ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ «МИСИС»

На правах рукописи

ЖАРОВА Ольга Юрьевна

Моделирование параметров воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия

Специальность 2.3.1 – Системный анализ,
управление и обработка информации, статистика

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель
проф., д.т.н. Гончаренко С.Н.

Москва 2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность. Исследования различных инцидентов кибердавления на промышленных предприятиях показали стабильную динамику роста их количества, а также неэффективность действий персонала в случае возникновения кибератак на технические системы. То есть технические системы промышленного предприятия являются привлекательными мишенями для реализации атак с применением различного вредоносного программного обеспечения.

В силу недостаточного бюджетирования, сложностей в модернизации и обновлении аппаратно-программных средств промышленного предприятия быстро исправить ситуацию бывает весьма затруднительно. К тому же имеют место большая инертность и запоздалые реакции на случившиеся инциденты, и даже правильные управленческие решения зачастую не действуют из-за бюрократических проволочек.

В настоящее время выявлены доминирующие факторы, влияющие на надежность и эффективность технических систем промышленного предприятия, обнаружены сотни новых уязвимостей, исследованы новые векторы атак на объекты управления, проведен анализ случайных заражений промышленных систем, обнаружены целевые атаки на промышленные предприятия, а также установлены показатели инцидентов безопасности в области технологических сетей предприятий. Эти вопросы отражены в работах отечественных и зарубежных исследователей: Грачков И.А., Мосолов А.С., Краснов А.Е., Урбан Н.А., Колосова С.П., Корнеева Н.В., Комарова А.А., Gülay Öke, Dr. Georgios Loukas, Ковалева Д.А., Тернового О.С.

Технологические сети как элемент сложных технических систем, содержащих большое число разнородных объектов управления, включают в себя технические средства, обеспечивающие функционирование технологических процессов на предприятии, состоящих из совокупности технических и программных средств, реализующих оперативную и надёжную систему связи с

целью передачи служебной информации и контролирования технологических процессов и операций.

В настоящее время промышленные технологические сети во многих странах мира подвергаются разнообразным атакам с использованием инструментария, ранее применяемого исключительно в корпоративных сетях, а наибольший удельный вес по величине причиняемого ущерба имеют атаки на отказ в обслуживании, представляющие собой воздействие деструктивных потоков данных на объект управления. Данный вид воздействия организуется на управляющие узлы различных уровней технологических сетей, к которым можно отнести: серверы, автоматизированные рабочие места, управляющие контроллеры, концентраторы.

Воздействие деструктивных потоков данных, направленное на технологические сети, не являются инцидентом информационной безопасности, так как не нарушают целостность, конфиденциальность и доступность информационных ресурсов промышленного предприятия. Данный вид воздействия представляет угрозу технологическим процессам и, как следствие, отрицательно влияет на эффективность и надежность функционирования технологических сетей промышленного предприятия.

Таким образом, разработка методов повышения надежности функционирования управляющих узлов технологических сетей промышленного предприятия в условиях угрозы воздействий деструктивных потоков данных является актуальной научно-практической задачей.

Цель работы – повышение эффективности и надежности функционирования управляющих узлов различных уровней технологических сетей промышленного предприятия в условиях угрозы воздействия деструктивных потоков данных.

Идея работы заключается в определении вида и характера воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия, прогнозировании на основе результатов имитационного

моделирования исходов воздействий и в разработке эффективных мер по предотвращению последствий воздействия деструктивных потоков данных.

Задачи:

- формирование исходного множества критериев оценки деструктивных потоков данных;
- определение вида воздействия на основе анализа взаимосвязей и закономерностей изменения статистических параметров потоков данных;
- разработка иерархической модели воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия;
- разработка алгоритма прогнозирования последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия;
- разработка универсальной методики определения ущерба и предотвращения последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия.

Новизна научных исследований заключается:

1) в разработке способа идентификации вида воздействия деструктивных потоков данных на основе решения задачи распознавания образа воздействия, сформированного на базе определения взаимосвязей статистических параметров потоков данных;

2) в разработке многоуровневой иерархической модели воздействия деструктивных потоков данных, отличающейся учетом системных связей и закономерностей функционирования управляющих узлов технологической сети промышленного предприятия, позволяющей прогнозировать исход воздействий на узлы и повысить эффективность управления в промышленных технических системах в условиях угрозы воздействия деструктивных потоков данных, а также демонстрирующей развитие воздействия – от вида источника и характера

генерируемого деструктивного потока данных до прогнозируемого состояния подвергшегося воздействию управляющего узла;

3) в разработке алгоритма прогнозирования последствий воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия, позволяющего оценить последствия воздействий, имеющих в своей основе различные механизмы;

4) в разработке методики определения ущерба и предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия, адаптированной для управляющих узлов технологических сетей, отличающейся наличием возможности разработки и оценки эффективности комплекса антирисковых мер.

Методы исследования включают системный, факторный и статистический анализ данных, полученных на основе имитационного моделирования, теорию принятия решений, математическое моделирование параметров потока данных, теорию вероятностей, теоретико-информационный анализ функционирования управляющих узлов технологической сети промышленного предприятия.

Научные положения:

1) Повышение результативности реагирования и повышение надежности функционирования управляющих узлов технологической сети промышленного предприятия в условиях воздействия деструктивных потоков данных возможно осуществить на основе выявленных корреляционных взаимосвязей показателей вариации, определяющих начало воздействия деструктивных потоков данных на управляющий узел, и закономерностей изменения значений статистических и динамических параметров потоков данных.

2) Прогнозирование последствий воздействия деструктивных потоков данных на управляющие узлы технологических сетей промышленного предприятия необходимо осуществлять на основе разработанной многоуровневой иерархической модели, включающей: уровень источника и вид воздействия; взаимосвязи совокупности динамических параметров и статистических

параметров воздействия; характеристики видов пакетов деструктивных потоков данных и уровень прогнозируемого состояния узла.

3) Минимизацию ущерба от воздействия деструктивных потоков данных необходимо осуществлять на основе разработанной универсальной методики предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы технологических сетей промышленного предприятия, включающей в себя процедуру классификации видов воздействия, прогнозирование величины потенциального ущерба и разработку комплекса организационно-технических антирисковых мер.

Обоснованность и достоверность результатов исследования обеспечиваются: репрезентативностью исходных статистических выборок данных; корректным использованием в обработке информации методов математической статистики и теории принятия решений; использованием современного программного обеспечения, оборудования и апробированных методик.

Объектом исследования являются управляющие узлы технологической сети промышленного предприятия, функционирующие в условиях воздействия деструктивных потоков данных.

Предметом исследования являются системные взаимосвязи и закономерности изменения показателей вариации потоков данных в технологических сетях промышленного предприятия.

Практическая значимость:

1) Разработанный алгоритм прогнозирования исхода воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия позволяет оценить базовые факторы воздействия и уровень риска его реализации.

2) Разработанная универсальная методика предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы в сложных технических системах промышленного предприятия позволяет модернизировать программное обеспечение автоматизированных рабочих мест операторов,

программируемых контроллеров и прочих управляющих узлов технологической сети, повысив их эффективность и надежность функционирования в условиях воздействия деструктивных потоков данных.

Реализация выводов и рекомендаций работы

Основные положения диссертации приняты к использованию ООО «Рекрипт» при построении узлов технологической сети и в ООО «НИЛАКТ ДОСААФ» проектировании, производстве и эксплуатации контрольно-проверочной аппаратуры и аппаратуры наземных станций управления космическими аппаратами, что подтверждается соответствующими актами внедрения.

Публикации.

Материалы диссертации изложены в 8 научных работах и опубликованы в изданиях, в том числе в 4 рекомендованных ВАК РФ.

Объем и структура диссертации. Диссертация состоит из введения, 4 глав, заключения, библиографического списка из 147 наименований и представлена на 136 страницах, включая 68 рисунков, 9 таблиц.

1. ПРОБЛЕМА УГРОЗ ВОЗДЕЙСТВИЯ ДЕСТРУКТИВНЫХ ПОТОКОВ ДАННЫХ НА УПРАВЛЯЮЩИЕ УЗЛЫ ТЕХНОЛОГИЧЕСКИХ СЕТЕЙ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

1.1 Анализ проблемы кибердавления на промышленных объектах

Последние 10 лет промышленные предприятия испытывают постоянно возрастающее давление кибератак. До определенного момента киберугрозы были актуальны исключительно для корпоративных сетей. Но, после инцидента с червем Stuxnet в 2010 году, атакующим SCADA (система диспетчерского контроля и сбора данных), стало ясно, что промышленные предприятия подвержены киберугрозам, при этом риски весьма велики. Атаки на промышленные технологические сети трудоёмки и производятся зачастую в несколько этапов. Так, например, предполагаемая первоначальная цель Stuxnet – заводы по производству обогащенного урана – шестая по счету жертва, тогда как первые пять компаний, подвергшихся атаке, работали в сфере разработки промышленных систем или поставки соответствующих комплектующих в Иране. Пятая по счету жертва помимо продуктов для индустриальной автоматизации также производит центрифуги для обогащения урана. По данным специалистов «Лаборатории Касперского», злоумышленники рассчитывали, что компании будут обмениваться данными со своими клиентами – в том числе, заводами по производству обогащенного урана – тем самым прокладывая путь вредоносным программам к их конечной цели. В тот год было выведено из строя порядка 1000 из 5000 работающих центрифуг IR-1 по обогащению урана, что стало следствием атаки червя Stuxnet [2, 30, 140, 141].

В последние годы создаются все более благоприятные условия для реализации кибератак на промышленные технологические сети, так как идет

активная автоматизация различных технологических процессов промышленных предприятий.

В 2017 году количество инцидентов, связанных с информационной безопасностью промышленных систем стало неуклонно расти, принимать глобальные масштабы. Только за первую половину 2017 года промышленные информационные системы в 63-х странах мира подверглись множественным атакам с использованием программ-шифровальщиков. Данная цифра значительно увеличивается если учесть другие виды воздействия вредоносным программным обеспечением, и тот факт, что не все атаки были внесены в статистику [2, 141].

Факторы, влияющие на киберугрозы в технологических сетях:

1. Растущая поверхность атаки – число автоматизированных систем растет, средства автоматизации становятся все разнообразнее, все больше организаций и отдельных сотрудников имеют прямой или удаленный доступ к АСУ ТП (автоматизированная система управления технологическим процессом), появляются коммуникационные каналы для мониторинга и удаленного контроля ранее независимых объектов — все это дает киберпреступникам больше возможностей для планирования и осуществления атаки [1].

2. Растущий интерес киберпреступников – сокращение прибыльности и увеличение риска атак, направленных на традиционные жертвы, заставляет киберпреступников искать новые цели, в том числе среди промышленных организаций.

Принимая во внимание сложившийся геополитический контекст, тенденции в разработке АСУ ТП, а также повсеместный переход на новые процессы управления, модели производства и экономической деятельности в ближайшие годы кибердавление на промышленные компании будет только нарастать.

3. Недооценка общего уровня угроз – сведения о проблемах информационной безопасности в промышленных компаниях крайне скудны, так как, зачастую, обнародование каких-либо фактов, с ней связанных, несет в себе репутационные риски. И это негативно влияет на то, как владельцы и

управляющие промышленных компаний, а также их персонал, оценивают степень опасности.

1.2 Особенности системных связей и функционирования управляющих узлов технологической сети промышленного предприятия

Специфика и архитектура промышленных и технологических сетей такова, что сложные системы защиты в них неприменимы. Более того, в силу стоимости оборудования и программного обеспечения для построения технологических сетей, затраты на реализацию защитных модулей промышленными предприятиями зачастую даже не рассматриваются.

АСУ ТП – собирательный термин, имеющий отношение ко всему многообразию управляющих компьютерных устройств и их объединений, которые имеют целью обеспечить управление разнообразными процессами, при этом технологическая сеть рассматривается, как среда передачи данных для АСУ ТП (рисунок 1, А.2).

Система может иметь два или три уровня, на которых производится управление технологическими процессами. Специфика каждой конкретной системы управления определяется используемой на каждом уровне программно-аппаратной платформой [6].

Структура АСУ содержит следующие подсистемы:

1.полевое оборудование, включающее в себя интеллектуальные средства измерения, контроля, регулирующие отсечные и запорные клапаны, электроприводы;

2. кабельные линии связи, кроссовое оборудование;

3. барьеры искробезопасности, нормирующие преобразователи;

4. программируемые контроллеры, модули ввода-вывода аналоговых и дискретных сигналов;

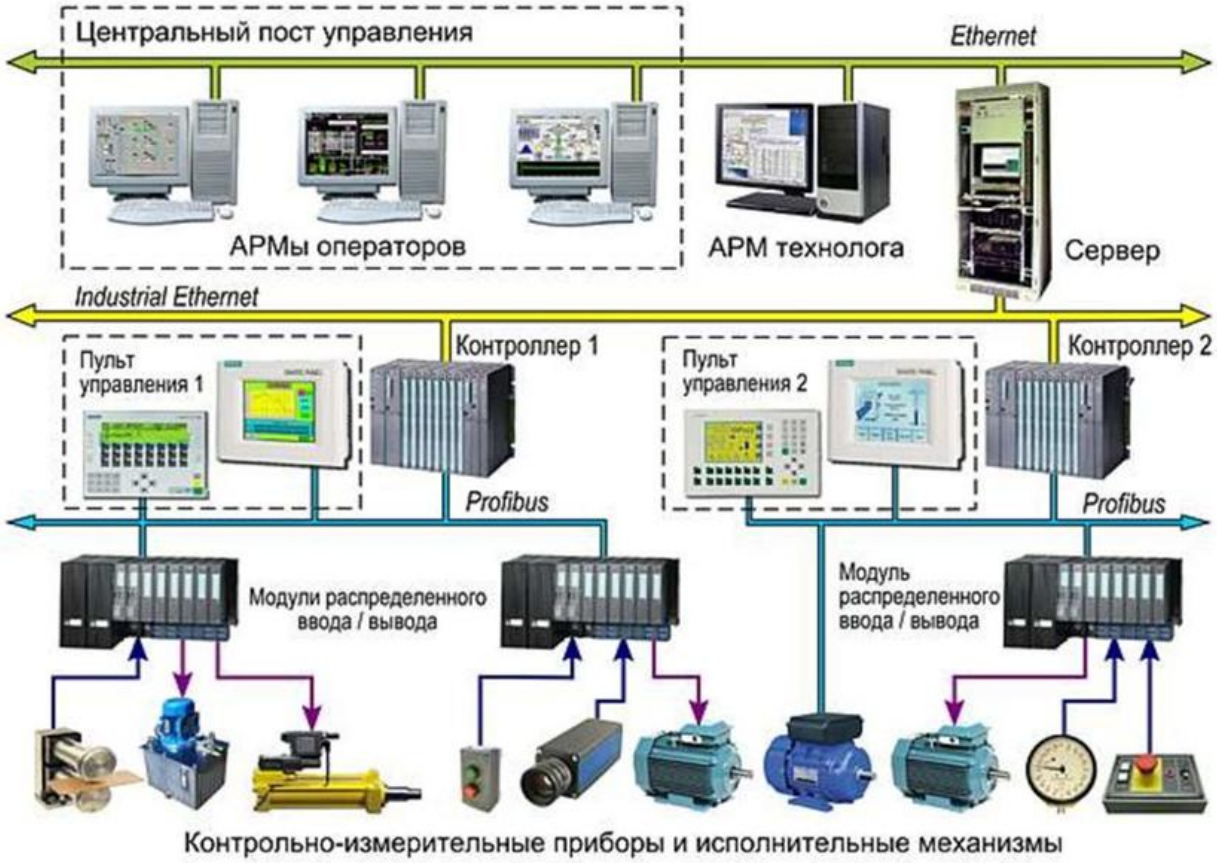


Рисунок 1 - Обобщенная архитектура АСУ ТП

5. операторские станции – компьютеры, устройства на магнитных носителях, мониторы, печатающие устройства и так далее;

6. кабельные, оптоволоконные и радиоканалы связи;

7. система пожарной автоматики и контроля загазованности;

8. система бесперебойного электропитания.

Нижний уровень(полевой) – уровень объекта (контроллерный) – включает различные датчики (измерительные преобразователи) для сбора информации о ходе технологического процесса, электроприводы и исполнительные устройства для реализации регулирующих и управляющих воздействий. Датчики поставляют информацию локальным контроллерам (PLC), которые могут обеспечить реализацию следующих функций:

- сбор, первичная обработка и хранение информации о состоянии;
- оборудования и параметрах технологического процесса;
- автоматическое логическое управление и регулирование;

- исполнение команд с пункта управления;
- самодиагностика работы программного обеспечения и состояния самого контроллера;
- обмен информацией с пунктами управления.

В качестве локальных PLC в системах контроля и управления различными технологическими процессами в настоящее время применяются контроллеры как отечественных, так и зарубежных производителей. На рынке представлены сотни типов контроллеров, способных обрабатывать от нескольких десятков до нескольких тысяч и даже десятков тысяч переменных.

Разработка, отладка и исполнение программ контроллерами осуществляется с помощью специализированного программного обеспечения, широко представленного на рынке. Это, прежде всего, многочисленные пакеты программ для программирования контроллеров, предлагаемые производителями аппаратных средств.

Информация с локальных контроллеров может направляться в сеть диспетчерского пункта непосредственно, а также через контроллеры верхнего уровня. В зависимости от поставленной задачи контроллеры верхнего уровня (концентраторы, коммуникационные контроллеры) реализуют различные функции. Некоторые из них перечислены ниже:

- сбор данных с локальных контроллеров;
- обработка данных, включая масштабирование;
- поддержание единого времени в системе;
- синхронизация работы подсистем;
- организация архивов по выбранным параметрам;
- обмен информацией между локальными контроллерами и верхним уровнем;
- работа в автономном режиме при нарушениях связи с верхним уровнем;
- резервирование каналов передачи данных и др.

Так как информация в локальных контроллерах предварительно обрабатывается и частично используется на месте, существенно снижаются требования к пропускной способности каналов связи. Данный факт создает уязвимость технологической сети перед деструктивными потоками данных, вызывающими отказ в обслуживании [7, 29, 83].

1.3 Проблема воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия

Исходя из всего вышесказанного можно сделать вывод о том, что АСУ ТП включает в себя различные компоненты, в том числе компьютеры — служащие источником вредоносного ПО. Современное вредоносное программное обеспечение является комплексом программ, библиотек и различного инструментария, способного проводить мониторинг всей системы в целом, поражать все программируемые устройства технологической сети различными видами вредоносных программ, содержащихся в комплексе или дополнительно скачиваемые из сети Интернет с сервера злоумышленников.

Заражение технологической сети возможно при подключении хотя бы одного компьютера, участвующего в управлении технологическими процессами к сети Интернет, или при подключении этого компьютера к локальной сети предприятия, к которой, в том числе, подключены компьютеры, подключённые к сети Интернет. Также заражение может быть совершено инсайдером с применением специализированного оборудования, подключаемого непосредственно к управляющим узлам технологической сети. Помимо этого, новые аппаратные средства могут содержать программные и аппаратные закладки, установленные на заводе производителе или при транспортировке [147].

К наиболее простым в реализации относятся атаки на отказ в обслуживании, при которых один или несколько зараженных узлов начинают генерировать

деструктивные потоки данных, воздействуя на устройства, управляемые ими, или соединенным с ними сетью, а так как в обычном режиме к каналам связи не предъявляются требования на высокую пропускную способность, они достаточно быстро заполняются деструктивными потоками данных, и не могут проводить требуемую информацию и как следствие – происходит отказ в обслуживании. Результатом воздействия деструктивных потоков данных может быть, как остановка технологического процесса с необходимостью перезагрузки аппаратных средств, так и полный вывод из строя оборудования. Данный вид воздействий организуется с использованием зараженных управляющих узлов различных уровней технологических сетей, к которым можно отнести: серверы; автоматизированные рабочие места; управляющие контроллеры; концентраторы (рисунок 2). При этом управляющие узлы верхних уровней под действием вредоносного программного обеспечения направляют деструктивные потоки данных на соседние узлы или на узлы нижних уровней (рисунок 3). Источником деструктивных потоков данных также могут быть неисправные узлы, вследствие своей некорректной работы воздействующие на соседние узлы [2, 6, 8].

