ПРОДУКЦИОННОЙ МОДЕЛИ ДЛЯ АНАЛИЗА СЕТЕВЫХ ПОТОКОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Кабулов Анвар

Профессор Национального университета Узбекистана имени Мирзо Улугбека

Жўраев Маъруф

Старший преподаватель TMCI

E-mail: juraevmaruff@gmail.com

Аннотация: В настоящее время интерес к экспертным системам растёт среди представителей различных сфер, в том числе экономистов, финансистов, врачей, психологов, программистов, специалистов по сетевой безопасности. Эти системы помогают решать широкий спектр задач: интерпретация данных, диагностика, мониторинг, прогнозирование и многое другое. В данной статье рассматривается разработка модели принятия решений на основе экспертной системы в области мониторинга и анализа сетевых потоков. В частности, было использовано 38 продукционных правил, на основе которых сформировано дерево решений. Такой подход обеспечивает ясность относительно потока данных в сети, выявляет проблемные ситуации и позволяет пользователю принимать быстрые и обоснованные решения. Предлагаемая модель направлена на повышение эффективности мониторинга и анализа сетевой активности в режиме реального времени.

Ключевые слова: правило продукционной, знания, сетевой поток, действия, производство, экспертная система

Annotatsiya: Hozirgi vaqtda ekspert tizimlariga bo‘lgan qiziqish turli soha vakillari, jumladan, iqtisodchilar, moliyachilar, shifokorlar, psixologlar, dasturchilar va tarmoq xavfsizligi mutaxassislari orasida tobora ortib bormoqda. Bu tizimlar keng ko‘lamdagi masalalarni hal etishga yordam beradi: ma’lumotlarni talqin qilish, diagnostika, monitoring, bashorat qilish va boshqalar. Ushbu maqolada tarmoq oqimini monitoring qilish va tahlil qilish sohasida ekspert tizimi asosida qaror qabul qilish modelini ishlab chiqish masalasi ko‘rib chiqiladi. Xususan, 38 ta produksion qoidadan foydalanilgan bo‘lib, ular asosida qarorlar daraxti shakllantirilgan. Ushbu yondashuv orqali tarmoqdagi ma’lumotlar oqimi haqida aniqlik kiritish, muammoli holatlarni aniqlash va foydalanuvchi uchun tezkor va asosli qaror qabul qilish imkoniyati yaratiladi. Taklif etilayotgan model real vaqt rejimida tarmoqdagi harakatlarni kuzatish va ularni tahlil qilishda samaradorlikni oshirishga qaratilgan.

Kalit so‘zlar: produksion qoida, bilim, tarmoq oqimi, harakatlar, produksiya, ekspert tizim

ISSN 3030-3907

Abstract: Currently, interest in expert systems is growing among representatives of various fields, including economists, financiers, doctors, psychologists, programmers, and network security specialists. These systems help solve a wide range of problems: data interpretation, diagnostics, monitoring, prediction, etc. This article considers the development of a decision-making model based on an expert system in the field of monitoring and analyzing network traffic. In particular, 38 production rules were used, based on which a decision tree was formed. This approach provides clarity about the data flow in the network, identifies problematic situations, and allows the user to make quick and informed decisions. The proposed model is aimed at increasing the efficiency of monitoring and analyzing network traffic in real time.

Keywords: production rule, knowledge, network flow, actions, production, expert system

Введение:

Данное исследование посвящено вопросу выявления проблем, возникающих при мониторинге сетевых потоков данных, и автоматизации их эффективной диагностики системным администратором. В современной быстро развивающейся цифровой инфраструктуре сложность информационных систем возрастает. Своевременное обнаружение сетевых сбоев, угроз безопасности или необычного использования ресурсов и соответствующее реагирование являются актуальной проблемой [3].

При традиционном подходе такие проблемы вручную анализируются администратором, а решения принимаются человеком. Однако в больших и сложных информационных системах администратору сложно одновременно отслеживать все потоки, оценивать их и быстро принимать решения. Поэтому внедрение экспертных систем в области сетевого мониторинга имеет большое значение. Экспертные системы это интеллектуальное программное обеспечение для принятия решений, основанное на знаниях опытных специалистов, что позволяет им в режиме реального времени оценивать состояние сети, выявлять проблемные ситуации и разрабатывать рекомендуемые решения [6].

