ИБ) промышленных систем и сетей сегодня считается применение системного риск-ориентированного подхода, заключающегося в оценке потенциальных рисков нарушения ИБ в результате воздействия возможных угроз, что, в свою очередь, обеспечивает возможность обоснованного выбора эффективных контрмер по снижению этих рисков. Данный подход наиболее четко сформулирован в «Методике оценки угроз безопасности информации», утвержденной 5 февраля 2021 г. ФСТЭК России.

Методика ФСТЭК ориентирована на оценку антропогенных угроз безопасности информации (БИ), вызванных действиями внешних и внутренних нарушителей (злоумышленников). В качестве рекомендуемой модели угрозы БИ рассматривается следующая формула:

$УБИ_i$ = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия].

Актуальность возможных угроз БИ определяется наличием сценария их реализации, что предполагает установление последовательности возможных тактик и техник, применение которых возможно нарушителем с использованием существующих уязвимостей объектов воздействия. В качестве исходных данных для оценки угроз БИ при этом могут использоваться как общий перечень угроз, содержащийся в Банке данных угроз безопасности информации (БДУ) ФСТЭК

1 Васильев Владимир Иванович, доктор технических наук, профессор, Уфимский государственный авиационный технический университет, г. Уфа, Россия. E-mail: vasilyev@ugatu.ac.ru

2 Вульфин Алексей Михайлович, кандидат технических наук, доцент, Уфимский государственный авиационный технический университет, г. Уфа, Россия. E-mail: vulfin.alexey@gmail.com

3 Кучкарова Наиля Вакилевна, старший преподаватель, Уфимский государственный авиационный технический университет, г. Уфа, Россия. E-mail: nailya_kuchkarov@mail.ru

России, так и описания векторов атак (шаблоны) компьютерных атак, содержащиеся в базах данных CAPEC, ATT&CK, OWASP, STIX, WASC и др.

В то же время, следует отметить, что, располагая возможностью открытого доступа к указанным источникам информации, специалист по ИБ пока вынужден вручную справляться с огромным объемом данных. Указанная информация хранится в виде текстовых описаний, анализ которых требует существенных временных затрат и определенных профессиональных навыков. Отсюда понятен тот интерес, который проявляется к использованию методов семантического анализа текстов (Text Mining) [1], применение которых позволило бы в той или иной степени решить проблему автоматизации поиска и анализа необходимой специалисту полезной информации в перечисленных выше источниках данных.

В ряде публикаций [2-5], в том числе в работах авторов [6-8], рассматривались отдельные аспекты решения данной проблемы с применением методов Text Mining. Ниже основное внимание будет уделено исследованию возможностей и особенностей применения одного из новых и перспективных направлений в области обработки естественного языка (ЕЯ) – технологии трансформеров для решения задач оценки актуальных угроз ИБ АСУ ТП.

1. Построение языковых моделей с использованием технологии трансформеров

Считается, что технологии обработки естественного языка (Natural Language Processing, NLP) переживают сегодня вторую революцию. Первая революция была связана с разработкой языковых моделей, основанных на векторном представлении слов (Word Embedding) с помощью алгоритмов Word2Vec и Doc2Vec. Суть данного подхода, предложенного в [9], заключается в том, что произвольные слова из корпуса текстов представляются в виде числовых векторов фиксированной длины в многомерном семантическом пространстве. Компоненты этих векторов обучаются с помощью методов обучения без учителя с учетом соседнего окружения этих слов в тексте (т.е. контекста) таким образом, что близкие по смыслу слова порождают близкие вектора в семантическом пространстве. Соответствующие преобразования базируются на использовании глубоких нейронных сетей (НС) [10] и поддержаны развитыми инструментальными средствами (библиотеки TensorFlow, Gensim и др.).

Вторая революция в NLP началась с публикации в 2017 г. статьи [11], в которой была предложена идея построения языковой модели с использованием механизма внутреннего внимания (Self-Attention), получившей название «трансформер» (transformer). Архитектура трансформера состоит из двух частей – энкодера (encoder) и декодера (decoder), каждый из которых состоит, в свою очередь, из повторяющихся слоев, содержащих механизмы внутреннего внимания (Self-Attention) и НС прямого распространения (Feed-Forward NN). Энкодер преобразует входную последовательность слов в множество векторов (эмбеддингов) в семантическом пространстве, декодер генерирует из этих векторов последовательность выходных слов, в соответствии с запросом на решение конкретной прикладной задачи (классификация, поиск, перевод и т.п.). Роль механизмов внимания в данном случае – выделить из текста наиболее важные, значимые слова, отражающие смысловое содержание текста, организовав с учетом этого процесс обработки информации в энкодере и декодере. Особенностью построения трансформера является параллельная и независимая обработка входных слов, что сокращает вычислительные затраты и одновременно повышает качество обучения языковой модели.

Наиболее популярными языковыми моделями на базе трансформеров являются модели GPT и BERT [12]. Модель GPT (Generative Pre-trained Transformer) – «Генеративный предобученный трансформер» – выпущена компанией Open AI (Сан-Франциско) в 2018 г., в последующие 2 года появились новые версии этой модели GPT-2 и GPT-3. Языковая модель BERT (Bidirectional Encoder Representations from Transformers) – «Двунаправленное представление энкодера на базе трансформеров» – продукт компании Google, выпущена, как и GPT, в 2018 г. Несмотря на общие черты, GPT и BERT имеют и принципиальные различия. Так последняя модель трансформера GPT-3, выпущенная в 2020 г., содержит 96 слоев энкодера, общее число настраиваемых параметров – 175 млрд., в процессе предобучения она использовала 600 Гб текста на 104 языках. Особенностью GPT-3 является использование однонаправленного трансформера, т.е. при обучении энкодера используется только левый контекст каждого входного слова. Языковая модель BERT – это двунаправленная многослойная НС, т.е. в процессе предобучения энкодера используется весь набор входных слов в предложении или запросе (как слева, так и справа от каждого рассматриваемого слова). Базовая версия модели BERT – Base – это 12-слойный трансформер со 110 млн параметров, максимальная версия BERT – Large – 24 слоя с 240 млн. параме-

тров. В отличие от GPT, для доступа к которой сегодня требуется специальная лицензия от Open AI, предобучение модели BERT находится в открытом доступе в каталоге моделей для использования с репозиторием Transformers от HuggingFace.

