Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.056

БУБНОВ
Яков Васильевич

МОДЕЛИ И АЛГОРИТМЫ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК НА ОСНОВЕ АНАЛИЗА ХАРАКТЕРИСТИХ DNS-ЗАПРОСОВ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Минск, 2021

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Научный руководитель	**Иванов Николай Николаевич**, кандидат физико-математических наук, доцент, доцент кафедры электронных вычислительных машин учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
Официальные оппоненты:	**Краснопрошин Виктор Владимирович**, доктор технических наук, профессор, заведующий кафедрой информационных систем управления факультета прикладной математики и информатики Белорусского государственного университета
	Маликов Владимир Викторович, кандидат технических наук, доцент, заведующий кафедрой бизнес-анализа и математического моделирования учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО».
Оппонирующая организация	Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси»

Защита состоится 21 октября 2021 г. в 14:00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, тел. 293-89-89, e-mail: dissovet@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан «20» сентября 2021 г.

Ученый секретарь
совета по защите диссертаций
кандидат технических наук, доцент О. В. Бойправ

ВВЕДЕНИЕ

Современное вредоносное программное обеспечение использует систему доменных имен как способ организации канала коммуникации с удаленным злоумышленником. Во-первых, данный канал используется для передачи украденной информации, корпоративных секретов, интеллектуальной собственности путем кодирования и инкапсуляции данных в запрашиваемое доменное имя, а саму методику называют туннелированием системы доменных имен. Во-вторых, образованный канал используют для получения команд от удаленного злоумышленника, в частности для организации распределенной ботнет-сети. Данную методику называют генерированием доменных имен, так как основной задачей является сокрытие реального месторасположения серверов злоумышленника.

В диссертационной работе ставится задача разработать эффективные способы обнаружения несанкционированного доступа к узлам компьютерной сети средствами туннелирования системы доменных имен, а также усовершенствовать существующие способы определения генерируемых доменных имен. Помимо этого, стоит задача определить наиболее эффективное использование детекторов независимо от конфигурации компьютерной сети. Эффективность способов оценивается с помощью быстродействия и вычислительной сложности алгоритмов, обеспечивающих безопасность сети.

Исходя из предположения об использовании для организации рассматриваемых видов атак исключительно секции DNS-запроса, выдвигается гипотеза о возможности использования методов обработки естественных языков с целью детектирования угроз. Таким образом, в работе рассматриваются нейросетевые модели для классификации доменных имен и анализируется применимость моделей для детекции DNS-туннелирования в задаче классификации сгенерированных доменных имен.

В работе рассматривается метод эффективного использования предложенных детекторов. Исходя из влияния внедренного детектора на производительность системы доменных имен, моделируется частично наблюдаемый марковский процесс принятия решения. Рассматриваемый процесс принятия решения определяет политику управления детекторами для изоляции зараженных узлов компьютерной сети. Предлагается альтернативный вариант выбора узлов для блокировки, эта задача моделируется скрытым марковским процессом. Данный подход учитывает возможность применения злоумышленником новых инструментов зашумления детекторов и алгоритмов генерирования доменных имен.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель – разработать модели и алгоритмы предотвращения кибератак, эксплуатирующих систему доменных имен. Целью определяются следующие задачи исследования:

1. Разработать модель обнаружения туннелирования системы доменных имен, используемых для эксфильтрации данных из корпоративных компьютерных сетей.
2. Усовершенствовать модель определения сгенерированных доменных имен, используемых для организации распределенных ботнетов.
3. Разработать модель управления детекторами DNS-атак для принятия решения о блокировке вредоносного узла компьютерной сети.
4. Разработать алгоритм принятия решения о блокировке зараженного узла при условии зашумленности детекторов DNS-атак.

Объект и предмет исследования

Объект исследования – программные средства защиты компьютерных сетей от целевых кибератак. Предмет исследования – модели обнаружения и классификации угроз, эксплуатирующих систему доменных имен, а также методы защиты корпоративных компьютерных сетей от целевых кибератак, осуществляемых с помощью системы доменных имен.

Научная новизна

1. Модель детектора DNS-туннелирования на основе нейронной сети со стековыми слоями свертки для текстовой классификации слов доменного имени. Особенностью данной модели является символьная свертка слов, что позволяет использовать модель для классификации доменных имен на любом естественном языке.
2. Усовершенствована модель нейронной сети для обнаружения DGA-имен. Особенностью модели является использование слоя двунаправленных LSTM-ячеек, что обеспечивает сходимость нейросети в результате обучения.
3. Модель управления детекторами DNS-угроз для блокировки зараженных узлов средствами RPZ на основе моделирования компьютерной сети как частично наблюдаемого марковского процесса. Особенностью данной модели является статичность обученной политики взаимодействия

с окружением при изменении конфигурации и топологии компьютерной сети.

4. Алгоритм классификации временного ряда событий DNS-активности для принятия решения о блокировке зараженных узлов компьютерной сети. Алгоритм основан на скрытой марковской модели, что позволяет повысить качество классификации в сравнении с BOW-алгоритмами. Особенность алгоритма заключается в отсутствии стадии обучения.

Положения, выносимые на защиту

1. Модель детектора DNS-туннелирования, основанная на сверточной нейронной сети со стековыми слоями свертки для текстовой классификации слов доменного имени. На тестовом наборе данных DTQBC модель обеспечивает точность распознавания механизма DNS-туннелирования до 0,9997 в задаче бинарной классификации. В задаче многоклассовой классификации модель оценивается значением 0,9981 по F_1-метрике при микро- и макроусреднении.

2. Модель детектора вредоносного программного обеспечения, использующего сгенерированные доменные имена для организации распределенных ботнетов, основанная на сверточно-рекуррентной нейронной сети со стековыми слоями свертки и двунаправленными LSTM-ячейками для текстовой классификации слов доменного имени. Модель обеспечивает точность распознавания DGA-имен равную 0,9645 на тестовом наборе данных UMUDGA, что на 0,0011−0,4654 выше точности известных моделей.

3. Модель управления детекторами DNS-атак, основанная на моделировании компьютерной сети как частично наблюдаемого марковского процесса принятия решений, где оптимальная политика взаимодействия с окружением вычисляется посредством DDQN-агента с дуэльной архитектурой нейросети. Среднее вознаграждение DDQN-агента составляет 0,6160.

4. Алгоритм классификации временного ряда регистраций DNS-активности узлов компьютерной сети, основанный на скрытой марковской модели для принятия решения о блокировке узла посредством RPZ. Алгоритм по F_1-метрике превосходит существующие алгоритмы, базирующиеся на BOW-модели, на 0,0491−0,4704.

Личный вклад соискателя

Постановка задач, фомулирование математических моделей и обсуждение результатов проводились с научным руководителем

канд. физ.-мат. наук Ивановым Николаем Николаевичем. Модели и алгоритмы разработаны автором самостоятельно. Соавтор опубликованных работ Н. Н. Иванов принимал участие в проведении экспериментальных исследований и обсуждении их результатов.

