МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
КРАСНОЯРСКИЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
им.В.П. АСТАФЬЕВА
(КГПУ им. В.П. Астафьева)

Факультет иностранных языков
Кафедра английской филологии

Благинина Полина Сергеевна

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Терминология киберпреступности и особенности ее перевода

Направление подготовки 45.03.02 Лингвистика
Направленность (профиль) Перевод и переводоведение

ДОПУСКАЮ К ЗАЩИТЕ

Зав. кафедрой Бабак Т. П.
кандидат филологических наук, доцент
"5" июня 2019 г. _____

Руководитель Софронова Т. М.
кандидат филологических наук, доцент
14.05.2019 _____

Дата защиты "19" июня 2019 г.

Обучающийся Благинина П. С.
"7" мая 2019 г. _____

Оценка отлично

Красноярск
2019

Содержание

Введение

Проблема терминологии и перевода терминов на различные языки интересует многих ученых и является очень актуальной, что связано с очевидным ростом терминологической лексики во многих языках. Терминологические исследования занимают одно из ведущих мест в отечественном и зарубежном языкознании последних десятилетий. Но при этом, терминоведение до сих пор не обозначило определенного и единого объяснения понятия “термин” [Володина, 1998]. Разные ученые определяют его по-разному.

Терминология используется в самых различных сферах жизни. С давних времен человек хранил и передавал информацию - как обыденную, повседневную, так и крайне важную, секретную. С развитием технологий преступления с похищением такой информации стали более изощренней и появилась киберпреступность.

Активное развитие терминологии киберпреступности также связано с постоянным развитием отношений между странами в области юриспруденции, криминалистики и пр. Правоохранительным органам для обеспечения безопасности населения стало необходимо уметь общаться на одном языке. Им и стал английский язык. Большинство компьютерных преступлений происходит на международном уровне, многие уголовные дела рассматриваются в международных судах, где криминалистам необходимо предъявлять доказательства виновности и невиновности, и в связи с этим требуются знания различной терминологии, а точнее - как она выглядит в терминологии международной, для того, чтобы предъявлять более точные и верные доказательства.

Таким образом, помимо определения отличительных характеристик терминологии киберпреступности, перед учеными стоит задача определения основных способов ее перевода. Несмотря на весь интерес к данной

проблеме, единой классификации способов такого перевода с одного язык на другой не существует. Также недостаточно существует исследований о его сложностях.

Все вышеизложенное обусловило *актуальность* представленного исследования. Новые термины, новые ситуации, требующие новых терминов, появляются каждый год [Гореликова, 2002]. Очень важно иметь представление не только о терминологическом корпусе своего языка, но и других. На данный момент каких-либо исследований о терминологии выбранной тематики не имеется. Существуют работы о научно-технической лексике (“научная литература представляет интерес не только по содержанию, но и по форме; ежегодно публикуется миллионы статей по вопросам науки и техники” [Пумпянский, 2004]) и о компьютерных неологизмах, но они рассматривают лишь части темы и не охватывают все нюансы, требуемые для анализа терминологического корпуса и его перевода по теме “киберпреступность”.

Объектом исследования является терминология киберпреступности. *Предметом* стали особенности перевода терминов киберпреступности с английского на русский язык.

Цель данной работы - изучение терминологии киберпреступности в сравнительно-сопоставительном аспекте на примере конкретных языков, анализ корпуса терминологии киберпреступности на основе программы TermoStat и особенностей их перевода на примере книги 2011 года “Cyber Security Essentials” под редакцией Джеймса Грэма, Ричарда Ховарда и Райана Олсона. Для реализации цели исследования нами были поставлены следующие *задачи*:

1. изучить и определить понятия “термин” и “терминология”;

2. выработать классификацию терминологии киберпреступности по структуре образования для определения тенденции в образовании новых терминов;
3. определить функции и классификацию способов перевода терминов в указанной сфере;
4. рассмотреть роль корпусной лингвистики в переводческой деятельности и конкретные характеристики лингвистического корпуса по терминологии киберпреступности;
5. выявить основные сложности перевода по выбранной тематики и рассмотреть основные способы перевода терминов;
6. на примере фрагмента из книги "*Cyber Security Essentials*" осуществить предпереводческий анализ и переводческий комментарий.

Для осуществления поставленных задач как метод исследования применялся сравнительно-сопоставительный анализ.

Теоретическую базу составили: учебные пособия С. В. Гринев-Гриневича о терминах и терминологии в целом [Гринев-Гриневич, 2008], о лингвистических аспектах перевода - В.Н. Комиссарова; книги о месте терминологии в составе языка Д. С. Лотте [Лотте, 1961], Л. А. Капанадзе [Капанадзе, 1965], В. П. Даниленко [Даниленко, 1971]; для определения зарождения и развития терминологии киберпреступности и кибербезопасности - доклады и исследования В. А. Мещерякова [Мещеряков, 2001], А.И. Усова [Усов, 2002].

Глава 1. Теоретические основы изучения терминологии киберпреступности

1.1 Определение понятий “термин”, “терминология”

Ранее XX века, все вопросы, касаемые терминологии, относились только к ученым и таковым специалистам, но компьютеризация всех видов деятельности и сфер начала процесс появления специальной лексики в речи обычного человека. На данный момент под пристальным вниманием лингвистов находится проблема функционирования терминологии в разных сферах и текстах. Это объясняется тем фактом, что свыше 90% новых слов, образующихся в языке, относится к специальной лексике, т.е. терминам [Арбекова, 2002]. Это означает, что их количество даже обгоняет количество лексики общеупотребительной. Кроме того, как отмечает С.В. Гринев-Гриневич, все больше терминов проникают в общеупотребительный корпус языка, что влияет на язык в целом [Гринев-Гриневич, 2008, с. 3-5].

Само слово *термин* образовалось от латинского *ter*, которое означает - перешагивать, достигать цели, которая по ту сторону. Отсюда следует, что изначально смысл термина относился к религии - “стража всего, что в пределах охраняемой границы”. Со временем, он появился в философии и в других научных дисциплинах - медицине, теологии, лингвистике и пр. [Сусименко, Рожденственская, 2012, с. 135].

Сейчас все понимают слово *термин* по-разному, так как единого объяснения не существует, хотя многие лингвисты пытались отразить в нем все нюансы, все свойства и разновидности. Все это связано с тем, что терминоведение - это относительно молодая наука. И, конечно, не стоит забывать об изменчивости самого языка со временем. Меняется язык - меняется и понятие.

Одно из объяснений термина А.А. Реформатским подтверждает, что в современной лингвистике терминология - часть специальной лексики:

термин - это “слова специальные, ограниченные своим особым назначением; слова, стремящиеся быть однозначными как точное выражение понятий и называние вещей” [Реформатский, 1967, с. 110].

Таким образом, главная функция термина - номинация. Термины служат для наименования точных специальных понятий, они обеспечивают ясность и понимание научной мысли.

Также является актуальной проблема определения места терминологии в составе языка. Существует две основных точки зрения на этот вопрос:

1. сторонники нормативного подхода (Д. С. Лотте, Л. А. Капанадзе, Н. З. Котелова, Е. Н. Толикина, А. В. Косов и др.) — “извлекают терминологию из состава общенационального языка и приходят к выводу об искусственности термина как специальной единицы. Они понимают терминологию как систему искусственно созданных знаков. А к термину предъявляются следующие требования” [Лантюхова, Загоровская, Литвинова, 2013]:
    a. фиксированное содержание (определенность)
    b. точность
    c. однозначность
    d. отсутствие синонимов
    e. краткость и др.
2. сторонники дескриптивного подхода (Н. П. Кузькин, А. И. Моисеев, Р. А. Будагов, Р. Ю. Кобрин, В. П. Даниленко, Б. Н. Головин и др.) — понимают терминологию как составную часть лексики литературного языка, т.е. отказываются от ограничения термина какими-либо требованиями, подчеркивая необходимость изучения реальных процессов функционирования терминологии. По словам Г. О. Винокура, “термины - это не особые слова, а только слова в особой функции... В роли термина может

выступать всякое слово, как бы оно не было тривиально” [Винокур, 1939, с. 5]. Как отмечает В. П. Даниленко, “терминология расценивается как подсистема общелитературного языка, т. е. терминология находится в пределах общелитературного языка, но на правах самостоятельного “сектора”. Такое положение терминологии подчеркивает, с одной стороны, обязательность для нее общих тенденций развития общелитературного языка, а с другой стороны, известную свободу, самостоятельность в развитии терминологии и даже возможность влияния ее на развитие общелитературного языка” [Даниленко, 1971, с. 11].

На данный момент второй подход считается более признанным при исследованиях.

Как было сказано ранее, однозначность - одна из главных особенностей терминов. Эта особенность реализуется двумя способами, согласно двум существующим категориям терминов:

1. Общенаучные и общетехнические;
2. Специальные (номенклатурные).

Первые - передают общие понятия науки и техники; они существуют не только в языке, а в рамках определенной терминологии [Винокур, 1939]. Это значит, что одно слово в общем языке многозначно, но в определенной терминологии оно становится однозначным.

Вторая категория представляет те термины, что появляются в непосредственно в среде научной или производственной деятельности и функционируют, соответственно, только в ней.

Термину не обязателен контекст, так как его контекстом является сама терминология, к которой он принадлежит, и это делает его однозначным.

1.2 Развитие киберпреступности и ее терминологии

На протяжении всего развития человечества человек собирал, хранил и передавал информацию. Все сферы деятельности охвачены непрерывным процессом информатизации - от межличностного общения до государственных проблем.

С развитием технологий, все больше сфер стало зависеть от правильной работы электронных устройств. Малейшая неисправность может остановить работу целого банка, что приведет к большим убыткам. Такие неисправности могут быть как и результатом случайности, так и угрозой извне.

Киберпреступность - это новое понятие, которое уже смогло достичь масштабов мирового сообщества.

Согласно экспертам ООН термин “киберпреступность” относится к любому преступлению, которое совершается с помощью компьютерных систем или сетей [Доклад X Конгресса ООН, 2000].

В XXI веке это считается масштабной проблемой. Пишутся вредоносные программы, программируются вирусы, как правило, с целью получения денег или информации. Ключевой фактор такого развития - это развитие самого Интернета. Никто не может представить жизнь без него, Интернет охватывает все больше и больше сфер, систем и операций. Отсюда появилось осознание, как много можно заработать с помощью одного кода и нескольких нажатий клавиш.