Следует отметить, что обучение указанных моделей требует большого объема вычислительных ресурсов и длительного времени обучения. Для того чтобы ускорить процесс обучения, обычно используются методы дистилляции, или переноса знаний (transfer learning), с больших многозадачных моделей на более простые (редуцированные) модели, также построенные в классе трансформеров, но решающие более узкий (ограниченный) круг задач и, соответственно, требующие меньших вычислительных затрат [13]. В рамках этого направления сегодня, в частности, разработаны дообученные русскоязычные модели – трансформеры ruBERT (лаборатория DeepPavlov) [14], ruROBERTa (SberDevice от Сбера), ruBERT-tiny и др.

2. Методика оценки актуальных угроз безопасности информации на основе технологий семантического анализа текстов

Функциональная модель процесса оценки актуальных угроз ИБ, построенная в соответствии с Методикой ФСТЭК, приведена на рис. 1.

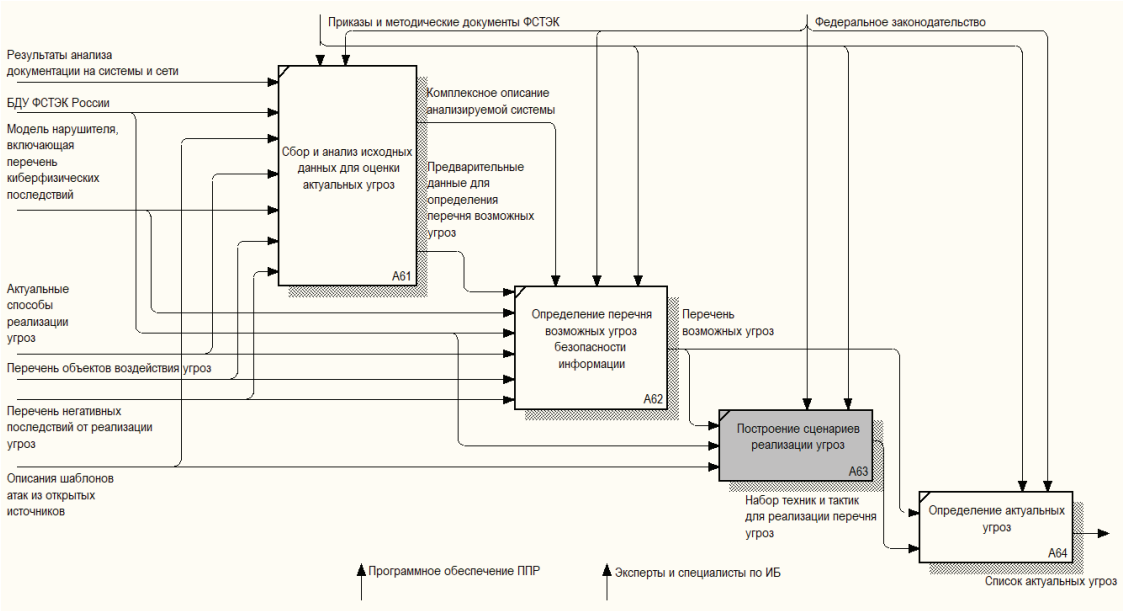


Рис. 1. Функциональная модель процесса оценки актуальных угроз БИ

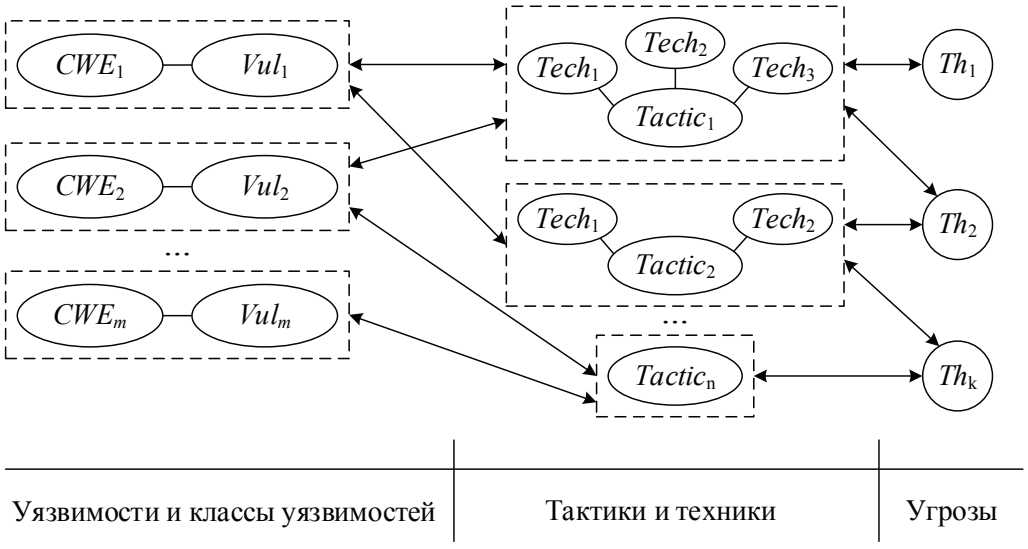


Рис. 2. Граф соответствия множеств угроз, уязвимостей, тактик и техник их эксплуатации

TT_v \ Th_v	Th_v^1	Th_v^2	Th_v^3	…	Th_v^{221}	Th_v^{222}
TT_v^1						
TT_v^2						
…				…		
TT_v^{10}						

а)

TT_v \ Vu_v	Vu_v^1	Vu_v^2	Vu_v^3	…	Vu_v^k
TT_v^1					
TT_v^2					
…				…	
TT_v^{10}					

б)

Рис. 3. Матрицы попарной семантической близости объектов двух множеств: а) MTT_Th – тактик (техник) и угроз; б) MTT_Vu – тактик (техник) и уязвимостей

Наиболее трудоемким этапом здесь является построение сценариев реализации угроз на основе совокупности возможных тактик и техник с учетом располагаемой экспертом информации о перечнях актуальных уязвимостей, типах доступа, типах нарушителей, видах ущерба, объектов воздействия, целей и т.п. Первый этап построения сценариев реализации угроз при этом сводится к установлению соответствия между множеством угроз Th, выявленных уязвимостей Vul и тактик и техник их эксплуатации (Tactic, Tech) в виде графа (рис. 2).

