DOI 10.37539/2949-1991.2023.5.5.002

Дуров Семён Сергеевич, студент,
Финансовый университет при Правительстве РФ, г. Москва

Резниченко Сергей Анатольевич,
кандидат технических наук, доцент, доцент департамента информационной безопасности Финансового университета при Правительстве РФ, Финансовый университет при правительстве РФ, г. Москва

Хохлов Евгений Александрович, студент,
Финансовый университет при Правительстве РФ, г. Москва

ЛОЖНЫЕ СРАБАТЫВАНИЯ В СИСТЕМАХ IDS: СПОСОБЫ ИДЕНТИФИКАЦИИ И МЕТОДЫ СНИЖЕНИЯ ИХ КОЛИЧЕСТВА
FALSE POSITIVES IN IDS SYSTEMS: IDENTIFICATION METHODS AND WAYS TO REDUCE THEIR QUANTITY.

Аннотация. Кибербезопасность все более важна в связи с ростом кибератак. Системы обнаружения вторжений (IDS) созданы для обнаружения и предотвращения таких атак.

Цель этой статьи - обзор существующих исследований по проблеме ложных срабатываний в IDS. Основное внимание уделяется методам идентификации, которые помогают уменьшить количество ложных срабатываний. В работе анализируется производительность различных алгоритмов для снижения ложных срабатываний в IDS.

Abstract. Cybersecurity is increasingly important due to the rise of cyber-attacks. Intrusion Detection Systems (IDS) are designed to detect and prevent such attacks.

The purpose of this article is to review existing research on the problem of false positives in IDS. The focus is on identification methods that help reduce the number of false positives. The paper analyzes the performance of various algorithms to reduce false positives in IDS.

Ключевые слова: системы обнаружения вторжений, ложные срабатывания, методы идентификации, корреляция оповещений, интеллектуальный анализ данных, кибербезопасность.

Keywords: intrusion detection systems, false positives, identification methods, alert correlation, data mining, cybersecurity.

Введение

Поскольку компьютерные сети становятся все более важными для современного общества, защита их от атак приобретает все большее значение. Системы обнаружения вторжений (IDS) широко используются для обнаружения вторжений и оповещения сетевых администраторов. Однако идентификаторы генерируют огромное количество предупреждений, многие из которых являются ложными срабатываниями, дубликатами или событиями низкой важности. Подавляющее количество этих предупреждений может быть неуправляемым для людей, занимающихся аналитикой, особенно когда подавляющее большинство из них ложные. Ложные срабатывания могут возникать, когда IDS ошибочно классифицирует обычную активность как атаку. Чтобы решить эту проблему, исследователи предложили различные подходы к сокращению числа ложных срабатываний, при этом часто предлагаются методы интеллектуального анализа данных и корреляции предупреждений.

В этой статье представлен обзор методов, предложенных для уменьшения ложноположительных результатов в идентификаторах, с акцентом на методы интеллектуального анализа данных и корреляции предупреждений. Ниже представлена краткая характеристика о главах:

I. В разделе 1 обсуждаются основные показатели для оценки различных методов уменьшения ложноположительных срабатываний, включая точность, эффективность и действенность.

II. В разделе 2 рассматриваются различные методы, которые могут быть использованы для уменьшения количества ложных срабатываний, включая методы, основанные на пороговых значениях, методы, основанные на аномалиях, и методы, основанные на сигнатурах.

III. В разделе 3 описывается использование методов интеллектуального анализа данных для уменьшения ложных срабатываний. Методы интеллектуального анализа данных могут использоваться для выявления закономерностей и корреляций в данных, которые могут помочь отличить подлинные угрозы от ложных тревог.

IV. В разделе 4 обсуждаются методы, используемые для сопоставления предупреждений и вторжений. Эти методы включают временную корреляцию, пространственную корреляцию и логическую корреляцию

V. В разделе 5 мы представляем классификацию методов корреляции оповещений, основанную на типах данных, используемых для корреляции, и используемых алгоритмах корреляции.