Рисунок 2 – Узлы технологической сети, реализующие воздействие деструктивных потоков данных

Рисунок 3 - Узлы технологической сети наиболее уязвимые для воздействия деструктивных потоков данных

Ущерб от успешной реализации подобного воздействия может исчисляться миллионами рублей, так как управляемое оборудование может быть высокотехнологичным и дорогим. Такого рода воздействия могут быть таргетированы и выполняться с участием инсайдеров, причем как осознанных, так и халатных сотрудников. Отнести этот вид воздействия к инцидентам информационной безопасности нельзя, так как страдают не информационные ресурсы промышленного предприятия, а оборудование, участвующее в технологических процессах.

Таким образом, проблема воздействия деструктивных потоков данных в обслуживании актуальна для любой распределенной информационно системы.

Изначально методика, заложенная в основу организации воздействия, приводящего к отказу в обслуживании оборудования, зародилась при проведении экспериментов по проверке систем на устойчивость нагрузкам. Активное развитие началось в конце 90-х годов прошлого столетия, в частности в 1999 году были выведены из строя web-сервера таких корпораций как Amazon, Yahoo, CNN, eBay. В 2002 году масштабное воздействие затронуло 8 из 13 корневых серверов DNS, системы, без которой невозможно существование ни одного web-сервиса. В

октябре 2006 атаке подвергся Национальный банк Австралии, в 2007 году по причине атак на отказ в обслуживании была парализована работа правительственных сайтов Эстонии. По данным Координационного центра FIRST, который объединяет центры CERT по всему миру (Computer Emergency Response Team), количество атак на отказ в обслуживании в локальных и глобальных сетях резко возросло в последние 7 лет [144].

1.3.1 Анализ статистических данных по деструктивным воздействиям, приводящим к отказу в обслуживании в корпоративных сетях промышленных предприятий

Ниже приведена статистика на первый квартал 2019 года по данным отчета DDoS Intelligence (Система DDoS Intelligence является частью решения Kaspersky DDoS Protection и осуществляет перехват и анализ команд, поступающих с серверов управления и контроля, и не требует при этом ни заражения каких-либо пользовательских устройств, ни реального исполнения команд злоумышленников) [49]:

- С точки зрения географического распределения атак лидером остается Китай (рисунок 4), сдавший было позиции в конце 2018 года, он вновь укрепил их в первом квартале 2019-го, при этом его доля от общего числа атак выросла до 67,89%. На втором месте традиционно США (17,17%), на третьем — Гонконг (4,81%), поднявшийся с седьмого места [49].
- Географическое распределение мишеней примерно повторяет географическое распределение атак, так, например, в первой тройке так же Китай (59,85%), США (21,28%) и Гонконг (4,21%) [49].
- В обеих «географических» десятках количество перестановок относительно невелико по сравнению с прошлыми кварталами. Внезапного роста активности ботнетов на неожиданных территориях больше не наблюдалось [49].
- Максимальное количество DDoS-атак отмечено во второй половине

марта. Самым тихим периодом ожидаемо оказался январь [49].

- В течение недели наиболее опасным с точки зрения DDoS-атак днем стала суббота, воскресенье же по-прежнему остается самым спокойным [49].
- Максимальная длительность атаки по сравнению с прошлым кварталом сократилась больше чем на сутки, однако процентная доля долгих DDoS-сессий продолжает расти и составила 21,34% (по сравнению с 16,66% в четвертом квартале 2018 г.) [49].
- Доля SYN-флуда повысилась, достигнув 84%. В связи с этим снизились доли UDP- и TCP-флуда, доли же HTTP и ICMP-атак на этом фоне возросли до 3,3% и 0,6% соответственно [49].
- Доля Linux-ботнетов несколько уменьшилась, однако по-прежнему остается довлеющей (95,71%) [49].
- Больше всего командных серверов ботнетов по-прежнему находится в США (34,10%), на втором месте теперь Нидерланды (12,72%), а на третьем Россия (10,40%). В десятку вернулся прежний бессменный лидер, Южная Корея — правда, всего лишь на последнее место (ее доля составила 2,31%) [49].

Статистика DDoS Intelligence (рисунок 4) ограничена только теми ботнетами, которые были обнаружены и проанализированы “Лабораторией Касперского”. Следует также иметь в виду, что ботнеты – лишь один из инструментов осуществления DDoS-атак, и представленные в настоящем отчете данные не охватывают все без исключения атаки, произошедшие за указанный период [49].

Из приведенной статистики можно сделать вывод, что корпоративные сети промышленных предприятий давно страдают от атак на отказ в обслуживании. Эта технология за последние 20 лет стала кибероружием для осуществления различного рода давления от экономического до политического (в случае таргетированных атак на государственные информационные ресурсы) [49, 121].

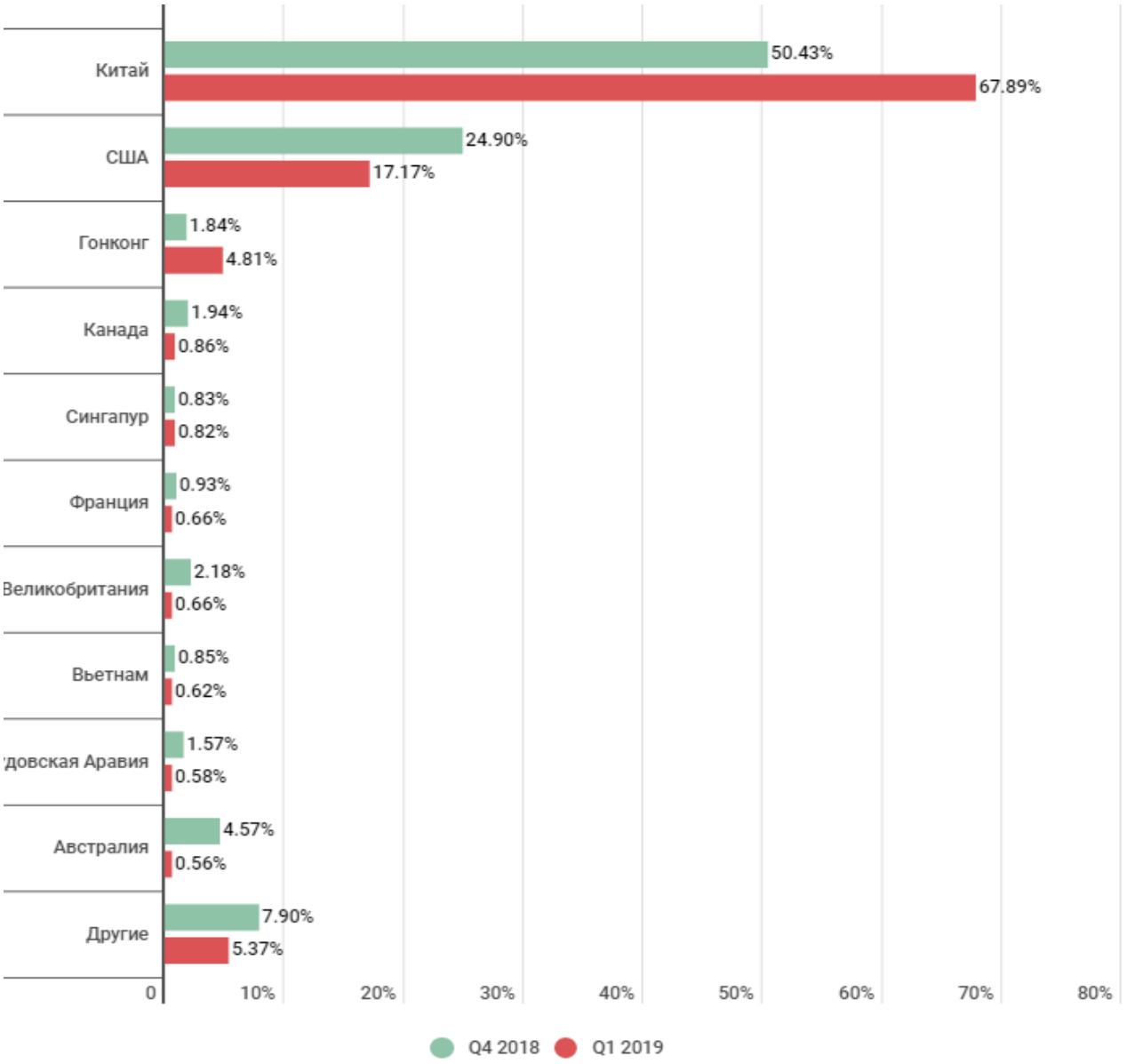


Рисунок 4 - Распределение атак на 4 квартал (Q4) 2018г. – 1 квартал (Q1) 2019 г.

В настоящее время существует инструментарий, позволяющий применить это кибероружие к технологическим сетям промышленных предприятий, это используемое для атак на энергосистемы вредоносное ПО CrashOverride/Industroyer. Современные тенденции таковы, что разработка нового подобного вредоносного ПО – вопрос времени.

Принимая во внимание все изложенные факты, можно сделать вывод о том, что воздействие деструктивных потоков данных, успешно реализуемое на промышленной технологической сети, это не столько проблема информационной безопасности, так как информационные ресурсы предприятия не затрагиваются, а воздействие способное снизить эффективность и надежность управляющих узлов

технологической сети промышленного предприятия, а также спровоцировать угрозу жизни, если речь идет о технологических процессах связанных с обеспечением безопасности персонала.

1.3.2 Воздействие деструктивных потоков данных, как угроза надежности управляющих узлов технологической сети промышленного предприятия

Из основ теории надежности известно, что, надежность, как сложное свойство в зависимости от назначения объекта и условий его применения состоит из сочетаний свойств: безотказности; ремонтопригодности; долговечности и сохраняемости. Для объектов, работающих непрерывно, из этих свойств наиболее важны три первые. Объекты, работающие сезонно, напротив, должны кроме приемлемой безотказности иметь высшие показатели ремонтопригодности, долговечности и сохраняемости [65].

Управляющие узлы в технологических сетях промышленных предприятий относятся к непрерывно работающим объектам, следовательно, имеет смысл рассмотреть, как воздействие деструктивных потоков данных влияет на безотказность, ремонтопригодность, долговечность.

Безотказность, как свойство объектов, позволяющее сохранять работоспособное состояние в течение некоторого времени, рассматривается применительно к режиму эксплуатации объекта. При оценке безотказности объекта перерывы в его работе (плановые и внеплановые) не учитываются. Безотказность характеризуется техническим состоянием объекта: исправностью; неисправностью; работоспособностью; неработоспособностью; дефектом; повреждением и отказом. Каждое из этих состояний характеризуется совокупностью значений параметров, описывающих состояние объекта и качественных признаков. Номенклатура этих параметров и признаков, а также

пределы допустимых изменений устанавливаются нормативной документацией на объект.

Влияние деструктивных потоков данных на объект в технологической сети опасно, прежде всего, из-за многократно возросшей нагрузкой на управляющий узел. На данный момент известно множество случаев, когда воздействие деструктивных потоков данных провоцировало не только остановку корректной работы оборудования или отказ в обслуживании, но и приводила к пожарам, связанным с перегревом и последующим воспламенением узлов, испытавших воздействие высокой интенсивности. Подобную ситуацию можно спровоцировать в технологической сети путем многократного превышения вычислительной мощности управляющего узла, и, как следствие, перевести его в состояния: сбоя, если управляющий узел восстановил работу после самостоятельной/ручной перезагрузки; повреждения, если нанесены незначительные повреждения программному или аппаратному обеспечению; отказа и неработоспособности, с необходимостью последующей замены управляющего узла.

Ремонтопригодность, как свойство объекта, заключающееся в приспособленности к предупреждению и обнаружению причин отказов, повреждений и восстановлению работоспособного состояния путем проведения технического обслуживания и ремонтов, полностью определяется его конструкцией, т. е. предусматривается и обеспечивается при разработке, изготовлении и монтаже объектов, с учетом будущего целесообразного уровня их восстановления, который определяется соотношением ремонтопригодности и внешних условий для выполнения ремонта, в том числе устанавливаемых для этого пределов соответствующих затрат. Отсюда происходит относительность деления объектов на восстанавливаемые и невосстанавливаемые применительно к определенным внешним условиям (точнее, на подлежащие и не подлежащие восстановлению). Один и тот же элемент в зависимости от окружающих условий и этапов эксплуатации может считаться восстанавливаемым или невосстанавливаемым.

Интенсификация деструктивных потоков данных таким образом изменяет

окружающие условия объекта, что даже новый элемент может стать невосстанавливаемым. Так как данный элемент изначально не был рассчитан на подобные нагрузки, они не учитывались при разработке [126].

Долговечность – свойство объектов сохранять работоспособное состояние до наступления предельного состояния при установленной системе технического обслуживания и ремонта. Предельное состояние объекта характеризуется таким состоянием, при котором дальнейшее его применение по назначению недопустимо или нецелесообразно, либо восстановление исправного или работоспособного состояний невозможно или нецелесообразно. Критерием предельного состояния служит признак или совокупность признаков предельного состояния объекта, установленных в нормативно-технической и конструкторской документации. Объект может перейти в предельное состояние, оставаясь работоспособным, если его дальнейшее применение по назначению станет недопустимым по требованиям безопасности, экономичности или эффективности.

Воздействие деструктивных потоков данных может считаться успешным не только в том случае, если объект переведен в состояние неработоспособности, но и при сокращении скорости обработки запросов до некоторого значения, при котором выполнение техпроцесса прекращается. В этом случае воздействие значительно изнашивает ресурс объекта, и влияет на его долговечность, сокращая срок службы. Регламент технического обслуживания объекта, подвергшегося подобному воздействию, необходимо изменить, и внести дополнительную, внеочередную проверку его состояния [7, 81].

1.4 Анализ методов, продуктов и механизмов противодействия деструктивным потокам данных, используемых в корпоративных сетях

Воздействие, направленное на отказ в обслуживании, имеет высокую степень опасности для корпоративных сетей, так как существующие ботнеты

(распределенные источники деструктивных потоков данных) насчитывают сотни тысяч инфицированных компьютеров, ущерб от успешной реализации такого воздействия, по оценке специалистов, может быть очень велик. Современные ботнеты в состоянии полностью блокировать ресурсы и сайт крупной компании, а ущерб по статистике варьируется от $20 000 до $100 000 за час простоя. Поэтому компаниями тратятся внушительные средства на защиту от данного вида угроз [49, 121].

Все существующие методы противодействия можно разделить на две группы.

К первой группе относятся методы уничтожения ботнетов. Для уничтожения любого ботнета необходимо изучить его механизм управления, архитектуру, маску запросов, принципы взаимодействия узлов и т.д., вывести из строя контролирующие узлы называемые Command & Control, или C&C. Учитывая современные технологии по сокрытию следов, владельца ботнета вычислить не представляется возможным, но есть способы остановить отправку деструктивных потоков данных. Так, в 2010-2011 годах, компания Microsoft боролась с ботнетом Waledac, и победила, применив не только технические, но и правовые меры. Велись судебные разбирательства по вопросу приостановки работы DNS-серверов, являющихся основой управления ботнетом, в котором применялась киберприступная технология Fast Flux DNS. Противостояние шло на территории США и Китая, и влекло большие финансовые затраты, что говорит о том, что данная группа методов доступна только для больших IT-корпораций, обладающих необходимыми ресурсами [49].

Ко второй группе относятся непосредственно методы противодействия. Они могут иметь программную или программно-аппаратную реализацию на стороне узла-цели воздействия, или заключаться в перенаправлении деструктивных потоков данных на ресурсы сторонних организаций, специализирующихся в противодействии подобным угрозам.

В результате работы большинства существующих систем для выявления воздействия деструктивных потоков производится постоянный сбор данных,

характеризующих состояние системы, после чего производится обработка собранных данных и анализ на предмет отличия от эталонных значений. При обнаружении аномалий происходит активация механизмов обнаружения источника деструктивных потоков данных.

Существуют различные методы сравнения деструктивных потоков данных с эталонными данными. К наиболее простым относятся методы, реализованные на основе правил. Суть этих методов заключается в установке определенных правил, характеризующих нормальное и аномальное поведение системы. Правила могут описывать как поведение системы в целом, так и поведение её отдельных частей, например, частоту запросов, определенный набор полей запроса и т.д. [91]

К наиболее популярным методам можно отнести группу методов, основанных на количественном анализе. Методы данной группы пытаются обнаружить воздействие деструктивных потоков данных по возрастающей нагрузке. Среди этой группы методов можно выделит, следующие [91]:

- метод MULTOPS анализирует соотношение принятых и отправленных пакетов в потоке данных [91];
- метод MIB variables учитывает количество пакетов в потоке данных, их тип и количество запросов [91];
- методы ACC учитывают количество пакетов в потоке данных из различных подсетей [91];
- в Network-Aware Clustering происходит группировка входящих запросов по подсетям и их сравнение [91];
- в Hop-Count Filtering ведется учет расстояний в хопах (скачках) до подсетей для фильтрации пакетов с ложным адресом отправителя [91];
- метод Gateway based, разделяет проходящий поток данных на отдельные потоки на основе величины «поражающего воздействия» [91];
- метод D-Ward проверяет легитимность потока данных по следующим протоколам: по протоколу TCP проверяется количество пакетов TCP-ACK; по протоколу ICMP проверяется количество пакетов ICMP; по

протоколу UDP - количество соединений и пакетов в соединении [91].

Вышеприведенные методы в той или иной степени применяются во всех существующих программных и программно-аппаратных продуктах, используемых в настоящее время. Выбор метода зависит от назначения продукта, топологии сети, мощности аппаратных средств. Так в некоторых случаях является неоправданно затратным по вычислительным ресурсам постоянный подсчет количества пакетов, определение их типа и количества запросов, и более оптимальным будет определить количество пакетов из различных подсетей, или соотнести количество принятых и отправленных пакетов, в случаях где они должны быть примерно равны и т.д. Таким образом, различные методы применяются в продуктах отличающихся друг от друга по целевому назначению. Универсального метода или продукта, гарантированно определяющего воздействие деструктивных потоков данных на настоящий момент времени, не существует [112].

Сервис компании Prolexic

Перенаправление DNS и использование Proxy. Данный способ заключается в том, что атакуемому web-серверу присваивается DNS IP-адрес сети компании Prolexic, после чего весь поток данных направляется в эту сеть и там очищается, после чего поставляется защищаемому серверу, который в свою очередь отвечает на запросы в штатном режиме. Этот вариант подходит интернет-банкам, интернет-магазинам или электронным журналам [1].

BGP маршруты и GRE туннели. У компании Prolexic реализована возможность, при использовании протокола маршрутизации BGP, сделать так, что атакуемая сеть для всех пользователей будет находиться в сети Prolexic, куда будет перенаправляться весь поток данных, и где он будет очищаться от вредоносного содержимого, после чего перенаправляться при помощи протокола GRE в атакуемую сеть (рисунок 5) [1].

Прямое подключение к Prolexic. Существует возможность напрямую подключить защищаемую сеть к Prolexic и постоянно находиться под защитой, но это не всегда возможно, например, если компания международная [1].