Для борьбы с такими преступлениями была выделена область криминалистики - цифровая криминалистика (digital criminalistics). В России она зародилась в 90-х годах, когда в одном из документов о заключении экспертов появилась фраза “судебно-кибернетическая экспертиза”. Предметом экспертизы были чип-карты для таксофона.

После этого стала формироваться экспертная специализация. Все чаще и чаще под осмотр попадали системные блоки, жесткие магнитные диски и пр. А “судебно-кибернетическая экспертиза” превратилась в “компьютерно-техническую” (к-т.).

В начале XXI века начался процесс обмена экспертным опытом. Среди выпущенных в то время докладов и исследований можно было наблюдать:

- Сборник докладов “Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств”, Москва: 2000 г.;
- Мещеряков Владимир Алексеевич “Основы методики расследования преступлений в сфере компьютерной информации”, 2001 г.;
- Усов Александр Иванович “Концептуальные основы судебной компьютерно-технической экспертизы”, 2002 г.

Затем началась профессиональная краткосрочная переподготовка экспертов компьютерной (к-т. экспертизы):

- 2002-2003: подготовка программы обучения экспертов к-т. экспертизы для Минюста России и МВД России только в Саратовском юридическом институте МВД России;
- 2003: первые в России сборы экспертов к-т. экспертизы для Минюста России;
- 2004: первые в России сборы экспертов компьютерной экспертизы для МВД России.

В Саратовском юридическом институте появились такие рабочие программы, как “Компьютерная экспертиза” и программы повышения квалификации экспертов по спецкурсу. Именно в этот период стали появляться учебные пособия по расследованию компьютерных преступлений.

В последнее десятилетие появилось высшее образование по цифровой криминалистике на базе МГТУ им. Н.Э. Баумана. Там изучаются преступления с использованием IT-технологий, виртуальные следы в кибернетическом пространстве, цифровые доказательства и разрабатываются специальные приемы, методы и средства.

Терминологический корпус цифровой криминологии, как таковой, никогда не был отдельно рассмотрен - в основном, из-за новизны науки и отсутствия конкретных источников информации. Из того небольшого количества материала, что было обнаружено, можно заметить, что очень много понятий, которые можно “перенести” в компьютерный мир из криминологии без измены сути термина, просто приобрели приставку “кибер” или “компьютерно-” и т.д. А другие были заимствованы из зарубежных научных баз, где темп развития киберкриминалистике был гораздо быстрее. Такие термины уже подвергались некоторым изменениям - это может быть транскрибирование, калькирование, описания. На данный момент перевод сводится к минимуму. В силу того, что, в основном, киберпространство наполнено молодыми людьми, специалистами, они менее подвержены переносу термина в свой язык, нахождению эквивалента и пр., предпочитая использовать уже существующую английскую единицу. С одной стороны, это гораздо упрощает пользование различными механизмами, так как много работы, алгоритмов, языков программирования осуществляются именно на английском. Его знание, можно сказать, обязательно, в такой сфере деятельности. Но с другой, для незнающего человека, для неопытного переводчика такого рода тексты могут стать препятствием. Хотя также могут стать целым “полем” для исследования терминологического корпуса.

Трудно сказать, из-за чего за рубежом этот процесс происходит быстрее. Однако, это очевидно. В ходе поиска материала для анализа в

практической части, были найдены различные электронные ресурсы-глоссарии. Они не носили официальный характер и были составлены скорее из-за нужды обычных пользователей, нежели ради упрощения и структуризации исследований о таких терминах. Но сам факт наличия показывает, что происходит процесс накопления информации по выбранной тематике, и он происходит быстрее, чем в России.

На данный момент, в России в этой сфере происходит реализация ее перспектив. Одной из задач, поставленных специалистами, является развитие методической, образовательной, научной базы цифровой криминалистики. Можно сказать, что данное исследование - это начало исполнения такой задачи.

1.3 Структурная классификация терминов киберпреступности

Однословные термины считаются одними из самых распространенных терминов в английском языке. Для образования терминов используются различные суффиксы и префиксы, которые общеиспользуемы в обычных словах языка. Что является специфичным в образовании специальных терминов, так это закрепление за некоторыми суффиксами какого-либо терминологического значения.

Такое особенно характерно в химической, медицинской, биологической и криминалистической терминологии. В других отраслях значений суффиксов почти совсем нет. В связи с этим, они имеют гораздо более широкое значение - они показывают категорию самого термина.

Например, при помощи суффиксов *-er*, *-or*, *-ist* образуются существительные, именующие работников и специалистов:

1. (computer) special*ist* (компьютерщик)
2. develop*er* (разработчик)
3. (security) offic*er* (сотрудник службы безопасности)
4. hack*er* (хакер)

Существительные, определяющие конкретные предметные значения, образуются с помощью суффиксов *-ing*, *-ment*:

1. e-Govern*ment* (электронное правительство)
2. spoof*ing* (подмена, подделка)

Отвлеченное значение в существительных передается через суффиксы свойств и качеств *-ness, -ty*:

1. (system) integri*ty* (целостность системы, уровень надежности с.)
2. weak*ness* (уязвимость, слабое место)

Технологические процессы и действия отражаются в суффиксе *-ing*:

1. trunk*ing* (перемещение лиц между адресами)
2. broadcast*ing* (трансляция)

Однословные термины могут состоять из любого количества словообразовательных компонентов. Поэтому их можно разделить на такие группы:

1. с одной основой
    a. byte (байт)
    b. filter (фильтр)
    c. monitor (дисплей)
    d. net (сеть)
2. с основой и с одним или более аффиксом
    a. transceiver (передатчик)
    b. selector (ручка настройки)

Термины-словосочетания гораздо более устойчивы, чем общелитературные словосочетания. В них компоненты не могут быть заполнены любым словом, только словом определенной семантической группы.

В терминологии киберпреступности существует огромное количество таких многокомпонентных терминов. Грамматическое оформление в них может быть выражено тремя способами:

1. суффиксами
    a. outsid*er* threat (внешняя угроза безопасности)
2. предлогами
    a. Continuity *of* Operations (обеспечение непрерывности действий)
3. окончаниями
    a. risk-bas*ed* data (данные с учетом рисков)

Вся классификация, изложенная выше, представлена в виде таблицы в Приложении А.

1.4 Трудности перевода терминологии киберпреступности с английского языка на русский язык

Одними из самых распространенных трудностей при переводе текстов о киберпреступности являются аббревиатуры, в силу того, что “аббревиация рассматривается как один из наиболее продуктивных способов словообразования” [Ступин, 2003].

Их основная задача - экономия речи; перенос смысловой единицы в максимально емкой форме [Волошин, 2005]. Преимущества такой экономии есть, но только не для переводчика. Зачастую, аббревиатуры становятся настоящим препятствием на пути к правильному переводу [Гончаров, 2003]. Даже часто употребляемые сокращения могут поставить в тупик. Например, *AIC* (Aeronautical Information Circular) правильно переведется как *АИЦ* (Аэронавигационный информационный циркуляр), однако переводчики часто называют его АИК. Что же тогда говорить об аббревиатурах из редко упоминающихся сфер, если даже известные могут вызывать вопросы.

Перепутать два разных сокращения с двух разных тематик перевода достаточно легко. Например, рассмотрим аббревиатуру *DAC*.

В компьютерной безопасности, *DAC* расшифровывается как *Discretionary Access Control* и переводится как избирательное управление доступом - управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа [33; 34].

В научных текстах *DAC* можно увидеть в значении ячейки с алмазными наковальнями - *Diamond Anvil Cell*. Это конструкция, используемая в определенных научных экспериментах с давлением и температурой [36].

В сети также можно найти такое сокращение как название игры *Divide and Conquer*.

Divide-and-conquer algorithm - термин используемый в информатике, означающий алгоритм рекурсивного разбиения задачи на подзадачи [34].

Два термина из четырех вышеупомянутых относятся к родственным тематикам - информатика, компьютерная безопасность, но обозначают совершенно разные вещи.

Переводчик должен обладать достаточными знаниями, чтобы суметь выбрать требуемый вариант перевода. Один из самых принятых методов решения такой проблемы - это, конечно же, обращение к словарям. Но это далеко не всегда легко. Например, могут быть расхождения в значении термина в английском и русском языках - следовательно, использовать казалось бы эквивалентное слово нельзя.

Огромную сложность также могут составить слова-ловушки, которые переводчики привыкли видеть только в общеупотребительной лексике. С такими терминами как *packet* (сетевой блок данных) можно не беспокоиться - и в русском языке это называют пакетом, но, например, слово *flooding* может ввести в заблуждение. Всем известно, что оно переводится как затопление, наводнение. Но в компьютерной области, *flooding* - это алгоритм атаки системы путем перенасыщения ее информации. В русскоязычных источниках, это, как правило, переводят как флудинг.

Неологизмы - явление, не редко встречающееся на просторах сети. Именно в компьютерной сфере для них заключается большая потребность. Один из самых популярных типов неологизмов в терминологии киберпреступности - омофоны - “слова, которые произносятся одинаково, а пишутся по-разному” [Стариченок, 1999, с. 94].

Например, *pharming* (созвучное с *farming*) - процедура скрытного перенаправления жертвы на ложный IP-адрес. Это явление, согласно многим владельцам крупных корпораций, так назвали ради маркетингового хода, чтобы привлечь больше компаний к покупке защитных программ. Тоже самое относится к термину *phishing* (созвучное с *fishing*) - вид интернет-мошенничества для получения доступа к конфиденциальным

данным пользователей. К счастью, такого рода термины на русский язык переводятся просто - с помощью транскрибирования: *фарминг* и *фишинг*. Отсюда, задача переводчика лишь в том, чтобы научиться разбираться, когда термин устоялся в русском языке через такие способы как транслитерация или транскрипция, а когда его нужно переводить.

1.5 Корпусная лингвистика и ее важность при переводе

Для лингвистических исследований, для обработки большого количества информации и извлечения из них еще б*о*льшего количества лингвистических и литературоведческих данных появилась потребность в более эффективном и масштабном способе решения таких задач.