Апробация результатов диссертации

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях: 52-я научная конференция аспирантов, магистрантов и студентов «Компьютерные системы и сети» (БГУИР, Минск, Беларусь, 2018); VI Международная научно-техническая конференция «Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT-2016)» (ПВГУС, Тольятти, Россия, 2016); 54-я научная конференция аспирантов, магистрантов и студентов «Компьютерные системы и сети» (БГУИР, Минск, Беларусь, 2018); 55-я конференция аспирантов, магистрантов и студентов «Компьютерные системы и сети» (БГУИР, Минск, Беларусь, 2019); XI Республиканская научная конференция молодых ученых и студентов (БрГТУ, Брест, Беларусь, 2019); 56-я конференция аспирантов, магистрантов и студентов «Компьютерные системы и сети» (БГУИР, Минск, Беларусь, 2020).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 12 печатных работ. Из них 6 статей в научных рецензируемых журналах, включенных в перечень научных изданий для опубликования результатов диссертационных исследований (3,1 авторских листа), 6 статей в сборниках материалов научных конференций (1,07 авторских листа).

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, библиографического списка и двух приложений. Общий объем диссертации составляет 163 страницы, из них 107 страниц основного текста, 40 иллюстраций на 30 страницах, 20 таблиц на 16 страницах, библиографический список из 77 наименований на 9 страницах, список собственных публикаций из 12 наименований на 2 страницах, 2 приложения на 34 страницах.

ОСНОВНАЯ ЧАСТЬ

В **первой главе** рассматривается принцип организации туннелирования системы доменных имен вредоносным программным обеспечением, использующим данную методику для эксфильтрации данных с зараженного узла. Проводится анализ современных методов обнаружения DNS-туннелирования, на основании которого делается вывод о необходимости усовершенствования существующих подходов. Для этого формулируется задача определения DNS-туннелирования относительно запрашиваемого доменного имени.

Пусть $\boldsymbol{X} = \{x_0, x_1, ..., x_n\}$ – запрашиваемое доменное имя, с которым ассоциирована метка $y \in \boldsymbol{Y}$ с вероятностью p. Тогда стоит задача нахождения функции:

$$\mathrm{y} : \boldsymbol{X} \to \boldsymbol{Y}. \tag{1}$$

Дан алфавит символов $\boldsymbol{A}$, из которого состоит доменное имя, такое что $x_i \in \mathbf{A}$, а само доменное имя представляет собой подмножество размещений алфавита $\boldsymbol{X} \subset \boldsymbol{A}^k$, где $k = |\boldsymbol{X}| = 256$ – максимальная длина доменного имени, установленного в спецификации протокола DNS. Таким образом, стоит задача отнесения слов некоторого заданного алфавита к одному из классов множества $\boldsymbol{Y}$.

Так как нейронная сеть определяется относительно действительных величин, предлагается использовать символьное встраивание для преобразования символьного вектора. Пусть дана функция $\mathrm{I}(\boldsymbol{X})$, которая ставит каждому элементу из $\boldsymbol{A}$ в соответствие некоторый индекс, то есть упорядочивает элементы $\boldsymbol{X}$. Тогда встраивание – это преобразование вектора символов в вектор целых чисел, где каждому символу в соответствие поставлен индекс из алфавита $\boldsymbol{A}$:

$$\begin{aligned} &\mathrm{I} : \boldsymbol{A} \to \{0, ..., |\boldsymbol{A}|\}, \\ &\mathrm{cemb}(\boldsymbol{X}) = [\mathrm{I}(x_1), \mathrm{I}(x_2), ..., \mathrm{I}(x_n)] = \boldsymbol{E}. \end{aligned} \tag{2}$$

Далее рассматриваются несколько вариантов нейронных сетей, используемых в задачах классификации текстовых последовательностей естественных языков.

Предлагается сверточная нейронная сеть со стековой организацией слоев, где в каждом сверточном слое используется свой размер окна свертки:

$$\begin{aligned} &\boldsymbol{h}^{(1)} = \mathrm{cemb}(\boldsymbol{E}), \\ &\boldsymbol{h}_k = \left(a_{\mathrm{conv1d}(\boldsymbol{Q};\boldsymbol{H},k)} \circ a_{\mathrm{maxpool}}\right)(\boldsymbol{h}^{(1)}). \end{aligned} \tag{3}$$

Конечный вид классификатора выглядит следующим образом:

$$\mathrm{y}(\boldsymbol{X}) = \left(a_{\mathrm{selu}} \circ \mathrm{D}_{0,1} \circ a_{\mathrm{softmax}}\right)\left(\bigcup_{k=\{10,7,5,3\}} \boldsymbol{h}_k\right). \tag{4}$$

Аналогично формулируется рекуррентная нейронная сеть с однонаправленными LSTM-ячейками:

$$\begin{aligned} \boldsymbol{h}^{(1)} &= \mathrm{cemb}(\boldsymbol{X}), \\ \boldsymbol{h}^{(2)} &= a_{\mathrm{lstm}}{}^{256}(\boldsymbol{h}^{(1)}), \\ \mathrm{y}(\boldsymbol{X}) &= \left(a_{\mathrm{softmax}} \circ \mathrm{D}_{0,5}\right)\left(\boldsymbol{h}^{(2)}\right). \end{aligned} \tag{5}$$

Помимо моделей, описанных относительно символьного представления доменного имени, рассматривается полносвязная нейронная сеть, использующая стационарные характеристики DNS-запроса $\boldsymbol{X}'$: тип запроса, информационная энтропия доменного имени, время жизни ресурсной записи и т. д. Данная модель формулируется следующим образом:

$$\begin{aligned} \boldsymbol{h}^{(1)} &= a_{\mathrm{relu}}(\boldsymbol{X}'), \\ \hat{\mathrm{y}}(\boldsymbol{X}') &= \left(\mathrm{D}_{0,1} \circ a_{\mathrm{relu}} \circ a_{\mathrm{tanh}} \circ \mathrm{D}_{0,1} \circ a_{\mathrm{softmax}}\right)\left(\boldsymbol{h}^{(1)}\right). \end{aligned} \tag{6}$$

Обучение предложенных нейронных сетей производится с помощью эталонного набора данных DTQBC, содержащего как доменные имена, используемые при DNS-туннелировании, так и доменные имена сервисов Интернет. Функции потерь нейронных сетей оптимизируются мини-пакетным стохастическим градиентным алгоритмом Adam. При данном подходе исходный набор данных разбивается на пакеты по 128 примеров, для которых оценивается ошибка модели. Полученная ошибка усредняется по количеству примеров в мини-пакете и используется для обновления параметров модели.