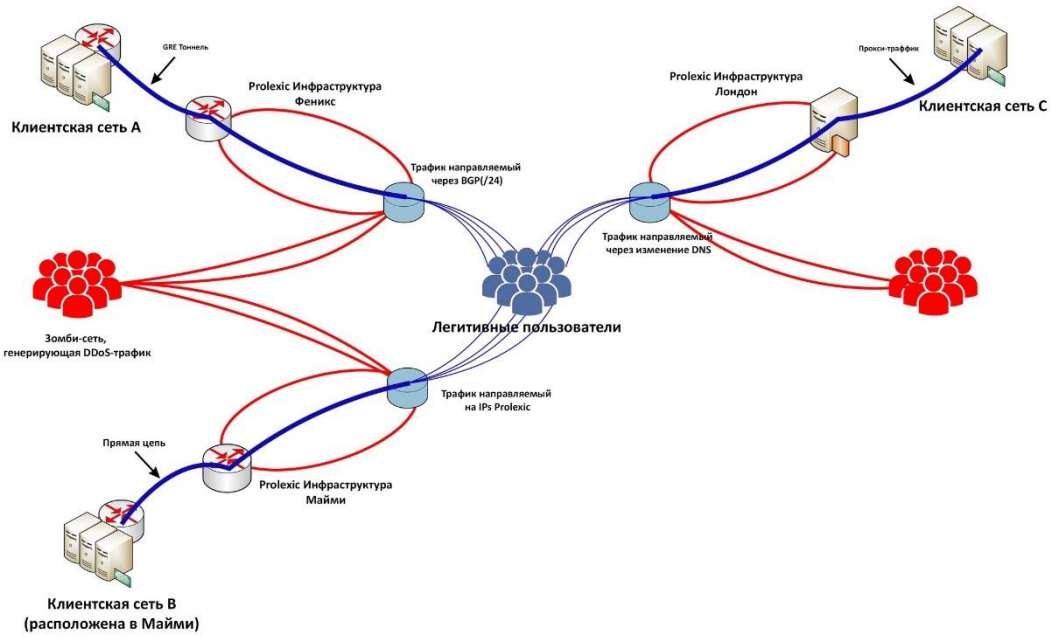


Рисунок 5 - Очистка потока данных от вредоносных пакетов по методу компании Prolexic

Сервис от провайдинговой компании Akamai [71]

Большие компании, такие как IBM, Microsoft, Apple, Sony, AMD, BMW, Toyota, FedEx, NASA, NBA, MTV защищают свои web-сайты от атак на отказ в обслуживании при помощи сервиса от оператора связи Akamai, но это лишь одна из возможностей Akamai. Этот сервис позволяет компаниям иметь зеркало своих сайтов в тысячах различных точек по всему земному шару, гарантируя 100% доступность в любое время. Обычно на зеркалах лежат мультимедийные данные, такие как видео, аудио и графика. Akamai использует математические алгоритмы для решения проблем с перегрузками, возникающими на web-серверах в глобальном масштабе. Эти алгоритмы были разработаны в Массачусетском технологическом институте (MIT) [71].

В 2004 году Akamai был выведен из строя на час в следствии массированной распределенной атаки на отказ в обслуживании. В 2013 году Akamai выкупил компанию Prolexic. Поглощение Prolexic дало Akamai улучшенную облачную безопасность для защиты своих внутренних центров обработки данных и корпоративных IP-приложений от атак на отказ в обслуживании. В настоящее время можно выбрать один из наиболее подходящих

продуктов Akamai для защиты своего ресурса от атак на отказ в обслуживании. Prolexic же является подразделением компании отвечающим за внутреннюю безопасность и предоставляющим сторонник клиентам сервис от лица Akamai [71].

Система защиты Phalanx [1]

Исследователи из Вашингтонского университета для защиты от распределенных атак на отказ в обслуживании предлагают использовать ту же тактику, которую применяют киберпреступники, т.е. ограждать серверы большим количеством компьютеров, принимающих запросы. Эти компьютеры будут играть роль перевалочных пунктов, передающих пакеты данных на сервер только лишь по его требованию. В результате сам сервер не будет испытывать перегрузок и сможет работать в обычном режиме [1].

Система безопасности получила название Phalanx. В качестве компьютеров, формирующих защиту, ученые предлагают использовать узлы сетей доставки, которые могут насчитывать не одну тысячу машин. Исследователи подчеркивают, что теоретически система Phalanx позволяет отразить распределенную атаку на отказ в обслуживании любого масштаба – достаточно лишь увеличить количество компьютеров, принимающих запросы к серверу [1].

Кроме того, комплекс Phalanx может несколько снизить быстродействие вредоносного ботнета, так как каждому компьютеру, который пытается получить доступ к серверу, система предлагает решить несложную вычислительную задачу. Для легитимных пользователей задержка будет незаметна, однако в случае, когда речь идет о генерации большого количества запросов, скорость работы вредоносных машин может значительно снизиться [1].

Практические эксперименты показали, что комплекс Phalanx, состоящий из примерно семи тысяч компьютеров, принимающих запросы, может защитить сервер от ботнета, насчитывающего до миллиона устройств [1].

Программно-аппаратный комплекс FloodGuard [64]

Принцип работы заключается в том, что на брандмауэрах, свитчах и маршрутизаторах располагаются детекторы, которые постоянно проверяют поток

данных и создают его «профиль» (или «маску»), исходя из таких характеристик, как объём пакетов данных, их тип, источник, направление и так далее [64].

В случае обнаружения каких-либо аномалий детектор поднимает тревогу и активизирует исполнительные модули, посылая им информацию об этих аномалиях, об источнике атаки, объёмах и типах вредоносных пакетов в потоке данных. Исполнительные модули, размещённые в разных сегментах сети на маршрутизаторах, также постоянно отслеживают поток данных, и, получив данные о появлении вредоносных пакетов, начинают искать их в тех данных, которые проходят через них [64].

Если вредоносные пакеты обнаруживаются, исполнительный модуль посылает сигнал тревоги предыдущему по ходу потока данных модулю вместе с рекомендациями по активизации фильтров на соответствующих маршрутизаторах [64].

Таким образом, потоку вредоносных пакетов возводится восходящий заслон, но при этом блокируется не все входящие транзакции, а именно деструктивный поток данных. Заслон может возводиться в автоматическом режиме, но существует возможность ручной настройки [64].

Предложение от Intel [1]

Запатентованная инженерами Дэвидом Патзолу (David Putzolu) и Тоддом Андерсоном (Todd Anderson) система подразумевает модификацию маршрутизаторов таким образом, чтобы они автоматически реагировали на сигнал тревоги со стороны атакованного компьютера [1].

Предполагается, что сигнал тревоги будет содержать копию вредоносного пакета. После чего маршрутизаторы создают его профиль (маску) и отсекают все похожие сообщения. Если обнаружится, что вредоносное сообщение обходит возведённый барьер, то сигнал тревоги изменяется и барьер подстраивается так, чтобы полностью заблокировать деструктивный поток данных [1].

Чтобы злоумышленники не смогли заставить компьютеры блокировать легитимный поток данных, маршрутизатор и атакованный компьютер должны идентифицировать друг друга с помощью цифровых сертификатов, подобно тем,

что используются для обеспечения безопасности финансовых транзакций через Интернет [1].

Решение Cisco DDoS Protection [71]

Компания Cisco предлагает ряд системных проверенных архитектур. Данное решение интегрирует роутеры Cisco с продуктами линеек Cisco Guard и Cisco Traffic Anomaly Detector в систему защиты, которая определяет DDoS-аномалии и смягчает их последствия. Продукты Guard и Detector используют анализ сетевого поведения для определения и смягчения атаки на отказ в обслуживании. Cisco Traffic Anomaly Detector обеспечивает отслеживание отклонений поведения от нормы, а Cisco Guard поддерживает подробную, масштабируемую очистку потока данных от аномалий. На основании сигнала тревоги от Detector продукт Guard проводит анализ потока данных для различения легитимных и злонамеренных источников с целью облегчения последствий атаки. Cisco Guard обеспечивает масштабируемую, гранулярную очистку потока данных от аномалий в режиме реального времени. Роутеры Cisco используют возможность NetFlow программного обеспечения Cisco IOS для отслеживания тенденций в сети. Сведения о потоке данных, получаемые по технолигиям Arbor Networks, партнера Cisco Technology Developer Program, позволяют сервис-провайдерам получить информацию, необходимую для борьбы с атаками на безопасность по мере их появления [71].

Алгоритм работы Cisco DDoS Protection [71]:

1. Детектирование – процесс, направленный на определение факта аномалии в сети клиента. Детектирование включает определение типа атаки и ее источника. Как только установлен факт атаки, Guard получает уведомление по внеполосному каналу, использование которого гарантирует доставку сообщений. Сервис-провайдер, обладающий большими данными о своей сети и сетях своих клиентов, может детектировать аномалии более точно. Для получения этих данных Cisco Traffic Anomaly Detector анализирует нормальный поток данных в сети клиента и за счет этого может определить аномальное поведение [71].

2. Ослабление последствий атаки – во время этого шага происходит

удаление вредоносных пакетов из потока данных. Cisco Guard осуществляет подробный анализ потока данных, и блокирует отдельные потоки. Обучение (обновление базы известных вредоносных пакетов) в периоды отсутствия атак позволяет получить большую точность фильтрации [71].

3. Перенаправление и инжектирование. Когда атака детектирована, загрязненный поток данных (как легитимный, так и вредоносный) перенаправляется в центр очистки, где Guard осуществляет процесс ослабления атаки, удаляя аномалии. Затем легитимный поток данных будет инжектирован обратно в сеть и направлен в исходную точку назначения [71].

Решение Juniper DDoS Secure

Juniper Networks выпустила решение DDoS Secure. На сегодня продукт помог избежать ущерба на сумму более $60 млрд для компаний, работающих в сфере массовой информации, онлайн-розницы, онлайн-игр, финансов, образования и правительственных органов [71].

В противоположность традиционным решениям, DDoS Secure использует несигнатурные (эвристические) технологии для обнаружения и отражения атак уровня приложений. Программа инспектирует весь входящий и исходящий поток данных на периметре центра обработки данных, а также осуществляет мониторинг производительности приложений с каждым входящим клиентским запросом. Перед использованием порогового метода или настройки для отражения атак, DDoS Secure использует специальный алгоритм CHARM, для количественной оценки рисков в режиме реального времени, связанной с двухсторонним потоком данных. Продукт анализирует ресурсы целевого приложения, если приложение атакуют, он поднимает порог CHARM, требуемый для доступа к приложению, блокируя поток данных с наибольшей вероятностью относящийся к вредоносному воздействию. Путем корреляции входящих рисков и исходящей реакции, DDoS Secure способен обнаруживать невидимые атаки, которые обходят традиционные сигнатурные решения защиты от атак на отказ в обслуживании. Архитектура DDoS Secure использует процесс «обратной связи» для анализа полного цикла входящих пакетов и ответа, который был отправлен

обратно запрашивающей стороне. DDoS Secure является самообучающимся продуктом и не требует настройки или определения пороговой величины. Он осуществляет мониторинг того, как приложение реагирует и анализирует каждое деструктивное воздействие. DDoS Secure можно установить в виде физического устройства размером 1U (1 unit – 1 секция в серверной стойке либо шкафу), или виртуальной машины. Поскольку решение проверяет входящую и исходящую информацию для оценки рисков, а не использует предопределенную пороговую величину, ложные позитивные срабатывания ограничены [71].

1.5 Особенности противодействия деструктивным потокам данных в технологических сетях промышленных предприятий

В решениях, предназначенных для корпоративных сетей, входящий поток данных постоянно анализируется в режиме реального времени, и как только в нем находится аномалия (вредоносный пакет), система защиты получает сигнал о том, что определенные пакеты являются вредоносными, на поток данных накладывается маска, а пакеты, являющиеся аномалией – не обрабатываются. К методу маски сводятся все решения из описанных выше, при этом они требуют дополнительной настройки или времени на обучение, как в случае с эвристическим подходом и, в любом случае, подразумевают реконфигурацию корпоративной сети предприятия [46, 60, 86, 136].

Основная проблема при разработке метода противодействия деструктивным потокам данных в технологических сетях промышленного предприятия заключается в многообразии и специфичности оборудования для каждого технологического процесса на отдельно взятом предприятии одной отрасли. Существующие методы, используемые для защиты в корпоративных сетях, не применимы для технологических сетей по следующим причинам:

• необходимость полной реконфигурации промышленной сети, затраты на которую во много раз превышают предотвращенные потери;

• специфичность протоколов связи, используемых для обмена данными на полевом уровне;

• нелегитимные потоки данных могут распространять легитимные узлы в отличии от корпоративных сетей, где узлами, осуществляющими воздействие деструктивными потоками данных, являются устройства, находящиеся в сети Интернет, или нелегитимно подключенные;

• деструктивный поток данных может содержать стандартные пакеты, которые при интенсификации потока несут угрозу [78, 137].

Решением данной проблемы может стать метод, основанный не на анализе непосредственно пакетов с последующим наложении маски на поток данных, а на статистическом анализе потока и своевременной сигнализации о начале воздействия деструктивных потоков данных (рисунок А.1). В технологической сети отсутствует возможность полноценной очистки потока данных от деструктивных пакетов, но в этом и нет необходимости, так как более оптимальным решением является своевременное устранение источников воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия [22, 72, 74, 101].

Выводы по главе 1

1. Проведенный анализ проблемы кибердавления различного рода на промышленных объектах показал актуальность научно-практической задачи разработки методов повышения надежности функционирования управляющих узлов технологических сетей промышленного предприятия в условиях угрозы воздействий деструктивных потоков данных. Определены особенности системных связей и функционирования управляющих узлов технологической сети промышленного предприятия.

2. Проведенный анализ статистических данных по воздействию деструктивных потоков в корпоративных сетях промышленных предприятий и рассмотренный инструментарий для организации подобных воздействий в технологических сетях, обозначили угрозу воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия. Где имеют место большая инертность и запоздалые реакции на случившиеся инциденты, в то время как методы и средства, применяемые в корпоративных сетях, для защиты от подобного рода воздействий, в технологических сетях не применимы в силу, в том числе, структурных различий. Было установлено, что воздействие деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия не относится к инцидентам информационной безопасности, а представляет угрозу надежности для управляющих узлов, и, как следствие, снижает эффективность их работы.

3. Проведенный анализ методов, продуктов и механизмов противодействия деструктивным потокам данных, используемых в корпоративных сетях, позволяет говорить об актуальности задачи повышения надежности и эффективности функционирования управляющих узлов технологической сети промышленного предприятия в условиях угрозы воздействия деструктивных потоков данных.

2. ИССЛЕДОВАНИЕ СИСТЕМНЫХ ВЗАИМОСВЯЗЕЙ И ЗАКОНОМЕРНОСТЕЙ ФУНКЦИОНИРОВАНИЯ УПРАВЛЯЮЩИХ УЗЛОВ ТЕХНОЛОГИЧЕСКИХ СЕТИ В УСЛОВИЯХ УГРОЗЫ ВОЗДЕЙСТВИЯ ДЕСТРУКТИВНЫХ ПОТОКОВ ДАННЫХ

2.1 Классификация видов воздействия деструктивных потоков данных на управляющие узлы технологических сетей промышленного предприятия

Существует множество различных классификаций воздействий, направленных на отказ в обслуживании проводимых в корпоративных сетях. Одна из самых подробных была предложена Ковалевым Д.А. и приведена ниже (рисунок 6). Эта классификация, как и другие, наиболее часто используемые на настоящий момент, не учитывает специфику функционирования технологических сетей [87, 119].

Для определения параметров воздействия деструктивных потоков данных в сформировано исходное множество значимых факторов, характеризующих уровень и состояние воздействия.

1. Источник воздействия является значимым фактором, так как распределенная генерация вредоносных пакетов (от нескольких неисправных узлов) приводит к более интенсивному воздействию деструктивных потоков данных на управляющий узел-цель технологической сети, чем при действии одного узла-источника.

2. Динамические параметры при воздействии деструктивных потоков данных характеризуют динамические изменения потока данных, связанные с алгоритмом работы неисправного узла и характером его неисправности, определяющими закон генерации деструктивных потоков данных [71].

3. Статистические параметры потока данных выражают изменение количественных показателей деструктивного потока данных [1, 96, 106, 108].

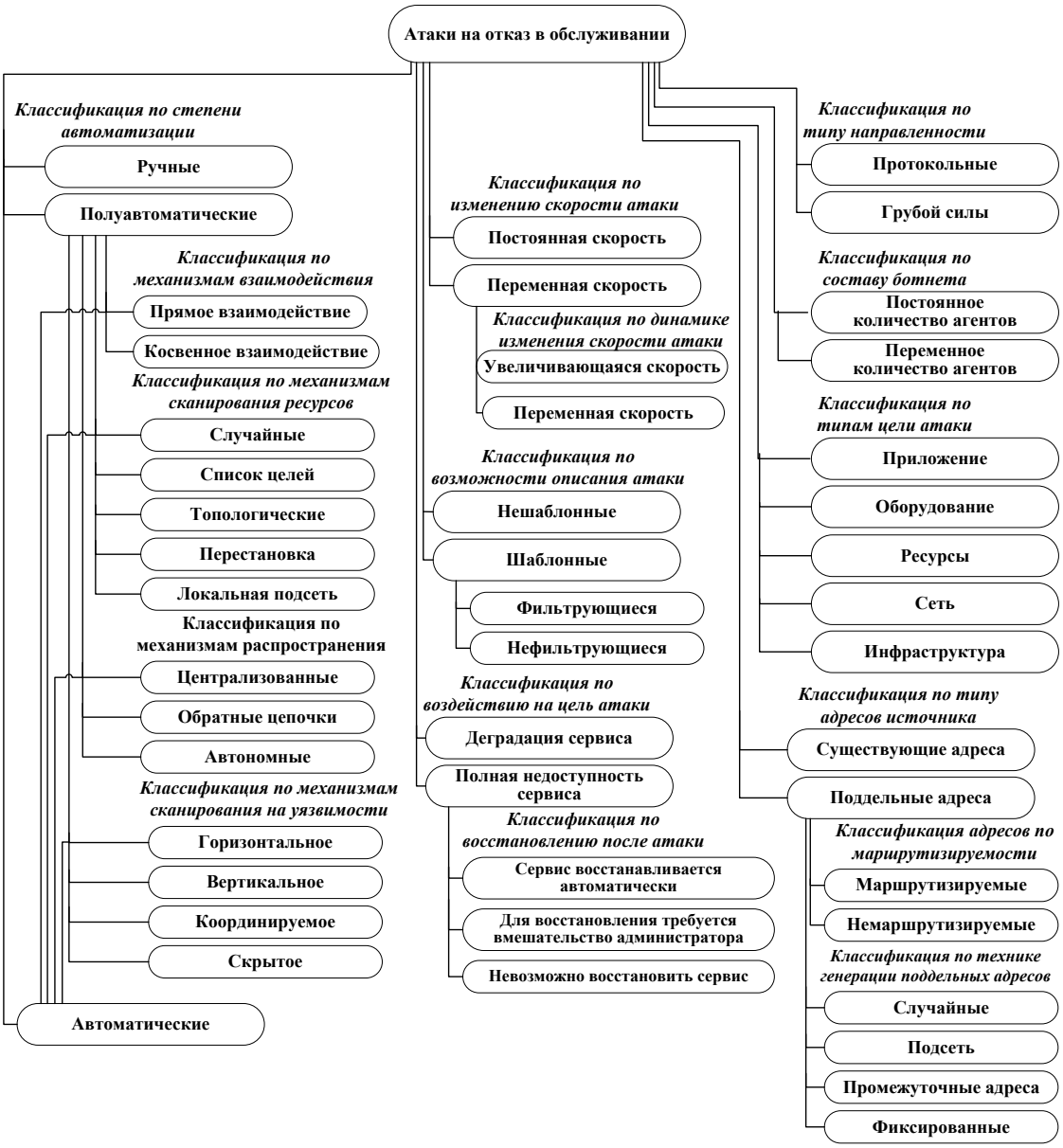


Рисунок 6 - Классификация атак на отказ в обслуживании Ковалева Д.А.

4. Вид воздействия – фактор, характеризующий воздействие деструктивных потоков данных на управляющий узел с позиции направленности. При направленном воздействии на уязвимость в программном обеспечении управляющего узла-цели, отказ в обслуживании может достигаться при низком уровне интенсификации потоков данных, в то время как при деструктивной интенсификации потоков данных источником генерируется максимально возможное количество пакетов. Чем выше уровень интенсификации, тем более вероятен отказ в обслуживании узла-цели. При этом пакеты могут иметь легитимный вид и присутствовать в потоках данных при исправном состоянии

управляющих узлов технологической сети, именно многократная интенсификация этих потоков ведет к отказу в обслуживании оборудования [1, 110].