VI. В разделе 6 мы завершаем изложением основных результатов и выделяем перспективные области для будущих исследований.

1. Параметры оценки для уменьшения количества ложных срабатываний

Одной из главных мер эффективности IDS является его способность правильно классифицировать события как атаку или нормальное поведение. Для оценки эффективности различных методов снижения ложных результатов IDS необходимо учитывать четыре возможных исхода:

- **Истинно отрицательный (TN – True negative):** события, которые на самом деле являются нормальными и успешно помечены как нормальные;

- **Истинно положительный (TP – True positive):** события, которые на самом деле являются атаками и успешно помечены как атаки;
- **Ложноположительный (FP – False positive):** нормальные события классифицируются как атаки;
- **Ложноотрицательный (FN – False negative):** атаки классифицируются как нормальные события.

Ниже приведены зависимости, позволяющие оценить эффективность системы IDS:

1. Ложноположительный показатель:

False Positive Rate (FPR)= FP/(FP+TN), где

FP – число ложноположительных срабатываний

TN – число истинно отрицательных срабатываний

2. Ложноотрицательный показатель:

False Negative Rate (FNR)= FN/(FN+TP), где

FN – число ложноотрицательных срабатываний

TP – число истинно-положительных срабатываний

3. Истинно положительный показатель:

True Positive Rate (TPR) = TP/(TP+FN), где

TP – число истинно-положительных срабатываний

FN – число ложноотрицательных срабатываний

4. Истинно отрицательный показатель:

True Negative Rate (TNR)= TN/(TN+FP), где

TN – число истинно-отрицательных срабатываний

FP – число ложноположительных срабатываний

5. Точность:

Данный параметр показывает, насколько близко среднее значение измерений к действительному значению

Accuracy = (TP+TN)/(TP+TN+FP+FN), где

TP – число истинно-положительных срабатываний

TN – число истинно-отрицательных срабатываний

FP – число ложноположительных срабатываний

FN – число ложноотрицательных срабатываний

6. Точность измерений:

Данный параметр отражает, насколько близки между собой результаты измерений

Precision = TP/(TP+FP), где

TP – число истинно-положительных срабатываний

FP – число ложноположительных срабатываний

Частота ложноположительных результатов (FPR) относится к доле случаев, в которых обычное поведение ошибочно идентифицируется как поведение во время атаки. Высокий FPR приведет к низкой производительности IDS, в то время как высокий уровень ложноотрицательных результатов (FNR) сделает систему уязвимой для вторжений. Истинно отрицательных показатель результатов (TNR) относится к доле обнаруженных атак среди всех событий реальных атак. Точность относится к доле событий, отнесенных к правильному типу, в общем количестве событий.

Оценка эффективности методов снижения ложноположительных результатов является важным вопросом. Простое снижение частоты ложноположительных результатов недостаточно. Некоторые методы, направленные на уменьшение ложных срабатываний, могут привести к низкой точности системы из-за операций, таких как чрезмерное обобщение и отсутствие реальных предупреждений об атаках. Эффективные методы снижения ложноположительных результатов должны позволять уменьшить их количество при одновременном повышении точности системы или, по крайней мере, сохранить ее без изменений.

2. Методы уменьшения количества ложных срабатываний

Все эти методы можно разделить на два подхода. Первый подход включает методы, которые работают на этапе обнаружения, мы называем их методами обнаружения, а второй относится к методам, которые работают с полученными предупреждениями после этапа обнаружения, мы называем их методами обработки предупреждений.

2.1. Метод обнаружения

Одним из распространенных методов обнаружения является **использование пороговых значений**. Этот метод включает в себя установку порогового значения для определенного показателя, такого как сетевой трафик, и классификацию любой точки данных выше этого порога как атаки. Однако этот метод может привести к ложным срабатываниям, когда допустимый трафик превышает пороговое значение или когда злоумышленники намеренно остаются ниже порогового значения.

Другим методом обнаружения является **использование алгоритмов машинного обучения**, таких как деревья решений или машины опорных векторов. Эти алгоритмы извлекают уроки из исторических данных, чтобы идентифицировать шаблоны и классифицировать новые данные как обычные или вредоносные. Этот метод может быть очень эффективным, но требует большого объема обучающих данных и может быть уязвим для атак противника.