При построении данного графа можно воспользоваться оценкой метрик семантической близости имеющихся текстовых описаний множеств угроз, уязвимостей и тактик (техник) с использованием методов Text Mining [6]. Схема алгоритма сопоставления векторов признаков для текстовых описаний выявленных уязвимостей, угроз и тактик (техник) представлена на рис. 4 В основе алгоритма лежит построение матриц попарной семантической близости объектов двух множеств: M^{TT_Vu} тактик (техник) (TT) и уязвимостей (Vu), M^{TT_Th} тактик (техник) (TT) и угроз (Th) (рис. 3). Далее матрицы сортируются построчно в порядке убывания семантической близости текстовых описаний с обрезкой по количеству элементов в строке: для угроз остается p = 10 наиболее схожих, для уязвимостей – q = 25 наиболее схожих с текстовым описанием тактик (техник).

3. Применение моделей трансформеров для оценки актуальных угроз безопасности информации

Задача сопоставления описаний уязвимостей (CVE) и шаблонов атак (CAPEC) для англоязычных баз знаний (NVD, CAPEC, ATT&CK) на основе семантического анализа их текстовых описаний рассматривалась ранее в работах [15-16]. Было выполнено сравнение возможностей различных языковых моделей векторных вложений для сопоставления множеств текстовых описаний и показано, что специализированная модель TF-IDF для ограниченного тестового подмножества показывает лучший результат по сравнению с более сложными моделями.

В данной работе предлагается для подготовленных русскоязычных текстовых описаний угроз и уязвимостей, полученных из БДУ ФСТЭК, применить методы построения векторных вложений в многомерном семантическом пространстве признаков (Word2Vec + TF-IDF, Doc2Vec, модели трансформеров). Отличительной особенностью данного подхода от предложенных ранее [6] является сопоставление множеств угроз, уязвимостей, техник (тактик) с использованием моделей трансформеров, что должно повысить качество результатов сопоставления за счет оценки контекста текстовых описаний не только на уровне отдельных слов, как это принято в моделях Word2Vec и Dov2Vec, но и на уровне предложений и фрагментов текстов. При этом используются модели трансформеров, обученные на значительном объеме (корпусе) русскоязычных текстов.

Обобщенная схема подготовки текстовых данных и формализации текстовых описаний на основе векторных вложений представлена на рис. 5. Применяемые на каждом этапе инструменты обработки текстовых данных представлены в таблице 1. Проблемно-ориентированный корпус текстов для анализа данных включает в себя текстовые описания на русском языке 36752 уязвимостей, 222 угрозы, 10 техник и соответствующих тактик, взятые из БДУ ФСТЭК России.

Далее для формализации признаков текстовых описаний были использованы (таблица 2):

— нейросетевая модель векторного вложения для текстовых документов Distributed memory (PV-DM) Doc2Vec [18];

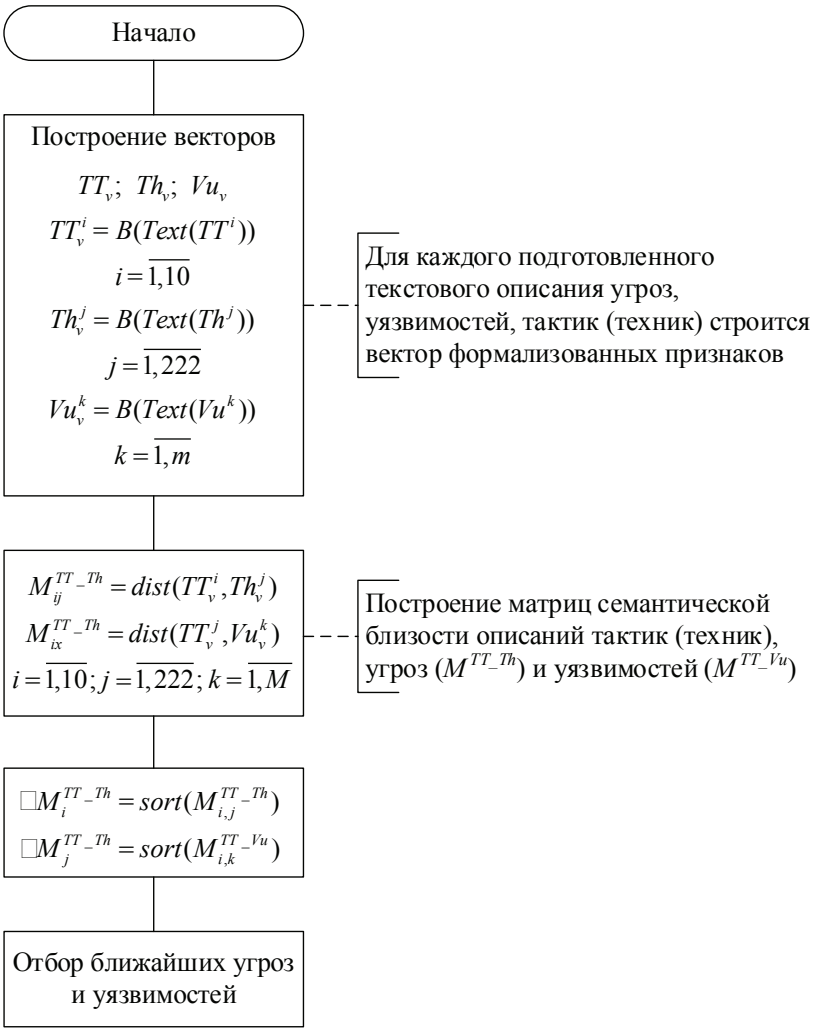


Рис. 4. Схема алгоритма сопоставления векторов признаков, полученных для текстовых описаний угроз (Th), уязвимостей (Vu), техник (тактик) (TT)