5. Уровень воздействия согласно модели OSI (англ. Open Systems Interconnection basic reference model - базовая эталонная модель взаимодействия открытых систем) это фактор, выражающий качественные показатели деструктивного потока данных направленного на управляющий узел технологической сети [111].

6. Прогнозируемое состояние узла-цели характеризует исход воздействия деструктивных потоков данных на управляющий узел технологической сети, выражающийся либо в блокировке канала связи, при сохранении работоспособности узла, либо в истощении вычислительных ресурсов узла, приводящем к отказу в обслуживании.

Данные факторы дают возможность классифицировать воздействие деструктивных потоков данных (рисунок 7), построить модель, позволяющую продемонстрировать механизм воздействия и спрогнозировать его исход.

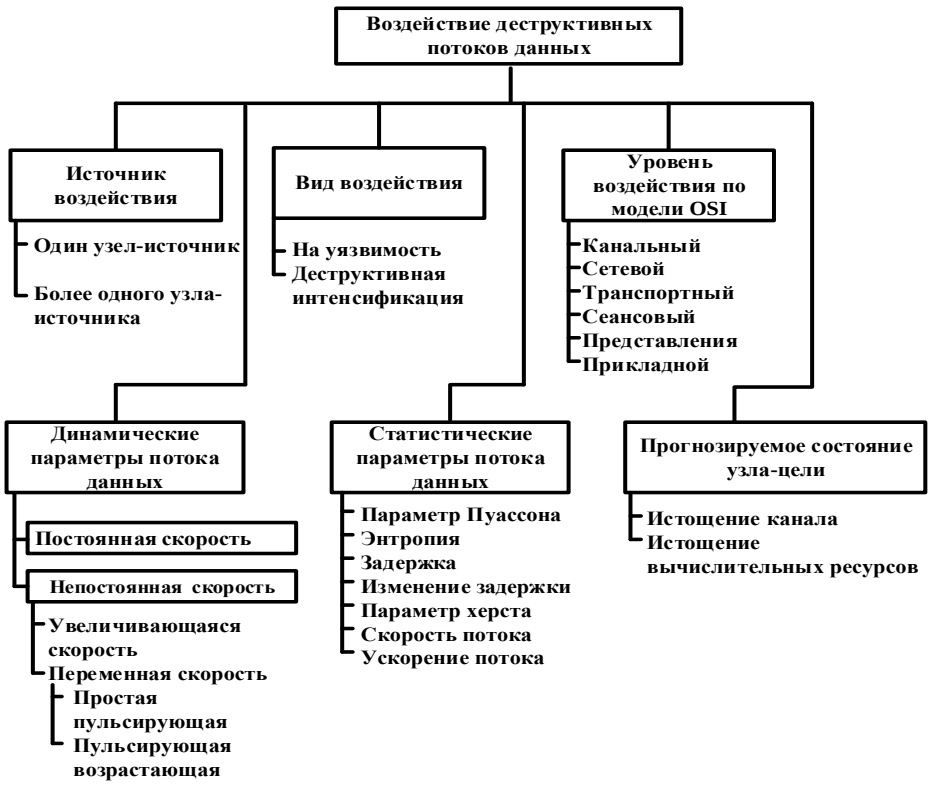


Рисунок 7 - Классификация воздействия деструктивных потоков данных в технологической сети промышленного предприятия

2.2 Построение имитационной модели воздействия деструктивных потоков данных на управляющие узлы технологических сетей промышленного предприятия

Для анализа взаимосвязей и закономерностей изменения статистических параметров потоков данных в работе предлагается использовать имитационное моделирование воздействия деструктивных потоков данных. При построении и реализации модели использовался дискретно-событийный подход, так как необходимо отслеживать состояние узла-цели и каналов связи при имитации воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия (рисунок 8) [3, 4, 10, 12].

В качестве воспроизводимого оригинала технологической сети выступает абстрактная сеть, состоящая из двух узлов: источника деструктивных потоков данных и цели воздействия.

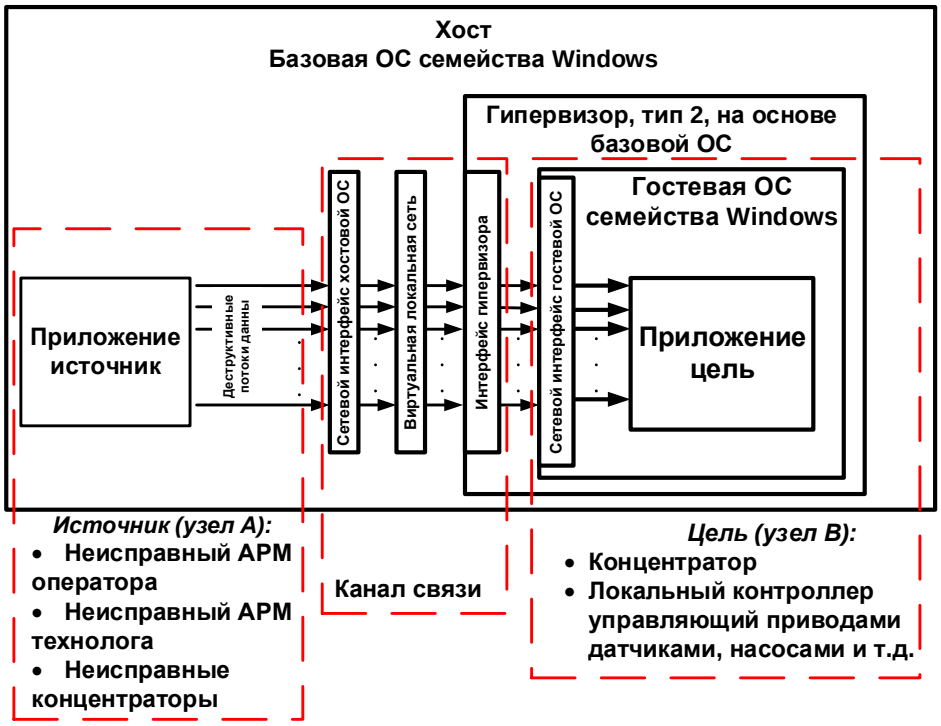


Рисунок 8 - Структурная схема имитационной модели воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия

Составляющими частями модели являются хост, гипервизор, виртуальная машина, узел-цель, приложение источник.

Хост – это, в данном контексте, ПК, на котором установлена базовая операционная система.

Гипервизор - монитор виртуальных машин, программное обеспечение, позволяющее выполняться нескольким операционным системам на одном компьютере. В имитационной модели используется гипервизор второго типа, а именно компонент, работающий на одном уровне (кольце) с ядром основной операционной системы, т.е. виртуализация на базе основной ОС.

В роли узла-источника (А) выступает программное обеспечение, позволяющее воздействовать на заданный узел деструктивными потоками данных с заданной интенсивностью.

В роли узла-цели выступает виртуальная машина под управлением гостевой операционной системой семейства Windows, с заданными, исходя из возможностей моделируемого узла, вычислительными ресурсами.

В роли канала связи выступает комплекс из сетевого интерфейса хостовой ОС, виртуальной локальной сети, интерфейса гипервизора.

Нагрузка на моделируемый узел (В) и канал связи, оказываемая приложением-источником деструктивных потоков данных, может варьироваться в зависимости от воспроизводимого типа воздействия [17, 23, 117].

При построении имитационной модели воздействия деструктивных потоков данных на управляющие узлы технологических сетей промышленного предприятия применялась методология функционального моделирования IDEF0. На рисунках 9 и 10 приведены диаграммы имитационной модели A-0 и A0 соответственно [32].

К управляющим воздействиям при построении функциональной модели отнесены:

- статистические данные по проводимым воздействиям, приводящим к отказу в обслуживании узлов, опубликованные в открытых источниках;

- сведения по характеристикам управляющих узлов представленные производителями оборудования для технологических сетей промышленных предприятий;
- сведения по характеристикам и возможностям программного обеспечения управляющего работой технологической сети, приведенные разработчиками.

Как входные данные рассматриваются:

- аппаратные характеристики модели узла-цели, такие как оперативная память и ресурсы, выделяемые от центрального процессора при виртуализации;
- скорость обработки запросов приложения, установленного на моделируемом узле-цели;
- скорость вредоносного потока данных, генерируемого источником;
- уровень пакета согласно модели OSI, позволяющий варьировать вид и содержание вредоносных пакетов, составляющих деструктивный поток данных.

В качестве механизма, при построении имитационной модели воздействия деструктивных потоков данных использовались технологии виртуализации.

Выходными являются статистические данные, позволяющие идентифицировать воздействие деструктивных потоков данных на управляющий узел технологической сети промышленного предприятия [47].

При детализации на диаграмме А0 приведено 5 процессов (рисунок 11-15).

Рисунок 9 - Имитационная модель воздействия деструктивных потоков данных. Диаграмма A-0

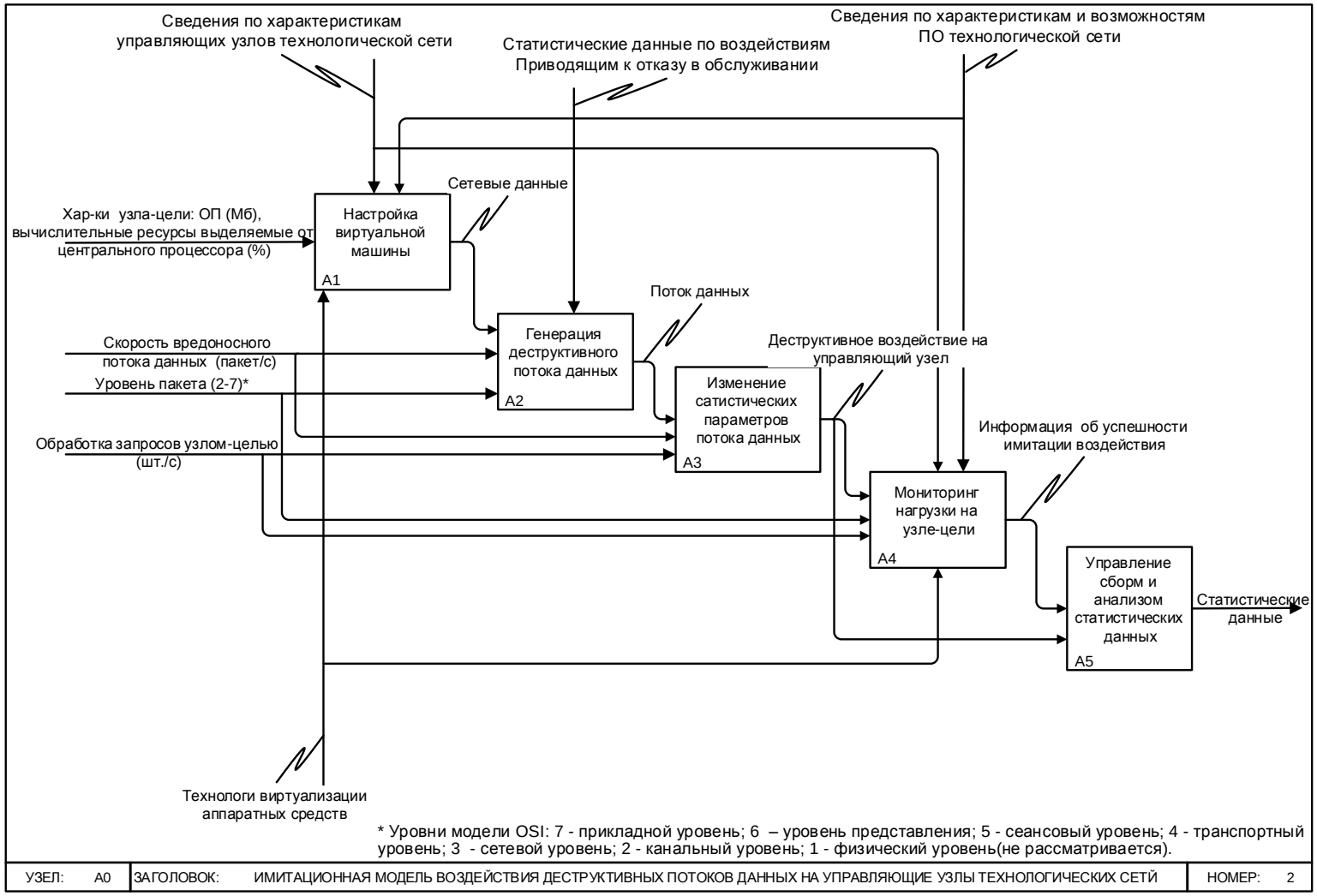


Рисунок 10 - Имитационная модель воздействия деструктивных потоков данных. Диаграмма A0