Экспертная система, разработанная в рамках данного исследования, основана на 38 продукционных правилах, которые используются для формирования дерева решений, реагирующего на конкретные ситуации. Это дерево решений помогает администратору выявить конкретную проблему в сети и определить, какие действия следует предпринять. Кроме того, экспертная система также взаимодействует с пользователем: анализирует его действия, выявляет проблемную ситуацию и предоставляет пользователю

ISSN 3030-3907

необходимые рекомендации или указывает на необходимость обращения к администратору. Таким образом, вопрос разработки экспертных систем является не только актуальным, но и важным для обеспечения эффективного обмена информацией между пользователем и администратором.

ЛИТЕРАТУРНЫЙ ОБЗОР: Луи и др. разработали производственные правила для задержки обнаружения в отношении антивирусного программного обеспечения. Представлен итерационный алгоритм решения модели путем применения к данной модели принципа максимума Понтрягина [1]. После выявления знаний производственно-механического состава металлургических предприятий в отрасли производства металлической упаковки был разработан набор правил, призванных помочь в выявлении причин возникновения дефектов в процессе производства [2]. Разработано 76 производственных правил для процесса сварки упаковки и 65 производственных правил для процесса нанесения наполнителя, всего 141 производственный правило. Эти производственные правила хранились в специальной базе знаний, которой ранее не было в организации, и этот процесс повысил эффективность производства. Чен и Фальман разработали базу знаний Scone. Он представляет знания в виде узлов и связей в сетевой структуре и может эффективно делать основные выводы о связях между различными элементами [3]. Доу и др. разработаны производственные правила для управления распределительной сетью в режиме реального времени [4]. Батиста и др., прогнозируя изменения в потоке данных IoT и предварительно настраивая правила OpenFlow, сократили время отклика при коммуникации примерно на 51%, поскольку широкое внедрение Интернета вещей (IoT) усугубляет проблемы предоставления адекватных инфраструктур IoT, которые отвечают таким критическим требованиям, как низкая задержка в динамических сетях [5].

МЕТОДОЛОГИЯ: Для достижения цели необходимо автоматизировать принятие решений с использованием экспертной системы мониторинга сетевого потока и обнаружения сбоев в нем, для чего были определены следующие научные и практические задачи [7]:

Знания в области мониторинга сетей должны быть выражены на основе производственной модели. Ситуации, проблемы и решения, связанные с работой сети, были формализованы и отображены в виде постановок, основанных на решениях опытного администратора. Эти правила служат для формирования базы знаний экспертной системы.

Для определения целевых и промежуточных действий между начальным и конечным состояниями в сети была определена цепочка

ISSN 3030-3907

процессов, от обнаружения проблемного состояния до его устранения. Например, с помощью мониторинга обнаруживаются задержки в сети, перегрузка трафика и потеря пакетов, и на основе этих данных определяются необходимые действия (например, оповещение пользователя, блокировка порта или перенаправление трафика).

Определяются условия, необходимые для выполнения каждого действия, а также определяются условия, необходимые для возникновения каждой проблемы (например, чрезмерное количество пакетов TCP - Transmission Control Protocol, трафик, поступающий с неправильного порта), и на их основе определяются условия, при которых активируется действие.

Определяется последовательность действий, выполняемых в сети, и последовательно анализируется порядок, в котором выполняются выявленные действия (например, сначала анализ, затем предупреждение, затем блокировка). Эти действия являются важными шагами в обеспечении безопасности сети.

Преобразовать полученную последовательность действий и соответствующие им условия в продукции. Все состояния, действия и соответствующие им причинные процессы выражаются в форме правил. Эти правила формируют логику работы экспертной системы и создают механизм автоматического принятия решений.