Это обусловило появление и рост таких ресурсов как лингвистические корпуса, которые изучает корпусная лингвистика - неотъемлемая часть деятельности лингвистов.

Корпус - это собрание электронных текстов, которые обработаны с помощью специальных программ (в данном исследовании - это TermoStat [33]) для поиска и анализа информации.

“Корпусная лингвистика занимается такими вопросами как:

- какие принципы лежат в основе устройства корпусов;
- как должна быть устроена стандартизованная разметка корпуса относительно различных языковых параметров;
- какие лингвистические и литературоведческие задачи можно решать с помощью корпусов;
- как пользоваться корпусами, включая специальные языки запросов к корпусам” [Захаров, Богданова, 2011].

Корпусная лингвистика рассматривает создание и использование параллельных корпусов, что помогает в решении вышеупомянутых задач, а также в “создании и настройки систем машинного перевода, сравнительном изучении языка, развитии теории переводоведения и обучении языкам” [Митрофанова, Захаров, 2009].

Параллельные корпуса также называются переводными - translation corpora. В них рассматриваются тексты-оригиналы на исходном языке и их переводы на одном или нескольких других языках. Результаты таких исследований приводят к выявлению более эффективных стратегий перевода

- анализируются стратегии, грамматика и лексика переводов в сравнении с оригиналом, стилистические явления и способы их передачи.

Корпус языка - это также ресурс извлечения терминов и терминологии. Корпуса особенно важны при изучении специальных текстов, тематик, которые отображают знания по конкретным предметным областям. Они позволяет наглядно увидеть их структуру, частотность определенных терминов, характеристику и пр. Они могут быть использованы при составлении терминологических ресурсов, классификаторов, при машинном переводе и информационном поиске.

Отсюда следует подчеркнуть важность корпусной лингвистики. Такие корпуса представляют огромный массив важного материала для лингвистов, переводчиков, переводоведов, особенно если этот материал нацелен на какие-либо новые, развивающиеся области знаний - такие, как компьютерно-технические экспертизы, кибербезопасность и киберпреступность.

В данном исследовании будет проведен статический терминологический анализ по книге выбранной тематики, чтобы пронаблюдать часть ее лингвистического корпуса и выявить основные черты и способы перевода. Это может послужить началом к будущему созданию специального корпуса по киберпреступности, который мог бы использоваться и как способ поиска информации, и как основа сравнительно-сопоставительных анализов научной терминологии (на примере киберпреступности).

Выводы по главе 1

Обобщив все вышеизложенное и соглашаясь с мнениями различных ученых, под термином можно понять слово или словосочетание, которое соотнесено со специальным понятием, предметом или явлением в системе какой-либо области знания. “Главными признаками терминологических языковых единиц считаются соотнесенность с определенным научным понятием, точность и системность. Такие требования как однозначность и краткость, в связи с полисемантичностью и многокомпонентностью многих терминов, не могут рассматриваться как обязательные для терминоединиц” [Лантюхова, Загоровская, Литвинова, 2013].

Терминология - составная часть лексики литературного языка, самостоятельная, но не изолированная, что подразумевает ее способность следовать общим тенденциям развития литературного языка с одной стороны, но и определенную независимость с другой. Функция ученого в большей степени заключается в изучении и описании состояния терминологических систем, а не в их жестком искусственном регулировании.

Была подчеркнута важность корпусной лингвистики. Благодаря корпусам переводчики могут решать различные проблемы с эквивалентностью и сочетаемостью терминов, что также играет большую роль при создании терминологических словарей [Берков, 2004].

В данном разделе определились сложности перевода перевода именно упомянутой тематики. Выделены две самые распространенные - аббревиатуры и сложные слова. И того, и другого в киберкриминалистике с избытком. Основная специфическая черта перевода аббревиатур киберпреступлений - то, что большинство из них никак не переводятся, используются английские аббревиатуры, а переводится только расшифровка. Переводчику важно знать, что определенные английские инициалы могут встречаться как и в оригинальной своей форме, так и в русской расшифровке.

Проанализировав многие термины электронного словаря *Cybrary* к структурной классификации можно добавить примерную классификацию основных сложностей перевода данной тематики и принятые способы их решения [33].

Составные аббревиатуры, такие как *DoS-attack*, переводятся лишь частично. Аббревиатура сохраняется на английском языке, а вторая часть, само слово, переводится, либо передается транскрипцией как с термином *SYN-flood*. Аббревиатуры инициального типа требуют самостоятельного изучения и проверки в соответствующих источниках - в их переводе определенной устоявшейся схемы не имеется. Однако, в большинстве случаев, они никак не переводятся и не изменяются.

Неологизмы, появляющиеся в корпусе терминологии киберпреступности и кибербезопасности в большинстве случаев транслитерируются или транскрибируются. Как например, фишинг - fishing.

Вышеизложенная классификация была оформлена в виде таблицы и представлена в Приложении Б.

Глава 2. Особенности перевода терминов киберпреступности с английского языка на русский язык

2.1 Статистический терминологический анализ

На основе материала *Cyber Security Essentials* был проведен статический терминологический анализ с помощью веб-сайта *TermoStat* [35].

TermoStat - это инструмент, разработанный Патриком Друином в Обсерватории лингвистики Sens-Texte (OLST) в Университете Монреаля; он представляет собой онлайновый экстрактор терминов, который использует гибридный (статистический плюс лингвистический) метод для определения подходящих терминов. Он учитывает не только структуру потенциальных терминов-кандидатов (используя программу, называемую *part of speech tagging* (отметкой части речи), чтобы идентифицировать существительные и прилагательные, и сложные структуры, которые содержат эти элементы), но также и относительные частоты этих потенциальных кандидатов в тексте. Этот метод позволяет *TermoStat* находить не только несколько слов, но и термины-кандидаты, состоящие из одного слова в одном процессе извлечения. Этот инструмент также позволяет сравнивать результаты различных подходов к извлечению терминов.

Чтобы получить точный подсчет количества вхождений каждого термина-кандидата, *TermoStat* использует процесс, известный как лемматизация: он преобразует изогнутые формы слов, которые появляются в корпусах, в базовые формы (например, преобразует множественное число существительных на единственное). После того, как это сделано, все формы могут считаться вхождениями одного термина, а не отдельными терминами.

Вследствие этого, результаты *TermoStat* включают два отдельных поля: в столбце “Кандидат” (вариант группировки) отображается форма предполагаемого члена с восстановленными в его базовой форме

компонентами, а в столбце “Варианты” отображаются формы, фактически найденные в самом тексте.

Обработка выбранного текста позволила напрямую увидеть терминологические составляющие текста тематики “киберпреступность”. Всего было обнаружено 2239 терминов.

Из них преобладают существительные (N) - всего их около 35%: *system, code, user, network,* и пр.

На втором месте - сочетание двух существительных (N+N) - 25%: *exploit tool, authentication system*, и пр.

И на третьем - сочетания прилагательного и существительного (Adj+N) - 21%: *malicious code, symmetric encryption, infected system,* пр.

Все стальные компоненты предложения заняли меньше 10%. В том числе и глаголы (V) - лишь 9%.

На рисунке в Приложении 3 изображено “облако” терминов, где можно увидеть соотношение используемых в тексте слов с конкретными примерами.

Стоит отметить, что вышеперечисленные термины можно разделить по степени сложности (по количеству компонентов), что также было отображено в таблице 1 Приложения А:

- однокомпонентные - 44% (990 слов):
  - N: *network*, *attack*;
  - V: *to operate*, *to execute*;
- двухкомпонентные - 46% (1032 слова):
  - N+N: *domain name*, *exploit tool*;
  - Adj+N: *malicious activity*, *initial thread*, *public key*;
- трехкомпонентные - 7.1% (166 слов):
  - Adj+N+N: *stack-based buffer overflow*, *central processing unit*;
  - N+Prep+N: *denial of service*;
  - N+N+N: *domain name system*, *rogue antivirus application*;

- N+Adj+N: *server takedown attempt*.

- и т.д.

Заметно, что в корпусе доминируют однокомпонентные и двухкомпонентные термины, при этом процент вторых чуть больше первых.

Однокомпонентные термины какой-либо сложности для перевода не представляют. Двухкомпонентные и более подразумевают перед переводом поиск главного слова и определение связи между компонентами.

Согласно классификации Л. С. Бархударова и В. М. Кулешовой, представленной в статье “Международного журнала гуманитарных и естественных наук” многокомпонентные термины также можно разделить по структуре [Васильева, 2017]:

1. Многокомпонентные терминологические словосочетания регрессивной структуры: модификатор (может быть представлен прилагательным, существительным, причастием и т.п.) + ядерный элемент (как правило, это существительное, последнее в ряду). В русском языке они меняются местами. Такие сочетания переводятся, начиная с главного слова [Гринев-Гриневич, 2008]:
    a. *server takedown attempt* - попытка захвата сервера
       (модификатор) (ядро) - (ядро) (модификатор)
    b. *domain name system* - служба имен доменов
       (модификатор) (ядро) - (ядро) (модификатор)
2. Многокомпонентные терминологические словосочетания прогрессивной структуры: ядро (первое в ряду) + модификатор. Перевод осуществляется с главного слова:
    a. *denial of service* - отказ в обслуживании
       (ядро) (мод.) - (ядро) (модификатор)

Благодаря такой классификации гораздо легче увидеть приемы перевода, относя их к определенному типу терминосочетания. Такие стратегии зависят от двух факторов.

Первый - порядок слов:

- дословный перевод, калькирование: использование русских терминосочетаний, в которых порядок элементов остается таким же как в английском языке:
- инверсия: смена порядка элементов

Второй - сам перевод, используемые приемы:

- грамматические трансформации
    - смена части речи (существительное в прилагательное)
    - перестановка и морфологическая трансформация (существительное в род. падеже)
    - добавления (например, предлогов для отображения разных типов связи в языках)
- лексические трансформации
    - конкретизация
    - опущение слов

Также довольно часто термин или терминосочетание требуют сочетание нескольких приемов - особенно, если разбить многокомпонентные термины - каждая связь отличается от другой и может переводится по-разному. Соответственно, для таких сочетаний конкретного, стандартного метода перевода быть не может. Он осуществляется только через разделение компонентов и их перевода.