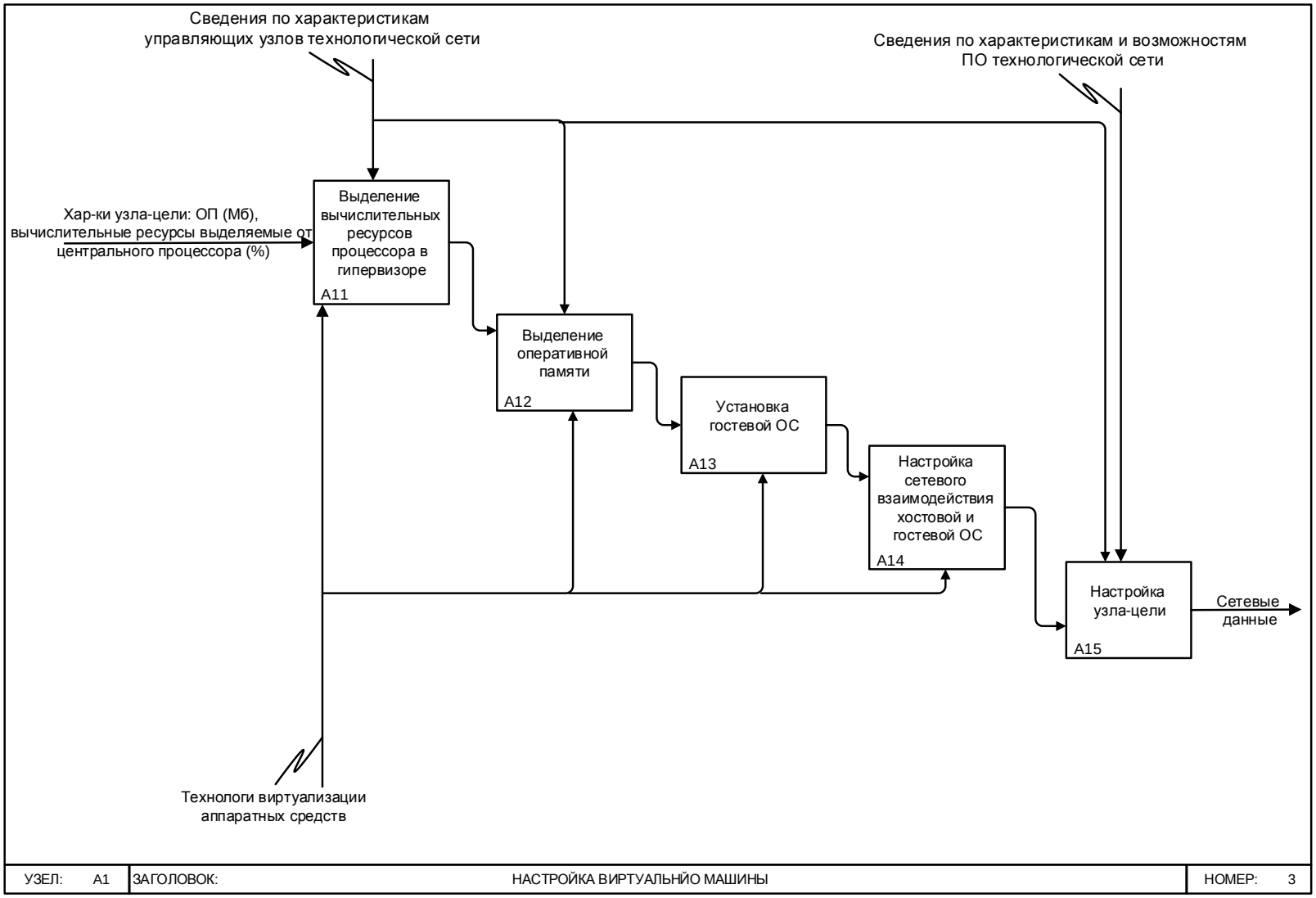


Рисунок 11 - Настройка виртуальной машины. Диаграмма A1

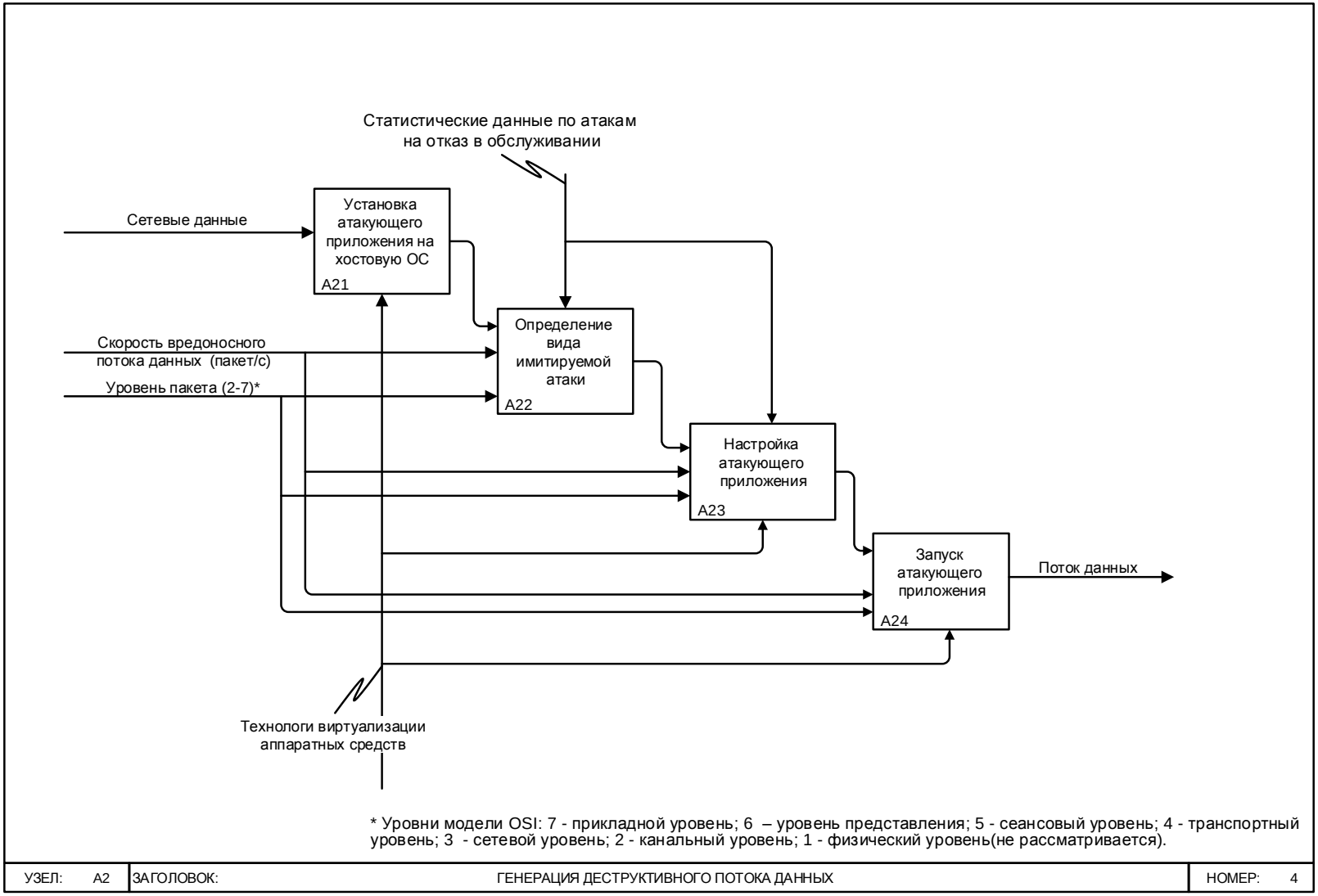


Рисунок 12 - Генерация деструктивного потока данных. Диаграмма A2

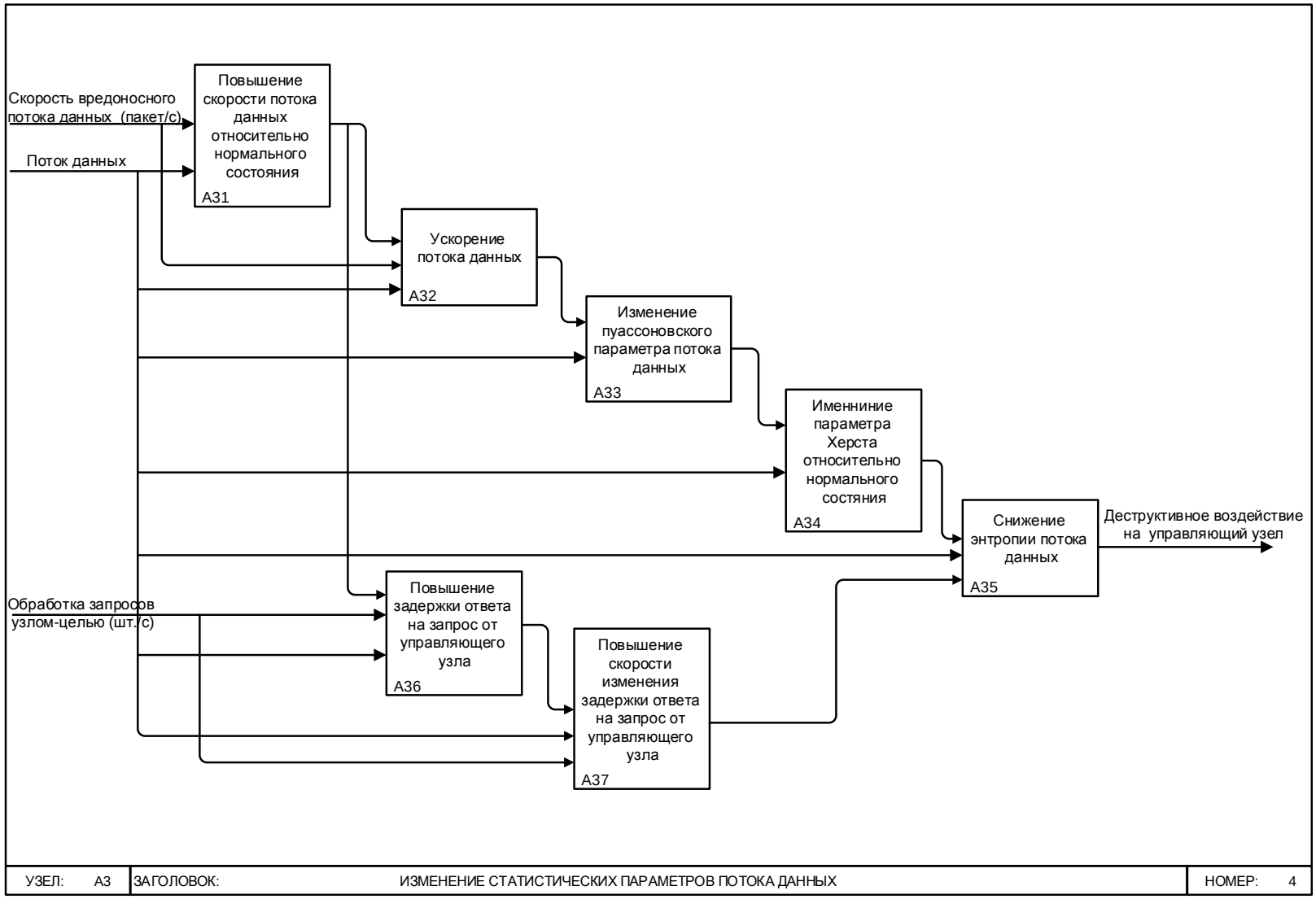


Рисунок 13 - Изменение статистических параметров потока данных. Диаграмм A3

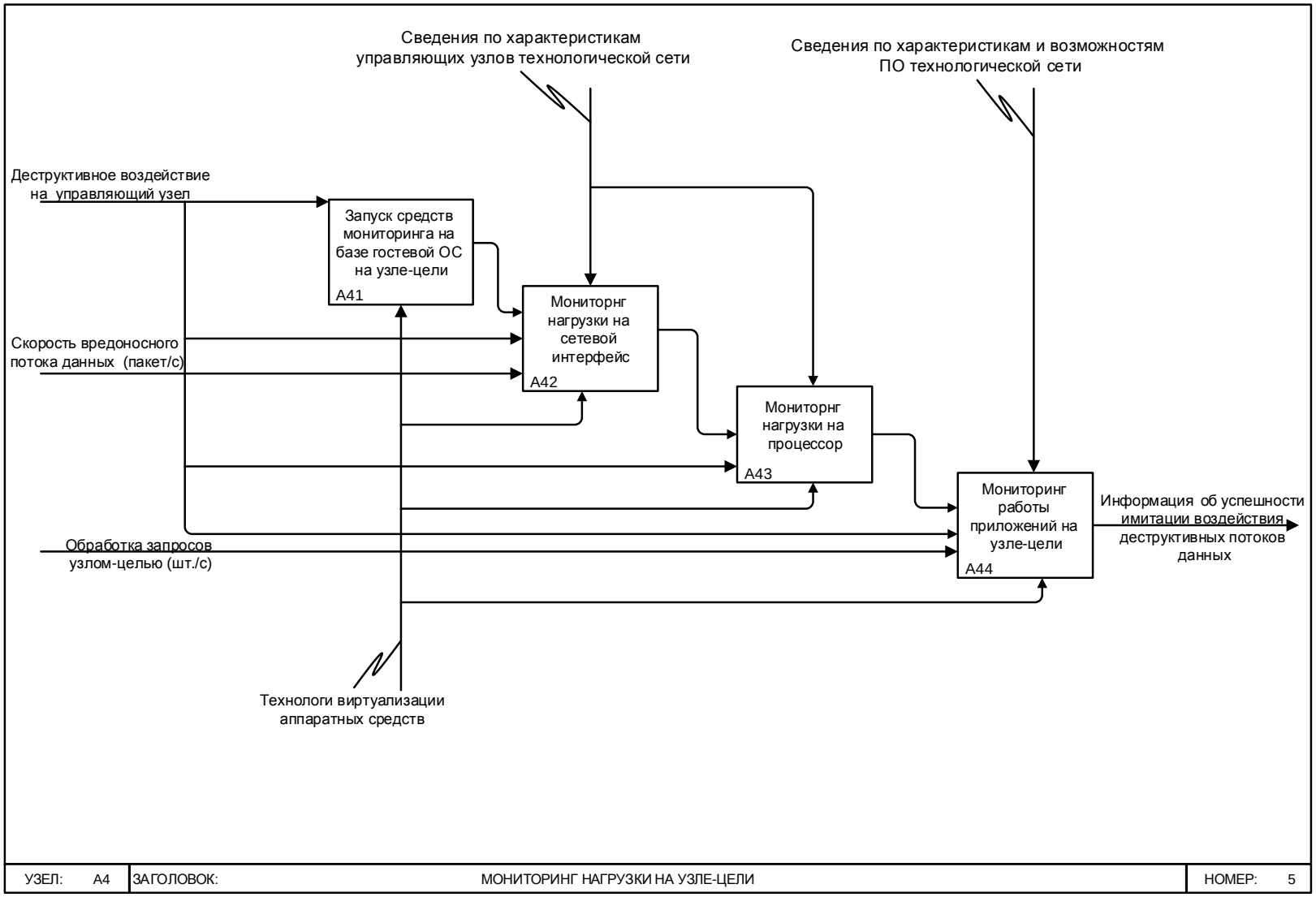


Рисунок 14 - Мониторинг нагрузки на узле-цели. Диаграмма А4

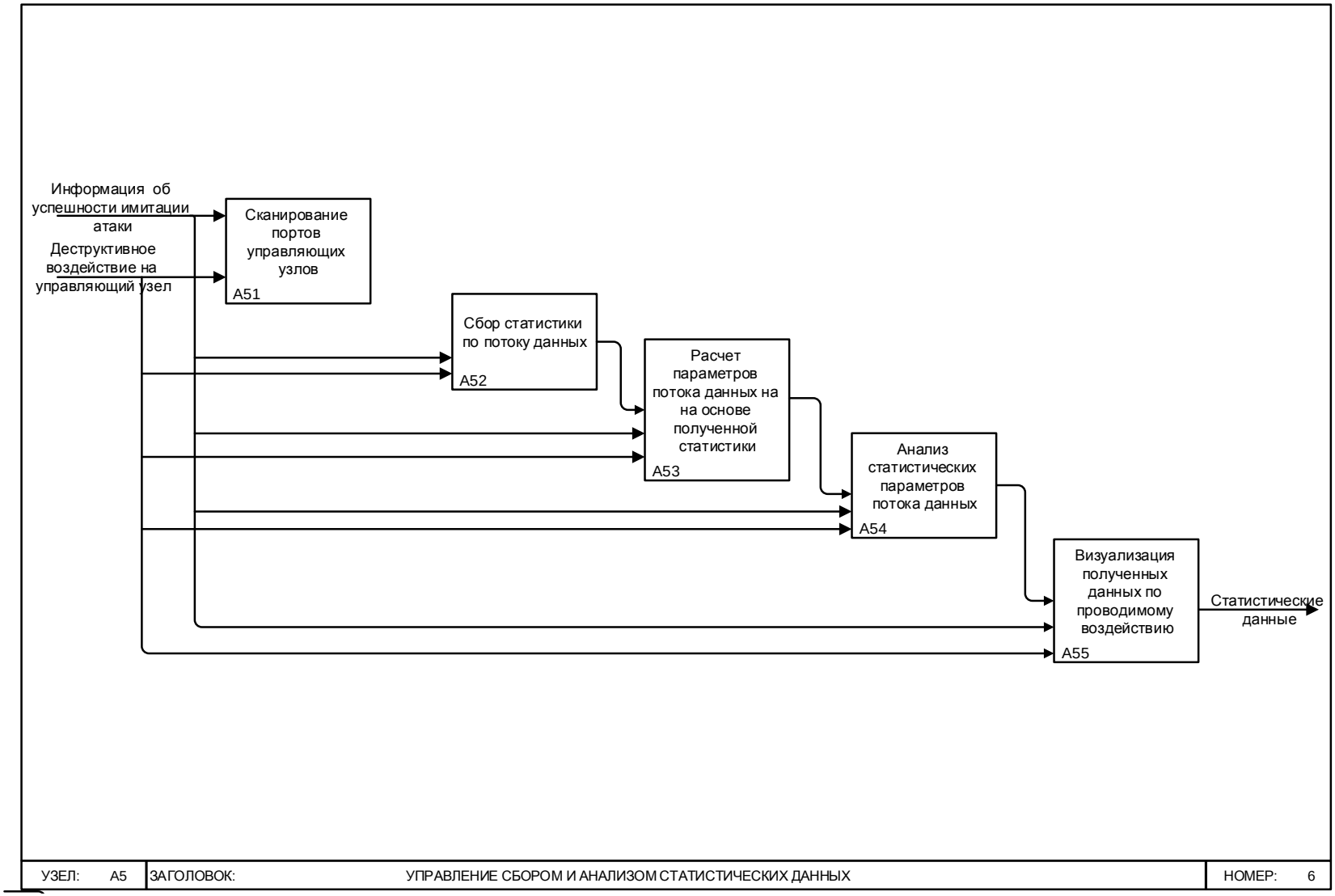


Рисунок 15- Управление сбором и анализом данных. Диаграмма A5

2.3 Разработка проблемно-ориентированной системы управления сбором и анализом статистических данных

Разработанная проблемно-ориентированная система позволяет управлять сбором и анализом статистических данных по нагрузке на управляющий узел в процессе экспериментов, проводимых с использованием имитационной модели воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия, а также осуществляет выделение контрольных характеристик, определяющих нормальное состояние технологической сети, на основании чего впоследствии становится возможным определение аномалий в потоке данных [11, 13, 19, 38, 144].

В систему входят 3 взаимодействующих модуля:

Модуль «Сканирование портов»

Данный модуль необходим для сбора статистических данных по состоянию управляющих узлов, участвующих в обмене потоками данных, он сканирует порты с указанием локальных адресов, локальных портов, внешних адресов, внешних портов, определяет информацию о состоянии активности портов, ID и имени процесса, участвующего в сетевом обмене [76, 89, 130, 134].

Модуль «Сбор сетевых данных»

Данный модуль перехватывает в режиме реального времени сетевые пакеты с указанием IP-адреса получателя и IP-адреса отправителя, времени перехвата, длины пакетов, портом отправителя и получателя, а также измеряет задержку ответов узла на запрос данных, направленный на управляющий узел [20, 37, 64, 75].

Модуль «Анализатор сетевой нагрузки»

Данный модуль обрабатывает статистические данные, полученные в результате сканирования сети модулем «Сбор сетевых данных» и определяет факт воздействия деструктивных потоков данных по аномалиям в рассчитанных статистических параметрах потока данных. После обработки данные

отображаются в виде следующих графиков: график скорости потока данных, график ускорения потока данных, график Пуассоновского параметра потока данных, график энтропии потока данных, график параметра Херста для потока данных, график задержки пакетов при передаче данных, график изменения задержки пакетов при передаче данных (частично приведены на рисунке 16) [90, 118, 143, 145].

Рисунок 16 - Интерфейс проблемно-ориентированной системы управления сбором и анализом статистических данных

Модуль «Анализатор сетевой нагрузки» обладает расширенными графическими инструментами для удобства анализа графиков, а именно: возможность отображать графики как по одиночке, так и группами, автоматическое масштабирование графиков, возможность изменить цветовой фон графиков на более удобный, возможность распечатать графики.

2.4 Имитационное моделирование воздействия деструктивных потоков данных на управляющие узлы технологических сетей промышленного предприятия

Для проведения эксперимента по воспроизведению воздействия деструктивных потоков данных на управляющие узлы технологической сети, виртуальной машине, имитирующей данный узел, в гипервизоре выделяются ресурсы, приближенные к характеристикам узла. Программное обеспечение на имитируемом узле-цели отвечает на запросы в режиме, приближенном к работе сервисов в технологической сети промышленного предприятия. Приложению-источнику задаются параметры согласно типу имитируемого воздействия деструктивных потоков данных, а именно, количество пакетов в единицу времени и вид пакетов. При этом параметры могут быть изменены динамически в процессе эксперимента [21, 44, 77, 105].

После предварительных настроек имитационной модели, проводится эксперимент с применением проблемно-ориентированной системы управления сбором и анализом статистических данных.

На основе результатов имитационного моделирования были определены пороговые значения перехода из нормального состояния технологической сети в состояние воздействия деструктивных потоков данных на управляющий узел [55, 56, 88, 135].

При проведении экспериментов с использованием имитационной модели получены данные по 7 статистическим параметрам воздействия деструктивных потоков данных (таблица 1): скорость потока данных; ускорения потока данных; Пуассоновский параметр потока данных; энтропия потока данных; параметр Херста для потока данных; задержка пакетов при передаче данных; изменение задержки пакетов при передаче данных [118].

Таблица 1 - Параметры потоков данных

Параметр потоков	Расчетная формула
Скорость (V) и ускорение (a) потоков данных	$V_{аном} = \frac{N_{аном} - N_{норм}}{\Delta t};\ \ a_{аном} = \frac{V_{аном} - V_{норм}}{\Delta t};$ где $N_{норм}$ - количество пакетов при нормальных потоках данных; $N_{аном}$ - количество пакетов при аномальных (деструктивных) потоках данных; $V_{норм}$ - нормальная скорость потоков данных; $V_{аном}$ - аномальная скорость потоков данных; $a_{аном}$ - аномальное ускорение потоков данных; Δt - промежуток времени.
Пуассоновский параметр потоков данных P(k); P(τ)	$\begin{cases} P(k) = \frac{(\lambda t)^k}{k!} \cdot e^{-\lambda t}, \\ P(\tau) = \lambda \cdot e^{-\lambda t}, \end{cases}$ где k=0,1,… - число сообщений; λ - интенсивность потоков ; t - интервал времени измерения количества запросов; τ - распределение интервала между соседними событиями.
Энтропия потоков данных (E)	$E = -\sum_i f_i \log_2 f_i$, где f_i – это функция плотности вероятности, полученная из нормализованных значений параметров потоков данных.
Параметр Херста для потоков данных (H)	$\begin{cases} (R/S)_N = \frac{\max_{1 \le n \le N} \sum_{n=1}^{N} (x - \bar{x}) - \min_{1 \le n \le N} \sum_{n=1}^{N} (x - \bar{x})}{\sqrt{\sum_{n=1}^{N} (x - \bar{x})^2 / N}}, \\ (R/S)_N = cN^H, \\ H = \log_N ((R/S)_N), \end{cases}$ где x – это скорость входящего потока данных, n – это время наблюдения, а N – это общее количество точек наблюдения.
Задержка (Z) и скорость изменения задержки (a_z) пакетов при передаче данных	$Z = t_{запр} - t_{отв},\ a_z = \frac{Z - Z_n}{\Delta t},$ где $t_{запр}$ - время отправки запроса, а $t_{отв}$ - время получения ответа от соседнего узла, $Z - Z_n$ - изменение задержки в промежуток времени.

Скорость потоков данных

Высокая скорость входящего потока данных на узле-цели – это общепризнанный индикатор воздействия деструктивных потоков данных. В данном случае аномалия заключается в резком возрастании количества пакетов (N) в единицу времени (t), относительно нормального состояние технологической сети. Скорость потока данных при нормальной сетевой нагрузке в среднем составляет менее 20 пакетов в секунду (рисунок 17) [34, 128, 129].

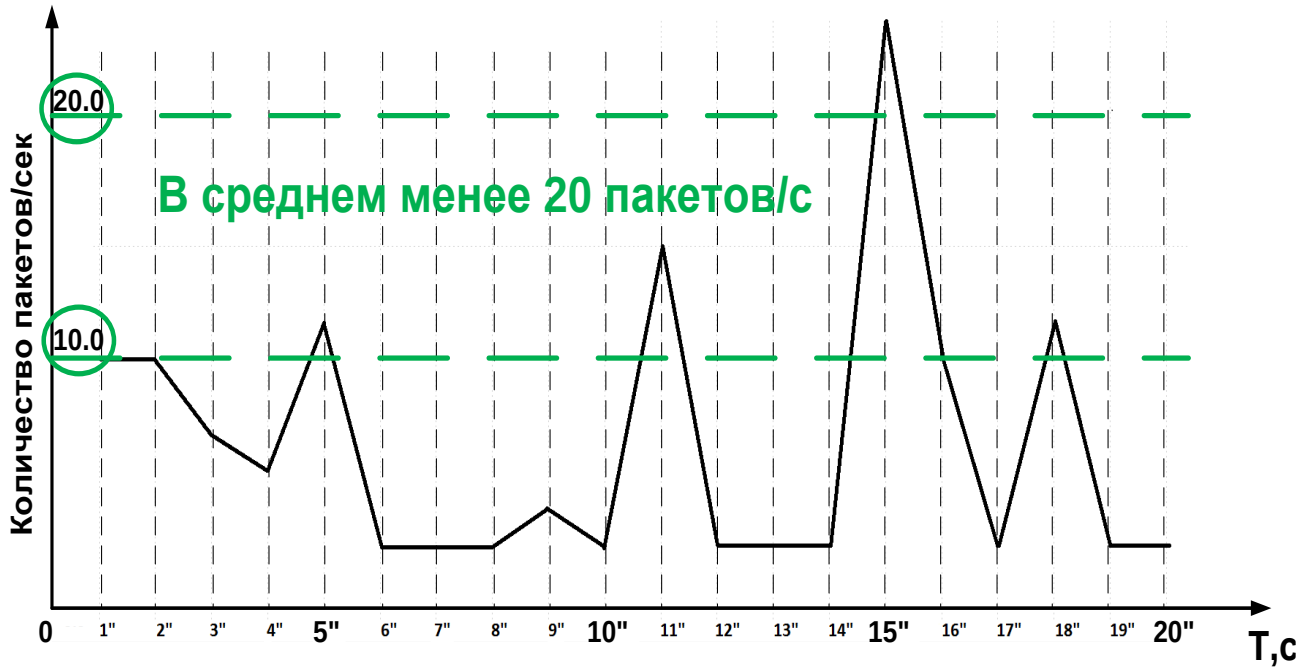


Рисунок 17 – Скорость потока данных при нормальной сетевой нагрузке

Скорость потока данных при аномальной нагрузке резко возрастает и в пике достигает 1500 пакетов в секунду (рисунок 18).

