IV. Кибербезопасность. Особенности обеспечения безопасности в социальных сетях

Алексеев В.М., Чичков С.Н.

Разработка модели анализатора фишинговых атак

Аннотация: В работе поднимается вопрос защиты информации в корпоративных сетях с применением двухуровневой архитектуры построения сети с полносвязным ядром. Описаны преимущества использования разработанной технологии в корпоративных сетях крупных организаций. Рассмотрены принципы построения анализаторов, предназначенных для выявления и блокирования компьютерных атак. Проанализированы математические методы, используемые при построении модели анализатора. Подробно описаны параметры, необходимые для выявления фишинговых атак.

Ключевые слова: двухуровневая модель защиты информации, полносвязная сеть, компьютерная атака, фишинговая атака, анализатор, фишинг, подсистема защиты информации

Количество компьютерных атак (КА) на информационную инфраструктуру и сервисы как коммерческих, так и государственных корпораций за последнее время кратно возросло. В целях защиты своих информационных ресурсов компании регулярно проводят мероприятия по оценке уровня защищенности, разрабатывают модели угроз для информационных и автоматизированных систем, модернизируют имеющиеся системы защиты и внедряют новые средства защиты информации (СЗИ). Методы и средства, которые используют злоумышленники, совершая КА, постоянно модернизируются, находятся все новые способы обхода имеющихся на рынке СЗИ. Разработчики СЗИ

также не стоят на месте и постоянно совершенствуют свои продукты, пополняя линейки новейшими разработками по обнаружению и нейтрализации компьютерных атак. Однако на практике в крупных организациях работы по внедрению новых СЗИ в уже эксплуатируемые системы не всегда удается провести в короткие сроки. Дополнительные трудности с оформлением проектной документации возникают в случае, когда систему необходимо аттестовывать в соответствии с требованиями регуляторов.

Для решения обозначенной проблемы была разработана и предложена двухуровневая структура построения защиты информации в корпоративной сети на основе полносвязности с применением интеллектуальных анализаторов различного типа, позволяющих распознать и блокировать КА [1-2]. Одно из основных преимуществ такой технологии состоит в гибкости и мобильности доработки, развертывания и усовершенствования установленных анализаторов, благодаря чему система остается всегда защищенной от актуальных угроз и выявленных уязвимостей.

Анализаторы могут работать на разных уровнях модели OSI [3]. Это необходимо для выявления большего числа КА, так как разные типа атак совершаются на разных уровнях с использованием соответствующих им протоколов. Таким образом, происходит анализ сетевого трафика на периметре сети на всех уровнях, начиная с побитового анализа на физическом уровне, заканчивая анализом трафика на уровне приложений (прикладном).

Для успешного выявления КА необходимо понимать, какие параметры поступают на анализатор, и какие из них и по каким критериям позволяют судить о протекающей атаке. Для этого необходимо понимать действия атакующего и происходящие в этот момент процессы в работе протокола. Дополнительным и необходимым помощником в работе анализатора является использование методов искусственного обучения. А также применяются различные методы математического аппарата, статистики, временных рядов, теории вероятностей и другие.

Анализаторы, используемые в предложенной технологии, обладают всем функционалом классических анализаторов трафика и специализированных утилит, таких как Wireshark, tcpdump,

SolarWinds Network Performance Monitor (NPM) и других. Анализаторы трафика могут захватывать и сохранять пакеты данных, проходящие через сеть, для последующего анализа. Это позволяет детально изучить содержимое сетевого трафика. В режиме реального времени анализаторы отображают текущую активность в сети, включая активные подключения, используемые порты и протоколы, а также объемы передаваемых данных. Анализаторы могут распознавать и анализировать различные сетевые протоколы (например, TCP, UDP, HTTP, DNS). Это помогает идентифицировать проблемы с совместимостью или уязвимости в реализации протоколов. Анализаторы способны производить оценку скорости передачи данных, задержек, потерь пакетов и других параметров, влияющих на производительность сети. Анализаторы могут выявлять аномальное поведение в сети, которое может указывать на попытки атаки, утечки данных или неисправности оборудования, могут фильтровать трафик по различным критериям (IP-адрес, порт, протокол) и сортировать данные для более детального анализа. Анализаторы могут автоматически генерировать отчеты о состоянии сети, обнаруженных проблемах и статистике трафика.