Таблица 1

Применяемые инструменты для предобработки данных

Этап	Шаги	Действия	Инструменты
Предобработка	Символьная фильтрация	Удаление нерелевантных символов, HTML-тегов	Набор регулярных выражений
	Токенизация	Разбивка текста на токены с помощью предобученной для русского языка нейросетевой модели	Razdel* [17] (фреймворк Natasha)
	Фильтрация нерелевантных токенов	Удаление дат, цифр, чисел, ссылок, сокращений	Регулярные выражения

* Rule-based token, sentence segmentation for Russian language. URL: https://github.com/natasha/razdel (дата обращения 27.12.2021).

Этап	Шаги	Действия	Инструменты
Нормализация	Лемматизация	Приведение слов в исходную форму с помощью предобученной нейросетевой модели	Morph (фреймворк Natasha)
Постобработка	Частеречная фильтрация	Остаются только существительные, глаголы, прилагательные, наречия, местоимения	Morph (фреймворк Natasha)
	Фильтрация на основе стоп-словарей	Фильтрация нерелевантных лемм с помощью составного стоп-словаря, включающего наиболее часто встречающиеся слова корпуса текстов	NLTK-russian
	Формирование документа-строки	Объединение лемм в нормализованную строку-документ	

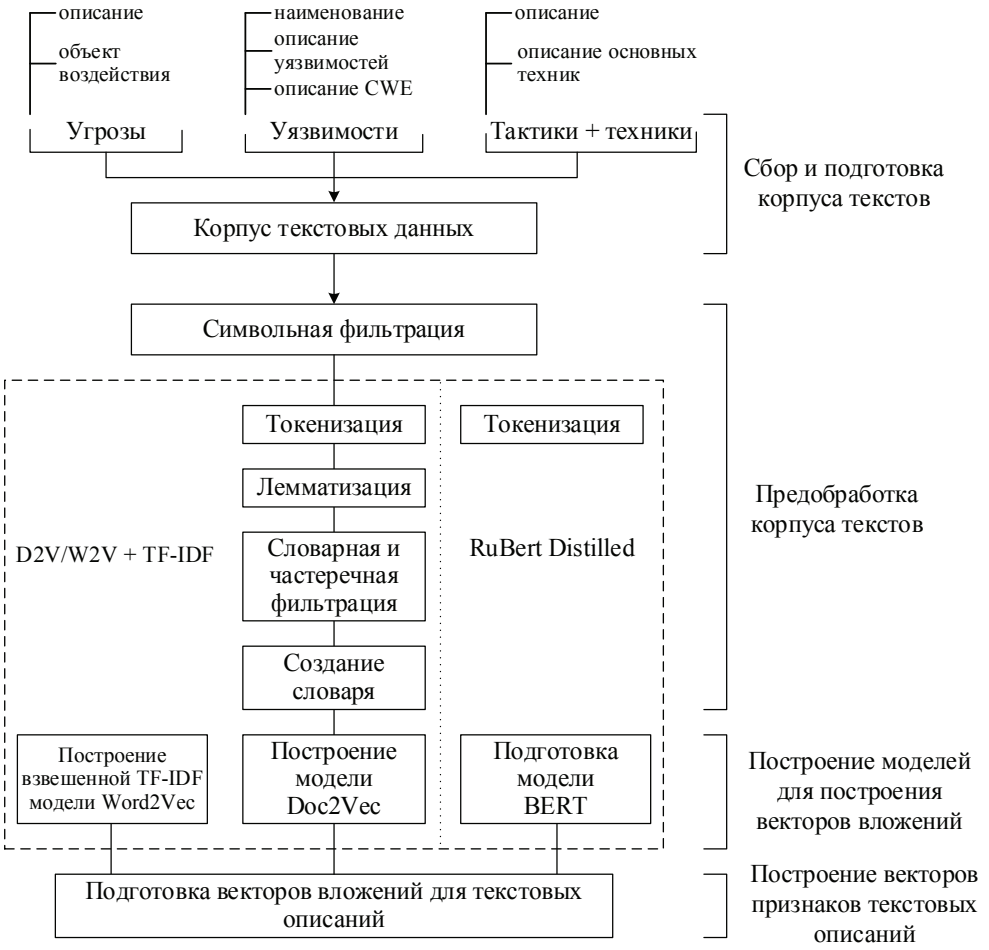


Рис. 5. Схема подготовки текстовых описаний угроз, уязвимостей, техник (тактик) и их формализации на основе векторных вложений

Таблица 2

Модели построения векторных вложений текстовых описаний

Модель	Обозначение	Параметр	Значение
Distributed memory Doc2Vec Model	Doc2Vec	Размерность вектора признаков	100
		Размер окна анализа	5
		Минимальная частота встречаемости слова для включения в модель	2
		Количество эпох обучения	100
CBOW Word2Vec Model + TF-IDF	Word2Vec	Размерность вектора признаков	100
		Размер окна анализа	3
		Минимальная частота встречаемости слова для включения в модель	1
		Количество эпох обучения	150
BERT- Large Model Multitask	BERT1	Размерность вектора признаков	1000
		Количество слоев	12
		Дополнительные модели-адаптеры	NLI, NER, TOX
		Общее количество токенов	120 тыс.
		Общее количество параметров	427 млн.
BERT- Large Model	BERT2	Размерность вектора признаков	1000
		Количество слоев	12
		Дополнительные модели-адаптеры	Нет
		Общее количество токенов	120 тыс.
		Общее количество параметров	427 млн.
ruBERT-tiny	BERT3	Размерность вектора признаков	312
		Количество слоев	3
		Общее количество токенов	120 тыс.