При проведении серии экспериментов (рисунок 19) было установлено, что скорость потока данных позволяет определить не только факт воздействия, направленного на отказ в обслуживании, но и начальную стадию воздействия деструктивных потоков данных на управляющий узел технологической сети промышленного предприятия.

Рисунок 18 - Скорость потока данных при аномальной сетевой нагрузке

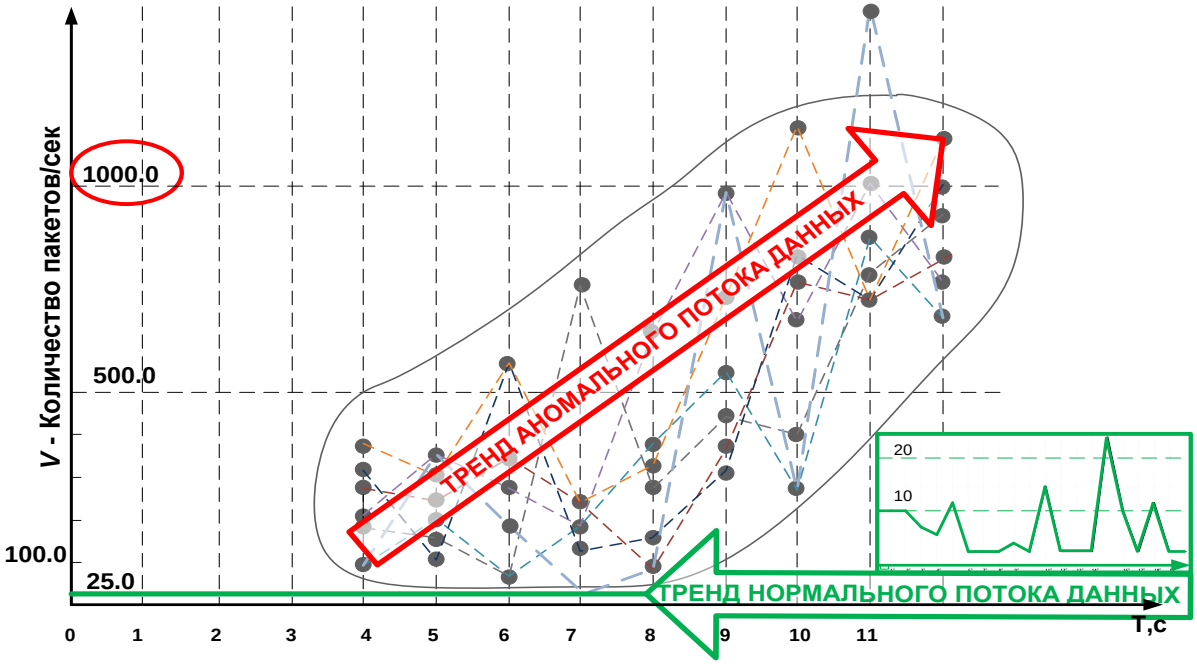


Рисунок 19 - Скорость потока данных при нормальном и аномальном состоянии технологической сети

Ускорение потоков данных

Ускорение потоков данных отражает изменения скорости потоков и при нормальной сетевой нагрузке снижается с момента начала взаимодействия между узлами (рисунок 20) до значений ниже 1 пакета/с^2 [36].

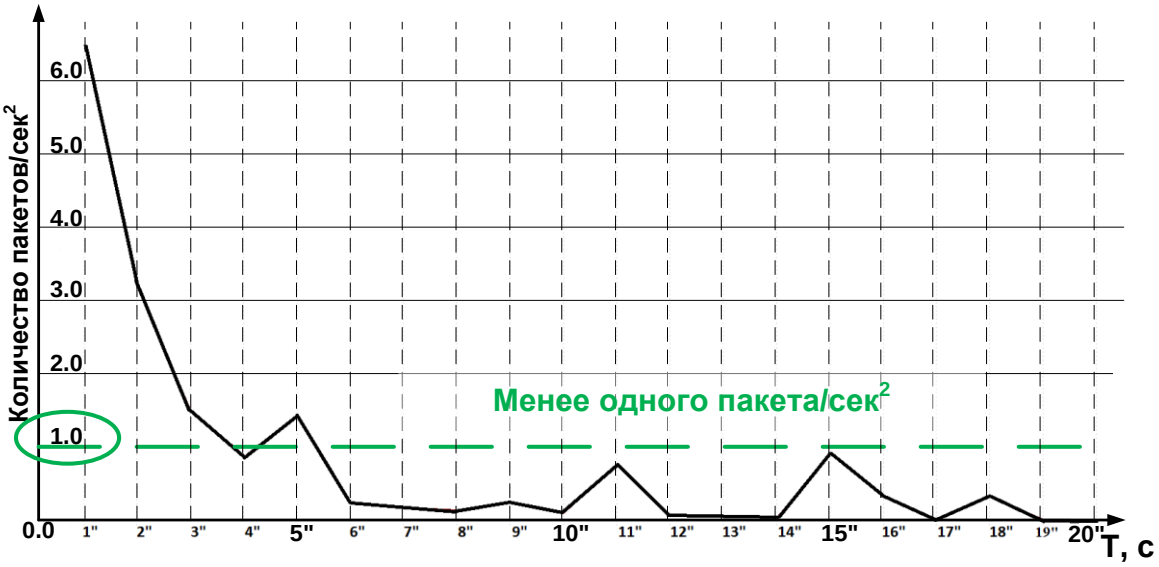


Рисунок 20 - Ускорение потока данных при нормальной сетевой нагрузке

Ускорение потоков данных при аномальной нагрузке возрастает, и может достигать более чем 120 пакетов/с^2 (рисунок 21).

Рисунок 21 - Ускорение потока данных при аномальной сетевой нагрузке

При проведении серии экспериментов (рисунок 22) было установлено, что ускорение потоков данных, как и предыдущий параметр, позволяет определить начальную стадию воздействия деструктивных потоков данных на управляющий узел технологической сети промышленного предприятия.

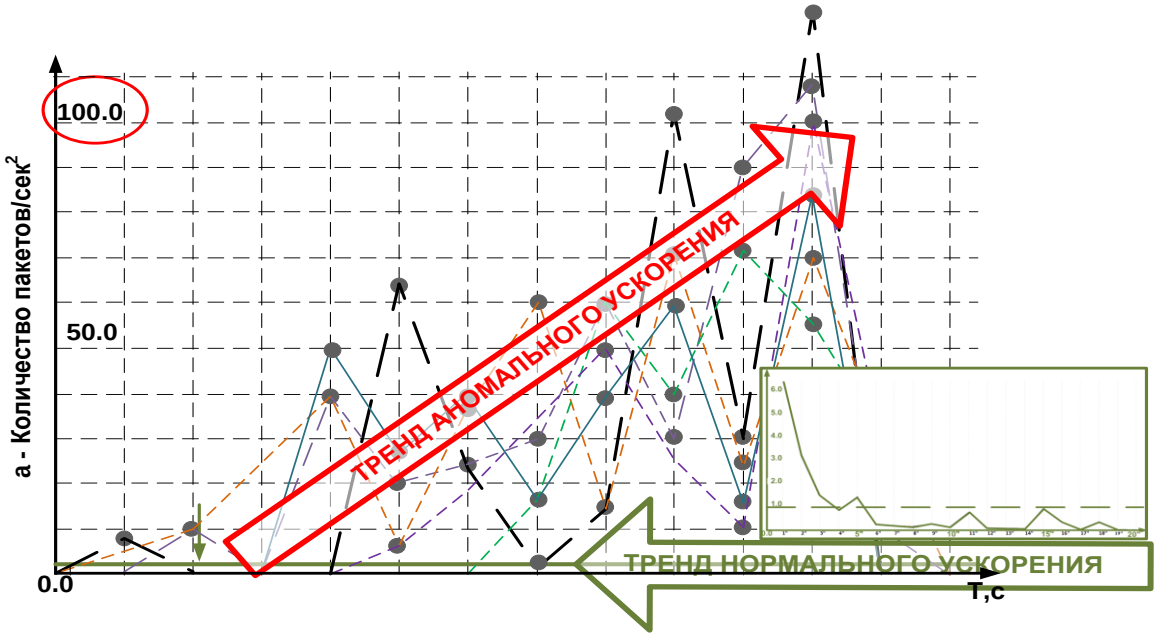


Рисунок 22 - Ускорение потока данных при нормальном и аномальном состоянии технологической сети

Пуассоновский параметр потоков данных

Это поток запросов, распределенный по пуассоновскому закону распределения. Он должен удовлетворять следующим требованиям: стационарности; отсутствия последствия и ординарности.

Поток стационарен, если вероятность поступления k запросов в течение промежутка времени t не зависит от момента начала этого промежутка.

Отсутствие последствий - вероятность поступлений k запросов после произвольного момента времени t_0 не зависит от количества и времени поступивших запросов до этого момента.

Свойство ординарности - вероятность появления двух или более запросов в течении малого интервала времени Dt есть величина бесконечно малая по сравнению с вероятностью появления одного события на этом интервале, т.е. $\lim_{\Delta t \to 0} P(n, \Delta t) = 0$.

Пуассоновский поток характеризуется набором вероятностей $P(k) = \frac{(\lambda t)^k}{k!} \cdot e^{-\lambda t}$. Интервал времени измерения количества запросов t и интенсивность потока λ являются постоянными величинами. Большее значение λ

соответствует более широкому и симметричному графику плотности вероятности (рисунок 23).

Пуассоновский поток характеризуется экспоненциальным распределением интервалов между событиями и отражает воздействие деструктивных потоков данных на управляющий узел технологической сети (рисунок 24) [95].

При проведении серии экспериментов было установлено, что чем более ассиметричный характер имеет функция пуассоновского распределения, тем более интенсивное воздействие деструктивных потоков данных имеет место (рисунок 25).

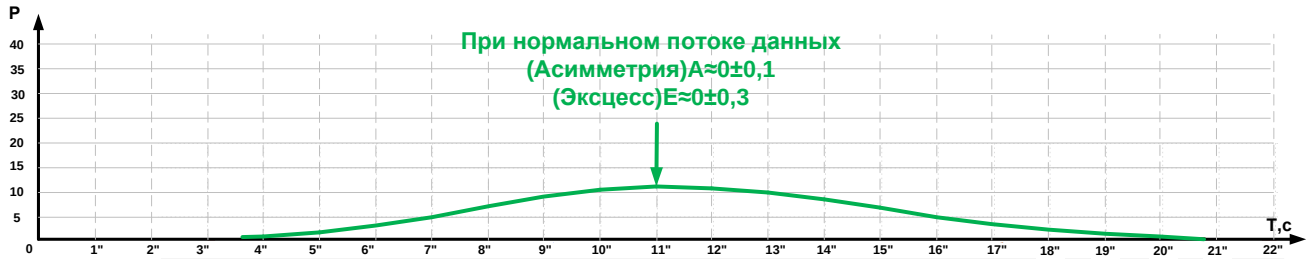


Рисунок 23 - Пуассоновский параметр потока данных при нормальной сетевой нагрузке

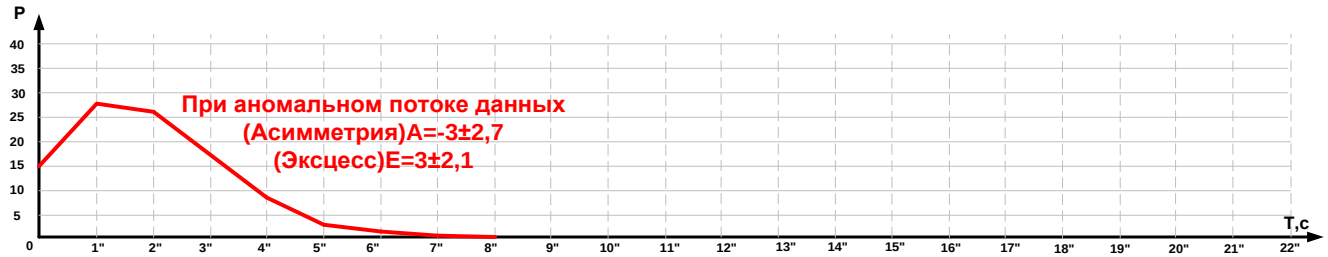


Рисунок 24 - Пуассоновский параметр потока данных при аномальной сетевой нагрузке

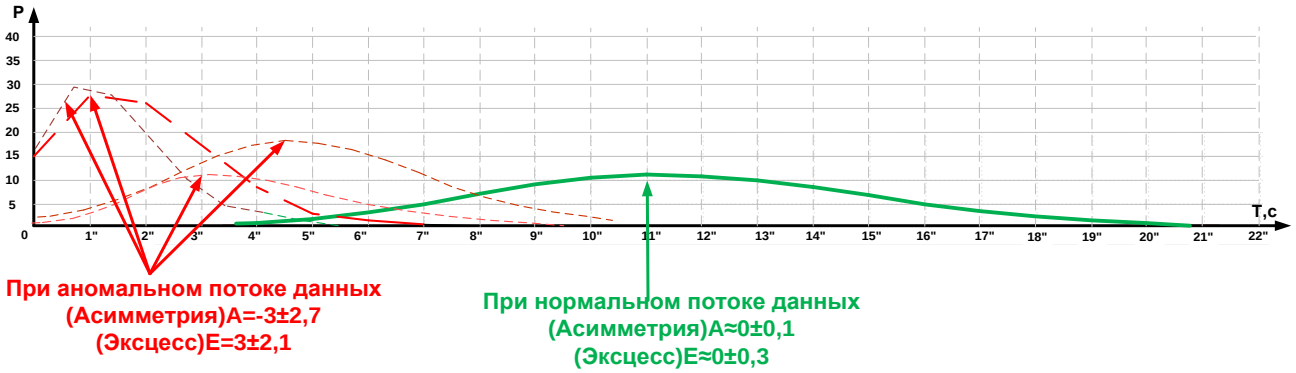


Рисунок 25 - Пуассоновский параметр потока данных при нормальной и аномальной сетевой нагрузке

Энтропия потоков данных

Так как данные имеют вероятностное описание, например, в терминах функций распределения вероятности, то энтропия будет, относиться к хаотичности или неопределенности информации в данных. При нормальном сетевом взаимодействии управляющих узлов технологической сети энтропия варьируется в некоторых постоянных пределах (рисунок 26) [24, 28].

При интенсивной генерации деструктивных потоков данных канал передачи заполняется одинаковыми пакетами, запросами, требующими одинаковых действий от управляющих узлов, подвергающихся воздействиям, таким образом, энтропия потока данных при воздействии деструктивных потоков данных будет существенно отличаться от нормального сетевого взаимодействия (рисунок 27).

При проведении серии экспериментов было установлено, что чем более интенсивное воздействие деструктивных потоков данных осуществляется в технологической сети, тем меньший промежуток времени потребуется для снижения до нуля энтропии потока данных [54, 94] (рисунок 28).

Рисунок 26 - Энтропия потока данных при нормальной сетевой нагрузке

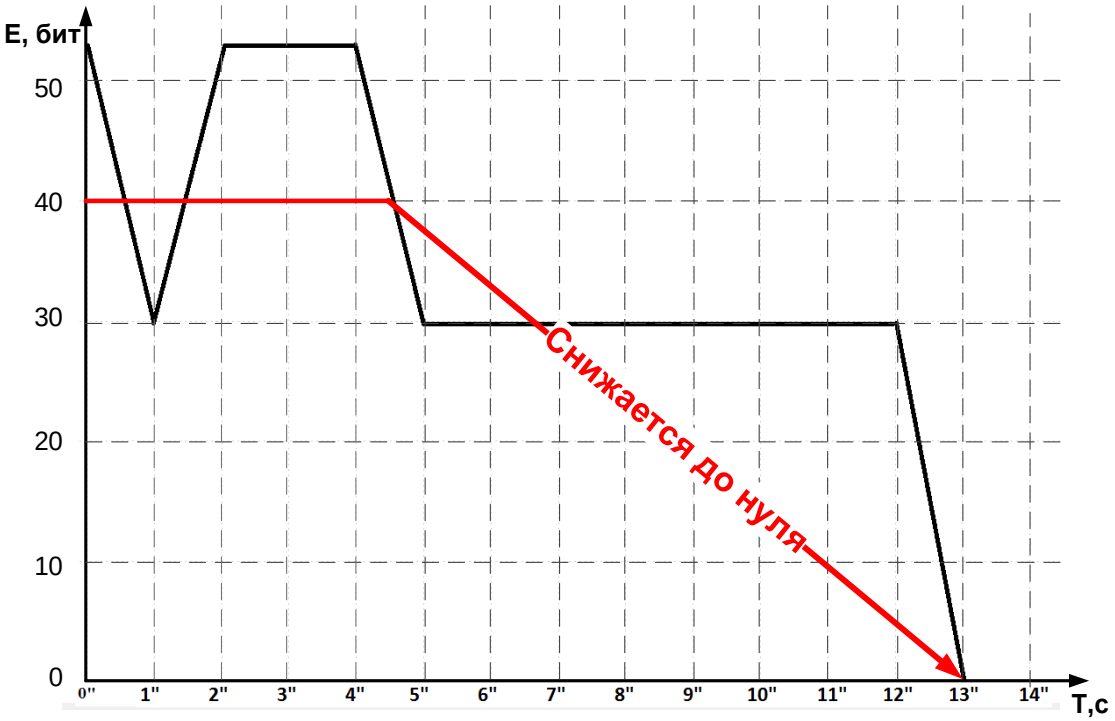


Рисунок 27 – Энтропия потока данных при аномальной сетевой нагрузке

Рисунок 28 – Энтропия потока данных при нормальной и аномальной сетевой нагрузке

Параметр Херста для потоков данных

Параметр Херста – это индикатор самоподобия потока данных. Под самоподобием подразумевается повторяемость распределения нагрузки во

времени при различных масштабах. Параметр Херста при нормальной (рисунок 29) и аномальной (рисунок 30) сетевой нагрузке отличаются не только графически, но и количественно [18].