Анализаторы имеют первостепенное значение в предложенной двухуровневой структуре построения защиты информации в корпоративной сети на основе полносвязности, являясь средством для мониторинга трафика как на периметре, так и внутри сети, средством выявления угроз на основе заранее определенных параметров, математического аппарата и искусственного интеллекта, средством обеспечения безопасности на различных уровнях сети. Двухуровневая структура построения защиты информации подразумевает использование двух слоев защиты, каждый из которых отвечает за нейтрализацию конкретных типов КА. Используя большее количество анализаторов на каждом уровне, удается оперативно обеспечить максимальную детальную защиту информации всей информационной инфраструктуры компании.

На первом «внешнем» уровне корпоративной сети анализаторы выявляют и предотвращают атаки типа «отказ в обслуживании» разных типов, фишинговые атаки, атаки на приложения и попытки

проникновения внутрь корпоративной сети, контролируя и анализируя потоки информации на входе в корпоративную сеть.

Анализаторы на втором уровне структуры построения защиты информации на основе полносвязности используются для мониторинга активности внутри корпоративной сети. Они просматривают внутренний трафик между автоматизированными рабочими местами пользователей и администраторов, серверами систем, подключенными мобильными устройствами, сетевым и периферийным оборудованием и другими объектами в сети. Это позволяет выявлять зараженные устройства, предотвращать распространение вредоносного ПО и также отслеживать вредоносную активность ПО, не распознаваемого сигнатурами средств антивирусной защиты, и блокировать ее.

На этом уровне анализаторы также отслеживают попытки безуспешной аутентификации и несанкционированного доступа к ресурсам сети и могут управлять политиками доступа на основе выявленных угроз, предотвращая нарушение правил доступа и политики безопасности и выявляя брутфорс атаки. Это становится возможным, отправляя на вход анализатора информацию о попытках подключения субъектов доступа к объектам доступа, а также заранее предоставив информацию о правах доступа для каждого субъекта и объекта в корпоративной сети.

На том же втором, «внутреннем» уровне корпоративной сети анализаторы выявляют и предотвращают утечки данных (в том числе, нелегитимные выгрузки из баз данных систем), контролируя и анализируя потоки информации внутри и за пределы сети. Они также могут отслеживать шифрование данных и предупреждать о возможных утечках через незащищенные каналы, мониторя использование протоколов, таких как HTTPS или TLS, для обеспечения безопасности передаваемых данных.

При разработке и реализации анализаторов используются различные математические методы, которые обеспечивают эффективное обнаружение, классификацию и анализ сетевых данных, позволяя обнаружить с максимальной точностью признаки КА.

Методы статистического анализа

Среднее значение, дисперсия и стандартное отклонение используются для анализа распределения сетевого трафика и выявления аномалий, таких как резкие изменения в объеме передаваемых данных. Ковариация и корреляция применяются для обнаружения зависимостей между различными параметрами трафика, что может помочь в выявлении аномальных паттернов, таких как внезапное увеличение числа соединений между двумя узлами. Гистограммы и плотность распределения используются для визуализации распределения различных параметров трафика (например, размер пакетов, время между пакетами) и поиска аномалий.

Методы временных рядов

Auto Regressive Integrated Moving Average (ARIMA) прогнозирует будущие значения трафика на основе предыдущих данных, помогая предсказать аномальные изменения в сети [4-5]. Exponential Smoothing применяется для анализа и прогнозирования трафика с учетом временных зависимостей, что позволяет сглаживать данные и выявлять тренды [6-7]. Seasonal Decomposition используется для выявления сезонных компонентов в трафике, таких как ежедневные или еженедельные паттерны, что помогает отличить нормальную активность от аномальной.

Методы теории вероятностей и статистики

Байесовские методы используются для классификации трафика, где каждый пакет или поток данных анализируется с точки зрения вероятности того, что он принадлежит определенному классу (например, нормальный трафик, подозрительный трафик). Марковские модели применяются для моделирования последовательностей пакетов и выявления подозрительных изменений в поведении трафика. Например, скрытые марковские модели (HMM) могут использоваться для обнаружения атак, основываясь на последовательностях сетевых событий. Гауссовские смеси (GMM) применяются для моделирования распределения различных характеристик трафика, таких как время между пакетами или размер пакетов, и выявления аномалий.

Методы машинного обучения

Алгоритмы классификации:

– SVM (Support Vector Machine) применяется для классификации трафика на категории, такие как нормальный трафик или трафик, связанный с атакой;

– Decision Trees и Random Forest используются для построения моделей, которые принимают решения на основе характеристик трафика, таких как порты, IP-адреса, типы протоколов.