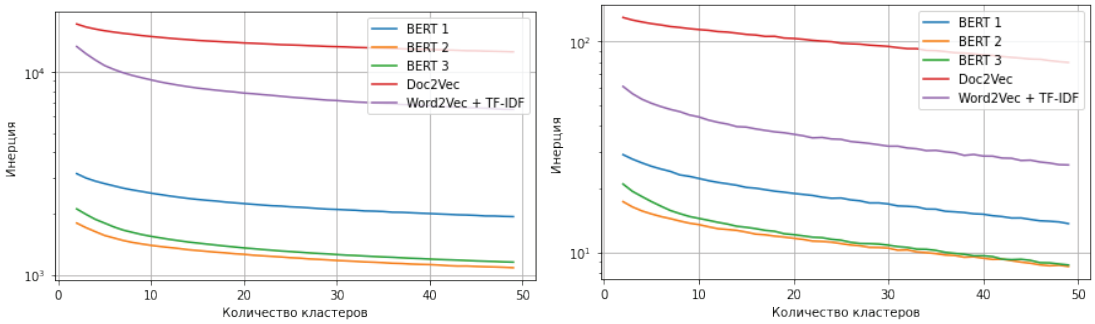
— нейросетевая модель векторного вложения для текстовых документов Word2Vec, взвешенная коэффициентами частотности терминов-обратной частотности документов – TF-IDF[4] [20];

— модели трансформеры [21]:
  - BERT Large Model Multitask (cased) for Sentence Embeddings in Russian Language – предложенная специалистами RnD NLP SberDevices модель-трансформер многозадачного обучения для построения универсальной модели ЕЯ на основе модели SBERT;
  - BERT Large Model (uncased) for Sentence Embeddings in Russian Language – также предложенная специалистами RnD NLP SberDevices модель-трансформер;
  - ruBERT-tiny – дистиллированная модель BERT-Multilingual, обученная с помощью больших моделей RuBERT, LaBSE, Laser и USE.

Для каждого документа корпуса с помощью указанных моделей вычисляются векторы формализованных признаков, на основе которых может быть оценена семантическая близость документов как косинусная мера расстояния между векторами [6].

Дальнейший анализ (сопоставление) формализованных представлений текстовых описаний угроз, уязвимостей, техник (тактик) основан на применении методов кластеризации многомерных данных. С помощью алгоритма кластеризации k-средних оценим структуру формализованных описаний в признаковом пространстве, сформированном на основе пяти

4 Ramos J. et al. Using tf-idf to determine word relevance in document queries. In Proceedings of the first instructional conference on machine learning, 2003, vol. 242, № 1, pp. 29-48.



а) *б)*

Рис. 6. Зависимость суммы внутрикластерных расстояний от числа кластеров для векторных представлений текстовых описаний уязвимостей (а) и угроз (б)

моделей вложений. В качестве меры близости используется косинус-мера. Количество кластеров задается в пределах от 1 до 50, оценивается сумма внутрикластерных расстояний для определения оптимального числа кластеров. На рис. 6 показана зависимость суммы внутрикластерных расстояний (инерция) от числа кластеров для формализованных представлений текстовых описаний множества уязвимостей (а) и множества угроз (б).

Из рис.6 видно, что применение предобученных моделей-трансформеров позволяет получить более компактное представление структуры текстовых описаний, формируемой алгоритмом кластеризации k-средних в пространстве признаков векторов вложений. Наилучший результат демонстрирует модель BERT 2. Незначительно хуже дистиллированная модель-трансформер BERT 3, которая работает существенно быстрее (векторное представление текстового описания строится примерно в 20 раз быстрее). Взвешенная модель вложений на уровне слов (Word2Vec + TF-IDF) позволяет получить менее компактную структуру кластеров. В каждом из экспериментов модель Doc2Vec демонстрирует менее пригодное для кластеризации представления признакового пространства.

4. Пример использования моделей трансформеров для оценки актуальных угроз безопасности информации

Пример построения набора матриц семантической близости M^{TT-Vu} и M^{TT-Th} в виде таблицы сопоставления тактик (техник), наиболее схожих угроз и уязвимостей, выявленных в ходе анализа для конкретного объекта [8] с помощью сканеров безопасности или определенных экспертом, представлен в таблице 3.

Визуализация графа семантической близости текстовых описаний тактик (техник), угроз и уязвимостей представлена на рис. 7.

Для анализируемого объекта [8] сформирован список из 22 уязвимостей ПО промышленной сети АСУ ТП. В ходе ручного анализа экспертом выявлены четыре потенциальные угрозы для целевых активов, время разработки сценариев их реализации составило более

Таблица 3

Фрагмент таблицы сопоставления тактик (техник), угроз и уязвимостей

№ тактики	Текстовое описание тактики и техник	Индексы семантически близких угроз	Текстовое описание семантически близких угроз	Индексы семантически близких уязвимостей	Текстовые описания семантических близких уязвимостей
8	Получение доступа (распространение доступа) к ...	[140, 98, 81, 23, 171, 84, 116, 27, 115, 80]	[Угроза приведения системы в состояние «отказ ...	[BDU:2019-02466, BDU:2019-02818, BDU:2020-0189...	[Уязвимость программного средства централизова...

№ тактики	Текстовое описание тактики и техник	Индексы семантически близких угроз	Текстовое описание семантически близких угроз	Индексы семантически близких уязвимостей	Текстовые описания семантических близких уязвимостей
2	Получение первоначального доступа к компонента...	[171, 203, 140, 80, 23, 84, 92, 77, 81, 116]	[Угроза скрытного включения вычислительного ус...	[BDU:2017-02265, BDU:2017-02264, BDU:2017-0226...	[Уязвимость протокола WPA2, связанная с ошибка...