Системы, основанные на правилах, — это еще один метод обнаружения, который использует набор предопределенных правил для выявления атак. Эти правила могут основываться на известных схемах атак или подозрительном поведении. Этот подход эффективен для выявления определенных типов атак, но может быть ограничен в своей способности выявлять новые и неизвестные атаки.

Поведенческий анализ — это еще один метод обнаружения, который отслеживает поведение системы и выявляет отклонения от нормальных моделей поведения. Этот метод может быть эффективным при выявлении атак нулевого дня и новых форм вредоносного ПО, но он требует значительных вычислительных мощностей и может быть сложным в реализации.

Наконец, **обнаружение на основе сигнатур** — это метод, который использует известные сигнатуры атак для выявления новых атак. Этот метод эффективен при выявлении известных атак, но может быть легко обойден злоумышленниками, использующими новые методы или варианты существующих атак.

В целом, методы обнаружения могут быть эффективными для уменьшения ложных срабатываний за счет повышения точности системы обнаружения вторжений. Однако у каждого метода есть свои сильные и слабые стороны, и выбор метода будет зависеть от конкретных потребностей организации и используемой системы.

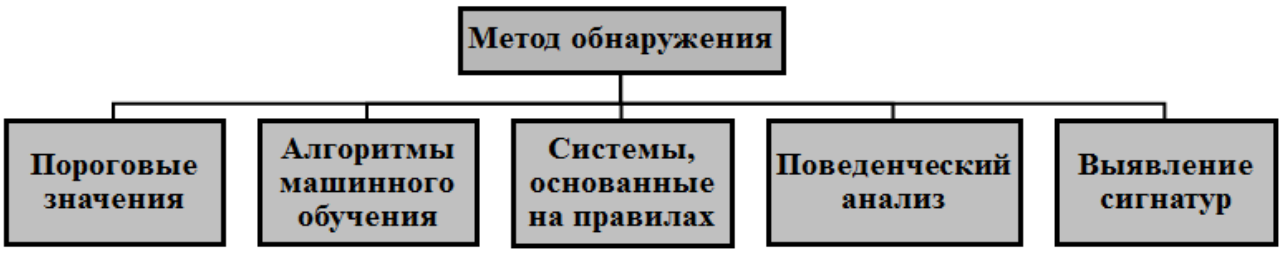

Рисунок 1 – Структура метода обнаружения

2.2. Метод обработки предупреждений

Второй подход к методам уменьшения ложноположительных результатов включает обработку предупреждений, генерируемых методами обнаружения. Эти методы направлены на уточнение и сопоставление предупреждений для предоставления более точной информации аналитику безопасности.

Одним из методов обработки предупреждений является **фильтрация.** Фильтрация включает в себя удаление предупреждений, которые менее важны или менее релевантны. Это может быть сделано вручную аналитиком по безопасности или автоматически с помощью компьютерной программы. Цель фильтрации - уменьшить количество ложных срабатываний, которые представляются аналитику, чтобы он мог сосредоточиться на наиболее важных предупреждениях.

Другим методом является **расстановка приоритетов**. Приоритезация включает в себя ранжирование предупреждений на основе их серьезности или важности. Это позволяет аналитикам сначала сосредоточиться на наиболее важных предупреждениях. Приоритезация может быть выполнена автоматически на основе предопределенных критериев или вручную аналитиком.

Корреляция — это еще один метод, используемый при обработке предупреждений. Корреляция включает в себя анализ множества предупреждений для выявления закономерностей и взаимосвязей между ними. Это может помочь выявить сложные атаки, которые могут быть пропущены отдельными методами обнаружения.

Объединение данных — это метод, который объединяет информацию из нескольких источников, чтобы обеспечить более полное представление о ситуации с безопасностью. Это может включать объединение данных из разных методов обнаружения или из разных сегментов сети. Цель data fusion - предоставить аналитику более точную и достоверную информацию, которая может помочь уменьшить количество ложных срабатываний.

Машинное обучение также используется при обработке предупреждений. Алгоритмы машинного обучения можно обучить распознавать закономерности в данных предупреждений и предсказывать, какие предупреждения с наибольшей вероятностью окажутся

ложноположительными. Это может помочь снизить нагрузку на аналитиков безопасности и повысить точность системы.