Далее проверяется эффективность разработанных моделей на основании сравнения метрик бинарной (см. таблицу 1) и многоклассовой классификации (см. таблицу 2). В сравнении также участвует *n*-граммный классификатор Qi et al. и SVM с линейным ядром Almusawi et al.

Таблица 1. – Результаты бинарной классификации на тестовом наборе DTQBC

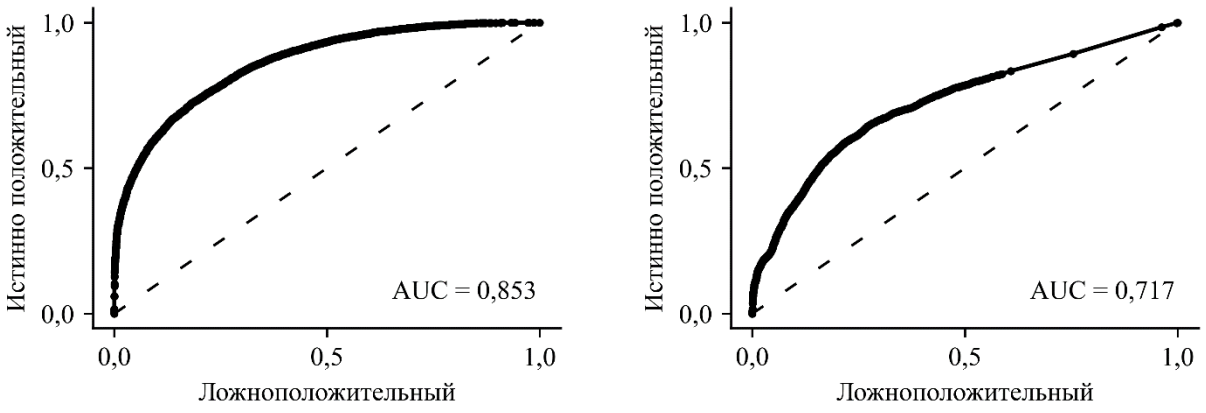
Модель	**Точность**	**Precision**	**Recall**	**F_1**
Предложенная модель (4)	0,9997	**1,0000**	0,9994	0,9997
Предложенная модель (5)	0,9998	0,9999	0,9998	0,9998
Предложенная модель (6)	**1,0000**	**1,0000**	**1,0000**	**1,0000**
Almusawi et al.	**1,0000**	**1,0000**	**1,0000**	**1,0000**
Qi et al.	0,5003	0,5001	**1,0000**	0,6667

Результаты оценки демонстрируют, что сверточная нейронная сеть (4) превосходит остальные модели обнаружения DNS-туннелирования на тестовом наборе DTQBC в задаче определения конкретного метода организации туннеля, а также успешно конкурирует с другими моделями в задаче обнаружения туннелирования в DNS-запросе.

Таблица 2. – Результаты многоклассовой классификации на тестовом наборе DTQBC

Модель	**Precision**		**Recall**		**F_1**	
	Микро	Макро	Микро	Макро	Микро	Макро
Almusawi et al.	0,9293	0,9470	0,9293	0,9287	0,9293	0,9268
Предложенная модель (4)	**0,9981**	**0,9982**	**0,9981**	**0,9981**	**0,9981**	**0,9981**
Предложенная модель (5)	0,2044	0,0409	0,2044	0,2000	0,2044	0,0679
Предложенная модель (6)	0,9595	0,9655	0,9595	0,9601	0,9595	0,9594

Во **второй главе** рассматривается принцип организации зараженных узлов в сети ботнет. Показано, что генерируемые доменные имена эксплуатируются для организации доступа к центральному серверу, от которого зараженный узел получает команды для начала децентрализованной атаки. Так как принцип организации DNS-туннелей подразумевает генерирование доменного имени, производится анализ предложенных в первой главе моделей для обнаружения доменных имен. Однако результаты (см. рисунок 1) демонстрируют неприменимость обученных нейронных сетей для классификации сгенерированных доменных имен.



а **б**

Рисунок 1. – ROC-кривые (а) сверточной нейросети и (б) рекуррентной нейросети для класса DGA-запросов; диагональной штриховой линией изображен график эфемерной модели, для которой классификация представляет собой процесс случайного гадания

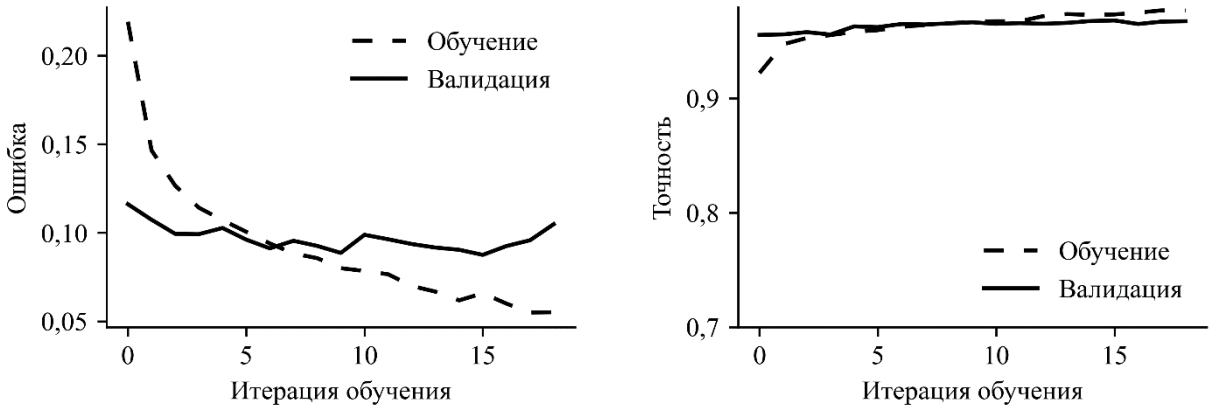
Делается вывод о необходимости построения модели, позволяющей более точно отличать DGA-запросы от безопасных DNS-запросов. Далее производится анализ существующих методов определения генерируемых

доменных имен. Для возможности сравнения результатов классификации предлагается использовать эталонный тестовый набор UMUDGA, содержащий доменные имена наиболее популярных ресурсов сети Интернет, сетей дистрибуции содержимого, а также сгенерированные доменные имена современных вредоносных программ.