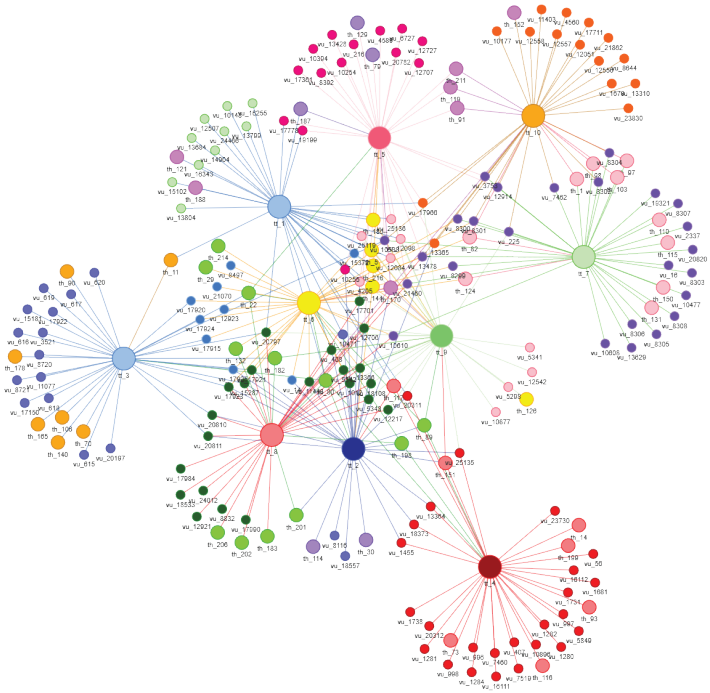


Рис. 7. Граф семантической близости текстовых описаний тактик (техник) (tt_i), угроз (th_j) и уязвимостей (vu_k)

часа. Семантический анализ с помощью предлагаемых решений Text Mining позволяет автоматизировать процедуру префильтрации множества релевантных угроз и способов их реализации, тем самым существенно сократив затраты времени эксперта. Сравнение процедуры анализа с решением [8] приведены в таблице 4.

Предложенные модели семантического анализа позволили упростить процедуру подбора актуальных угроз для выделенных информационных активов, предоставив их предварительный список из 8-10 позиций, из которых экспертом были одобрены от 50 до 85%. Для каждой из выбранных угроз и сопоставленных им уязвимостей сформирован набор возможных тактик и техник, что позволило эксперту сократить время на построение сценариев реализации угроз более чем в три раза.

Наилучшие рекомендации для эксперта были получены с помощью технологий семантического анализа на основе моделей-трансформеров (85% совпадений экспертной разметки и выдачи модели) и специализированной модели Word2Vec-TF-IDF (75%). Таким образом, несмотря на возросшие требования к вычислительным ресурсам в случае применения трансформеров, данные технологии позволяют добиться принципиального преимущества при работе со специализированными текстами, повышая эффективность работы эксперта за счет автоматизации процедуры префильтрации текстовых описаний и снижения когнитивной нагрузки при оценке и анализе актуальных угроз безопасности информации.

Таблица 4

Сравнение процедуры анализа уязвимостей, угроз и сценариев их реализации

<table>
<tr><td rowspan="2">Параметр</td><td rowspan="2">Экспертное сопоставление по тегам в БДУ ФСТЭК</td><td colspan="4">Автоматизированная система на основе технологий Text Mining</td></tr>
<tr><td colspan="2">Сопоставление уязвимостей и угроз [8]</td><td colspan="2">Сопоставление уязвимостей, угроз и тактик (техник)</td></tr>
<tr><td>Ввод информации</td><td>Вручную, WEB-интерфейс БДУ</td><td colspan="4">Автоматизированная обработка результатов работы сканеров уязвимостей</td></tr>
<tr><td>Тип сопоставления угроз</td><td>Ручное</td><td colspan="4">Задается пороговыми метриками, определяющими чувствительность фильтра</td></tr>
<tr><td>Количество сопоставленных угроз</td><td>4</td><td colspan="2">10</td><td colspan="2">8</td></tr>
<tr><td rowspan="4">Экспертная оценка корректности сопоставления угроз (техник и тактик)</td><td rowspan="4">-</td><td>Модель</td><td>оценка</td><td>Модель</td><td>оценка</td></tr>
<tr><td>Word2Vec + TF-IDF</td><td>6 из 10</td><td>Word2Vec + TF-IDF</td><td>6 из 8</td></tr>
<tr><td rowspan="2">Doc2Vec</td><td rowspan="2">5 и 10</td><td>Doc2Vec</td><td>5 из 8</td></tr>
<tr><td>BERT 3</td><td>7 из 8</td></tr>
<tr><td>Затраченное время на сопоставление угроз и уязвимостей</td><td>Более 15 минут</td><td colspan="2">< 5 с</td><td colspan="2">< 10 с</td></tr>
<tr><td>Возможность подбора техник и тактик реализации угроз</td><td>Да</td><td colspan="2">Нет</td><td colspan="2">Да</td></tr>
<tr><td>Затраченное время на построение сценариев реализации угроз</td><td>Более 1 часа</td><td colspan="2">-</td><td colspan="2">Менее 20 минут (включая работу эксперта)</td></tr>
</table>

Заключение

Рассмотрены технологии семантического анализа текстовых описаний угроз, уязвимостей, тактик и техник из Банка данных угроз безопасности информации ФСТЭК России с использованием технологии Text Mining на основе моделей трансформеров для векторизации представления текстовых описаний и оценки их семантической близости. Предложена методика оценки актуальных угроз нарушения ИБ, алгоритм и графовая модель сопоставления множества угроз, выявленных уязвимостей и тактик (техник) их эксплуатации.

Прототип программной реализации предложенных решений позволяет:

- автоматизировать процесс сопоставления и ранжирования угроз нарушения ИБ для выявленных уязвимостей ПО;
- сократить время анализа экспертом перечня выявленных уязвимостей за счет интеллектуальной фильтрации и ранжирования списка угроз;
- автоматизировать подбор техник и тактик для построения сценариев реализации угроз и уменьшить трудоемкость анализа для выполнения требований нормативных документов.