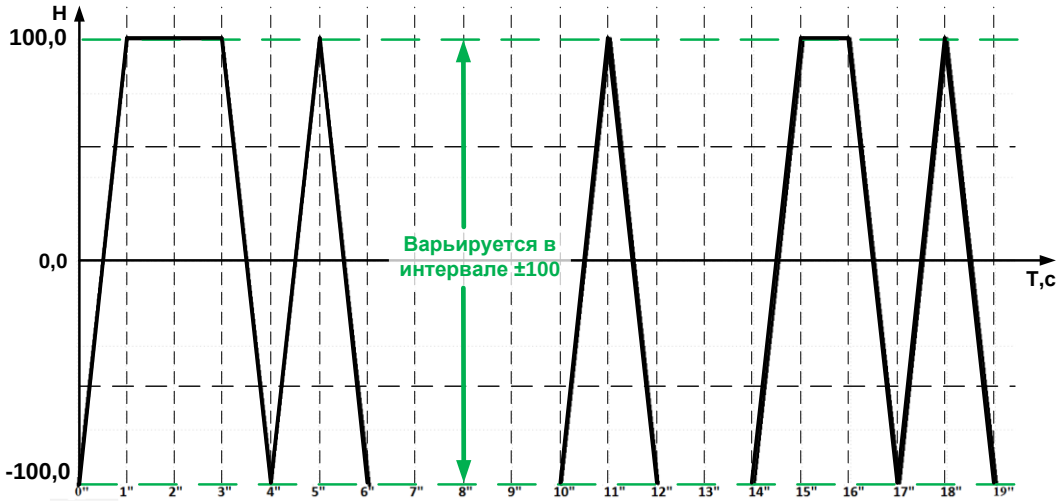


Рисунок 29 – Параметр Херста для потоков данных при нормальной сетевой нагрузке

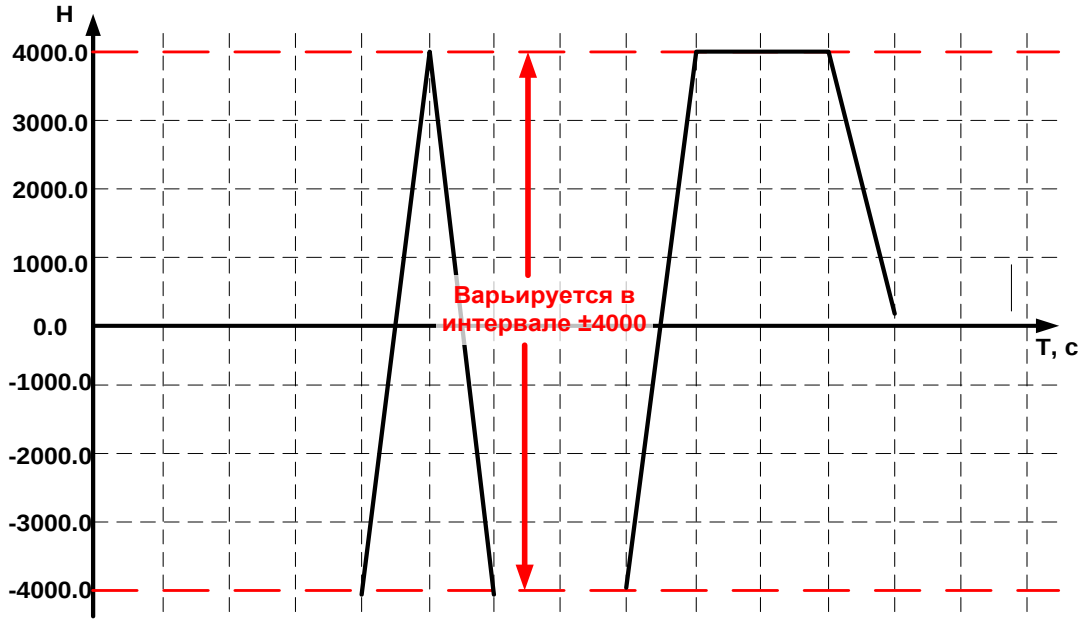


Рисунок 30 – Параметр Херста для потоков данных при аномальной сетевой нагрузке

Серия экспериментов показала, что интенсивность генерации деструктивных потоков данных источником влияет на количественный показатель параметра Херста (рисунок 31).

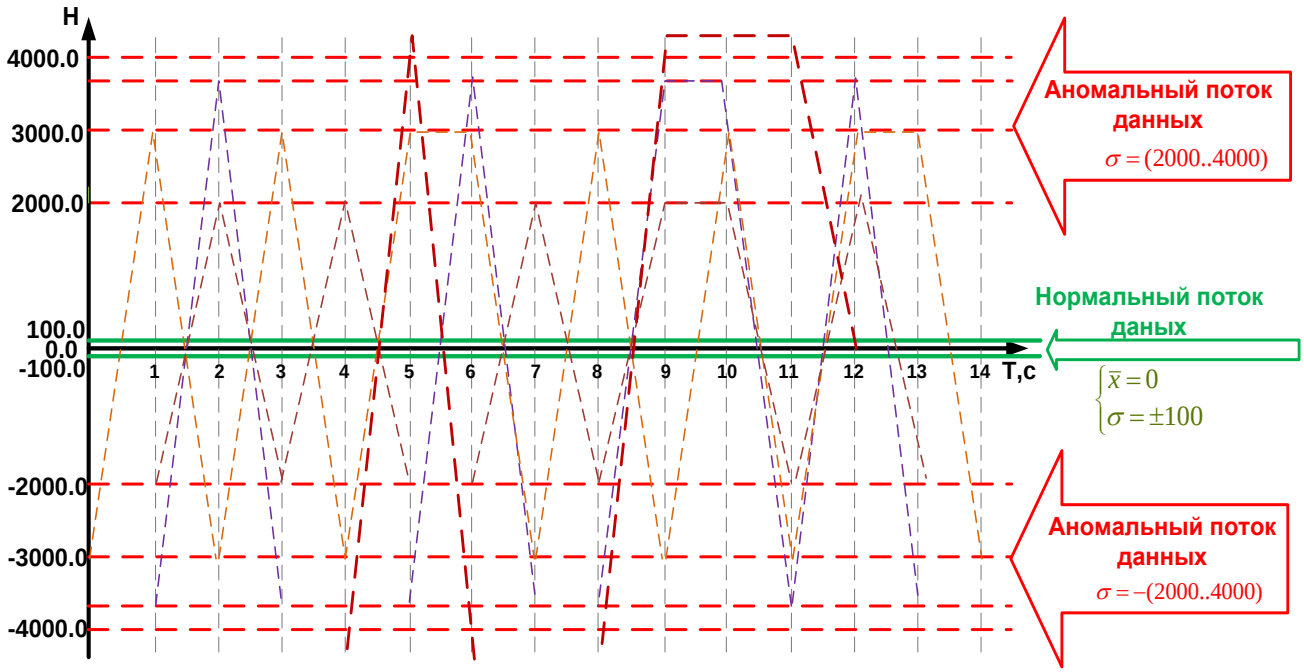


Рисунок 31 - Параметр Херста для потоков данных при нормальной и аномальной сетевой нагрузке

Задержка пакетов при передаче данных

При нормальном сетевом взаимодействии управляющих узлов технологической сети задержка пакетов связана с издержками в работе оборудования и спецификой среды передачи данных (рисунок 32).

Рисунок 32 – Задержка пакетов при нормальной сетевой нагрузке

Естественным следствием высокой скорости потока данных и увеличения загруженности канала связи является повышение задержки пакетов (рисунок 33).

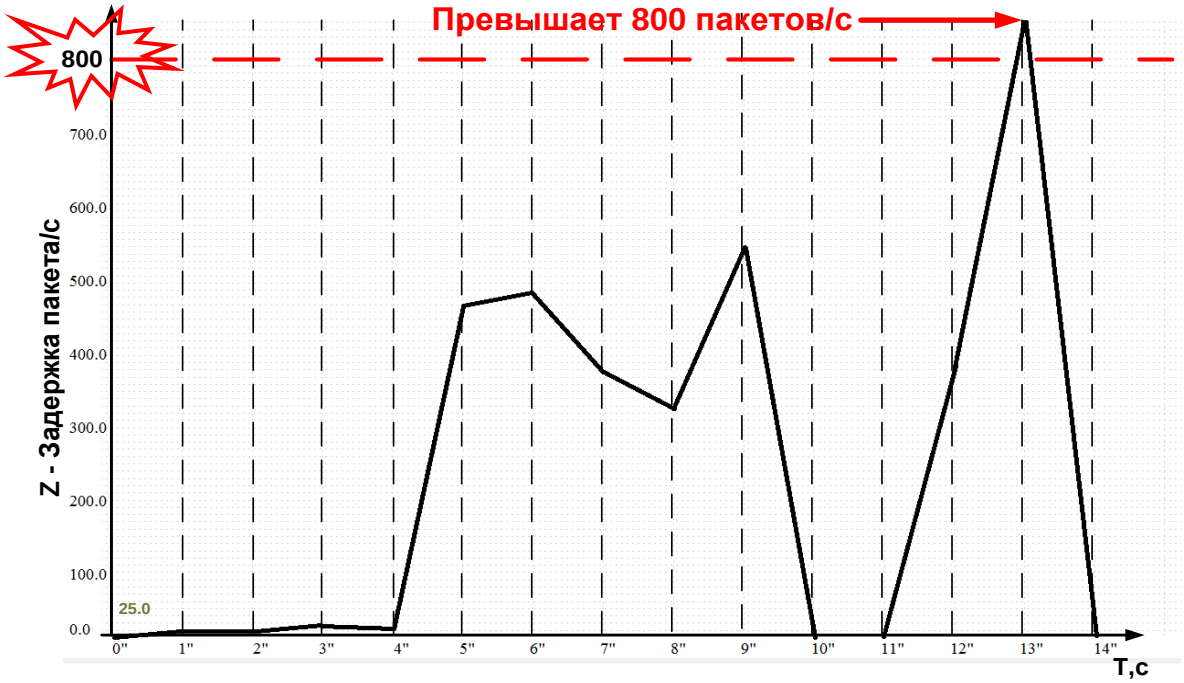


Рисунок 33 - Задержка пакетов при аномальной сетевой нагрузке

При проведении серии экспериментов было установлено, что, измеряя среднее время в пути вернувшихся ответов на запросы, можно получить информацию об истощении канала связи, что является следствием воздействия деструктивных потоков данных на управляющий узел технологической сети (рисунок 34).

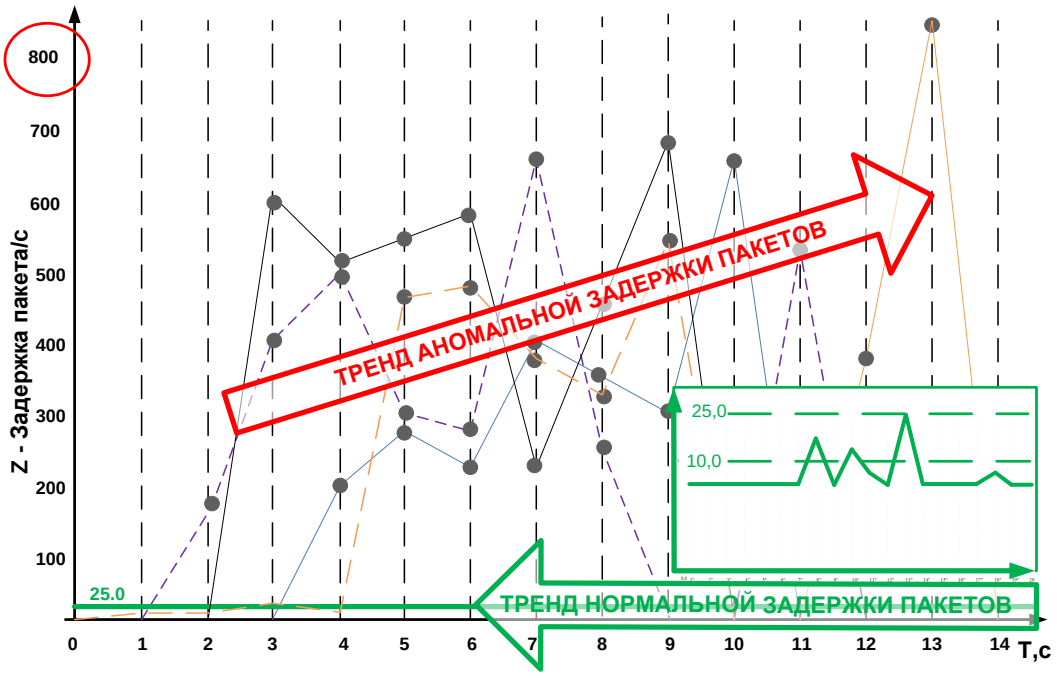


Рисунок 34 – Задержка пакетов при нормальной аномальной сетевой нагрузке

Скорость изменения задержки пакетов при передаче данных

По аналогии со скоростью потока данных, в зависимости от типа воздействия деструктивных потоков данных и на всей его длительности, задержки пакетов испытывают значительные изменения. При этом скорость изменения задержки при нормальной сетевой нагрузке (рисунок 35), подобно ускорению потоков данных, будет снижаться до значений близких к нулю, что существенно отличается от скорости изменения задержки при воздействии (рисунок 36).

При проведении серии экспериментов (рисунок 37) было установлено, что скорость изменения задержки пакетов при передаче данных по технологической сети позволяет судить не только о скорости истощения канала связи при проведении воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия.

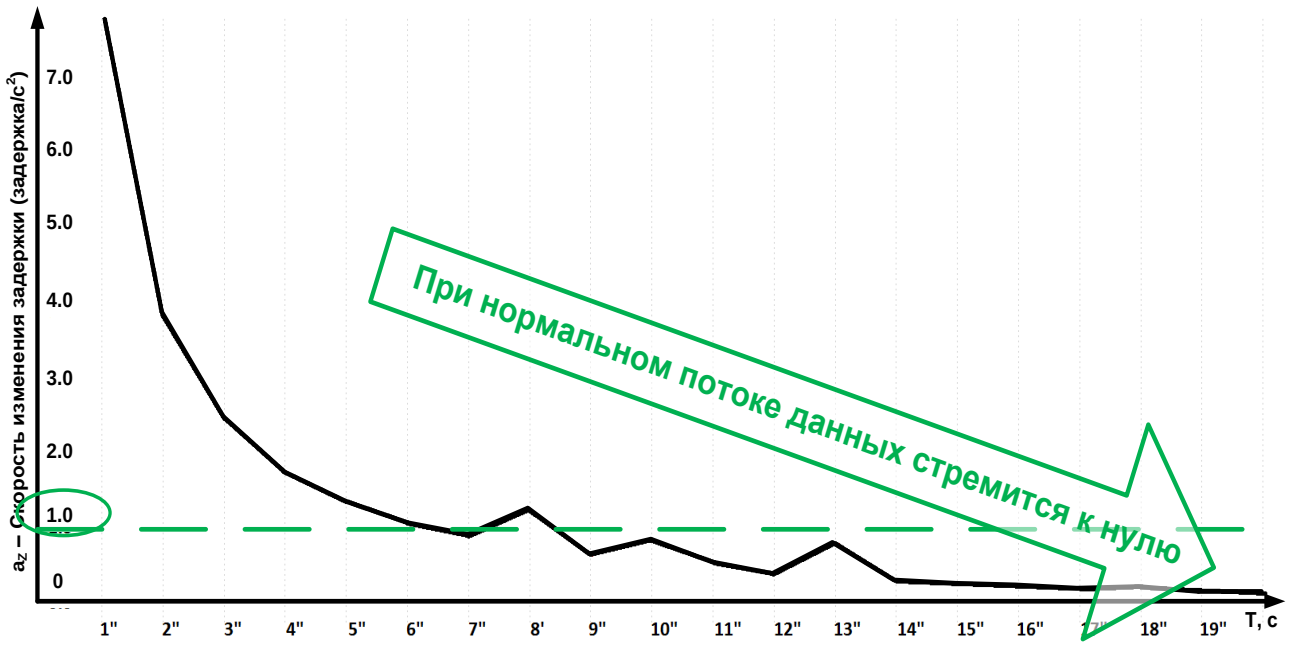


Рисунок 35 – Скорость изменения задержки пакетов при нормальной сетевой нагрузке

Рисунок 36 – Скорость изменения задержки пакетов при аномальной сетевой нагрузке

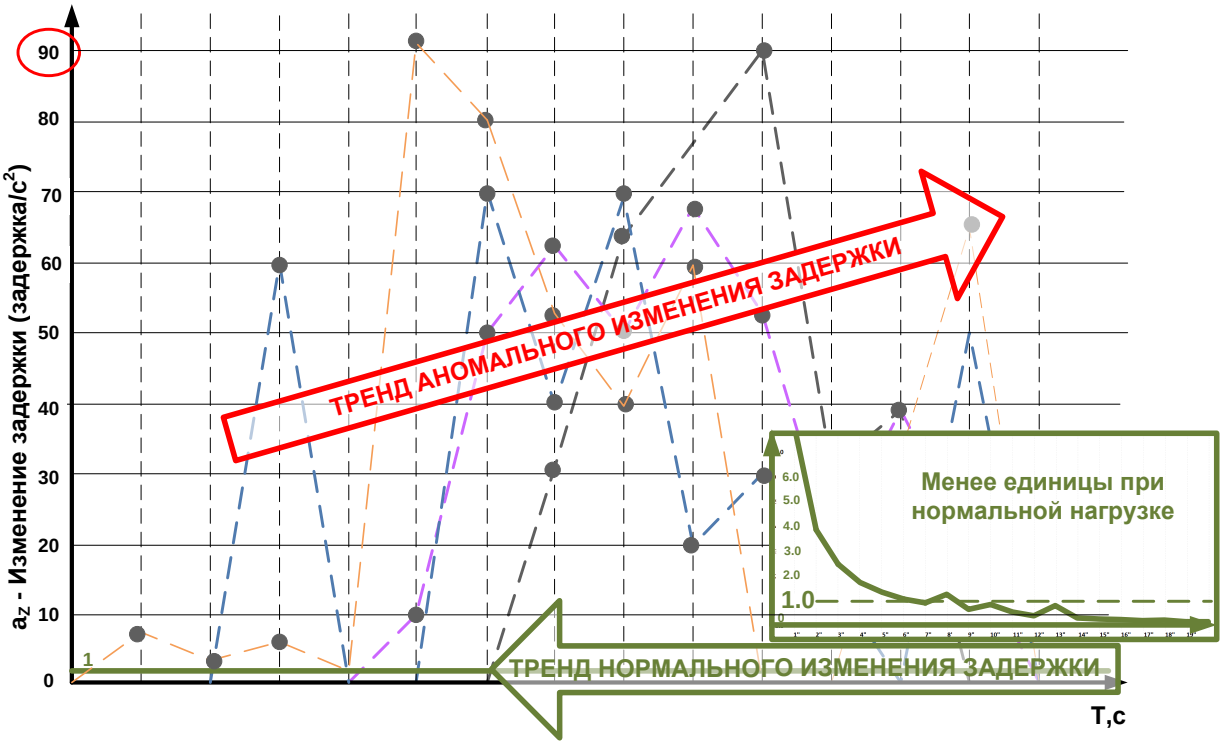


Рисунок 37 - Скорость изменения задержки пакетов при нормальной аномальной сетевой нагрузке

Выводы по главе 2

1. Анализ статистических данных, полученных при имитационном моделировании воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия позволяет говорить о том, что выбранные параметры (скорость потока данных, ускорения потока данных, Пуассоновский параметр потока данных, энтропия потока данных, параметр Херста для потока данных, задержка пакетов при передаче данных, изменение задержки пакетов при передаче данных) отражают проводимое воздействие.

2. Разработанная проблемно-ориентированная система позволяет определить факт воздействия деструктивных потоков данных на узел-цель по рассчитанным параметрам и визуализируемым графикам, построенным на основе анализа статистических данных за определенный промежуток времени. На основе проведенного анализа можно сделать вывод о том, что статистические параметры потоков данных позволяют определить воздействие на ранних стадиях его возникновения и в дальнейшем установить взаимосвязь закономерности изменения статистических параметров потоков данных и типом проводимого воздействия.

3. Разработанная модель позволяет имитировать воздействие деструктивных потоков данных на управляющие узлы в технологической сети промышленного предприятия, а выбранные для определения факта воздействия статистические параметры отражают ход воздействия и могут быть использованы для определения начала воздействия деструктивных потоков данных на малопроизводительном узле.

3. ПРОГНОЗИРОВАНИЕ ПОСЛЕДСТВИЙ ВОЗДЕЙСТВИЯ ДЕСТРУКТИВНЫХ ПОТОКОВ ДАННЫХ НА УПРАВЛЯЮЩИЕ УЗЛЫ ТЕХНОЛОГИЧЕСКИХ СЕТЕЙ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

3.1 Разработка иерархической модели воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия

Проведенный статистический анализ параметров потоков данных послужил основой построения иерархической модели воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия, отражающей параметры и свойства деструктивных потоков, начиная от момента его генерации источником и заканчивая состоянием узла-цели, что позволяет не только сделать вывод о типе воздействия, но и спрогнозировать его исход, основываясь на его параметрах. Разработанная модель имеет 6 иерархических уровней [9, 25, 33, 138].