Результаты анализа существующих сверточно-рекуррентных архитектур нейронных сетей с последовательным и параллельным расположением слоев свидетельствуют о склонности моделей к переобучению. Для решения данной проблемы предлагается использование двунаправленных ячеек, параллельно расположенных по отношению к одноразмерным сверточным слоям:

$$
\begin{aligned}
&\boldsymbol{h}^{(1)} = \mathrm{cemb}(\boldsymbol{X}),\\
&\boldsymbol{h}^{(2')} = \mathrm{D}_{0.5}\left(\bigcup_{k=2}^{6}\mathrm{conv}(\boldsymbol{h}^{(1)};k)\right),\\
&\boldsymbol{h}^{(2'')} = \mathrm{D}_{0.5}\left(a^{128}{}_{\text{bi-lstm}}(\boldsymbol{h}^{(1)})\right),\\
&\boldsymbol{h}^{(3)} = \mathrm{D}_{0.5}\left(a_{\text{relu}}(\boldsymbol{h}^{(2')}) \bigcup a_{\text{relu}}(\boldsymbol{h}^{(2'')})\right),\\
&\boldsymbol{h}^{(4)} = \mathrm{D}_{0.5}\left(a_{\text{relu}}(\boldsymbol{h}^{(3)})\right),\\
&\mathrm{y}(\boldsymbol{X}) = a_{\text{softmax}}(\boldsymbol{h}^{(4)}).
\end{aligned}
\tag{7}
$$

Как видно из графиков (см. рисунок 2), при использовании двунаправленных LSTM-ячеек удалось добиться уменьшения валидационной ошибки и избавиться от проблемы переобучения сети на ограниченном наборе данных. Аналогично на графике зависимости точности от итерации обучения наблюдается монотонный рост по мере обучения нейронной сети.



а **б**

Рисунок 2. – Процесс обучения комбинированной нейронной сети с двунаправленными LSTM-ячейками для определения DGA-имен; (а) ошибка обучения и валидации; (б) точность обучения и валидации после каждой итерации обучения

Далее производится оценка качества обнаружения DGA-имен (см. таблицу 3), а также определение типа вредоносного программного обеспечения (см. таблицу 4). Так как в тестовом наборе UMUDGA представлено 39 классов вредоносных доменных имен, для краткости передачи результатов в таблице 4 приведены усредненные результаты.

Таблица 3. – Метрики бинарной классификации в задаче определения DGA-имени на тестовом наборе UMUDGA

Модель	**Точность**	**Precision**	**Recall**	**F_1**
Предложенная модель (4)	0,9621	0,9453	0,9808	0,9628
Предложенная модель (7)	**0,9654**	**0,9581**	0,9734	**0,9657**
Highnam et al.	0,9643	0,9486	**0,9818**	0,9645
Vosoughi et al.	0,9599	0,9441	0,9777	0,9606
Woodbridge et al.	0,5000	0,0000	0,0000	0,0000

Таблица 4. – Метрики многоклассовой классификации в задаче определения DGA-алгоритма на тестовом наборе UMUDGA

Модель	**Precision**		**Recall**		**F_1**	
	Микро	Макро	Микро	Макро	Микро	Макро
Предложенная модель (4)	0,5936	0,6906	0,5936	**0,8650**	0,5936	0,7234
Предложенная модель (7)	0,5449	0,6308	0,5449	0,7940	0,5449	0,6655
Vosoughi et al.	**0,6562**	**0,7375**	**0,6562**	0,8236	**0,6562**	**0,7463**
Highnam et al.	0,4211	0,4678	0,4211	0,6489	0,4211	0,4807

Как видно из результатов, предложенная модель (7) в задаче бинарной классификации доменных имен превосходит существующие модели, а в многоклассовой задаче демонстрирует конкурентные результаты. Детальный анализ результатов классификации выявляет неспособность рассмотренных моделей отличить сгенерированные доменные имена «gozi» от безопасных доменных имен. Данное поведение объясняется тем, что класс доменных имен «gozi» формируется из слов естественного языка.

В **третьей главе** рассматривается проблема интеграции детекторов DNS-угроз (DNS-туннелирования и DGA-имен). Проблема заключается в ухудшении производительности и доступности DNS-сервисов в случае анализа каждого передаваемого DNS-запроса. Для преодоления данной проблемы предлагается моделирование компьютерной сети с помощью частично наблюдаемого марковского процесса принятия решений.

В контексте данной модели для каждого DNS-запроса может быть произведено одно из действий: получение состояния детектора – a_{acc}; увеличение степени внимания – a_{inc}; уменьшение степени внимания к узлу – a_{dec}; изоляция узла для предотвращения вредоносной активности – a_{blk}; продолжение функционирования системы без изменений – a_{ulk}. Таким образом, конечное множество действий можно задать множеством:

$$\boldsymbol{A} = \{a_{acc}, a_{inc}, a_{dec}, a_{blk}, a_{ulk}\}. \quad (8)$$

Блокировка и разблокировка являются конечными действиями, при которых система завершает работу.

Так как состояние POMDP-модели для агента не известно, анализировать систему возможно только благодаря наблюдениям, образованным непрерывным векторным пространством:

$$\Omega = \boldsymbol{I}^2 = \vec{a} \times \vec{\varphi}, \quad (9)$$

где $\vec{a} = [0;1]$ – вектор, определяющий диапазон допустимых значений для степени внимания детектора к узлу a, а $\vec{\varphi} = [0;1]$ – вектор, определяющий диапазон допустимых значений оценки вредоносной активности $\mathrm{M}[\hat{\Phi}]$.

Функция условных вероятностей переходов из одного состояния в другое определяется так, что при доступе к детектору туннелирования, увеличении или уменьшении степени внимания к детектору система не меняет своего состояния:

$$\mathrm{T}(s \mid s', a) = \begin{cases} 1, & a \in \{a_{blk}, a_{ulk}\} \\ 0, & \text{иначе} \end{cases}. \quad (10)$$

Функция условных вероятностей наблюдений определяется исходя из степени точности детектора q:

$$\mathrm{O}(o \mid s', a) = \begin{cases} q, & s' = s_{inf}; a = a_{acc} \\ 1-q, & s' = s_{hlt}; a = a_{acc} \\ 1, & a \in \{a_{inc}, a_{dec}\} \\ 0, & \text{иначе} \end{cases}. \quad (11)$$

Функция вознаграждения определяется таким образом, что агент получает негативное вознаграждение за доступ к детектору и изменение степени внимания, то есть чем больше агент проводит времени за попытками получить дополнительную информацию об узле, тем меньше будет финальное вознаграждение. При ошибке системы вводится дополнительный штраф:

$$\boldsymbol{R} = \begin{bmatrix} s_{inf}, a_{acc} & s_{inf}, a_{dec} & s_{inf}, a_{inc} & s_{inf}, a_{ulk} & s_{inf}, a_{blk} \\ s_{hlt}, a_{acc} & s_{hlt}, a_{dec} & s_{hlt}, a_{inc} & s_{hlt}, a_{ulk} & s_{hlt}, a_{blk} \end{bmatrix}, \quad (12)$$

где $\boldsymbol{R}_{i,j}$ определяет вознаграждение за a_j действие в состоянии s_i. Функция вознаграждения задается функцией:

$$\mathrm{R}(s, a) = \begin{cases} \boldsymbol{R}_{s,a}, & s \in \boldsymbol{S}, a \in A \\ 0 & \text{иначе} \end{cases}. \quad (13)$$

Для экспериментов предлагается рассматривать вознаграждения, нормированные в интервале [–1;1], где за ошибки первого и второго рода агент получает штраф -1, а за верно принятое решение вознаграждение 1. Оставшиеся вознаграждения оцениваются на основании изменения пропускной способности DNS-сервера:

$$\boldsymbol{R}_{:,a_i} = -\gamma b^i, \tag{14}$$

где γ – минимальный штраф за изменение пропускной способности в b раз, а i – позиция элемента в упорядоченном множестве действий $\boldsymbol{A}$.