Литература

1. Бенгфорт Б., Билбро Р., Океда Т. Прикладной анализ текстовых данных на Python. Машинное обучение и создание приложений обработки естественного языка / Пер. с англ. СПб: Питер, 2019. 368 с.
2. Datta P., Lodinger N., Namin S., Jones S. Cyber-Attack Consequence Prediction. In Proceedings of the 3rd Workshop on Big Data Engineering and Analytics in Cyber-Physical Systems. 9 p. URL: https://arxiv.org/pdf/2012.00648.pdf (дата обращения 27.12.2021).
3. Lee Y., Shin S. Toward Semantic Assessment of Vulnerability Severity: A Text Mining Approach. In Proceedings of ACM CIKM Workshop (EYRE'18). URL: https://www.CEUR-WS.org/Vol1-2482/papers.pdf (дата обращения 27.12.2021).
4. Noel S. Text Mining for Modeling Cyberattacks // Chapter 14 in the book: Handbook of Statistics. Elsevier B.V. (Part C: Applications and Linguistic Diversity). 2018, vol. 38, pp. 461-515. DOI: 10.1016/bs.host.2018.06.001

5. Доронин А.К., Липницкий В.А., Предсказательная модель машинного обучения для решения задачи классификации уязвимостей компьютерных систем // Материалы Междунар. научн. конф. «Информационные технологии и системы» (ИТС 2018), Минск, 25 окт. 2018 г., С. 94-95.
6. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Автоматизация анализа уязвимостей программного обеспечения на основе технологии Text Mining // Вопросы кибербезопасности. 2020. № 4(38). С.22-31. DOI: 10.21681/2311-3456-2020-4-22-31
7. Васильев В.И., Вульфин А.М., Кириллова А.Д., Никонов А.В. Система оценки метрик опасности уязвимостей на основе технологий семантического анализа данных // Вестник УрФО. Безопасность в информационной сфере. 2021. №2(40). С.31-43.
8. Васильев В.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В. Методика оценки актуальных угроз и уязвимостей на основе технологии когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. №3. С.110-134.
9. Mikolov T., Chen K., Corrado G., Dean J. Efficient Estimation of Word Representation in Vector Space // arXiv, 2013. URL: https://arxiv.org/abs/1301.3781/ (дата обращения 27.12.2021).
10. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение: Погружение в мир нейронных сетей. – СПб.: Питер. 2020. С. 219-480. ISBN 978-5-4461-1537-2
11. Vaswani A., Shazeer N. Parmar N., et al. Attantion is All You Need // arXiv, 2017. URL: https://arxiv.org/abs/1706.03762 (дата обращения 27.12.2021).
12. Куратов Ю.М. Специализация языковых моделей для применения к задачам обработки естественного языка / Дисс. к.ф.-м.н. по спец-ти 05.13.17. – М.: МФТИ, 2020. 121 с.
13. Sank V., Debut L., Chaumond J., Wolf Th. DistilBERT, a distilled verstion of BERT: smaller, faster, cheaper and lighter // arXiv:1910.01108 v4. URL: https://arxiv.org/abs/1910.01108 (дата обращения 27.12.2021).
14. Kuratov Yu., Arkhipov M. Adaptation of Deep Bidirectional Multilingual Transformers for Russian Language // arXiv, 2019. URL: https://arxiv.org/pdf/1905.07213.pdf (дата обращения 27.12.2021).
15. Kanakogi K. et al. Tracing CVE Vulnerability Information to CAPEC Attack Patterns Using Natural Language Processing Techniques // Information. 2021. Vol. 12. № 8. C. 298.
16. Kanakogi K. et al. Tracing CAPEC Attack Patterns from CVE Vulnerability Information using Natural Language Processing Technique. In Proceedings of the 54th Hawaii International Conference on System Sciences. January 2021. pp. 6996.
17. Sakhovskiy A. et al. RuSimpleSentEval-2021 shared task: evaluating sentence simplification for Russian //Proceedings of the International Conference “Dialogue. – 2021. – С. 607-617.
18. Mendsaikhan O. et al. Identification of cybersecurity specific content using the Doc2Vec language model // 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2019. Vol. 1. pp. 396-401.
19. Kim D. et al. Multi-co-training for document classification using various document representations: TF–IDF, LDA, and Doc2Vec // Information Sciences. – 2019. – Т. 477. – С. 15-29.
20. Li J., Zhang H., Wei Z. The weighted word2vec paragraph vectors for anomaly detection over HTTP traffic // IEEE Access. 2020. Vol. 8. pp. 141787-141798.
21. Shahid M.R., Debar H. CVSS- BERT: Explainable Natural Language Processing to Determine the Severity of a Computer Security Vulnerability from its Description //arXiv:2011.08510v1 [cs.CL] 16 Nov 2021.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-08-00668

ASSESSMENT OF CURRENT THREATS TO INFORMATION SECURITY USING TRANSFORMER TECHNOLOGY

Vasilyev V.I.[5], Vulfin A.M.[6], Kuchkarova N.V.[7]

Purpose: *development of an automated system for assessing current threats to the security of software of industrial automation systems based on the technology of Transformers.*

Methods: *comparison of the set of identified software vulnerabilities, corresponding tactics (techniques) and relevant threats to information security by assessing the semantic proximity metrics of their text descriptions using Text Mining technology based on transformers models.*

5 Vladimir I. Vasilyev, Dr.Sc.(Eng.), Professor, Ufa State Aviation Technical University, Ufa, Russia, E-mail: vasilyev@ugatu.ac.ru

6 Alexey M. Vulfin, Ph.D., Associate Professor, Ufa State Aviation Technical University, Ufa, Russia, E-mail: vulfin.alexey@gmail.com

7 Nailya V. Kuchkarova, Senior Lecturer, Ufa State Aviation Technical University, Ufa, Russia, E-mail: nailya_kuchkarov@mail.ru