Проверка продукций на согласованность и анализ производственной цепочки: проверяется согласованность созданных правил, их непротиворечивость, связи и логические последовательности. Каждая производственная цепочка должна быть способна реагировать на конкретную ситуацию и обеспечивать движение по определенному пути в дереве решений.

В результате этих шагов будет разработана интеллектуальная экспертная система, которая автоматически обнаруживает любые сбои, возникающие в сетевом потоке, предпринимает эффективные действия по их устранению и предоставляет инструкции в режиме реального времени между администратором и пользователем [8]-[10].

В ходе исследования были определены следующие целевые и промежуточные действия для эффективного выявления, классификации и устранения сбоев и проблем, возникающих в сетевых потоках [6]:*обнаружение проблем* — сетевой мониторинг анализирует поток трафика, количество пакетов, активность протоколов, уровни задержек и попытки доступа к портам; *устранение неполадок* — на основании обнаруженного

ISSN 3030-3907

сбоя или опасной ситуации системному администратору или пользователю даются необходимые инструкции.

Промежуточные действия: *проведение различных испытаний.*

Условия действий и их порядок: *убедитесь, что проблема существует; классификация ошибок в ходе тестирования.*

Рассматривается конкретная ситуация, состоящая из двух проблем: *ошибки программного обеспечения; аппаратные ошибки.*

На основании вышеперечисленных условий были разработаны правила для процессов, происходящих в сетевом потоке в информационной системе. Выявленные потенциальные действия сетевого потока были преобразованы в продукцию:

$$\{\text{ЕСЛИ} \dots, \text{ТО} \dots\} \quad (1)$$

На основе формулы 1 действия в 38 сетях были преобразованы в продукцию:

1. ЕСЛИ есть жалобы на производительность сети, ТО начнется мониторинг сети.
2. ЕСЛИ мониторинг обнаруживает потерю пакетов, ТО проверяется загрузка сети.
3. ЕСЛИ нагрузка на сеть высокая, ТО применяются правила фильтрации трафика.
4. ЕСЛИ нагрузка низкая, ТО ищите проблему маршрутизации.
5. ЕСЛИ задержка пакета высокая, ТО начинается оптимизация пути передачи.
6. ЕСЛИ таблица маршрутизации неверна, ТО проверяется конфигурация маршрутизатора.
7. ЕСЛИ в настройках роутера возникла ошибка, ТО настройки роутера будут сброшены.
8. ЕСЛИ настройки маршрутизатора верны, ТО проверяется состояние коммутаторов.
9. ЕСЛИ порт на коммутаторе не работает, ТО порт будет заменен.
10. ЕСЛИ таблица MAC-адресов на коммутаторе неверна, ТО таблица исправляется.
11. ЕСЛИ наблюдается задержка в ответах DNS (системы доменных имен – DNS), ТО проверяется DNS-сервер.
12. ЕСЛИ DNS не работает, ТО он переключится на альтернативный DNS.
13. ЕСЛИ приложение не запущено, ТО анализируются HTTP, FTP или другие протоколы.
14. ЕСЛИ сеансы TCP сброшены, ТО порты проверяются на открытость.
15. ЕСЛИ порты закрыты, ТО проверяется брандмауэр.