В таблице Приложения А, такие термины были поделены по типу связи - суффиксально-оформленные, предложно-оформленные, оформленные окончанием. При изучении можно обнаружить пересечения с предыдущей классификацией, например, предложно-оформленные многокомпонентные

термины также относятся (или даже составляют) многокомпонентные терминологические словосочетания прогрессивной структуры. В статистике TermoStat можно найти примеры к каждому типу:

- суффиксально-оформленные: *symmetr*ic *encryption*, *malic*ious *code*;
- предложно-оформленные: *denial* of *service*, *impact* of *fast-flux*;
- оформленные окончанием: *infect*ed *system*, *stack-bas*ed *buffer overflow*.

Сочетания (особенно такие, где больше двух компонентов) также можно разделить по устойчивости (по делимости и наличию терминов и терминосочетаний):

- устойчивые (неделимые смысловые единицы)
- неустойчивые: *maximum number of* iteration, malicious code *author* и пр.

В программе TermoStat также можно увидеть список терминов-кандидатов, которые группируются с другими.

Наиболее часто используемый кандидат в тексте - *system*. Он был использован более 600 раз. Он стал частью таких терминологических словосочетаний как: *infected system, authentication system, prevention systems, encryption system, host system, system administrator, obfuscation system, fast-flux system* и пр.

Этот термин можно назвать свободным. Он примыкает к словам в свободном порядке - и в качестве главного слова, и зависимого. При переводе это сохраняется в свободном выборе части речи - он то выступает в качестве прилагательного (*system* administrator - *системный* администратор), то существительного (encryption *system* - шифровальная *система*).

Такая морфологическая свобода - это реакция на “синтаксическую скованность и постоянство структуры в английском языке” [Черняховская,

2004]. Она называется конверсией (или нулевой деривацией) - приобретением словом качеств другой речи [Аполлова, 2004]. Как видно по анализу терминологического корпуса, его компоненты довольно часто проходят через процесс конверсии. Следовательно слова-термины можно поделить на:

- неконверсивные - выступают только в качестве главного слова, существительного:
    - *information* (268 случаев употребления): sensitive *information* - critical *information* - valuable *information* - nonpublic *information* - private *information* - personal *information*;
    - *attack* (292 с. у.): phishing *attack* - injection *attack* - social-engineering *attack*;
- конверсивные - выступают и в качестве главного слова и зависимого, меняют часть речи:
    - *user* (484 с. у.) : limited *user* - *user* interface - *user* input;
    - *network* (294 с. у.) : *network* traffic - *network* service - private *network*;

В переводе такое соотношение сохраняется. Смена частей речи или их неизменчивость отражается и в русском языке.

2.2 Анализ перевода терминов киберпреступности на материале “Cyber Security Essentials”

Cyber Security Essentials - книга, выпущенная в 2011 году в США под редакцией Джеймса Грэма, Ричарда Ховарда и Райана Олсона. Она представляет собой коллекцию статей о безопасности и разведывательных данных, рассказывает о терминах по тематике и об уязвимостях компьютерных систем.

Реципиент такого материала - широкий круг читателей, в частности те, кто интересуется кибербезопасностью или те, кто хотят обезопасить свое киберпространство - специалисты охраны, IT-специалисты и пр.

Текст написан в научном стиле - он строг и логичен. Использованы термины, излагается объективная информация. В нем отсутствует лишняя эмоциональность и присутствует обезличивание речи.

Коммуникативная цель авторов состояла в том, чтобы предоставить читателям информацию об опасностях цифрового мира и предписать безопасные действия, следовательно, ведущие функции текста - денотативные и командные.

Ведущая архитектонико-речевая форма - монолог, а композиционно-речевая - повествование.

В данном тексте содержатся следующие виды информации:

- когнитивная (объективные сведения)
- оперативная (побуждения)

При этом распределение данных видов является неоднородным. Оперативная информация является важной, однако ведущую роль играет все же когнитивная. На уровне текста это проявляется в атемпоральности (использовании настоящего времени), а на уровне предложения - в нейтральном порядке слов, без высокой эмоциональности и соответствующему тема-рематическому членению:

“*Computer worms constitute a large class of malicious code that spreads between computers by distributing copies of themselves in a variety of ways*.” - “*Компьютерные черви представляют собой большой класс вредоносного кода, который распространяется между компьютерами через саморепликацию различными способами*.”

При переводе эти характеристики нужно учитывать - сохранение времени, безэмоциональности.

“*The security community separates viruses into two groups based on how the virus infects other files after it executes: resident and nonresident*.” - “*Сообщество безопасности разделяет вирусы на две группы в зависимости от того, как вирус заражает другие файлы после своего запуска: резидентные и нерезидентные.*”

На уровне слова объективность проявляется в терминах, несущих однозначность и эмоциональную неокрашенность. В первом указанном примере это термины “*computer worm*” и “*malicious code*”. Первый построен по схеме существительное плюс существительное (атрибутивное сочетание), второй - прилагательное плюс существительное. Данные термины не представляют особых сложностей для перевода, они не являются неологизмами или аббревиатурами и переводятся дословно - “компьютерный червь” и “вредоносный код”.

Плотность (компрессивность) свойственна только когнитивной информации. Она выражается лексическими сокращениями, а именно аббревиатурами:

“*The XOR cipher uses a key and the XOR operator to encrypt the virus’s code, and the same key and XOR operator to decrypt the code.*”

В данном примере можно наблюдать все те же вышеупомянутые характеристики - атемпоральность, членение, безэмоциональность, и помимо этого новое выражение когнитивности на уровне слова - аббревиатуру *XOR*.

Как было установлено в теоретическом исследовании аббревиатур по киберпреступлениям, аббревиатуры такой тематики бывают двух типов. В этом случае, *XOR* - аббревиатура инициальная, следовательно, аббревиатура остается неизменной в переводе:

"*Шифр XOR для шифрования кода вируса использует ключ и оператор XOR, и то же самое для его дешифрования.*"

В этом же предложении можно заметить использование приема упущения при переводе - так как во второй части предложения речь идет о тех же компонентах "*the same key and XOR operator*", при переводе это можно опустить и заменить на "*то же самое*". Такое сокращение возможно в данном тексте за счет его стиля, которому свойственна плотность.

Были обнаружены и примеры составных аббревиатур, где переводится лишь ее часть:

"*The purpose of Blaster was to strike Microsoft's Windows Update website with a* DDoS-attack *that the worm would launch on August 15, 2003.*"

"*Цель Blaster состояла в том, чтобы поразить сайт Microsoft Windows Update с помощью* DDoS-атаки*, которую червь запустил 15 августа 2003 года*."

Оперативная информация - это побуждение к выполнению каких-либо действий через применение побудительных средств (все формы глагольного императива, инфинитив со значением императивности, модальные глаголы, глагольные конструкции со значением возможности и необходимости, модальные слова, лексические интенсификаторы (никогда, обязательно)). Например,

"*To minimize the chances of successful DLL injection, administrators* should *assign the least privileges necessary to users' account*s."

В приведенном примере, оперативная информация выражена через модальный глагол "*should*", тем самым выражая побуждение.

Также в этом примере присутствует термин *DLL*. Как и *XOR*, он является инициальным и не переводится:

“*Чтобы свести к минимуму шансы на успешное внедрение DLL, администраторы* должны *назначать только самые необходимые права, необходимые для учетных записей пользователей.*”

В следующем примере, оперативная информация передана модальным глаголом “*must*”:

“*To mitigate the threat from computer worms, administrators* must *protect systems from all propagation techniques*.” - “*Чтобы уменьшить угрозу со стороны компьютерных червей, администраторы* должны *защищать системы от всех методов распространения.*”

Опираясь на лингвостилистический анализ оригинала текста, были разработаны стратегии его перевода.

Однозначными эквивалентными или традиционными соответствиями переводились даты, имена собственные и общепринятые термины:

“*The Morris worm, released by Robert Morris in 1988, was one of the first worms to spread on the Internet*.”

“*Червь Морриса, запущенный Робертом Моррисом в 1988 году, был одним из первых червей, распространяющихся в Интернете*.”

Robert Morris - Роберт Моррис; the Morris worm - червь Морриса.

В некоторых случаях, перевод какой-либо лексемы происходил через вариантные соответствия. Например, если он зависел от контекста:

“*The worm spread over the Internet by exploiting multiple known* vulnerabilities.”

“*Vulnerability*” можно перевести и как уязвимость, и как ранимость, и как степень защищенности. Однако, в компьютерных технологиях возможен лишь первый вариант:

“*Червь распространился по Интернету, используя многочисленные известные* уязвимости.”

“*One of the most famous worms of 2009, Conficker spread through USB drives and through a* vulnerability *in the Windows Server Service (MS08-067).*” - “*Один из самых известных червей 2009 года, Conficker распространился по USB-накопителям и через* уязвимость *в Windows Server Service (MS08-067).*”

Некоторые предложения требовали грамматических трансформаций.

Например, перестановки. Английскому языку свойствен фиксированный порядок слов в предложении, в русском - он относительно свободный:

“*An often slow but effective propagation technique that worms use is copying themselves to USB drives.*” - “*Копирование на USB-накопители - это техника эффективного, но в большинстве случаев медленного, распространения.*”

“*To avoid detection of the decryption routine,* a technique *called polymorphism* surfaced.” - “*Чтобы избежать обнаружения процедуры расшифровки,* появилась методика*, называемая полиморфизмом*.”

Благодаря выведенной классификация терминов киберпреступности по словообразовательным компонентам в Приложении А, были определены типы терминов и стали видны типичные способы перевода каждого из них.

Многокомпонентные термины, оформленные суффиксальным способом, в русском языке связаны через тип связи “управление”:

“*Another technique, called metamorphism, allows a virus to change its appearance to avoid* antivirus detection.” - “*Другой метод, называемый метаморфизмом, позволяет вирусу изменять свой внешний вид, чтобы избежать* обнаружения антивирусом.”

“*Network worms, which often spread without any* user interaction, *can infect many computers in a very short amount of time.*” - “*Компьютерные черви,*

которые часто распространяются без какого-либо взаимодействия с пользователем*, могут заразить множество компьютеров за очень короткое время.*"

"*As with worms that spread through e-mail, those that spread through P2P networks must also rely on* social-engineering techniques *rather than automatic propagation*." - "*Как и в случае с червями, распространяющимися по электронной почте, те, которые распространяются по сетям P2P, должны также полагаться на* методы социальной инженерии*, а не на автоматическое распространение*."