Таким образом, вторая группа мер по уменьшению ложноположительных срабатываний фокусируется на обработке предупреждений, генерируемых методами обнаружения. Фильтрация, приоритезация, корреляция, объединение данных и машинное обучение — все это методы, используемые при обработке предупреждений. Уточняя и сопоставляя предупреждения, эти методы могут помочь уменьшить количество ложных срабатываний и предоставить более точную и достоверную информацию аналитикам безопасности.

Рисунок 2 - Структура метода обработки предупреждений

Вывод по 2 разделу.

Первый подход, включающий методы обнаружения, обычно используется для сокращения частоты ложных срабатываний в фазе обнаружения, когда данные еще не прошли полную обработку и могут содержать ошибки или неточности. Эти методы основываются на более точном анализе данных и уменьшении количества ложных предупреждений на этой стадии.

Второй подход, использующий методы обработки предупреждений, применяется после фазы обнаружения и нацелен на более точное определение, является ли предупреждение атакой или нет. Эти методы часто включают использование анализа контекста и данных из других источников для подтверждения или опровержения предупреждений об атаках.

Оба подхода могут быть эффективными, и часто применяются вместе для достижения более высокой точности и снижения частоты ложных

срабатываний. Тем не менее, каждый подход имеет свои преимущества и недостатки, которые должны быть учтены при выборе методов для конкретной системы обнаружения вторжений.

3. Техники обработки данных

Data Mining — это процесс извлечения знаний из больших баз данных или хранилищ данных. Это скрытая, неизвестная и потенциально полезная информация, которая представлена в виде концепции, правила, закона и модели.

Целью Data Mining является помощь принимающим решения в поиске потенциальных связей между данными, нахождение игнорируемых элементов, которые могут быть очень полезны для анализа тенденций и принятия решений.

Наиболее распространенными методами и технологиями обработки данных являются:

- **Корреляционный анализ:** также называемый ассоциативными правилами, это поиск знаний о модели набора элементов, которые часто встречаются в заданном наборе данных. Цель заключается в обнаружении скрытых взаимосвязей в данных.
- **Последовательные шаблоны:** цель заключается также в обнаружении связей между данными, но анализ временных рядов более фокусируется на связях между данными во времени.
- **Классификация:** цель заключается в поиске модели или функции, которая может описать типичные характеристики набора данных, чтобы можно было идентифицировать владельца или категории неизвестных данных. Типичные модели классификации включают линейную регрессионную модель, модель дерева решений, модель на основе правил и модель нейронной сети.
- **Кластеризация:** данные были разбиты на ряд значимых подмножеств в соответствии с определенными правилами. В одном кластере разрыв между отдельными элементами меньше, а в разных кластерах - больше.

- **Анализ отклонений:** поиск необычных данных в базе данных.
- **Прогнозирование:** поиск закономерностей в исторических данных, установление модели и прогнозирование типов, характеристик будущей информации, на основе составленной модели.

4. Методы корреляции предупреждений и вторжений

Эти методы направлены на объединение связанных предупреждений и вторжений в одно событие, предоставляя администраторам более полное представление об атаке.

4.1. Временная корреляция

Временная корреляция — это метод, используемый для группировки предупреждений и вторжений, которые происходят в одно и то же время. Этот метод предполагает, что атака включает в себя несколько этапов, и каждый шаг генерирует одно или более предупреждений. Сопоставляя время этих предупреждений, можно сгруппировать их в одно событие.

Например, если генерируется предупреждение о неудачной попытке входа в систему, а затем через несколько минут генерируется другое предупреждение о проверке порта, эти предупреждения могут быть сопоставлены и сгруппированы вместе как одно событие. Предполагается, что сканирование порта было частью фазы разведки злоумышленника, а неудачная попытка входа в систему была попыткой получить доступ.

4.2. Пространственная корреляция

Пространственная корреляция — это метод, используемый для группировки предупреждений и вторжений, которые происходят в одном и том же месте. Этот метод предполагает, что кибератака затрагивает несколько хостов и устройств, и каждое генерирует одно или более предупреждений. Сопоставляя местоположение этих предупреждений, можно сгруппировать их в одно событие.