ISSN 3030-3907

16. ЕСЛИ правила брандмауэра неверны, ТО правила брандмауэра изменяются.
17. ЕСЛИ ICMP-пакеты блокируются, ТО сетевые устройства проверяются с помощью ping-запроса.
18. ЕСЛИ устройства не отвечают на пинг, ТО кабель или устройства будут заменены.
19. ЕСЛИ обнаружен обрыв кабеля, ТО кабель будет заменен.
20. ЕСЛИ сетевой интерфейс не работает, ТО проверяется сетевая карта.
21. ЕСЛИ сетевая карта неисправна, ТО она будет заменена на новую.
22. ЕСЛИ у пользователя неверный IP-адрес, ТО проверяется статус DHCP (Dynamic Host Configuration Protocol – DHCP).
23. ЕСЛИ DHCP не работает, ТО будут использоваться статические настройки IP.
24. ЕСЛИ в сети обнаружен подозрительный трафик, ТО срабатывает система IDS/IPS.
25. ЕСЛИ IDS выдает предупреждение, ТО логи анализируются.
26. ЕСЛИ в журналах будут обнаружены признаки атаки, ТО будут приняты меры безопасности.
27. ЕСЛИ в пакетах обнаружены недействительные флаги TCP, ТО это считается признаком потенциальной атаки.
28. ЕСЛИ в сети есть подозрительный трафик, ТО выполняется глубокая проверка пакетов.
29. ЕСЛИ проблема только у одного пользователя, ТО проблема ищется в локальной системе.
30. ЕСЛИ проблема наблюдается у всех пользователей, ТО считается, что проблема в центральной сети.
31. ЕСЛИ обнаружено сканирование портов, ТО включается функция обнаружения сканирования портов.
32. ЕСЛИ обнаружены ответы ARP-спуфинга, ТО применяется защита от атаки ARP-спуфинга.
33. ЕСЛИ компьютер пользователя испытывает чрезмерный трафик, ТО анализируется возможность DDoS-атаки.
34. ЕСЛИ происходит DDoS-атака, ТО применяются правила, фильтрующие IP-адреса.
35. ЕСЛИ пользователь не может отправить электронное письмо, ТО проверяется, открыт ли порт SMTP.
36. ЕСЛИ возникли проблемы с подключением к FTP-серверу, ТО проверяются FTP-порты.

ISSN 3030-3907

37. ЕСЛИ порт SMTP закрыт, ТО брандмауэр будет перенастроен.
38. ЕСЛИ все проверки бесполезны, ТО устройства сетевой инфраструктуры будут отправлены на гарантийный ремонт.

Факты (f), действия (a) и продукции (p) были созданы в соответствии с разработанными продукциями.

Таблица 1.

Список фактов

№	Символ	Описание факта
1	f_1	Получена жалоба на производительность сети (например, пользователи жалуются на медленный интернет)
2	f_2	Возникают сбои в работе сети (отключения, задержки или потеря пакетов).
3	f_3	Возникла проблема на аппаратном уровне (коммутатор, маршрутизатор, кабель).
4	f_4	В программном обеспечении для мониторинга или управления сетью обнаружена ошибка.
5	f_5	Данные поступают от инструментов мониторинга через SNMP или NetFlow.
6	f_6	Возникла проблема с оперативной памятью устройств маршрутизации или NAT (переполнение буфера, задержка очереди).
7	f_7	Топология сети сложна или неправильно настроена.
8	f_8	Возникла проблема с точками ввода/вывода (пользовательские порты, точка доступа Wi-Fi, интерфейсы шлюзов).
9	f_9	В операционной системе (сервере, шлюзе) произошла сетевая ошибка.
10	f_{10}	Программное обеспечение (брандмауэр, VPN, DNS, DHCP) работает неисправно.
11	f_{11}	Нагрузка сети (использование полосы пропускания) превышает 80%.
12	f_{12}	Произошел сбой соединения с интернет-провайдером.
13	f_{13}	Высокая задержка в сегменте локальной сети.
14	f_{14}	Устройство пользователя не получает IP-адрес автоматически.
15	f_{15}	Дополнительный трафик (широковещательный, многоадресный, штормовой) забивает сеть.

ISSN 3030-3907

16	f_{16}	В файлах журналов на сетевых устройствах обнаружены ошибки.
17	f_{17}	Время ответа на DNS-запрос очень большое.
18	f_{18}	Обнаружено нарушение безопасности сети (сканирование портов, DDoS, несанкционированный доступ).

В ответ на сетевые процессы был разработан набор действий. В таблице 2 представлен список действий.

Таблица 2.