"*The concept of viruses and malware has been with us for decades, along with the development of* detection technologies." - "*Концепция вирусов и вредоносных программ была с нами на протяжении десятилетий, наряду с развитием* технологий обнаружения."

Предложно-оформленные многокомпонентные термины не имеют определенной схемы при переводе, они просто переводятся описательным методом:

"*Apply* patches for vulnerabilities *in network services in a timely manner.*" - "*Своевременно устанавливайте* патчи, направленные на закрытие уязвимостей *в сети.*"

Многокомпонентные термины, оформленные окончанием, при переводе могут обретать типы связи "согласование" или "управление":

"*Two common criteria used to infect other files are* timebased *(such as only infecting files on certain days) and* access-based *(such as only infecting copied files)* criteria." - "*Два распространенных критерия, используемых для заражения других файлов - это* критерий времени *(например, заражение файлов только в определенные дни) и* критерий доступа *(например, заражение только скопированных файлов).*"

“*USB worms configure the* infected drives *to execute the worm as soon as an unsuspecting user plugs it into a computer.*” - “*USB-черви настраивают* зараженные накопители *для запуска червя как только ничего не подозревающий пользователь подключает его к компьютеру.*”

“*A* virus*, on the other hand, is not* self-contained *and requires the infection of a host file to spread*.” - “*А вот* вирус *не является* автономным *и требует распространения зараженного файла*.”

Выводы по главе 2

На основании анализа текста и состава информации в нем можно сделать следующие выводы. Данный текст является довольно неоднородным, он содержит большое количество общей и специальной терминологии и общенаучной лексики. Все эти характеристики влияют, в первую очередь, восприятие текста, а также непосредственно перевод. Особая важность в том, что это научный текст, и вся информация должна быть передана точно, поэтому важно следить за эквивалентностью перевода.

При работе с TermoStat был наглядно показан корпус терминологии киберпреступности и проанализированы его компоненты, их процентность, связи между собой и употребление.

В целом, на основе и текста и статистического анализа можно выделить следующие свойственные черты такой терминологии:

- преобладание многокомпонентной лексики (особенно двухкомпонентной; на втором месте - однокомпонентная, на третьем - трехкомпонентная и т.д.);
- неустойчивость терминологических сочетаний;
- конверсивность терминов, сохраняющаяся при переводе;
- большое количество аббревиатур (и инициальных, и составных) и транскрибируемых неологизмов.

Заключение

Терминология и ее перевод - особенно более узких сфер, таких как киберпреступность - играют важную роль в переводоведении и в лингвистике (в частности, в корпусной лингвистике).

Данное исследование во многом было первооткрывателем, в силу новизны темы.

В ходе работы была изучена терминология киберпреступности в сравнительно-сопоставительном аспекте на примере английского и русского языков, проведен анализ корпуса терминологии киберпреступности на основе программы TermoStat и особенностей их перевода на примере книги 2011 года “Cyber Security Essentials” под редакцией Джеймса Грэма, Ричарда Ховарда и Райана Олсона.

Для достижения данной цели были изучены понятия “термин” и “терминология”, была выработана классификация терминологии киберпреступности по структуре образования для определения тенденции в образовании новых терминов, были определены функции и классификация способов перевода терминов в указанной сфере.

На практике были рассмотрены роль корпусной лингвистики в переводческой деятельности и конкретные характеристики лингвистического корпуса по терминологии киберпреступности, выявлены основные сложности перевода по выбранной тематики и рассмотрены основные способы перевода терминов. На примере выбранного фрагмента из книги “Cyber Security Essentials” был осуществлен предпереводческий анализ и переводческий комментарий.

Результаты, полученные на нынешнем этапе работы, могут послужить началом более глубоких исследований в этой малоизученной сфере и могут использованы при разработке терминологического корпуса.

Библиографический список

1. Аполлова М. А. Грамматические трудности перевода - М, 2004. - с. 110
2. Арбекова Т. И. Лексикология английского языка.- М, 2002. - с. 109.
3. Берков В. П. О словарных переводах/ Мастерство перевода - М, 2004. - с. 112.
4. Васильева С. Л. Особенности перевода многокомпонентных терминов в английском языке (на примере сферы природопользования) / С.Л. Васильева, А. В. Гаврилова // Международный журнал гуманитарных и естественных наук. – 2017. –Т. 2. №3. – С. 61-64.
5. Винокур Г. О. О некоторых явлениях словообразования в русской технической терминологии. М., 1939. С. 3-54.
6. Володина М. Н. Когнитивно-информационная природа термина и терминологическая номинация: Дисс. докт. филол. наук: М., 1998-178.
7. Волошин Е. П. Аббревиатуры в лексической системе английского языка: Дисс. канд. филол. наук. М, 2005. - с. 12.
8. Гончаров Б. А. К вопросу о типологии и переводе сокращений в англоязычной научно-технической литературе. // Теория и практика перевода. - Киев, 2003. - Вып. 17.
9. Даниленко В. П. Лексико-семантические и грамматические особенности слов-терминов. М.: Наука, 1971. С. 7-67.
10. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями. 2000.
11. Гореликова С. Н. Природа термина и некоторые особенности терминообразования в английском языке // Вестник ОГУ. 2002. №6.

12. Гринев-Гриневич С. В. Терминоведение / Учебное пособие для студентов высших учебных заведений. М.: Издательский центр Академия, 2008. 304 с.
13. Захаров В. П., Богданова С.Ю. Корпусная лингвистика / Учебник. Иркутск, 2011. - с. 43
14. Канделаки Т. Л. Семантика и мотивированность терминов. - М.: Наука, 1977. - с. 15
15. Капанадзе Л. А. О понятиях «термин» и «терминология» // Развитие лексики современного русского языка. М., 1965. С.75 - 86.
16. Комиссаров В. Н. Теория перевода (лингвистические аспекты): Учеб. для ин-тов и фак. иностр. яз. - М.: Высшая школа, 1990. - 253 с.29.
17. Кутина Л. Л. Языковые процессы, возникающие при становлении терминологических систем. / Л. Л. Кутина // Лингвистические проблемы научно-технической терминологии. — М., 1970. — С. 82-95.
18. Лантюхова Н. Н., Загоровская О. В., Литвинова Т. А. Термин: Определение понятия и его сущностные признаки. // Вестник Воронежского института ГПС МЧС России. 2013. №1 (6). - с. 42.
19. Лотте Д. С. Образование системы научно-технических терминов // Основы построения научно-технической терминологии М., 1961.
20. Митрофанова О. А., Захаров В.П. Автоматизированный анализ терминологии в русскоязычном корпусе текстов по корпусной лингвистике / Доклад: Санкт-Петербургский государственный университет. Институт лингвистических исследований РАН, 2009.
21. Овчаренко В. М. Термины, аналитическое наименование и номинативное определение // В кн. Современные проблемы терминологии в науке и технике. М., 1969.
22. Пумпянский А. Л. Введение в практику перевода научной и технической литературы по английскому языку. - М, 2004 г.

23. Реформатский А. А. Введение в языковедение: учеб. для филол. фак. пед. ин-тов / А. А. Реформатский. 4-е изд-е, испр. и доп. М.: Просвещение, 1967. — 542 с.
24. Реформатский А. А. Что такое термин и терминология? // Вопросы терминологии. М., 1961. С. 49 - 51.
25. Ступин Л. П. Аббревиатуры и проблема их включения в толковые словари. // Вопросы теории и истории языка. - С-Пб, 2003. - с. 291.
26. Современный русский язык: Анализ языковых единиц: Учеб. пособие для студентов филол. ф-тов пед. ун-тов и ин-тов. В 3-х ч. Ч. 1. Фонетика и орфоэпия. Графика и орфография. Лексикология и фразеология. Словообразование. Морфология / Под. общ. ред. В. Д. Стариченка. Мн., 1999.
27. Сусименко Е. В., Рождественская С. В. Проблемные аспекты в определении научного термина и его свойств. Филологические науки. Вопросы теории и практики. Тамбов, 2012. С. 136.
28. Толикина Е. Н. Некоторые лингвистические проблемы изучения термина // Лингвистические проблемы научно-технической терминологии.
29. Толикина Е. Н. Некоторые лингвистические проблемы изучения термина // Лингвистические проблемы научно-технической терминологии.
30. Черняховская Л. А. Перевод и смысловая структура. - М, 2004. - с. 44
31. Шаповалова А. П. Аббревиация и акронимия в лингвистике. Ростов н/Д., 2003. - с. 80-84
32. Cyber Security Glossary [Электронный ресурс]. URL: https://www.cybrary.it/glossary

33. Glossary. Explore Terms: A Glossary of Common Cybersecurity Terminology [Электронный ресурс]. URL: https://niccs.us-cert.gov/about-niccs/glossary
34. TermoStat Web [Электронный ресурс]. URL: http://termostat.ling.umontreal.ca
35. Wikipedia [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Main_Page

Приложение А

Таблица 1 - Классификация терминов киберпреступности по словообразовательным компонентам:

Категории	Типы	Подтипы	Примеры
Однокомпонентные	Непроизводные (одна основа)	-	byte, filter, monitor, net, etc.
	Производные (основа + аффиксы)	именительные	develop*er*, hack*er*,
		предметные	e-Govern*ment*
		отвлеченные	integri*ty*, weak*ness*
		процессные	trunk*ing*, broadcast*ing*
Многокомпонентные	суффиксально-оформленные	-	outsid*er* threat
	предложно-оформленные	-	Continuity *of* Operations
	оформленные окончанием	-	risk-bas*ed* data

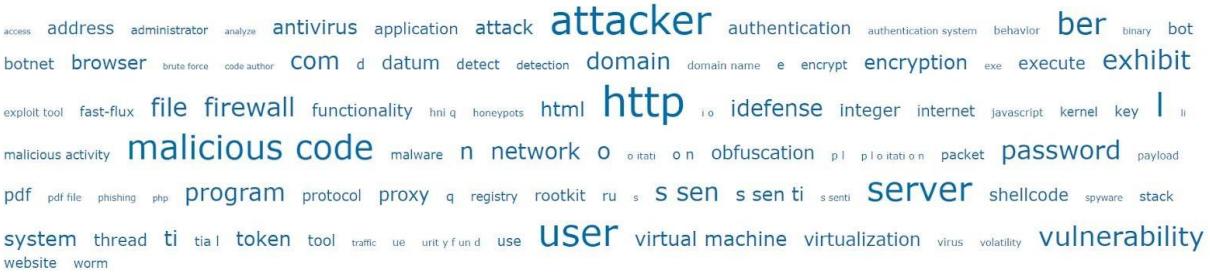
Приложение Б

Таблица 2 - Классификация основных сложностей перевода текстов о киберпреступности и способы их решения:

Тип термина	Подтип	Примеры	Способ перевода	Перевод
аббревиатуры	составные	DoS-attack SYN-flood	сохранение англ. аббревиатуры; перевод / транскр.	DoS-атака SYN-флуд
	инициальные	DDoS	сохранение английской аббревиатуры	DDoS
неологизмы	-	phishing pharming proxy crowdsourcing spam	транслитерация транскрибирование	фишинг фарминг прокси краудсорсинг спам

Приложение В

Рисунок 1 - Терминологическое “облако” на основе текста Cyber Security Essentials:



Приложение Г

Фрагмент из книги *Cyber Security Essentials* (4.1 Self-Replicating Malicious Code; 4.1.1 Worms; 4.1.2 Viruses):

Computer worms constitute a large class of malicious code that spreads between computers by distributing copies of themselves in a variety of ways. The worm is one of the earliest forms of malicious code and may be either benign or destructive. Malicious code is only a worm if it spreads to other systems by duplicating itself without attaching to other files.