– Алгоритмы кластеризации:

- k-means применяется для группировки похожих потоков трафика в кластеры, что позволяет идентифицировать аномалии на основе принадлежности к кластеру;
- Density-Based Spatial Clustering of Applications with Noise (DBSCAN) используется для обнаружения аномалий в виде малоплотных регионов данных.

Нейронные сети:

– рекуррентные нейронные сети применяются для анализа последовательностей сетевых пакетов и обнаружения аномальных паттернов во временных рядах;

– конволюционные нейронные сети используются для анализа многомерных данных трафика (например, временные ряды или матрицы данных) с целью обнаружения сложных паттернов [8-9].

–

Методы оптимизации

Линейное и нелинейное программирование применяются для оптимизации параметров сетевого мониторинга и распределения ресурсов для обеспечения эффективной работы анализаторов. Эволюционные алгоритмы используются для автоматической настройки параметров анализа и улучшения точности детекции на основе анализа исторических данных.

Алгоритмы обработки данных

Алгоритмы хеширования применяются для быстрого поиска и идентификации дубликатов пакетов или для создания сигнатур трафика. Алгоритмы сортировки и поиска используются для

организации и быстрого доступа к захваченным данным трафика, что ускоряет анализ и обработку данных.

Теория графов

Графовые алгоритмы применяются для моделирования сетевых взаимодействий. Например, узлы графа могут представлять устройства в сети, а ребра – соединения между ними. Это позволяет выявлять подозрительные связи или строить карты атак. Алгоритмы поиска кратчайшего пути и обхода графов используются для анализа маршрутов в сети и выявления узких мест или подозрительных изменений маршрутов.

Анализ потоков (Flow Analysis)

NetFlow и IPFIX анализ используются для сбора и анализа сетевых потоков. Методы статистического анализа применяются для интерпретации собранных данных и выявления аномалий на уровне потоков.

Анализатор фишинговых атак – это инструмент, предназначенный для обнаружения и предотвращения фишинговых атак, которые направлены на обман пользователей с целью получения их конфиденциальной информации, такой как пароли, номера кредитных карт, или личные данные. Фишинговые атаки могут принимать различные формы, включая фальшивые веб-сайты, электронные письма или сообщения, которые выглядят как законные, но на самом деле создаются злоумышленниками.

Основные методы и подходы в анализаторе фишинговых атак

1. Сигнатурный анализ.

Этот метод основан на использовании базы данных известных фишинговых шаблонов и их сигнатур для сравнения с текущими входящими данными. Например, если текст письма, структура URL, или IP-адрес соответствует сигнатуре из базы данных, сообщение помечается как фишинговое. Сигнатурный анализ эффективен для обнаружения уже известных атак, но может быть уязвим перед новыми, еще не документированными фишинговыми схемами.

2. Эвристический анализ.

Эвристический анализ основан на наборе правил и характеристик, часто встречающихся в фишинговых атаках. Примеры таких характеристик включают:

– подозрительные домены (например, легкие опечатки в названиях доменов, напоминающие легитимные сайты);

– необычные обращения или тон письма (например, слишком настойчивые призывы к действию);

– большое количество грамматических ошибок или неправильные форматы.

Этот метод полезен для обнаружения неизвестных или модифицированных атак, но может давать ложные срабатывания.

3. Анализ URL и доменов.

Проверка URL-адресов на наличие подозрительных признаков, таких как слишком длинные адреса, использование IP-адресов вместо доменов, или домены, недавно зарегистрированные или известные своей связью с фишингом. Используется для анализа веб-страниц и ссылок, чтобы определить их легитимность до того, как пользователь перейдет по ним.

4. Методы машинного обучения.

Использование алгоритмов машинного обучения для автоматического распознавания фишинговых атак на основе обучающей выборки из множества фишинговых и безопасных сообщений. Алгоритмы, такие как логистическая регрессия, случайные леса, или нейронные сети, используются для классификации сообщений как фишинговых или безопасных. Модели обучаются на таких признаках, как текстовые элементы (например, частота слов, наличие определенных фраз), структура URL, и метаданные. Машинное обучение позволяет анализатору адаптироваться к новым типам фишинговых атак и снижать количество ложных срабатываний.

5. Анализ содержимого.

Оценка содержания сообщений (например, текста писем или веб-страниц) на наличие типичных фишинговых приемов, таких как ложные предупреждения о безопасности, имитация официальных писем от банков, или просьбы о срочных действиях. Контентный анализ помогает обнаруживать фишинговые атаки, которые используют социальную инженерию для обмана пользователей.

6. Анализ метаданных.