Список действий

№	Символ	Описание
1	a_1	Администратор осуществляет общий мониторинг производительности сети (состояние, трафик, журналы).
2	a_2	Администратор тестирует сетевые устройства (коммутатор, маршрутизатор, модем).
3	a_3	Администратор проверяет сетевые службы (брандмауэр, DHCP, DNS).
4	a_4	Администратор проверяет возможность проведения индивидуальных блочных тестов на сегментах сети.
5	a_5	Администратор предоставляет пользователям сети инструкции по использованию сети.
6	a_6	Администратор тестирует операционную систему сервера для работы в сети.
7	a_7	Администратор тестирует приложения, использующие сеть.
8	a_8	Администратор переустанавливает прикладное программное обеспечение, работающее в сети.
9	a_9	Администратор переустанавливает операционную систему сервера или пользовательского устройства.
10	a_{10}	Администратор проверяет память или буферы сетевых устройств (маршрутизатор, коммутатор).
11	a_{11}	Администратор отправляет устройство в сервисный центр для гарантийного ремонта или замены.
12	a_{12}	Администратор заменяет поврежденную память маршрутизатора или коммутатора.
13	a_{13}	Администратор тестирует сетевые интерфейсы, установленные на материнской плате.
14	a_{14}	Администратор заменяет сетевую карту.

ISSN 3030-3907

15	a_{15}	Администратор тестирует сетевые адаптеры пользовательских устройств.
16	a_{16}	Администратор заменяет пользовательское устройство или периферийное сетевое устройство.
17	a_{17}	Администратор выявляет перегруженные точки сегмента и перенаправляет трафик.
18	a_{18}	Администратор связывается с интернет-провайдером и выявляет сбои на верхнем уровне.

Правила производства приведены в таблице 3. Правила представлены в виде формул и дано их описание. На основе разработанных продукционных правил построен их корреляционный график, представленный на рисунке 1.

Таблица 3.

Взаимозависимость между производствами

№	Продукция	Описание
1	$p_1(s_1 \to f_1) = a_1$	При наличии жалобы обычно проверяется работоспособность системы.
2	$p_2(s_2 \to a_1 \wedge f_2) = a_2$	Если выполняется a_1 и происходит сбой системы, то проверяется оборудование.
3	$p_3(s_3 \to a_2 \wedge f_3) = a_4$	Если возникают проблемы с оборудованием, проверяется возможность проведения блочного тестирования.
4	$p_6(s_4 \to a_3 \wedge f_2) = a_1$	При обнаружении аппаратной проблемы выполняется общая проверка производительности системы.
5	$p_4(s_5 \to a_2 \wedge \neg f_3) = a_3$	Если проблем с оборудованием не обнаружено, тестируется программное обеспечение.
6	$p_5(s_6 \to a_3 \wedge f_4) = a_6$	При наличии проблем с программным обеспечением будет проверена операционная система.
7	$p_7(s_7 \to a_3 \wedge \neg f_4) = a_5$	Если проблем с программным обеспечением не возникнет, будут предоставлены инструкции.
8	$p_8(s_8 \to a_6 \wedge f_9) = a_9$	Если возникнут проблемы с операционной системой, она будет переустановлена.
9	$p_9(s_9 \to a_7 \wedge f_{10}) = a_8$	Если возникнут проблемы с приложением, оно будет переустановлено.