Например, если предупреждение генерируется для проверки порта на определенном сервере, а затем генерируется другое предупреждение для неудачной попытки входа на другом сервере, эти предупреждения могут быть сопоставлены и сгруппированы вместе как одно событие. Предполагается, что злоумышленник пытается получить доступ к нескольким серверам и устройствам.

4.3. Логическая корреляция

Логическая корреляция — это метод, используемый для группировки предупреждений и вторжений, которые связаны с точки зрения их поведения или цели. Этот метод предполагает, что кибератака включает в себя несколько этапов, и каждый шаг генерирует одно или более предупреждений. Сопоставляя поведение или цель этих предупреждений, можно сгруппировать их в одно событие.

Например, если генерируется предупреждение для сканирования порта, а затем генерируется другое предупреждение для неудачной попытки входа в систему, а затем генерируется другое предупреждение для попытки удаления данных, эти предупреждения могут быть сопоставлены и сгруппированы вместе как одно событие. Предполагается, что злоумышленник пытается получить доступ к данным путем сканирования открытых портов, пытается получить доступ с помощью грубой силы, а затем удаляет данные.

4.4. Визуализация

Визуализация является важным аспектом методов корреляции оповещений и вторжений. Цель визуализации - предоставить администраторам полное представление об атаке, позволяющее им понять шаги, предпринятые злоумышленником, и причиненный ущерб. Существует несколько типов методов визуализации, используемых для корреляции предупреждений и вторжений, включая представления временной шкалы, представления топологии сети и представления дерева атак.

Вывод по 4 разделу.

Методы оповещения и корреляции вторжений являются важной частью систем обнаружения вторжений. Эти методы позволяют администраторам разобраться в большом количестве оповещений, генерируемых IDS, и обеспечивают всестороннее представление об атаке. Временная, пространственная и логическая корреляция - это три основных метода, используемых для корреляции оповещений и вторжений. Визуализация является важным аспектом этих методов, предоставляя администраторам визуальное представление атаки.

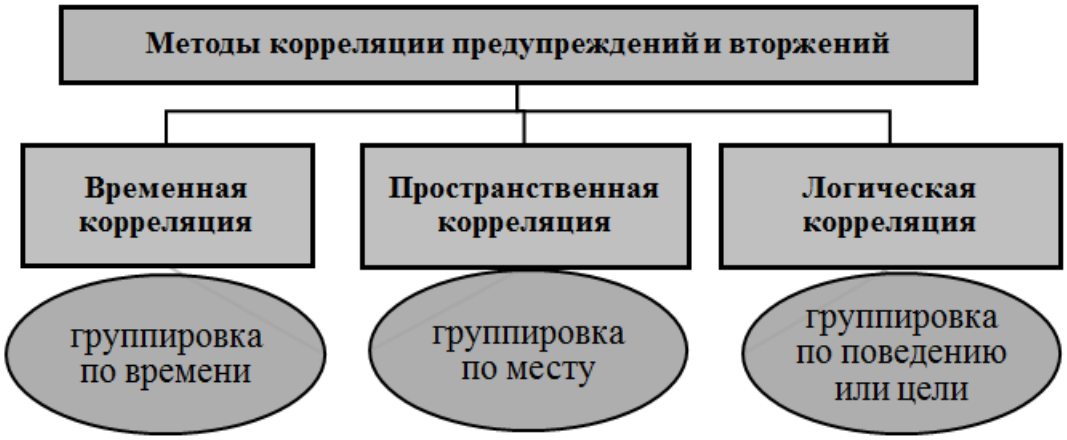

Рисунок 3 - Методы корреляции предупреждений и вторжений

5. Классификация методов корреляции предупреждений

В разделе 4 мы обсудили методы, используемые для сопоставления предупреждений и вторжений. Раздел 5 охватывает классификацию методов корреляции предупреждений. Корреляция предупреждений имеет решающее значение в системах обнаружения вторжений для определения источника атаки и методов, используемых злоумышленниками.

Существует несколько способов классификации методов корреляции предупреждений, и мы обсудим четыре из них: основанные на сходстве, предопределенные сценарии атак, предпосылки и последствия отдельных атак и статистический причинно-следственный анализ.