Unlike computer viruses that spread by infecting executables or other files, worms spread by distributing copies of themselves. The copies may not be identical to the original worm, but they have the same functionality and can continue to spread to additional computers. The Morris worm, released by Robert Morris in 1988, was one of the first worms to spread on the Internet.1 The worm spread over the Internet by exploiting multiple known vulnerabilities in common UNIX programs. Morris stated that the purpose of the worm was to gauge the size of the Internet at the time, but it spread so quickly that it caused a widespread denial of service (DoS) condition.

Worms typically have two roles. The first is to spread to additional computers, but most also have a secondary task known as a payload. A worm's payload is what the attacker programs the worm to accomplish after it spreads. In the case of the Morris worm, the intention was to gauge the size of the Internet, but most worms have a much more malicious payload. This can include distributed denial of service (DDoS) attacks, spam distribution, cyber crime, or anything else the attacker chooses.

In the years since Morris's program got out of control, many more worms have spread across the Internet. Many worms target vulnerabilities in popular network services like HTTP servers and NetBIOS. However, many do not use vulnerabilities to spread, instead using e-mail, peer-to-peer (P2P) networks, social

networks, and mobile device communication protocols. These propagation techniques rely on tricking the user into executing a program and cannot spread without any human interaction. Worms are not limited to a single propagation method but can use any or all of these methods at once (see Exhibit 4-1).

E-mail worms spread by sending a message designed to entice the recipient into clicking a link or downloading an attachment that contains a copy of the worm. One famous example of this type of malicious code is the ILOVEYOU worm, which began spreading in May 2000.2 ILOVEYOU quickly infected thousands of computers by sending an e-mail with the subject header "I love you." Another means of spreading worms is Instant Messaging (IM) technologies. As IMs have gained in popularity, worms have begun to use these popular networks to spread between systems.

Network worms, which often spread without any user interaction, can infect many computers in a very short amount of time. These worms may infect other systems by exploiting vulnerabilities in software or by attempting to guess passwords that protect systems from intrusion. Blaster, which began spreading in August 2003, was a network worm that spread through a vulnerability in the Microsoft Windows RPC interface (MS03-026). The purpose of Blaster was to strike Microsoft's Windows Update website with a DDoS attack that the worm would launch on August 15, 2003.3 Microsoft averted the attack by preemptively taking the website offline.

As with worms that spread through e-mail, those that spread through P2P networks must also rely on social-engineering techniques rather than automatic propagation. These worms copy themselves to directories that popular P2P applications use to share files. By renaming themselves so they appear to be movies or software, the worms entice other users into downloading and executing them.

An often slow but effective propagation technique that worms use is copying themselves to USB drives. USB worms configure the infected drives to execute the worm as soon as an unsuspecting user plugs it into a computer. Through this technique, the worm is able to spread to networks that it could not normally access. In 2008, the U.S. Army banned the use of USB drives in its networks because a worm had spread throughout its networks via that route. To mitigate the threat from these worms, Microsoft released an update that disabled the autorun feature that allowed malicious code to spread easily through USB drives. Worms can spread between mobile devices by sending copies of themselves attached to short message service (SMS) messages, or by including links to Web pages that host a copy of the worm. In 2009, the "Sexy View" worm spread to phones running the Symbian operating system (OS) and collected information about each device it infected. The latest entrants into the worm world are those that spread through social-networking sites like Facebook and MySpace. Koobface is a worm that steals credentials for social-networking websites, then uses the accounts to send links to the worm to the victim's contacts. When first released, Koobface only targeted Facebook, but it has since begun targeting MySpace, Bebo, Netlog, and other social networks. Many worms use multiple techniques to spread. One of the most famous worms of 2009, Conficker spread through USB drives and through a vulnerability in the Windows Server Service (MS08-067).

To mitigate the threat from computer worms, administrators must protect systems from all propagation techniques. The following measures will decrease the likelihood of a worm infection in a network:

- Use antivirus products to scan incoming e-mails and IMs for malicious links.
- Disable autorun functionality for USB devices.
- Apply patches for vulnerabilities in network services in a timely manner.

- Disable access to P2P networks.
- Educate users on the dangers of worms that use social-engineering techniques.

Like their malicious cousins, viruses and Trojan horses, worms are a significant threat to modern networks. In the twenty-plus years that have passed since Robert Morris released the first Internet worm, new tactics have developed that allow for faster propagation with a higher impact. With the arrival of new communication technologies, attackers also develop new ways to spread malicious programs.

4.1.2 Viruses

The concept of viruses and malware has been with us for decades, along with the development of detection technologies. In this section, we explain the differences between viruses and other types of malware that can infect users and organizations.

The Internet hosts many forms of malicious software, also known as malware, that vary in functionality and intent. Quite often, descriptions of malware, regardless of the type, incorrectly classify the malicious software as a virus. For years, the term computer virus has been the all-encompassing term for malicious software; however, in the world of computer security, a virus refers to a specific type of malware that spreads by infecting other files with its malicious payload. Laypersons often incorrectly refer to all types of malware as viruses, when they might actually mean that such malware are Trojan horses (Trojans) or worms. A Trojan is a piece of malicious software that appears to be a legitimate application. A Trojan runs on an infected system as if it were an application with a beneficial purpose. A worm is another type of malware that is a standalone executable that spreads through network shares and vulnerabilities.

A virus, on the other hand, is not self-contained and requires the infection of a host file to spread. A virus is parasitic, infecting a system by attaching itself to

other files. A computer virus spreads in a similar manner as a biological virus, which injects DNA into a host cell to replicate itself and causes the cell to burst, releasing the replicated viruses to spread to other cells. A computer virus achieves the technological equivalent by writing its code into a host file. The virus eventually runs when a user opens the infected host file.

Now that the distinction between viruses and other types of malware is clear, a brief history of computer viruses will provide some helpful background information. The first recorded IBM PC-based virus, called the "Brain," debuted in January 1986. The Brain copied itself into a floppy disk's boot sector, the space on the floppy disk used to run code when the system starts. Once in memory, it attempted to copy itself to other floppy disks; the main side effect of an infection was a change to the volume label to "(c) Brain."

The Brain virus was not particularly destructive but took advantage of the era's heavy use of floppy disks. Other viruses, however, were not as harmless and caused damage to infected systems. In 1987, the Jerusalem virus and its variants began infecting systems. This virus resided in memory and infected all executable files (.com and .exe) on the system. When a user opened an infected file, the virus deleted the infected file.

Viral code within infected host files often has three distinct parts: the discovery module, the replication module, and the payload. The discovery module enables the virus to locate host files, and the replication module carries out the infection by copying the entire viral code into the host file. Exhibit 4-2 shows an infected application replicating the virus by writing the entire virus to the host file.

Last, the payload contains code to perform additional actions on the infected system aside from file discovery and replication. The specific actions carried out by the payload depend on the purpose of the virus. Payloads range from harmless code, such as the Cascade virus that altered text displayed on screens, to

destructive code, such as the Jerusalem virus that deleted infected files. Exhibit 4-3 shows screenshots of the Cascade virus altering the text within MS-DOS.

The security community separates viruses into two groups based on how the virus infects other files after it executes: resident and nonresident. A nonresident virus infects other files only when the infected file runs. A resident virus differs by loading itself into memory and continuing to run after the infected file closes.

Resident viruses fall into two additional categories: fast infectors and slow infectors.11 Viruses loaded into memory have the ability to infect many files very quickly because they can infect any file on a system. Viruses that take advantage of this ability are fast infectors, as they try to infect as many files as quickly as possible. This type of virus lacks stealth, and the consumption of resources makes the infection obvious to the victim.

Slow infector viruses have specific criteria with which they infect other files. Two common criteria used to infect other files are timebased (such as only infecting files on certain days) and access-based (such as only infecting copied files) criteria. Infections occurring only during specific situations slow down the infection rate, making the virus inconspicuous and harder to detect.

To write code to another file, viruses generally add their code to the beginning or end of a file. Methods that are more sophisticated, however, can also write the virus code within empty or unused space within the file. Viruses that use these techniques, known as cavity viruses, can add their code to a host file without changing the file's size.

Once the virus writes its code to the file, there must be a way to run the code when opening the infected file. If the virus focuses on infecting executable program files, it can modify the executable's header (entry point) to point to the beginning of the virus code. Another method is to modify the executable file's binary code to include call or jump instructions to the virus code. A recently discovered method used by the Xpaj.B virus replaces one of the subroutines in a

host file with its viral code.12 While this technique is less reliable and does not guarantee that the code will run, it makes it more difficult for antivirus products to detect the virus.

The impact that viruses have on systems demands a solution to detect and clean up infections. Antivirus products attempt to detect viruses by searching files for discovery modules, replication modules, or the payload. Detection methods include specific pattern matches within the executable or heuristic methods to detect viral activity.