Для поиска оптимальной политики решения POMDP-модели предлагается использовать агентный подход, в частности рассматривается использование DQN-агента со следующей архитектурой нейронной сети:

$$\mathrm{y}(\boldsymbol{X}) = \left(\mathrm{D}_{0.5} \circ a_{\mathrm{relu}}\right)^4 (\boldsymbol{X}). \tag{15}$$

Помимо этого, рассматривается DDQN-агент (Dueling DQN), позволяющий бороться с чрезмерной оптимистичностью политики DQN-агента путем построения конкурентной архитектуры нейронной сети:

$$\mathrm{y}(\boldsymbol{X}) = \mathrm{Avg}\left(\left(\mathrm{D}_{0.5} \circ a_{\mathrm{relu}}\right)^4 (\boldsymbol{X})\right), \tag{16}$$

где оператор усреднения описывается выражением:

$$\mathrm{Avg}(\boldsymbol{z}) = \boldsymbol{z}_{:,0} + \boldsymbol{z}_{:,1:} - \mathrm{avg}(\boldsymbol{z}_{:,1:}). \tag{17}$$

Также рассматривается DDPG-агент, образованный двумя нейронными сетями – актором и критиком. В качестве модели-актора используется архитектура нейронной сети DQN-агента, а в качестве критика следующая модель:

$$\mathrm{y}^*(\boldsymbol{X}_A \cup \boldsymbol{X}_\Omega) = \left(\mathrm{D}_{0,5} \circ a_{\mathrm{relu}}\right)^4 (\boldsymbol{X}_A \cup \boldsymbol{X}_\Omega). \tag{18}$$

Так как DDPG формулируется относительно непрерывного пространства действий, к выходам y^* применяется функция argmax:

$$\mathrm{y}(\boldsymbol{X}_A \cup \boldsymbol{X}_\Omega) = \mathrm{argmax}\left(y^*(\boldsymbol{X}_A \cup \boldsymbol{X}_\Omega)\right). \tag{19}$$

Представленные агенты обучаются в течение 1000 эпизодов взаимодействия с окружением, после чего вычисляется среднее, минимальное и максимальное вознаграждение за все эпизоды (см. таблицу 5).

Исходя из метрик оценки эффективности политик агентов, наиболее эффективным агентом является DDQN, использующий дуэльную архитектуру нейронной сети.

Таблица 5. – Результаты взаимодействия агентов с окружением для определения зараженных узлов в сети

Агент	Среднее вознаграждение	Минимальное вознаграждение	Максимальное вознаграждение
DQN	0,6140	**–1,0000**	**1,0000**
DDQN	**0,6160**	**–1,0000**	**1,0000**
DDPG	–19,9999	–19,9999	–19,9999

В **четвертой главе** рассматривается проблема блокировки зараженных узлов компьютерной сети в случае зашумленного детектора. Зашумление детектора возникает в случае появления нового механизма DNS-туннелирования или алгоритма генерирования доменного имени, а также непосредственной недообученности детектора. Для решения данной проблемы предлагается рассматривать ряд результатов классификации детектора, упорядоченный во времени. Тогда принятие решения о блокировке на основании данного ряда можно смоделировать с помощью скрытой марковской модели.

HMM-модель определяется как кортеж $(\boldsymbol{X},\boldsymbol{Y},\mathrm{T},\mathrm{E})$, где $\boldsymbol{X}$ – конечное множество скрытых состояний системы; $\boldsymbol{Y}$ – конечное множество наблюдаемых состояний системы; $\mathrm{T}(y_i \mid x_i, y_k \mid x_k)$ – функция условных вероятностей перехода из одного состояния в другое; $E(y_i \mid x_i)$ – вероятность наблюдать y_i при условии нахождения системы в скрытом состоянии x_i.

Вероятность нахождения в конкретном состоянии определяется x_i с помощью нормального распределения:

$$\mathrm{E}(y_i \mid x_i) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left\{-\left(\frac{x_i - y_i}{\sigma}\right)^2\right\}, \tag{20}$$

где среднеквадратическое отклонение составляет σ, а x_i – вероятность отнесения запроса к классу вредоносных, зарегистрированная детектором.

Исходя из предположения, что наблюдаемые события образуют ординарный поток Пуассона, определяется вероятность перехода из состояния $y_i \mid x_i$ в состояние $y_j \mid x_j$ с помощью экспоненциального распределения:

$$\mathrm{T}(y_i \mid x_i, y_k \mid x_k) = \lambda \cdot \exp\left\{-\frac{t_k - t_i}{\exp\left((1 - y_k \oplus y_k)\cdot k\right)}\right\}, \tag{21}$$

где $y_i \oplus y_k$ представляет собой полином Жегалкина.

Цепь Маркова дополняется двумя виртуальными конечными состояниями (см. рисунок 3): безопасная и небезопасная последовательность DNS-запросов. Для выполнения классификации предлагается вычислить

вероятности обоих путей и, сравнив их, выбрать класс, которому соответствует наибольшая вероятность.

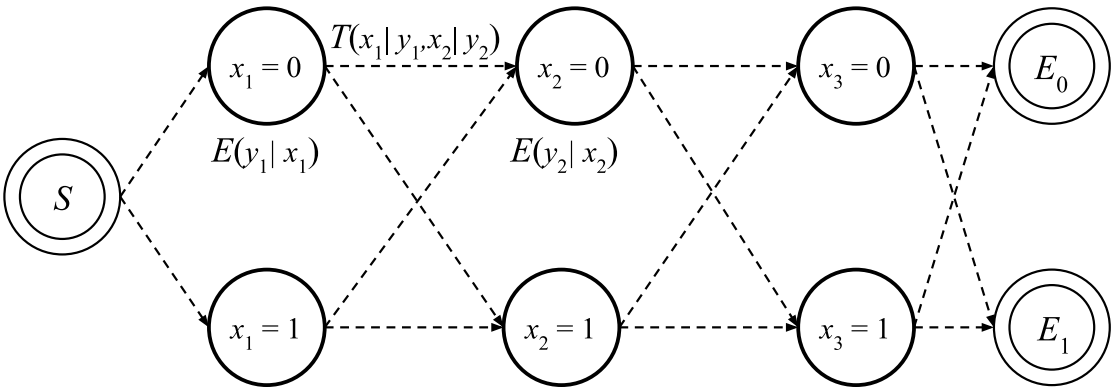


Рисунок. 3. – Схема цепи Маркова серии наблюдаемых событий с равновероятными конечными состояниями