ISSN 3030-3907

10	$p_{10}(s_{10} \rightarrow a_6 \wedge \neg f_9) = a_5$	Если с операционной системой проблем не возникнет, сотруднику будет предоставлено соответствующее указание.
11	$p_{11}(s_{11} \rightarrow a_4 \wedge \neg f_5) = a_{11}$	Если блочное тестирование невозможно, система будет отправлена на ремонт.
12	$p_{12}(s_{12} \rightarrow a_4 \wedge f_5) = a_{10}$	Если это блочный тест, то тестируется оперативная память.
13	$p_{13}(s_{13} \rightarrow a_{10} \wedge f_6) = a_{11}$	Если возникнут проблемы с оперативной памятью, система будет отправлена на ремонт.
14	$p_{14}(s_{14} \rightarrow a_{10} \wedge \neg f_6) = a_{12}$	Если проблем с оперативной памятью нет, будет проверена материнская плата.
15	$p_{15}(s_{15} \rightarrow a_8 \wedge f_4) = a_{13}$	Сетевые интерфейсы тестируются.
16	$p_{16}(s_{16} \rightarrow a_{12} \wedge \neg f_7) = a_{14}$	Если материнская плата исправна, будут проверены устройства ввода/вывода.
17	$p_{17}(s_{17} \rightarrow a_{14} \wedge f_8) = a_{15}$	Если возникнут проблемы с устройствами, они будут заменены.
18	$p_{18}(s_{18} \rightarrow a_{14} \wedge \neg f_8) = a_{11}$	Если устройства исправны, система будет отправлена на ремонт.
19	$p_{19}(s_{19} \rightarrow \mathrm{a}_4 \wedge f_3) = a_{16}$	Производится регулировка и замена необходимого устройства.
20	$p_{20}(s_{20} \rightarrow \mathrm{a}_{13} \wedge f_{12}) = a_{16}$	Если сетевой адаптер не работает, он будет заменен и будет настроен интернет.
21	$p_{21}(s_{21} \rightarrow \mathrm{a}_{16} \wedge f_8) = a_{11}$	Если возникнут проблемы с устройствами, они будут заменены.
22	$p_{22}(s_{22} \rightarrow \mathrm{a}_7 \wedge f_{14}) = a_{17}$	Если DNS не работает, настройки DNS будут изменены.
23	$p_{23}(s_{23} \rightarrow a_{16} \wedge f_{14}) = a_7$	Если ответа DNS нет, DNS будет исправлен с помощью конфигурации.
24	$p_{24}(s_{24} \rightarrow a_{17} \wedge f_{15}) = a_{18}$	Состояние системы отслеживается.
25	$p_{25}(s_{25} \rightarrow \mathrm{a}_{18} \wedge f_{16}) = a_1$	Если антивирус не активен, рекомендуется провести оптимизацию.

ISSN 3030-3907

26	$p_{26}(s_{26} \to \mathrm{a}_{18} \wedge f_{17}) = a_3$	Состояние сети проверяется.
27	$p_{27}(s_{27} \to \mathrm{a}_{17} \wedge f_{18}) = a_{18}$	При загрузке системы осуществляется управление ресурсами.
28	$p_{28}(s_{28} \to a_{18} \wedge f_1) = a_1$	Ресурсы организуются, и состояние системы снова проверяется.
29	$p_{29}(s_{29} \to a_1 \wedge f_{10}) = a_8$	Если во время проверки системы возникнет сбой в работе приложения, оно будет переустановлено.
30	$p_{30}(s_{30} \to a_{17} \wedge f_{10}) = a_8$	Если проблема сохраняется после переустановки операционной системы, прикладная программа также будет переустановлена.
31	$p_{31}(s_{31} \to a_5 \wedge f_{11}) = a_{16}$	Если указанный пользователь не подключен к Интернету, требуется настройка.
32	$p_{32}(s_{32} \to a_6 \wedge f_{16}) = a_{18}$	Если антивирус не работает в операционной системе, ее необходимо оптимизировать.
33	$p_{33}(s_{33} \to a_6 \wedge f_{15}) = a_7$	Если обновление недоступно, рекомендуется провести оптимизацию.
34	$p_{34}(s_{34} \to a_3 \wedge f_{13}) = a_{18}$	Проверяется состояние сети и освобождается буфер.
35	$p_{35}(s_{35} \to a_3 \wedge f_{18}) = a_3$	При высокой нагрузке на приложение ресурсы управляются.
36	$p_{36}(s_{36} \to a_{18} \wedge \neg f_{18}) = a_1$	Если проблема с ресурсами будет устранена, система будет проверена еще раз.
37	$p_{37}(s_{37} \to a_{18} \wedge f_9) = a_9$	Проблема состояния сети будет повторно оценена, и при необходимости система будет перезагружена.
38	$p_{38}(s_{38} \to a_9 \wedge \neg f_9) = a_5$	Если после переустановки операционной системы проблем не возникнет, будут предоставлены инструкции.