These antivirus products also attempt to clean the virus infection by removing the virus's code and restoring the original file's contents. The antivirus program cannot simply delete an infected file because doing so may have adverse effects on the system's operation. The antivirus must detect the technique the virus used to execute the viral code within the infected file as described earlier in this section. Once the antivirus determines this technique, the antivirus program must remove the file alterations to reconstruct the original file. If the reconstruction of the file is successful, then the virus infection is gone.

Over the years, virus developers introduced encryption, polymorphic, and metamorphic code to thwart antivirus products. Encryption is a common technique used by virus authors to help their malware avoid detection. By encrypting the instructions, the author hides the virus's actual functionality and makes it difficult for antivirus programs to detect the virus using pattern matching. Encrypted viruses start with a routine to decrypt the virus followed by the execution of the now decrypted virus. A simple encryption method commonly used is an exclusive OR (XOR) cipher. The XOR cipher uses a key and the XOR operator to encrypt the virus's code, and the same key and XOR operator to decrypt the code. This lightweight encryption method encrypts the virus, but antivirus products can detect the existence of the decryption routine. For example, Panda's XOR-encoded antivirus signature looks for viruses with an XOR decryption routine.

To avoid detection of the decryption routine, a technique called polymorphism surfaced. A polymorphic virus still relies on a decryption routine to decrypt the encrypted code; however, this type of virus has a polymorphic engine within its code that changes the encryption and decryption routines each time the virus infects another file. Therefore, polymorphic viruses change their entire appearance with each infection yet have the same functionality.

Another technique, called metamorphism, allows a virus to change its appearance to avoid antivirus detection. Metamorphic viruses use an embedded engine to alter their code much like a polymorphic virus; however, the metamorphic engine actually changes the virus's code. For example, the metamorphic engine can use different registers within the code, add no-operation-performed (NOP) instructions, or change the code's flow with different jump and call instructions. These changes alter the binary composition of the virus between infected files, which makes detection by an antivirus product difficult.

Viruses have been around for decades, but many consider viruses outdated and no longer a threat. The overwhelming number of Trojans and worms that plague today's networks overshadow viruses; however, many viruses still exist, including a sophisticated, feature-rich virus known as Virut. Virut surfaced in 2006 and evolved into a hybrid malware that possesses characteristics of Trojans and viruses. Virut first runs as a self-contained executable that is like a Trojan; however, it also infects executable files to establish persistence and longevity to the infection.

Virut is a resident polymorphic virus that infects other executables on the system upon access. Recent variants of Virut have infected Web page files with the extension HTM, PHP, or ASP by writing an inline frame (IFrame) to the file. The IFrame is an HTML element that embeds a frame within the browser window. These IFrames allow attackers to forward users to a malicious page without

interaction. Virut infects Web page files hoping to infect other users who visit the Web page with the virus.

In addition to Virut's infection methods, its payload opens a backdoor on the infected system and connects to an Internet Relay Chat (IRC) channel. The IRC channel allows the attacker to command the infected system to download executables, further infecting the system. These capabilities show the danger that contemporary viruses pose to infected systems.

Over the past few decades, the term computer virus evolved from applying to a common type of malicious code with specific characteristics to being an imprecise catchall term for all types of malware. The characteristic that sets apart a true virus from other malware types is the parasitic trait of needing to spread, as viruses do not propagate without infecting other files. Antivirus products search files for this parasitic characteristic to detect viruses. These searches look for binary values, file alterations, and viral behaviors within files and attempt to clean infected files. While this is not a perfect solution, antivirus programs provide systems with the best protection from virus infections.

Приложение Д

Перевод фрагмента из книги *Cyber Security Essentials* (4.1 Самореплицирующийся вредоносный код; 4.1.1 Черви; 4.1.2 Вирусы):

Компьютерные черви представляют собой большой класс вредоносного кода, который распространяется между компьютерами через саморепликацию различными способами. Червь является одной из самых ранних форм вредоносного кода и может быть как доброкачественным, так и разрушительным. Вредоносный код является червем только в том случае, если он распространяется на другие системы путем дублирования себя без прикрепления к другим файлам.

В отличие от сетевых вирусов, распространяющихся путем заражения исполняемых или других файлов, черви распространяются путем распространения своих копий. Копии могут не совпадать с исходным червем, но они имеют те же функции и могут продолжать распространяться на другие компьютеры. Червь Морриса, запущенный Робертом Моррисом в 1988 году, был одним из первых червей, распространяющихся в Интернете. Червь распространился по Интернету, используя многочисленные известные уязвимости в распространенных программах Unix. Моррис заявил, что целью червя было выявление размера Интернета, но он распространился так быстро, что вызвал повсеместный отказ в обслуживании (DoS).

Черви обычно имеют две роли. Первая - это распространение на другие компьютеры, но у большинства из них есть и вторичная задача, известная как полезная нагрузка. Полезная нагрузка червя - это выполнение того, на что злоумышленник программирует червя после его распространения. В случае червя Морриса, целью было определить размер Интернета, но большинство червей имеют гораздо более вредоносную нагрузку. Это может включать в себя атаки типа DDoS, распространение спама, киберпреступность или что-либо еще, выбранное злоумышленником.

За годы, прошедшие с того момента, как программа Морриса вышла из-под контроля, в Интернете появилось гораздо больше червей. Многие черви нацелены на уязвимости в популярных сетевых службах, таких как HTTP-серверы и NetBIOS. Однако многие распространяются не через уязвимости, а через электронную почту, одноранговые (P2P) сети, социальные сети и протоколы связи мобильных устройств. Эти методы распространения основаны на обмане пользователя при запуске программы и без какого-либо вмешательства человека распространяться не могут . Черви не ограничиваются одним методом, но могут использовать какой-то один или все эти методы одновременно (см. Приложение 4-1).

Черви электронных почт распространяются путем отправки сообщения, предназначенного для того, чтобы заставить получателя щелкнуть ссылку или загрузить вложение, содержащее копию червя. Одним из известных примеров вредоносного кода такого типа является червь ILOVEYOU, который начал распространяться в мае 2000 года. ILOVEYOU быстро заразил тысячи компьютеров, отправив электронное письмо с заголовком “Я тебя люблю”. Еще одним средством распространения червей являются системы мгновенного обмена сообщений (IM). По мере того, как IM приобретали популярность, черви начали использовать эти популярные сети для распространения между системами.

Компьютерные черви, которые часто распространяются без какого-либо взаимодействия с пользователем, могут заразить множество компьютеров за очень короткое время. Эти черви могут заразить другие системы, используя уязвимости в программном обеспечении или пытаясь угадать пароли, которые защищают системы от вторжения. Blaster, который начал распространяться в августе 2003 года, был компьютерным червем, распространяющимся через уязвимость в интерфейсе удаленного вызова процедур (RPC) Microsoft Windows (MS03-026). Цель Blaster состояла в том,

чтобы поразить сайт Microsoft Windows Update с помощью DDoS-атаки, которую червь запустил 15 августа 2003 года. Microsoft предотвратила атаку, поставя веб-сайт в оффлайн-режим.

Как и в случае с червями, распространяющимися по электронной почте, те, которые распространяются по сетям P2P, должны также полагаться на методы социальной инженерии, а не на автоматическое распространение. Эти черви копируют себя в каталоги, которые используются популярными приложениями P2P для обмена файлами. Переименовывая себя в фильмы или программы, черви побуждают других пользователей их загружать и запускать.

Используемая червями медленная, но эффективная техника распространения - это копирование на USB-накопители. USB-черви настраивают зараженные накопители для запуска червя как только ничего не подозревающий пользователь подключает его к компьютеру. С помощью этого метода червь может распространяться на сети, к которым он обычно не имеет доступа. В 2008 году армия США запретила использование USB-накопителей в своих сетях, поскольку по этому маршруту червь распространился по всем сетям. Чтобы смягчить угрозу от этих червей, Microsoft выпустила обновление, где была отключена функция автозапуска, которая позволяла легко распространять вредоносный код через USB-накопители. Черви могут распространять свои копии между мобильными устройствами, прикрепляясь к сообщениям службы коротких сообщений (SMS) или через ссылки на веб-страницы, на которых размещена копия червя. В 2009 году червь “Sexy View” распространился на телефонах с операционной системой Symbian, собирая информацию о каждом зараженном устройстве. В последнее время участники мира червей распространяются через социальные сети, такие как Facebook и MySpace. Koobface - червь, который крадет учетные данные для веб-сайтов социальных

сетей, а затем использует учетные записи для отправки ссылок на червя контактам жертвы. Когда Koobface был впервые выпущен, он предназначался только для Facebook, но с тех пор он начал работать с MySpace, Bebo, Netlog и другими социальными сетями. Многие черви используют несколько методов распространения. Один из самых известных червей 2009 года, Conficker распространился по USB-накопителям и через уязвимость в Windows Server Service (MS08-067).

Чтобы уменьшить угрозу со стороны компьютерных червей, администраторы должны защищать системы от всех методов распространения. Следующие меры уменьшат вероятность заражения червем в сети:

- Используйте антивирусные программы для сканирования входящих сообщений электронной почты и IM на наличие вредоносных ссылок.
- Отключите функцию автозапуска для USB-устройств.
- Своевременно устанавливайте патчи, направленные на закрытие уязвимостей в сети.
- Отключите доступ к P2P-сетям.
- Расскажите пользователям об опасностях червей, использующих методы социальной инженерии.

Как и их злобные кузены (вирусы и троянские кони), черви представляют собой серьезную угрозу для современных сетей. За двадцать с лишним лет, прошедшие с того момента, как Роберт Моррис выпустил первого интернет-червя, были разработаны новые тактики, позволяющие более быстрое распространение с более высоким воздействием. С появлением новых коммуникационных технологий злоумышленники также разрабатывают новые способы распространения вредоносных программ.

4.1.2. Вирусы

Концепция вирусов и вредоносных программ была с нами на протяжении десятилетий, наряду с развитием технологий обнаружения. В этом разделе мы объясняем различия между вирусами и другими типами вредоносных программ, которые могут заразить пользователей и организации.