Для вычисления вероятности предлагается алгоритм *gpp* (алг. 1), представляющий собой модифицированный алгоритм поиска Витерби. Данный алгоритм обладает недостатком, связанным с необходимостью пересчета марковской модели для каждого нового события, а для использования алгоритма требуется представление модели в виде матрицы следующего вида:

$$\boldsymbol{A}^T = \left[\bigcup_i^n \{t_i, y_i\} \right]^T \times \{x', x''\}, \tag{22}$$

где t_i – время наблюдения события; y_i – вероятность отнесения DNS-запроса к классу вредоносных; x_i' и x_i'' – возможные наблюдаемые состояния системы.

maxprob (A, J, i)
1) $p_1 = J \cdot T(\mathbf{A}_{1,i-1} \mid \mathbf{A}_{1,j}) \cdot E(\mathbf{A}_{1,i})$
2) $p_2 = J \cdot T(\mathbf{A}_{2,i-1} \mid \mathbf{A}_{2,j}) \cdot E(\mathbf{A}_{2,i})$
3) **if** $p_1 \geq p_2$
4) **do return** (p_1, $\mathbf{A}_{1,i}$)
5) **return** (p_2, $\mathbf{A}_{2,i}$)

gpp (**A**, s, e)
1) J ← E(s)
2) N ← $|\mathbf{A}_1|$
3) **for** i = 2 **to** N
4) (p, s) ← *maxprob*(**A**, s, i)
5) J ← J · p
6) **return** J · T(s | e) · E(e)

Так как алгоритм *gpp* не хранит вероятности предыдущих состояний, а на каждой итерации производится обновление кумулятивной вероятности, пространственная сложность алгоритма является константной $O(1)$, а временная сложность составляет $O(n)$.

Далее в главе предлагается параметрически настраиваемый алгоритм *rsamp*, предназначенный для решения проблемы пересчета модели. Результатом работы данного алгоритма является последовательность скрытых состояний, на основании которых принимается решение о блокировке узла. То есть превышение отношения количества безопасных запросов к общему числу запросов заданного порога является сигналом для блокировки узла:

$$y(\boldsymbol{z}) = \begin{cases} 1, & \text{wcount}(\boldsymbol{z};1) \geq T \\ 0, & \text{иначе} \end{cases}, \tag{23}$$

где $\boldsymbol{z} = \text{rsamp}(\boldsymbol{A}, s)$, а T – минимальное количество допустимых запросов, а функция $\text{wcount}(\boldsymbol{z};k)$ определяется следующим образом:

$$\text{wcount}(\boldsymbol{z};k) = \frac{1}{|\boldsymbol{z}|}\sum_{i}^{|\boldsymbol{z}|} 1 - \boldsymbol{z}_i \oplus k. \tag{24}$$

Алгоритм вычисления скрытых состояний марковской цепи (алг. 2):

rsamp (**A**, s)
1) H ← { s }
2) N ← |$\mathbf{A}_1$|
3) J ← E(s)
4) **for** i = 1 **to** N – 1
5) (p, s) ← *maxprob*(**A**, J, i+1)
6) H ← H ∪ {s}
7) J ← J · p
8) **return** H

В рамках сравнительного анализа используются наиболее успешные на данный момент алгоритмы классификации временных последовательностей: BOSSVS, предложенный в работе P. Shafer (2016), а также SAXVSM, описанный в работе P. Senin and S. Malinchik (2013). Так как оба рассматриваемых алгоритма реализуют модель BOW (англ. Bag-of-words), то установим размер окна 36, а размер слова 12.

Для проверки эффективности использования предложенного алгоритма проводится серия экспериментов. В рассматриваемой серии экспериментов будем использовать значение p_0 из интервала $[0;½]$, а значение p_w

из интервала (½;1]. Размер окна будет увеличиваться дискретно от 0 до 90 % небезопасных DNS-запросов от общего числа запросов в наблюдаемой последовательности. Для каждой последовательности вычисляются метрики классификации: чувствительность и специфичность, а также F_1-метрика (см. таблицу 6).

Таблица 6. – Сравнение алгоритмов классификации временных последовательностей регистраций детектором DNS-угроз

Процент небезопасных запросов, %	**Precision**			**Recall**			**F_1**		
	BOSSVS	SAXVSM	Предложенный алгоритм (алг. 2)	BOSSVS	SAXVSM	Предложенный алгоритм (алг. 2)	BOSSVS	SAXVSM	Предложенный алгоритм (алг. 2)
0	**0,0000**	**0,0000**	**0,0000**	**0,0000**	**0,0000**	**0,0000**	**0,0000**	**0,0000**	**0,0000**
10	0,0000	0,0000	**0,9903**	0,0000	0,0000	**0,9912**	0,0000	0,0000	**0,9905**
20	0,0000	0,0000	**0,9932**	0,0000	0,0000	**0,9939**	0,0000	0,0000	**0,9935**
30	**1,0000**	**1,0000**	0,9948	0,6383	0,7518	**0,9966**	0,7792	0,8583	**0,9956**
40	**1,0000**	**1,0000**	0,9976	0,5950	0,8512	**0,9958**	0,7461	0,9196	**0,9967**
50	**1,0000**	**1,0000**	0,9969	0,6535	0,4554	**0,9974**	0,7904	0,6258	**0,9971**
60	**1,0000**	**1,0000**	0,9973	0,5185	0,3580	**0,9980**	0,6829	0,5273	**0,9977**
70	**1,0000**	**1,0000**	0,9987	0,7213	0,7213	**0,9980**	0,8381	0,8381	**0,9983**
80	**1,0000**	**1,0000**	0,9997	0,7805	0,7805	**0,9986**	0,8767	0,8767	**0,9992**
90	**1,0000**	**1,0000**	0,9989	0,8095	0,9048	**0,9992**	0,8947	0,9500	**0,9991**

Как видно из результатов, при зашумленном детекторе скрытая марковская модель позволяет корректно классифицировать последовательность регистраций детектора для принятия решения о блокировке зараженного узла компьютерной сети.