❖ **Подход, основанный на сходстве**, основан на принципе, что вторжения имеют схожие шаблоны и поведение. Метод сравнивает новое предупреждение с ранее обнаруженными предупреждениями и присваивает оценку сходства. Если показатель сходства превышает определенный порог, метод приходит к выводу, что новое предупреждение связано с предыдущим вторжением. Этот подход эффективен при выявлении атак с похожими шаблонами, но он может не подходить для выявления новых и неизвестных атак.

❖ **Подход с предопределенным сценарием атаки** предполагает, что атаки следуют определенному шаблону, а система обнаружения вторжений предназначена для обнаружения конкретных сценариев атаки. Система использует предопределенные сценарии атаки и проверяет, соответствует ли входящее предупреждение какому-либо из них. Этот подход эффективен при выявлении известных атак, но он может не подходить для обнаружения новых и неизвестных атак.

❖ **Подход, основанный на предпосылках и последствиях отдельных атак**, рассматривает предпосылки и последствия атаки для определения источника атаки. Метод анализирует системные журналы, чтобы идентифицировать любые события, которые предшествовали атаке, и любые события, которые произошли после атаки. Анализируя эти события, метод может идентифицировать источник атаки и методы, используемые злоумышленниками.

❖ **Подход статистического причинно-следственного анализа** основан на статистических методах для выявления причинно-следственной связи между событиями. Метод использует байесовские сети или другие статистические методы для моделирования системы и выявления причинно-следственных связей между событиями. Выявляя причинно-следственные связи, метод может определить источник атаки и методы, используемые злоумышленниками.

В заключение классификация методов корреляции предупреждений имеет важное значение в системах обнаружения вторжений для определения источника атаки и методов, используемых злоумышленниками. Подход, основанный на сходстве, подход с предопределенными сценариями атак, подход с предпосылками и последствиями отдельных атак и подход со статистическим причинно-следственным анализом — это четыре широко используемых метода для сопоставления предупреждений. У каждого метода есть свои сильные и слабые стороны, и выбор подходящего метода зависит от конкретных требований системы.

5. Преимущества и недостатки подходов

В целях подведения итогов, рассмотрим основные преимущества и недостатки рассмотренных методов уменьшения числа ложных срабатываний.

Таблица 1

Преимущества и недостатки подходов

Подход	**Преимущества**	**Недостатки**
Подход, основанный на сходстве	• Может уменьшить количество ложных срабатываний, генерируемых несколькими датчиками.	• Ложное предупреждение может быть обнаружено в том случае, если несколько датчиков обнаружат одну и ту же атаку. • Невозможно обнаружить многоэтапную атаку.
Подход с предопределенным сценарием атаки	• Может уменьшить количество ложных срабатываний. • Можно сгруппировать несколько связанных предупреждений.	• Может создавать большое количество ложноположительных срабатываний. • Необходимо вносить сценарии атак вручную. • Многоэтапная атака игнорируется

Подход, основанный на предпосылках и последствиях отдельных атак	• Многоэтапная атака может быть обнаружена. • Генерируется график, отображающий цели нарушителя.	• Автоматическая генерация правил корреляции может повлечь за собой увеличение ложных срабатываний
Подход статистического причинно-следственного анализа	• Не требуется информация возможных сценариях атак. • Может использоваться для определения новых сценариев атак	• Не подходит для полного процесса корреляции

6. Заключение

Системы обнаружения вторжений играют жизненно важную роль в обеспечении безопасности цифровой инфраструктуры. Однако большое количество ложных срабатываний, генерируемых IDS, может создать серьезную проблему для аналитиков кибербезопасности. В этой работе представлен обзор различных методов, которые могут быть использованы для уменьшения количества ложных срабатываний при идентификации.

Различные подходы, рассмотренные в этой статье, включают методы на основе пороговых значений, аномалий, сигнатур, интеллектуального анализа данных и корреляции оповещений. Каждый из этих методов имеет свои преимущества и ограничения, и аналитики могут использовать их комбинацию для достижения большей точности, оперативности и действенности.