В Интернете размещается много видов вредоносных программ, также известных как вредоносы, которые различаются по функциональности и назначению. Довольно часто описания вредоносных программ, независимо от их типа, неправильно классифицируют вредоносное программное обеспечение как вирус. В течение многих лет термин “компьютерный вирус” был всеобъемлющим термином для вредоносного программного обеспечения; однако в мире компьютерной безопасности вирус относится к определенному типу вредоносных программ, которые распространяются путем заражения других файлов своей вредоносной нагрузкой. Непрофессионалы часто неправильно называют все типы вредоносных программ вирусами, когда они могут означать, что такие вредоносные программы являются троянскими конями (троянами) или червями. Троянец - это вредоносная программа, которая выглядит как законное приложение. Троянец работает в зараженной системе, как если бы это было приложение с положительной целью. Червь - это другой тип вредоносного ПО, представляющий собой отдельный исполняемый файл, распространяющийся через сетевые ресурсы и уязвимости.

А вот вирус не является автономным и требует распространения зараженного файла. Вирус паразитирует, заражая систему, прикрепляя себя к другим файлам. Компьютерный вирус распространяется аналогично биологическому вирусу, который впрыскивает ДНК в клетку-хозяина, чтобы размножиться, и заставляет клетку взрываться, выпуская реплицированные вирусы, чтобы распространиться на другие клетки. Компьютерный вирус

достигает технологического эквивалента, записывая свой код в файл хоста. В конечном итоге вирус запускается, когда пользователь открывает зараженный файл хоста.

Теперь, когда различие между вирусами и другими типами вредоносных программ становится ясным, краткая история компьютерных вирусов предоставит некоторую полезную справочную информацию. Первый зарегистрированный вирус на основе IBM PC, названный “Brain”, дебютировал в январе 1986 года. Brain скопировал себя в загрузочный сектор дискеты - место на гибком диске, используемое для запуска кода при запуске системы. Оказавшись в памяти, он попытался скопировать себя на другие дискеты; основным побочным эффектом инфекции было изменение метки тома на “(c) Brain”.

Вирус Brain не был особенно разрушительным, но он сумел сыграть на интенсивном использовании гибких дисков, свойственному тому времени. Другие вирусы, однако, не были столь безобидными и наносили ущерб зараженным системам. В 1987 году вирус Jerusalem и его разновидности начали заражать системы. Этот вирус находился в памяти и инфицировал все исполняемые файлы (.com и .exe) в системе. Когда пользователь открыл зараженный файл, вирус удалил зараженный файл.

Вирусный код внутри зараженных файлов хоста часто состоит из трех отдельных частей: модуля обнаружения, модуля репликации и полезной нагрузки. Модуль обнаружения позволяет вирусу обнаруживать файлы хоста, а модуль репликации выполняет заражение, копируя весь вирусный код в файл хоста. В Приложении 4-2 показано, как зараженное приложение воспроизводит вирус, записывая весь вирус в файл хоста.

Наконец, полезная нагрузка содержит код для выполнения дополнительных действий в зараженной системе помимо обнаружения и репликации файлов. Конкретные действия, выполняемые полезной

нагрузкой, зависят от назначения вируса. Полезные нагрузки варьируются от безвредных кодов, таких как вирус Cascade, который изменял текст, отображаемый на экранах, до деструктивных кодов, таких как вирус Jerusalem, который удалял зараженные файлы. В Приложении 4-3 показаны снимки экрана вируса Cascade, изменяющего текст в MS-DOS.

Сообщество безопасности разделяет вирусы на две группы в зависимости от того, как вирус заражает другие файлы после своего запуска: резидентные и нерезидентные. Нерезидентный вирус заражает другие файлы только при запуске зараженного файла. Резидентный вирус отличается тем, что загружает себя в память и продолжает работать после закрытия зараженного файла.

Резидентные вирусы делятся на две дополнительные категории: быстрые и медленные. Вирусы, загруженные в память, могут очень быстро заразить многие файлы, потому что они могут заразить любой файл в системе. Вирусы, использующие эту возможность - быстрые, поскольку пытаются заразить как можно больше файлов. Этому типу вирусов не хватает скрытности, а потребление ресурсов делает заражение очевидным для жертвы.

У медленных вирусов есть определенные критерии, по которым они заражают другие файлы. Два распространенных критерия, используемых для заражения других файлов - это критерии времени (например, заражение файлов только в определенные дни) и критерии доступа (например, заражение только скопированных файлов). Инфекции, возникающие только в определенных ситуациях, замедляют скорость заражения, делая вирус незаметным и более трудным для обнаружения.

Чтобы записать код в другой файл, вирусы обычно добавляют свой код в начало или конец файла. Однако более сложные методы также могут записывать код вируса в пустое или неиспользуемое пространство файла.

Вирусы, использующие эти методы, называемые cavity-вирусами, могут добавлять свой код в файл хоста, не изменяя его размер.

Как только вирус записывает свой код в файл, должен быть способ запустить код при открытии зараженного файла. Если вирус фокусируется на заражении исполняемых программных файлов, он может изменить заголовок (точку входа) исполняемого файла, указав начало кода вируса. Другой метод заключается в изменении двоичного кода исполняемого файла для включения инструкций вызова или перехода в код вируса. Недавно обнаруженный метод, используемый вирусом Xpaj.B, заменяет одну из подпрограмм в файле хоста своим вирусным кодом. Хотя этот метод менее надежен и не гарантирует выполнение кода, он усложняет работу антивирусных продуктов. обнаружить вирус.

Влияние вирусов на системы требует решения для обнаружения и устранения инфекций. Антивирусные программы пытаются обнаружить вирусы путем поиска файлов для модулей обнаружения, модулей репликации или полезной нагрузки. Методы обнаружения включают в себя определенные совпадения шаблонов в исполняемых или эвристических методах для обнаружения вирусной активности.

Эти антивирусные программы также пытаются вылечить вирусную инфекцию, удалив код вируса и восстановив исходное содержимое файла. Антивирусная программа не может просто удалить зараженный файл, поскольку это может отрицательно сказаться на работе системы. Антивирус должен обнаруживать метод, используемый вирусом для выполнения вирусного кода в зараженном файле, как описано ранее в этом разделе. Как только антивирус определяет эту технику, антивирусная программа должна удалить изменения файла, чтобы восстановить исходный файл. Если восстановление файла прошло успешно, вирусная инфекция исчезла.

На протяжении многих лет разработчики вирусов внедряли шифрование, полиморфный и метаморфический код для защиты антивирусных продуктов. Шифрование - это распространенный метод, используемый авторами вирусов, чтобы помочь своим вредоносным программам избежать обнаружения. Зашифровывая инструкции, автор скрывает фактическую функциональность вируса и затрудняет антивирусным программам обнаружение вируса с помощью сопоставления с шаблоном. Зашифрованные вирусы начинаются с процедуры расшифровки вируса с последующим исполнением расшифрованного вируса. Обычно используемый простой метод шифрования - это шифр “исключающий “или” (XOR). Шифр XOR использует ключ и оператор XOR для шифрования кода вируса, и то же самое для его дешифрования. Этот легкий метод шифрует вирус, но антивирусные продукты могут обнаруживать существование процедуры дешифрования. Например, сигнатурная антивирусная сигнатура Panda ищет вирусы с помощью процедуры расшифровки XOR.

Чтобы избежать обнаружения процедуры расшифровки, появилась методика, называемая полиморфизмом. Полиморфный вирус все еще полагается на процедуру дешифрования для расшифровки кода; однако этот тип вируса имеет полиморфный механизм в своем коде, который изменяет процедуры шифрования и дешифрования каждый раз, когда вирус заражает другой файл. Следовательно, полиморфные вирусы меняют свой внешний вид при каждой инфекции, но имеют одинаковую функциональность.

Другой метод, называемый метаморфизмом, позволяет вирусу изменять свой внешний вид, чтобы избежать обнаружения антивирусом. Метаморфные вирусы используют встроенный движок, чтобы изменить свой код так же, как и полиморфный вирус; однако метаморфический движок фактически изменяет код вируса. Например, механизм метаморфизма может использовать разные регистры в коде, добавлять инструкции без выполнения

операций (NOP) или изменять поток кода с помощью различных инструкций перехода и вызова. Эти изменения изменяют бинарный состав вируса между зараженными файлами, что затрудняет обнаружение антивирусной программой.

Вирусы существуют уже несколько десятилетий, но многие считают вирусы устаревшими и больше не представляют угрозы. Подавляющее число троянских программ и червей, поражающих современные сети, затмевают вирусы; однако, многие вирусы все еще существуют, включая сложный, многофункциональный вирус, известный как Virut. Virut появился в 2006 году и превратился в гибридное вредоносное ПО, обладающее характеристиками троянов и вирусов. Virut сначала запускается как автономный исполняемый файл, похожий на троянский; тем не менее, он также заражает исполняемые файлы, чтобы установить постоянство и долговечность инфекции.

Virut является резидентным полиморфным вирусом, который заражает другие исполняемые файлы в системе при доступе. Последние варианты вируса заразили файлы веб-страниц с расширением HTM, PHP или ASP, написав встроенный фрейм (IFrame) в файл. IFrame - это элемент HTML, который встраивает рамку в окно браузера. Эти IFrames позволяют злоумышленникам перенаправлять пользователей на вредоносную страницу без взаимодействия. Virut заражает файлы веб-страниц, надеясь заразить других пользователей, которые посещают веб-страницу с вирусом.

Помимо методов заражения Virut, его полезная нагрузка открывает черный ход в зараженной системе и подключается к каналу Internet Relay Chat (IRC). IRC-канал позволяет злоумышленнику дать команду зараженной системе загрузить исполняемые файлы, еще более заразив систему. Эти возможности показывают опасность, которую современные вирусы представляют для зараженных систем.

За последние несколько десятилетий термин “компьютерный вирус” развился от применения к распространенному типу вредоносного кода с особыми характеристиками до точного универсального термина для всех типов вредоносных программ. Особенностью, которая отличает настоящий вирус от других типов вредоносных программ, является паразитная черта необходимости распространения, поскольку вирусы не распространяются без заражения других файлов. Антивирусные продукты ищут в файлах эту паразитическую характеристику для обнаружения вирусов. Эти поиски ищут двоичные значения, изменения файлов и вирусные поведения в файлах и пытаются очистить зараженные файлы. Хотя это не идеальное решение, антивирусные программы обеспечивают наилучшую защиту систем от вирусных инфекций.