В приложениях представлены листинги программных кодов, а также копия акта о практическом использовании результатов исследования в деятельности по планированию и выполнению проектов.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Сформулирована математическая модель классификации доменного имени. Разработана модель обнаружения туннелирования системы доменных имен, основанная на текстовом анализе запрашиваемого имени с помощью сверточной нейронной сети со стековой организацией слоев, а также рекуррентной нейронной сети с LSTM-ячейками. Помимо этого,

представлена полносвязная нейронная сеть, классифицирующая DNS-запросы по атрибутам. Проведен сравнительный анализ существующих подходов обнаружения туннелирования системы доменных имен, а также представленных нейросетевых моделей. Предложенная сверточная модель на тестовом наборе данных DTQBC демонстрирует точность до 0,9997 в задаче распознавания DNS-туннелирования. В задаче многоклассовой классификации модель оценивается значением 0,9981 по F_1-метрике при микро- и макроусреднении [1, 2, 4, 7–9].

2. Проведен анализ моделей обнаружения DNS-туннелирования для решения задачи обнаружения сгенерированных доменных имен. Результаты анализа демонстрируют несостоятельность использования ранее рассмотренных моделей для классификации DGA-запросов. Разработана модель определения DGA-запросов, основанная на использовании сверточно-рекуррентной нейронной сети с двунаправленными LSTM-ячейками и стековыми сверточными слоями. Проведен сравнительный анализ моделей классификации DNS-запросов, результаты которого демонстрируют превосходство предложенной модели над существующими в задаче бинарной классификации на 0,0011–0,4654 для тестового набора данных UMUDGA [6].

3. Предложен частично наблюдаемый марковский процесс принятия решений, моделирующий зашумленные детекторы DNS-атак в компьютерной сети, для определения оптимальной политики блокировки зараженных узлов. Оптимальная политика блокировки определяется с помощью агентов на основе глубоких нейронных сетей. Производится сравнительный анализ DQN-, DDQN- и DDPG-агентов, по результатам которого делается вывод об эффективности политики, образованной DDQN-агентом на основании среднего вознаграждения за взаимодействие с POMDP-окружением – 0,6160 [3, 6, 10].

4. Предложен алгоритм классификации временного ряда событий DNS-угроз на основе скрытой марковской модели. Данный алгоритм предназначен для определения момента времени, в который требуется отправка уведомления о возникшей угрозе безопасности администраторам компьютерной сети. Проведен экспериментальный анализ предложенного алгоритма, результаты которого демонстрируют его эффективность. По F_1-метрике предложенный алгоритм превосходит существующие аналоги, базирующиеся на BOW-модели, на 0,4704–0,0491 [5, 11, 12].

Рекомендации по практическому использованию результатов

Разработанные модели обнаружения атак, эксплуатирующие систему доменных имен, ориентированы на защиту корпоративных компьютерных

сетей. Представленные нейросетевые модели могут быть описаны с помощью распространенных библиотек, таких как Keras, TensorFlow, PyTorch, и в дальнейшем интегрированы в корпоративный DNS-сервер для блокировки единичных запросов.

Модель управления детекторами DNS-атак, основанная на POMDP, может быть использована для автоматизации блокировки зараженных узлов компьютерной сети с помощью зон с политикой ответов RPZ.

Алгоритм классификации временных рядов регистраций DNS-запросов может быть интегрирован в существующие системы мониторинга, такие как Zabbix, Prometheus, Nagios, для построения на их базе системы уведомлений о возникающих угрозах либо встроен в корпоративный DNS-сервер для автоматизации процесса блокировки зараженных узлов средствами RPZ.

Разработанные модели и алгоритмы внедрены в компанию «Лифт БиЭлЭр», а также в учебный процесс кафедры электронных вычислительных машин УО «БГУИР».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в рецензируемых научных журналах, входящих в перечень ВАК

1. Bubnov, Y. DNS Tunneling Detection / Y. Bubnov // International Journal of Recent Trends in Engineering & Research. – 2016. – Volume 02, Issue 04. – P. 241–245.

2. Bubnov, Y. DNS Tunneling Detection Using Feedforward Neural Network / Y. Bubnov // European Journal of Engineering Research and Science. – 2018. – Volume 03, Issue 11. – P. 16–19.

3. Bubnov, Y. DNS Data Exfiltration Detection Using Online Planning for POMDP / Y. Bubnov // European Journal of Engineering Research and Science. – 2019. – Volume 04, Issue 09. – P. 22–25.

4. Бубнов, Я. В. Текстовый анализ DNS-запросов для защиты компьютерных сетей от эксфильтрации данных / Я. В. Бубнов, Н. Н. Иванов // Информатика. – 2020. − Т. 17, № 3. – С. 78–86.

5. Бубнов, Я. В. Скрытая марковская модель для определения вредоносных узлов компьютерной сети / Я. В. Бубнов, Н. Н. Иванов // Журнал Белорусского государственного университета. Математика. Информатика. – 2020. – № 3. – С. 73–79.

6. Бубнов, Я. В. Обнаружение DGA доменов и предотвращение botnet средствами Q-обучения для POMDP / Я. В. Бубнов, Н. Н. Иванов // Доклады БГУИР. – 2021. – № 2. – С. 91–99.

Статьи в сборниках материалов научных конференций

7. Бубнов, Я. В. Детектирование DNS туннелей / Я. В. Бубнов // Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT 2016): сборник статей VI международной заочной научно-технической конференции, Тольятти, 31 марта, 2016 г. / Поволжский государственный университет сервиса. – Тольятти: ПВГУС, 2016. – С. 85–91.

8. Бубнов, Я. В. Кластеризация данных методом устойчивых гомологий / Я. В. Бубнов // Компьютерные системы и сети: материалы 52-й научной конференции аспирантов, магистрантов и студентов, Минск, 25–30 апреля 2016 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск : БГУИР, 2016. – С. 11–13.

9. Бубнов, Я. В. Обнаружение DNS-туннелей с помощью Feedforward нейронной сети / Я. В. Бубнов // Компьютерные системы и сети: материалы 54-й научной конференции аспирантов, магистрантов и студентов, Минск, 23–27 апреля 2018 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск : БГУИР, 2018. – С. 19–20.

10. Бубнов, Я. В. Выявление DNS туннелирования в компьютерной сети методом POMDP / Я. В. Бубнов // Компьютерные системы и сети: 55-я юбилейная научная конференция аспирантов, магистрантов и студентов, Минск, 22–26 апреля 2019 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск : БГУИР, 2019. – С. 20–22.

11. Бубнов, Я. В. Фильтрация DNS запросов с помощью динамических зон с политикой ответов в открытых компьютерных сетях / Я. В. Бубнов // Современные проблемы математики и вычислительной техники : сборник материалов XI Республиканской научной конференции молодых ученых и студентов, Брест, 21–22 ноября 2019 года / Министерство образования Республики Беларусь, Брестский государственный технический университет ; редкол.: В. А. Головко. – Брест: БрГТУ, 2019. – С. 66–68.

12. Бубнов, Я. В. Скрытая марковская модель для принятия решений о классификации временного ряда событий в компьютерной сети / Я. В. Бубнов // Компьютерные системы и сети: материалы 56-й научной конференции аспирантов, магистрантов и студентов, Минск, 21–24 апреля 2020 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск : БГУИР, 2020. – С. 12–13.