В обзоре также представлена классификация методов корреляции оповещений, основанная на типах используемых данных и используемых алгоритмах корреляции. Эта классификация может помочь аналитикам выбрать подходящую методику для своих конкретных нужд и предоставить дорожную карту для будущих исследований в этой области.

В целом, результаты дают ценную информацию о текущем состоянии исследований по снижению количества ложноположительных результатов при идентификации. Опрос может помочь аналитикам определить перспективные методы и предоставить рекомендации для будущих исследований по повышению эффективности IDS в обнаружении и предотвращении киберугроз.

Список литературы:

1. Андресс Джейсон. Защита данных. От авторизации до аудита. — СПб.: Питер, 2021. — 272 с.: ил. — (Серия «Для профессионалов»)

2. Белова А.Л., Бородавкин Д.А. Сравнительный анализ систем обнаружения вторжений // Актуальные проблемы авиации и космонавтики. 2016. №12. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-sistem-obnaruzheniya-vtorzheniy (дата обращения: 21.05.2023).

3. Бондяков Алексей Сергеевич Основные режимы работы системы предотвращения вторжений (IDS/IPS Suricata) для вычислительного кластера // Современные информационные технологии и ИТ-образование. 2017. №3. URL: https://cyberleninka.ru/article/n/osnovnye-rezhimy-raboty-sistemy-predotvrascheniya-vtorzheniy-ids-ips-suricata-dlya-vychislitelnogo-klastera (дата обращения: 20.05.2023).

4. Васильева И. Н. Расследование инцидентов информационной безопасности: учебное пособие / И. Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 113 с

5. Крючков А.В., Прус Ю.В., Резниченко С.А., Технологические основы национальной информационной безопасности // Сборник статей, Международной научно-практической конференции Российского государственного гуманитарного университета. 2018. С. 58–63.

6. Лоскутов И.А., Резниченко С.А. Угрозы информационной безопасности госкорпораций Российской Федерации //Вестник Дагестанского

государственного технического университета. Технические науки. Том 49, №3, 2022. Herald of Daghestan State Technical University. Technical Sciences. Vol.49, No.3, 2022. http://vestnik.dgtu.ru/ ISSN (Print) 2073-6185 ISSN (On-line) 2542-095X

7. Марков, Р. А. Исследование нейросетевых технологий для выявления инцидентов информационной безопасности / Р. А. Марков, В. В. Бухтояров, А. М. Попов, Н. А. Бухтоярова. — Текст: непосредственный // Молодой ученый. — 2015. — № 23 (103). — С. 55–60. — URL: https://moluch.ru/archive/103/23866/ (дата обращения: 23.05.2023).

8. Резниченко С.А., Чмыхалова А.В. Анализ рисков ИБ - идентификация рисков ИБ /Особенности управления инцидентами ИБ в кредитно-банковской системе //Флагман науки: научный журнал. Май 2023.-СПб., Изд.ГНИИ "Нацразвитие"-2023. №4(4).

9. Сильнов Д.С., Тараканов О. В. О ложных срабатываниях средств защиты информации // Прикладная информатика. 2015. №2 (56). URL: https://cyberleninka.ru/article/n/o-lozhnyh-srabatyvaniyah-sredstv-zaschity-informatsii (дата обращения: 19.05.2023).

10. Силаков Николай Владимирович Метод обнаружения аномальных вторжений в компьютерной сети, использующий критерий Фишера // StudNet. 2020. №10. URL: https://cyberleninka.ru/article/n/metod-obnaruzheniya-anomalnyh-vtorzheniy-v-kompyuternoy-seti-ispolzuyuschiy-kriteriy-fishera (дата обращения: 19.05.2023).

11. Стрижова Ю. С., Перова М.В. Внедрение ERP-систем на российских предприятиях // Актуальные вопросы экономических наук. 2014. №40. URL: https://cyberleninka.ru/article/n/vnedrenie-erp-sistem-na-rossiyskih-predpriyatiyah (дата обращения: 28.05.2023).

12. Форшоу Дж. Атака сетей на уровне протоколов / пер. с англ. Д. А. Беликова. – Москва.: ДМК Пресс, 2021. – 340 с.: ил.