ISSN 3030-3907

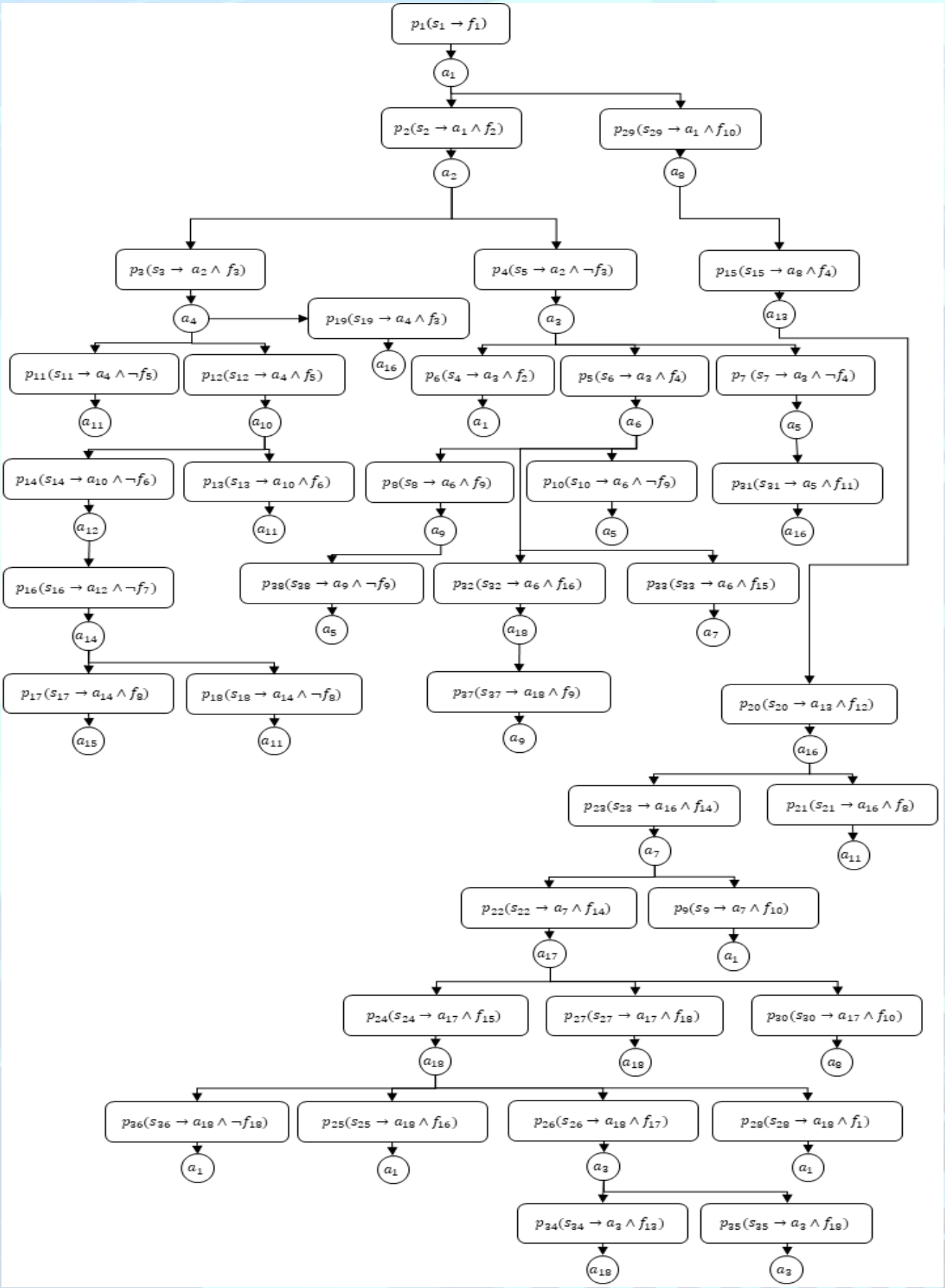


Рисунок 1. График, показывающий взаимосвязь между производствами.