РЭЗЮМЭ

Бубноў Якаў Васільевіч

Мадэлі і алгарытмы для выяўлення сеткавых атак на аснове аналізу характарыстык DNS-запытаў

Ключавыя словы: мэтавая кібератака, сістэма даменных імёнаў, эксфільтрацыя дадзеных, тэкставая класіфікацыя, маркоўскі працэс прыняцця рашэнняў.

Мэта працы: распрацоўка метадаў абароны інфармацыі ў карпаратыўных камп'ютарных сетках ад шкодаснага праграмнага забеспячэння, якое эксплуатуе сістэму даменных імёнаў.

Метады даследвання: тэкставы аналіз, глыбокае навучанне, навучанне з падмацаваннем, тэорыя прыняцця рашэнняў, тэорыя алгарытмаў.

Атрыманыя вынікі і іх навізна. Прапанавана мадэль нейронавай сеткі для выяўлення DNS-тунэлявання, якая дазваляе класіфікаваць даменныя імёны на любой натуральнай мове з дапамогай стэкавых слаёў сімвальнай скруткі. Удасканалена мадэль нейронавай сеткі для выяўлення згенераваных даменных імёнаў дзякуючы выкарыстанню слоя з двубокавымі LSTM-вочкамі. Гэта забяспечвае збежнасць функцыі страт па выніках навучання. Прадстаўлена мадэль кіравання дэтэктарамі DNS-пагроз, якая базуецца на часткова назіральным маркаўскім працэсе. Мадэль забяспечвае незалежнасць навучанай палітыкі ўзаемадзеяння з асяроддзем ад змен тапалогіі і канфігурацыі камп'ютарнай сеткі. Распрацаваны алгарытм класіфікацыі часовай паслядоўнасці падзей DNS для прыняцця рашэння аб блакаванні заражаных вузлоў камп'ютарнай сеткі. Алгарытм заснаваны на схаванай маркаўскай мадэлі, што забяспечвае паляпшэнне якасці класіфікацыі ў параўнанні з BOW-алгарытмамі і дазваляе выключыць стадыю навучання.

Ступень выкарыстання: нейрасеткавыя мадэлі могуць быць апісаны з дапамогай прыкладных бібліятэк і ў далейшым інтэграваны як частка DNS-сервера для блакавання запытаў. Метад кіравання дэтэктарамі DNS-пагроз можа быць выкарыстаны для аўтаматызацыі блакавання шкоднасных вузлоў. Алгарытм класіфікацыі часовай паслядоўнасці можа быць выкарыстаны для паведамлення адміністратараў камп'ютарнай сеткі аб узніклай пагрозе бяспекі праз сістэму падзейнага маніторынгу.

Сфера ўжывання: сродкі абароны карпаратыўных камп'ютарных сетак ад мэтавых кібератак.

РЕЗЮМЕ

Бубнов Яков Васильевич

Модели и алгоритмы для обнаружения сетевых атак на основе анализа характеристик DNS-запросов

Ключевые слова: целевая кибератака, система доменных имен, эксфильтрация данных, текстовая классификация, марковский процесс принятия решений.

Цель работы: разработка методов защиты информации в корпоративных компьютерных сетях от вредоносного программного обеспечения, эксплуатирующего систему доменных имен.

Методы исследования: текстовой анализ, глубокое обучение, обучение с подкреплением, теория принятия решений, теория алгоритмов.

Полученные результаты и их новизна. Предложена модель нейронной сети для обнаружения DNS-туннелирования, позволяющая классифицировать доменные имена на любом естественном языке за счет стековых слоев символьной свертки. Усовершенствована модель нейронной сети для обнаружения сгенерированных доменных имен благодаря использованию слоя с двунаправленными LSTM-ячейками. Это обеспечивает сходимость функции потерь по результатам обучения. Представлена модель управления детекторами DNS-угроз, базирующаяся на частично наблюдаемом марковском процессе. Модель обеспечивает независимость обученной политики взаимодействия с окружением от изменений топологии и конфигурации компьютерной сети. Разработан алгоритм классификации временного ряда событий DNS для принятия решения о блокировке зараженных узлов компьютерной сети. Алгоритм основан на скрытой марковской модели, что обеспечивает улучшение качества классификации в сравнении с BOW-алгоритмами и позволяет исключить стадию обучения.

Степень использования: нейросетевые модели могут быть описаны с помощью прикладных библиотек и в дальнейшем интегрированы как часть DNS-сервера для блокировки запросов. Модель управления детекторами DNS-угроз может быть использована для автоматизации блокировки вредоносных узлов. Алгоритм классификации временной последовательности может быть использован для уведомления администраторов компьютерной сети о возникшей угрозе безопасности через систему событийного мониторинга.

Область применения: средства защиты корпоративных компьютерных сетей от целевых кибератак.

SUMMARY

Yakov V. Bubnov

Models and algorithms for detecting network attacks based on analysis of characteristics of DNS-requests

Keywords: advanced persistent threat, domain name system, data exfiltration, text classification, Markov decision process.

Objective: research of information protection methods against malware exploiting domain name system in corporate computer networks.

Research methods: text analysis, deep learning, reinforcement learning, decision theory, algorithms theory.

The results obtained and their novelty. The neural network model for DNS-tunneling detection, which allows to classify domain names in any natural language by means of stacked layers of symbolic convolution, is proposed. The neural network model for detecting generated domain names is improved by using a bidirectional LSTM-cell layer. This ensures convergence of the loss function based on training results. The model for managing DNS-threat detectors based on a partially observable Markov process is presented. The model ensures the independence of the trained policy of interaction with the environment from changes in the topology and configuration of a computer network. The algorithm for classifying time series of DNS-events is developed for making a decision on blocking infected nodes of a computer network. The algorithm is based on a hidden Markov model, which provides an improvement in the quality of classification in comparison with BOW algorithms and eliminates the learning stage.

Use level: neural network models can be described using application libraries and later integrated as part of a DNS-server to block requests. DNS threat detector management method can be used to automate blocking of malicious hosts. The time series classification algorithm can be used to notify administrators of a computer network about an emerging security threat through the event monitoring system.

Application area: corporate computer networks protection facilities against advanced persisted threats.

Научное издание

Бубнов Яков Васильевич

МОДЕЛИ И АЛГОРИТМЫ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК НА ОСНОВЕ АНАЛИЗА ХАРАКТЕРИСТИХ DNS-ЗАПРОСОВ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Подписано в печать 14.09.2021. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 1,63. Уч. изд. л. 1,4. Тираж 60 экз. Заказ 60.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный инверситет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий № 1/238 от 23.04.2014,
№ 2/113 от 07.04.2014, № 3/615 от 07.04.201
ЛП № 02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6