Practical relevance: *an automated system for assessing current software security threats has been developed, which makes it possible to compare and rank information and cyber security threats for identified vulnerabilities from the FSTEC of Russia Information Security Threats Databank, to automate the selection of techniques and tactics for constructing threat scenarios. The results of the comparative analysis show that the use of this system makes it possible to simplify the procedure for selecting potential threats and comparing vulnerabilities to them, in addition, a possible set of tactics and techniques is automatically generated, which makes it possible to reduce the time spent on building scenarios for the implementation of threats.*

Keywords: *software vulnerabilities, information security threats, Text Mining, vector word representation, semantic similarity.*

References

1. Bengfort B., Bilbro R., Okeda T. Prikladnoj analiz tekstovy`x danny`x na Python. Mashinnoe obuchenie i sozdanie prilozhenij obrabotki estestvennogo yazy`ka / Per. s angl. SPb: Piter, 2019. 368 p.
2. Datta P., Lodinger N., Namin S., Jones S. Cyber-Attack Consequence Prediction. In Proceedings of the 3rd Workshop on Big Data Engineering and Analytics in Cyber-Physical Systems. 9 p. Available at: https://arxiv.org/pdf/2012.00648.pdf (accessed December 27, 2021).
3. Lee Y., Shin S. Toward Semantic Assessment of Vulnerability Severity: A Text Mining Approach. In Proceedings of ACM CIKM Workshop (EYRE'18). Available at: https://www.CEUR-WS.org/Vol1-2482/papers.pdf (accessed December 27, 2021).
4. Noel S. Text Mining for Modeling Cyberattacks // Chapter 14 in the book: Handbook of Statistics. Elsevier B.V. (Part C: Applications and Linguistic Diversity). 2018, vol. 38, pp. 461-515. DOI: 10.1016 / bs.host.2018.06.001.
5. Doronin A.K., Lipniczkij V.A., Predskazatel`naya model` mashinnogo obucheniya dlya resheniya zadachi klassifikacii uyazvimostej komp`yuterny`x sistem // Materialy` Mezhdunar. nauchn. konf. «Informacionny`e texnologii i sistemy» [Information Technologies and Systems 2018 (ITS 2018)]. Minsk, 25 October 2018. pp 94-95.
6. Vasilyev V.I., Vulfin A.M., Kuchkarova N.V. Avtomatizaciya analiza uyazvimostej programmnogo obespecheniya na osnove texnologii Text Mining // Voprosy` kiberbezopasnosti [Cybersecurity issues], 2020, no. 4(38), pp. 22-31.
7. Vasilyev V.I., Vul`fin A.M., Kirillova A.D., Nikonov A.V. Sistema ocenki metrik opasnosti uyazvimostej na osnove texnologij semanticheskogo analiza danny`x // Vestnik UrFO. Bezopasnost` v informacionnoj sfere [Bulletin of the Ural Federal District. Security in the Information Sphere], 2021, no. 2(40), pp. 31-43.
8. Vasilyev V.I., Vulfin A.M., Kirillova A.D., Kuchkarova N.V. Metodika ocenki aktual`nny`x ugroz i uyazvimostej na osnove texnologii kognitivnogo modelirovaniya i Text Mining // Sistemy upravleniya, svyazi i bezopasnosti [Systems of Control, Communication and Security], 2021, no. 3, pp. 110-134.
9. Mikolov T., Chen K., Corrado G., Dean J. Efficient Estimation of Word Representation in Vector Space // arXiv, 2013. Available at: https://arxiv.org/abs/1301.3781/ (accessed 27 December 2021).
10. Nikolenko S., Kadurin A., Arxangel`skaya E. Glubokoe obuchenie: Pogruzhenie v mir nejronny`x setej. – SPb.: Piter. pp. 219-480.
11. Vaswani A., Shazeer N. Parmar N., et al. Attantion is All You Need // arXiv, 2017. Available at: https://arxiv.org/abs/1706.03762 (accessed December 27, 2021).
12. Kuratov Yu.M. Specializaciya yazy`kovy`x modelej dlya primeneniya k zadacham obrabotki estestvennogo yazy`ka / Diss. k.f.-m.n. po specz-ti 05.13.17. – M.: MFTI, 2020. 121 p.
13. Sank V., Debut L., Chaumond J., Wolf Th. Distil BERT, a distilled verstion of BERT: smaller, faster, cheaper and lighter // arXiv:1910.01108 v4. Available at: https://arxiv.org/abs/1910.01108 (accessed December 27, 2021).
14. Kuratov Yu., Arkhipov M. Adaptation of Deep Bidirectional Multilingual Transformers for Russian Language // arXiv, 2019. Available at: https://arxiv.org/pdf/1905.07213.pdf (accessed December 27, 2021).
15. Kanakogi K. et al. Tracing CVE Vulnerability Information to CAPEC Attack Patterns Using Natural Language Processing Techniques // Information, 2021, vol. 12, no. 8, pp. 298.
16. Kanakogi K. et al. Tracing CAPEC Attack Patterns from CVE Vulnerability Information using Natural Language Processing Technique. In Proceedings of the 54th Hawaii International Conference on System Sciences. 2021, pp. 6996.
17. Sakhovskiy A. et al. RuSimpleSentEval-2021 shared task: evaluating sentence simplification for Russian //Proceedings of the International Conference "Dialogue. – 2021. – C. 607-617.
18. Mendsaikhan O. et al. Identification of cybersecurity specific content using the Doc2Vec language model // 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2019, vol. 1, pp. 396-401.
19. Kim D. et al. Multi-co-training for document classification using various document representations: TF–IDF, LDA, and Doc2Vec // Information Sciences. – 2019. – T. 477. – C. 15-29.
20. Li J., Zhang H., Wei Z. The weighted word2vec paragraph vectors for anomaly detection over HTTP traffic // IEEE Access, 2020, vol. 8, pp. 141787-141798.
21. Shahid M.R., Debar H. CVSS- BERT: Explainable Natural Language Processing to Determine the Severity of a Computer Security Vulnerability from its Description //arXiv:2011.08510v1 [cs.CL] 16 Nov 2021.