Проверка метаданных электронных писем (например, заголовков, адресов отправителей, времени отправки) на подозрительные элементы. Например, может быть выявлен отправитель, замаскированный под легитимный сервис, но использующий неофициальный домен. Этот метод помогает идентифицировать фальшивые сообщения, маскирующиеся под сообщения от надежных источников.

Пример работы анализатора фишинговых атак.

1. Сбор данных: Анализатор получает данные о входящих электронных письмах, URL-адресах и веб-страницах, которые могут быть потенциальными источниками фишинговых атак.

2. Предварительная обработка: Данные нормализуются и подготавливаются для анализа. Например, текст письма может быть токенизирован, а URL-адреса разбиты на составляющие.

3. Анализ сигнатур: Проверка входящих данных на соответствие известным фишинговым шаблонам.

4. Эвристический анализ: Применение правил для обнаружения подозрительных характеристик в данных.

5. Машинное обучение: Использование обученной модели для классификации сообщений как фишинговых или безопасных.

6. Отчет и реагирование: если атака обнаружена, анализатор может отправить уведомление администратору или пользователю, заблокировать подозрительное письмо или URL, и/или записать информацию о выявленной атаке для дальнейшего анализа.

Предварительная обработка данных – это важный этап, на котором данные нормализуются и подготавливаются для последующего анализа, что особенно важно в контексте обнаружения фишинговых атак. Этот процесс помогает улучшить качество данных, устранить шум и привести данные к форме, наиболее подходящей для анализа. В контексте фишинговых атак предварительная обработка может включать несколько шагов.

Математическая интерпретация фишинговых атак заключается в создании моделей и методов, которые позволяют обнаруживать и классифицировать такие атаки на основе формализованных подходов. Фишинговые атаки можно интерпретировать как задачу классификации или обнаружения аномалий, где используются различные математические и статистические методы.

Основные аспекты математической интерпретации фишинговых атак

1. Моделирование признаков (Feature Engineering).

Для анализа фишинговых атак важна правильная идентификация признаков (features). Признаки могут включать:

– лингвистические особенности текста (частотность слов, наличие грамматических ошибок, характерные фразы);

– метаданные (IP-адреса отправителей, заголовки писем, время отправки);

– структура URL (наличие подозрительных символов, длина URL, совпадение с известными легитимными доменами);

– характеристики сетевого трафика (частота отправки запросов, объем передаваемых данных).

Пусть $X_1, X_2, \ldots, X_n$ – это набор признаков, характеризующих электронное письмо или URL. Каждый признак X_i может быть бинарным (например, присутствует ли подозрительное слово) или числовым (например, количество внешних ссылок).

2. Классификация (Classification).

Классифицировать входящие сообщения как фишинговые или безопасные можно различными методами.

– Логистическая регрессия: модель логистической регрессии строится на основе линейного сочетания признаков и оценивает вероятность того, что сообщение является фишинговым. Пусть y – бинарная переменная (1 – фишинговое, 0 – безопасное), тогда вероятность $p(y = 1|X)$ может быть выражена через логистическую функцию:

$$p(y = 1|X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n)}}. \quad (1)$$

– Деревья решений и случайные леса: Дерево решений строит рекурсивные разбиения пространства признаков на основе критериев, которые минимизируют неопределенность. Случайный лес (ensemble метод) строит множество деревьев и агрегирует их решения.

– Методы на основе нейронных сетей: нейронные сети могут использоваться для более сложного анализа признаков, включая текстовые данные и изображения. Это позволяет захватывать нелинейные зависимости между признаками и результатом.

3. Обнаружение аномалий (Anomaly Detection).

Выявление фишинговых атак как аномалий в потоке данных возможно следующими методами.

– Метод ближайших соседей (k-NN): определяет, является ли новое сообщение фишинговым на основе его расстояния до известных примеров в пространстве признаков. Если сообщение слишком далеко от большинства примеров безопасных писем, оно может быть классифицировано как фишинговое.

– Метод главных компонент (PCA): используется для снижения размерности данных и выявления основных компонент, которые объясняют большую часть вариаций в данных. Фишинговые атаки могут выявляться как выбросы или аномалии в уменьшенном пространстве признаков.

– Кластеризация (например, алгоритм k-means): сообщения группируются в кластеры. Если сообщение попадает в «отдельный» кластер, оно может быть рассмотрено как аномалия и, возможно, фишинг.

4. Байесовские методы (Bayesian Methods).

Оценка вероятности фишинговой атаки на основе апостериорной вероятности.