ISSN 3030-3907

ЗАКЛЮЧЕНИЕ: В результате исследования создана продукционная модель представления знаний, представляющая собой экспертную систему, анализирующую проблемы сетевого потока в информационной системе и предлагающую пути их решения. Развитие исследования заключается в программной реализации экспертной системы на основе предложенной модели представления производственных знаний для анализа сбоев в информационных системах.

В рамках данного исследования была разработана концепция экспертной системы, позволяющая автоматизировать процесс выявления проблем и эффективно решать их на основе мониторинга и анализа сетевого трафика. Основная цель системы упростить процесс принятия решений администратором сети, повысить точность и скорость обнаружения ошибок, а также обеспечить бесперебойное взаимодействие пользователя и администратора.

Разработанная в ходе исследования экспертная система была основана на модели производственных знаний. Система сформировала 38 четких и логически связанных продукционных правил. Каждое правило отображает определенную ситуацию в состоянии сети и содержит соответствующее решение или рекомендацию.

В дальнейшем имеются перспективы обогащения таких экспертных систем методами искусственного интеллекта и машинного обучения, внедрения механизмов автоматического обновления и адаптации правил, и продолжение исследований в этой области является одной из важных задач.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Liu, G., Fu, C., Yang, X., Yang, L., Feng, Y., & Yang, Q. (2025). Study of the antivirus patch testing problem through optimal control modeling. PLoS One, 20(5) doi:https://doi.org/10.1371/journal.pone.0319916

2. Rosario, C. R., Liane, M. K., & Frozza, R. (2014). Tecnicas de elicitac?o de conhecimento tacito coletivo: Um estudo de caso aplicado a uma empresa do ramo metalurgico. Informação & Sociedade, 24(1) Retrieved from https://www.proquest.com/scholarly-journals/tecnicas-de-elicitac-o-conhecimento-tacito/docview/1542581445/se-2

3. Chen, J., & Fahlman, S. E. (2023). Score: A rule engine for the scone knowledge base system. Ithaca: Retrieved from https://www.proquest.com/working-papers/score-rule-engine-scone-knowledge-base-system/docview/2811358468/se-2

4. Dou, W., Tong, Y., Song, Z., Zhang, M., Lu, S., & Zhu, H. (2024). Real-time voltage control of centralized and distributed coordination in active distribution

ISSN 3030-3907

network under multiple coupling. Journal of Physics: Conference Series, 2855(1), 012008. doi:https://doi.org/10.1088/1742-6596/2855/1/012008
5. Batista, E., Alencar, B., Silva, E., Canário, J., Rios, R. A., Dustdar, S., . . . Prazeres, C. (2024). A new intelligent scheduler to improve reactive OpenFlow communication in SDN-based IoT data streams. Discover Internet of Things, 4(1), 15. doi:https://doi.org/10.1007/s43926-024-00068-3
6. Dyachenko R.A., Belchenko I.V., Terekhov V.V. Illyustratsiya primeneniya metoda delfi dlya resheniya zadachi vybora napravleniya razvitiya predpriyatiya // Avtomatizirovannye informatsionnye i elektroenergeticheskie sistemy. 2012. S. 243-244.
7. Sharovatov A.S., Loba I.S., Reshetnyak M.G. Razrabotka algoritma poiska optimalnoy modeli // Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agarnogo universiteta. 2012. № 77. S. 413-422.
8. Kabulov A. . & Juraev M. . (2025). A NEW APPROACH TO INTELLIGENT NETWORK TRAFFIC FLOW ANALYSIS. Development Of Science, 6(2), pp. 363-372. https://doi.org/0
9. Jo‘Rayev Ma’Ruf To‘Raqul O‘G‘Li (2024). TARMOQ OQIMINI MONITORING QILISH DASTURIY TIZIMI. Al-Farg’oniy avlodlari, (3), 73-77. doi: 10.5281/zenodo.13954907
10. Jo‘rayev, M. R. (2024). TARMOQ TRAFIGINI MONITORING QILISH VA TARMOQ PAKETLARI TAHLILI. International Journal of scientific and Applied Research, 1(3), 190-192.

ISSN 3030-3907