Наивный байесовский классификатор. Использует правило Байеса для вычисления апостериорной вероятности того, что письмо является фишинговым, на основе наблюдаемых признаков.

$$P(y = 1|X) = \frac{P(X|y = 1) \cdot P(y = 1)}{P(X)}. \quad (2)$$

Если известно, что определенные слова или фразы часто встречаются в фишинговых письмах, наивный байесовский классификатор может использовать эту информацию для оценки вероятности того, что новое письмо является фишинговым.

5. Теория графов и сетевой анализ (Graph Theory and Network Analysis).

Моделирование связей между различными элементами (например, IP-адресами, доменами, пользователями) как графа для выявления подозрительных паттернов реализуется с использованием нижеперечисленных способов.

– Обнаружение сообществ: определение кластеров

(сообществ) внутри сети, которые могут представлять собой группы связанных фишинговых сайтов или IP-адресов.

– Алгоритмы центральности: оценка важности узлов в сети (например, IP-адресов, используемых в атаках), что позволяет выявить ключевые элементы в инфраструктуре фишинга.

– Анализ путей: обнаружение типичных путей перехода от безопасных сайтов к фишинговым. Например, определение «цепочек» редиректов, ведущих на фишинговые страницы.

Математическая интерпретация фишинговых атак включает создание моделей, которые могут предсказывать или выявлять такие атаки на основе анализа большого количества признаков и данных. Эти методы включают статистические подходы, машинное обучение, байесовские методы и теорию графов. Такой подход позволяет эффективно обнаруживать фишинговые атаки даже при наличии сложных и меняющихся шаблонов атак.

Заключение

В работе рассмотрена технология построения анализаторов для выявления компьютерных атак, базирующаяся на предложенной ранее технологии построения двухуровневой модели корпоративной сети. Подробно описаны параметры, необходимые для выявления фишинговых атак в корпоративной сети. На базе проведенного исследования представляется возможной реализация разработанной технологии на практике.

Литература:

1. *Hamed Taherdoos.* Understanding Cybersecurity Frameworks and Information Security Standards // A Review and Comprehensive Overview Electronics. – 2022. – Vol. 11 (14). – 2181. – DOI: 10.3390/electronics11142181.

2. *Simon N. Foley, Stefano Bistarelli, Barry O'Sullivan, John Herbert & Garret Swart.* Multilevel Security and Quality of Protection / Security Measurements and Metrics Conference proceedings. – 2006. – P. 93-105. – DOI: 10.1007/978-0-387-36584-8_8.

3. *Ross Anderson.* Multilevel Security / Security Engineering. A Guide to Building Dependable Distributed Systems. – Indianapolis: Wiley & Sons, Inc., 2020. – P. 315-339. – DOI: 10.1002/9781119644682.ch9.

4. *Альтшулер С.В.* Методы оценки параметров процессов авторегрессии-скользящего среднего // Автоматика и телемеханика. – 1982. – №. 8. – С. 5-18.

5. *Рунова Л.П.* Модель авторегрессии и скользящего среднего (ARMA). – Ростов-на-Дону: Издательство Южного федерального университета, 2013. – 59 с.

6. *Дубровин М.Г., Глухих И.Н.* Применение модели Хольта-Винтерса для прогнозирования работоспособности серверных систем // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2019. – №. 4. – С. 35-41.

7. *Поздняков А.С.* Применение метода Хольта-Винтерса при анализе и прогнозировании динамики временных рядов / Сборник научных трудов студентов, магистрантов, аспирантов, молодых ученых и их научных руководителей (материалы межвузовской научно-практической конференции) «Проблемы организации и управления на транспорте». Выпуск 11 (230). – Екатеринбург: Уральский государственный университет путей сообщения, 2017. – С. 57-64.

8. *Дмитриев К.В.* Методы машинного обучения в анализе изображений и временных рядов. Teach-in. Лекции ученых МГУ. – Москва: ФИЗФАК МГУ, 2022. – 173 с.

9. *Кугаевских А.В., Муромцев Д.И., Кирсанова О.В.* Классические методы машинного обучения. – СПб: Университет ИТМО, 2022. – 53 с.

Лещенко В.В., Пантелеймонов И.Н.

Исследование развития патентного и непатентного научно-технического ландшафта лазерной космической связи

Аннотация: Рассмотрены результаты интеллектуальной деятельности в научно-техническом развитии создания систем высокоскоростной лазерной космической связи. Приведены пояснения о повышенной информационной безопасности такой передачи информации. Выполнен