Первый уровень модели

На первом уровне иерархической модели воздействия деструктивных потоков данных представлен узел-источник A в случае воздействия, реализуемого при помощи одного узла, или распределенный источник $\sum_{i=2}^{N} A_i$, состоящий из N узлов в случае распределенного воздействия. В зависимости от принципа работы программного обеспечения, установленного на источнике, деструктивный поток может иметь различное количество пакетов $N_{\text{ген}}$, генерируемых в единицу времени $T_{\text{ген}}$, причем $T_{\text{ген}}$ также задается программным обеспечением.

$$M_{\text{ген}} = N_{\text{ген}} \cdot T_{\text{ген}}\ , \qquad (1)$$

где $M_{\text{ген}}$– объем деструктивных потоков данных, отправляемых в сторону узла-цели B, или эффективность источника [80, 82].

До узла-цели доходят не все вредоносные пакеты, сгенерированные узлами/узлом *A*, т.к. часть их теряется при передаче по каналам связи. Поэтому к узлу-цели приходит объем деструктивных потоков данных, равный $M_{\text{Ц}}$, который можно получить, зная объем сгенерированных деструктивных потоков данных $M_{\text{ген}}$ и объем потерянных пакетов ΔM.

$$M_{\text{Ц}} = M_{\text{ген}} - \Delta M. \quad (2)$$

Так как $\Delta M \to 0$ в сравнении с $M_{\text{ген}}$, можно говорить о том, что:

$$M_{\text{Ц}} \cong M_{\text{ген}}. \quad (3)$$

Скорость V_T прохождения вредоносных пакетов от узла/узлов источника до узла *B* также напрямую зависит от работы каналов связи, т.е. от среды передачи данных, и чем выше данная скорость, тем больше скорость поступления деструктивных потоков данных.

Таким образом, интенсивность воздействия $\vec{p}$ узлов/узла *A* на узел *B* можно посчитать аналогично физическому понятию импульса тела:

$$\vec{p} = M_{Ц} \cdot \vec{V}_T, \quad (3)$$

где $\vec{p}$ - воздействие узла/узлов (*A)* на узел (*B).*

Второй уровень модели

На втором уровне иерархической модели деструктивных потоков данных, представлены динамические параметры деструктивных потоков, а именно скорости (V_{const} , V_{var}) поступления пакетов к узлу (B), определяющие количество пакетов (N) в единицу времени (t). Скорость поступления вредоносных пакетов к узлу (B) может варьироваться и ограничивается скоростью работы каналов связи. Источник генерирует пакеты с определенной периодичностью и интенсивностью поступления, и данный процесс можно описать, используя функции распределения количества пакетов (N) в единицу времени (t).

По изменению динамических параметров потоков данных воздействия можно классифицировать следующим образом:

- Воздействия с постоянной скоростью – это тип воздействий (рисунок

38) при которых количество пакетов (N) относительно постоянно. Т.е.: $\sigma(N) = \sqrt{\frac{(N(t)-\bar{N})^2}{t}} \to 0; => \frac{\Delta N}{\Delta t} \to 0 \; \forall t$, где $\Delta N = N_{max} - N_{min}$.

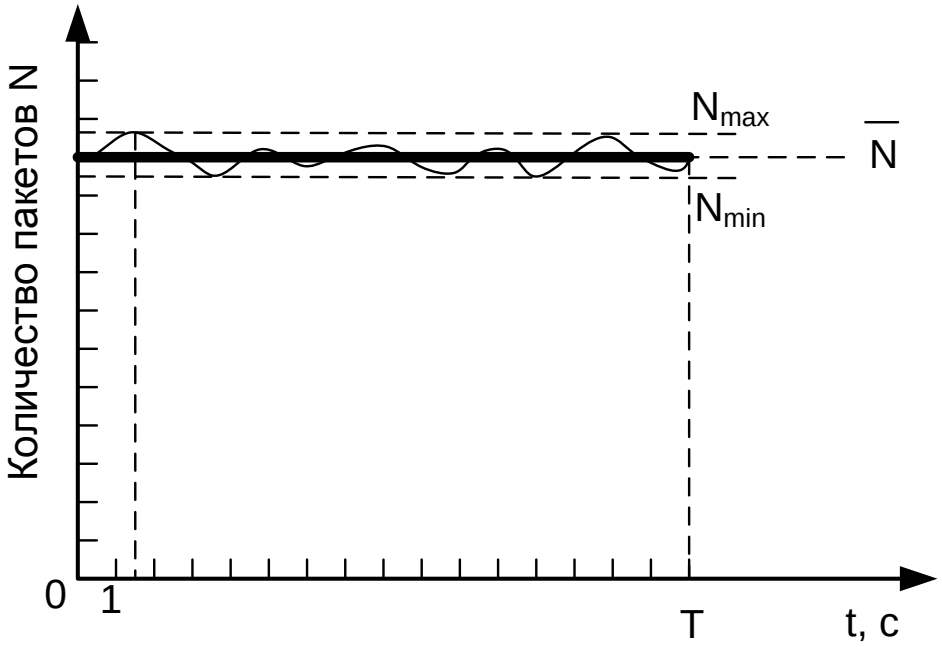


Рисунок 38 - Постоянная скорость деструктивных потоков данных

Воздействие с постоянной скоростью используется для заполнения канала деструктивным потоком данных и, как следствие, происходит либо затруднение, либо полная блокировка доступа к узлу (B) в зависимости от характера функции [92].

- Воздействия с непостоянной скоростью характеризуются изменением скорости поступления вредоносных пакетов с течением времени. Их можно классифицировать по динамике изменения скорости:
  - Воздействия с увеличением скорости – увеличение может происходить по любой функции N=f(t) (Рисунок 39).

Таким образом $N = f(t) + a; => \frac{\Delta N}{\Delta t} \gg 0$; где a - среднее количество пакетов при нормальной сетевой нагрузке.

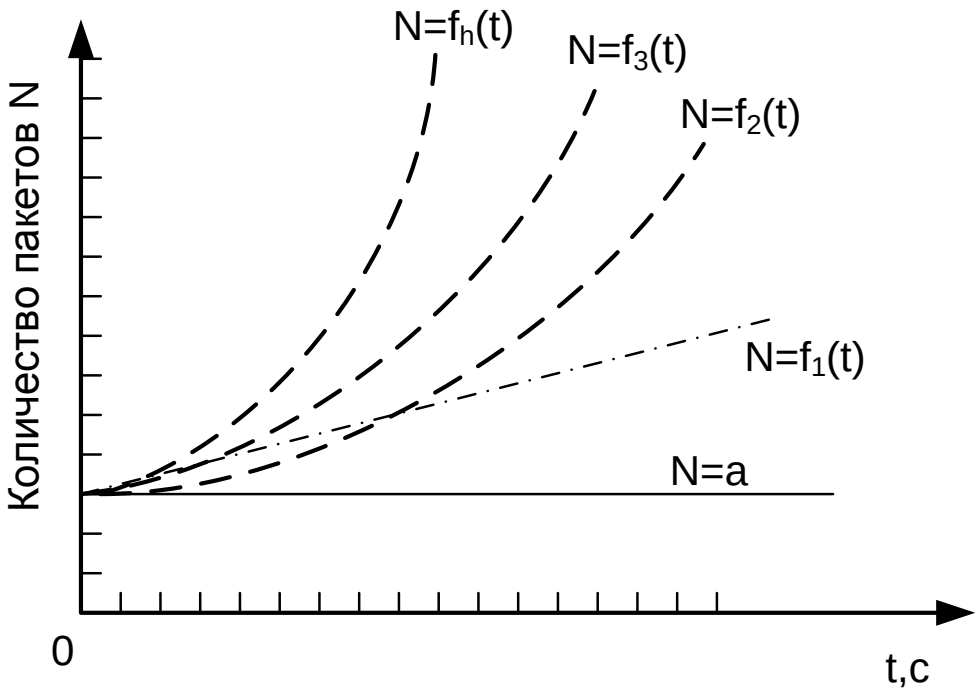


Рисунок 39 - Воздействие с увеличением скорости деструктивных потоков данных

- Воздействия с переменной скоростью, в которых скорость может регулярно падать, вплоть до полного исчезновения вредоносных пакетов из среды передачи данных. Именно такой тип наиболее сложно поддается идентификации.

Воздействия деструктивных потоков данных на управляющие узлы, осуществляемые с переменной скорость, можно разделить на простые пульсирующие и пульсирующие воздействия с возрастающей скоростью в зависимости от характера функции тренда.

Для простого пульсирующего воздействия деструктивных потоков данных на управляющие узлы технологической сети характерна высокая периодичность и наличие трендовой составляющей. Такое воздействие можно описать как

$$N = -cos(t) + \xi(t), \quad (4)$$

где $\xi(t)$ – тренд воздействия, N=a - среднее количество пакетов при нормальной сетевой нагрузке. (Рисунок 40).

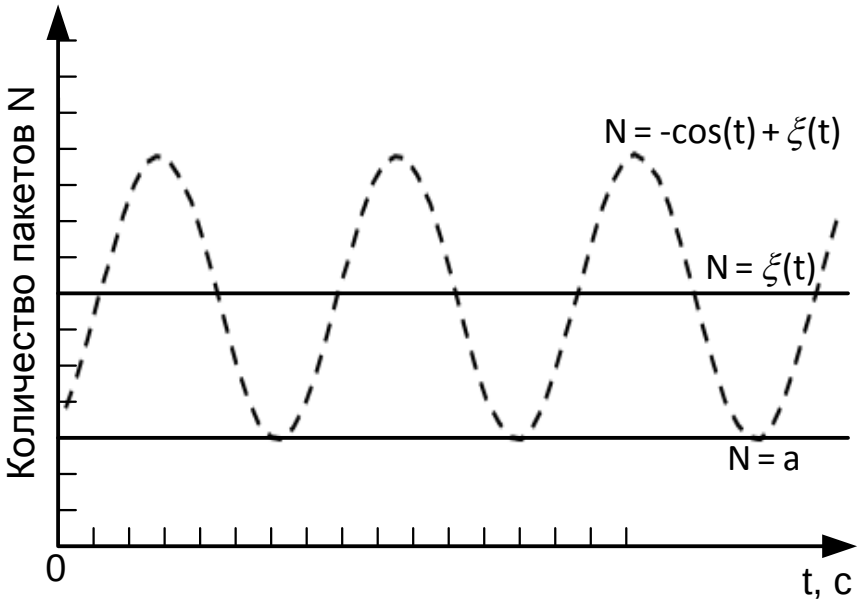


Рисунок 40 - Простая пульсирующая скорость деструктивного потока данных

Для воздействия с переменной увеличивающейся скоростью деструктивных потоков данных характерна высокая периодичность и возрастающий тренд. Пример такого воздействия можно описать как в предыдущем случае $N = -cos(t) + \xi(t)$, но в этом случае $\xi(t)$ - возрастающая функция тренда. При этом N=a - также среднее количество пакетов при нормальной сетевой нагрузке (Рисунок 41).

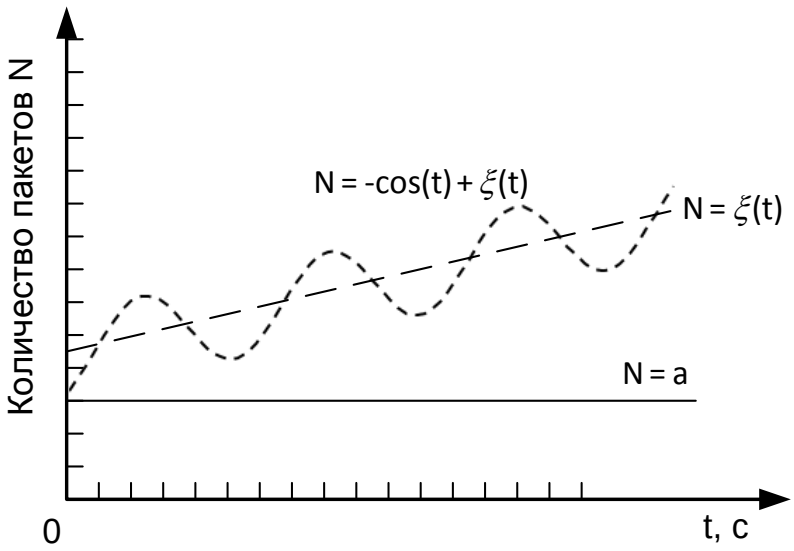


Рисунок 41 - Переменная увеличивающаяся скорость деструктивного потока данных

Третий уровень модели

На третьем уровне иерархической модели воздействия деструктивных потоков данных представлены статистические параметры (скорость потоков данных, ускорение потоков данных, пуассоновский поток данных, энтропия, параметр Херста, задержка, скорость изменения задержки), позволяющие классифицировать поток данных как деструктивный при условии превышения пороговых значений данных параметров [73, 84].

Четвертый уровень модели

На четвертом уровне иерархической модели воздействия деструктивных потоков данных представлены возможные виды воздействий (на уязвимость, деструктивная интенсификация потоков данных) при которых производится классификация по направленности воздействия.

Если при организации воздействия деструктивных потоков данных на управляющий узел использованы уязвимости в протоколе или в приложениях, а также логические ошибки, то имеет место воздействие на уязвимость (Рисунок 42). Для организации воздействия на уязвимость проводятся предварительные исследования управляющего узла *B* на предмет наличия уязвимостей и целенаправленного формирования эффективной модели нарушителя, а в дальнейшем производится таргетированная массовая отсылка запросов, эксплуатирующих обнаруженную уязвимость. Для успешной организации воздействия данного вида объем деструктивных потоков данных может быть на порядки ниже, чем при деструктивной интенсификации потоков данных [59, 102].

В случае, если воздействие деструктивных потоков данных на управляющий узел технологической сети промышленного предприятия не имеет характерных особенностей, а представляет собой массовую отсылку пакетов узлу-цели, то имеет место деструктивная интенсификация. Для организации деструктивной интенсификации потока данных предварительное исследование узла (B) не проводится, а эффективность воздействия напрямую зависит от количества узлов-источников при распределенном воздействии или вычислительной мощности одного узла-источника (Рисунок 43).

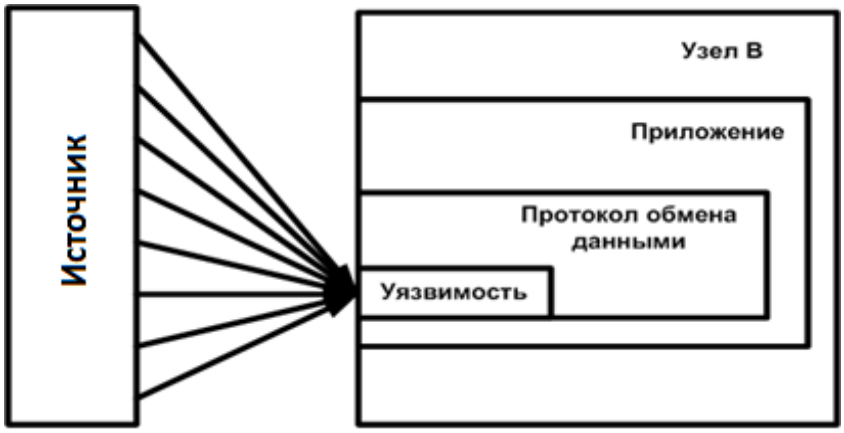


Рисунок 42 - Воздействие деструктивных потоков данных на уязвимость

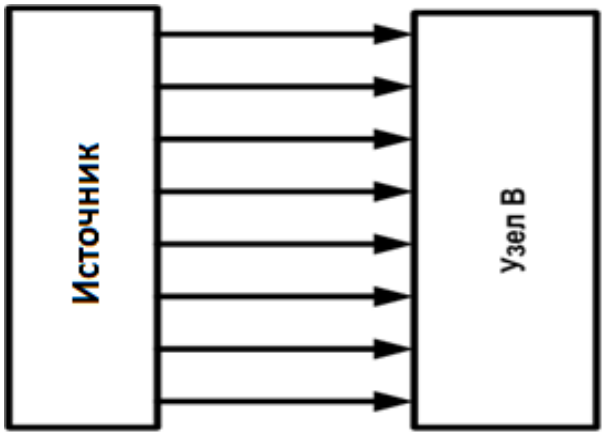


Рисунок 43 – Деструктивная интенсификация потоков данных на управляющий узел технологической сети

Для установления взаимосвязей и закономерностей изменения статистических параметров потоков данных, а также вида воздействия использовались элементы теории нечетких множеств и нечеткой логики. С этой целью введены лингвистические переменные «интенсификация», «воздействие на уязвимость», «нормальное состояние сети». При этом совокупность значений лингвистической переменной x_l образует терм-множество «параметр потока данных», а исходная переменная x называется базовой. Переход от абсолютных значений базовой переменной x к соответствующим значениям лингвистической переменной нелинеен и различным термам могут соответствовать разные диапазоны базовой переменной. На рисунке 47 представлены функции принадлежности $\mu(x)$ в треугольной форме, образующие терм-множество

«скорость потока данных», при этом μ_N определяет терм «нормальное состояние сети», μ_U определяет терм «воздействие на уязвимость», μ_F определяет терм «интенсификация» для статистического параметра – скорость потока данных [57, 120, 123, 125].

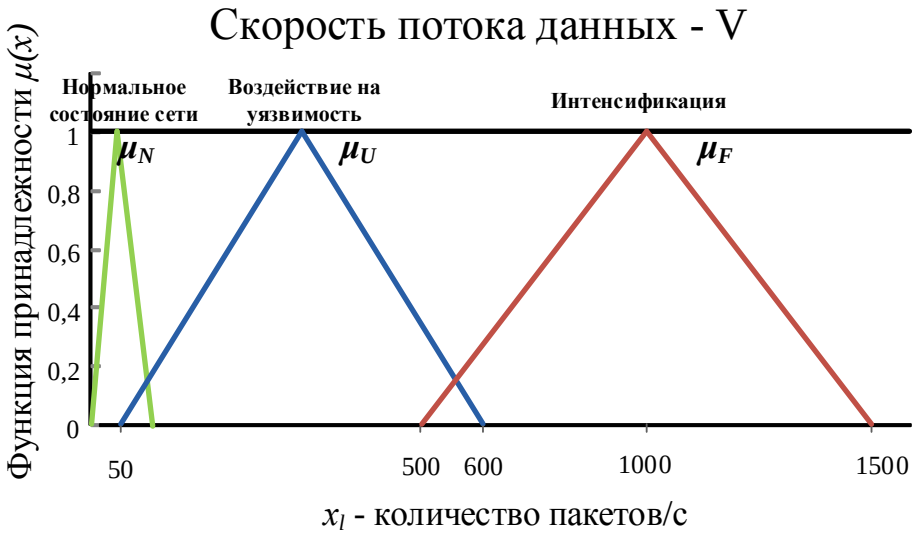


Рисунок 44 - Функция принадлежности $\mu(x)$ для скорости потока данных (V)

Заключительная процедура сводится к определению точного воздействия y и выполняется чаще всего по методу поиска центра площади, согласно которому для некоторой непрерывной результирующей функции принадлежности $\mu_p^*(y)$ искомое значение воздействия определяется как абсцисса центра тяжести площади фигуры, образованной этой функцией и осью y, а именно: $y^* = \int y\mu_p^*(y)dy / \int \mu_p^*(y)dy$. Здесь коэффициенты значимости для воздействия на уязвимость и интенсификации K_f определяются как $K_u / (K_f) = 1 - \frac{S_{пер}}{S_U / (S_f)}$, где – S_U, S_f площадь треугольника, построенного по значениям воздействия на уязвимость, а $S_{пер}$ – площадь пересечения треугольников, построенных по значениям обоих видов воздействий.

Таким образом определяются коэффициенты значимости каждого статистического параметра потока данных при различных видах внешнего

воздействия K_u и K_f на узлы технологической сети промышленного предприятия (рисунок 45-46).

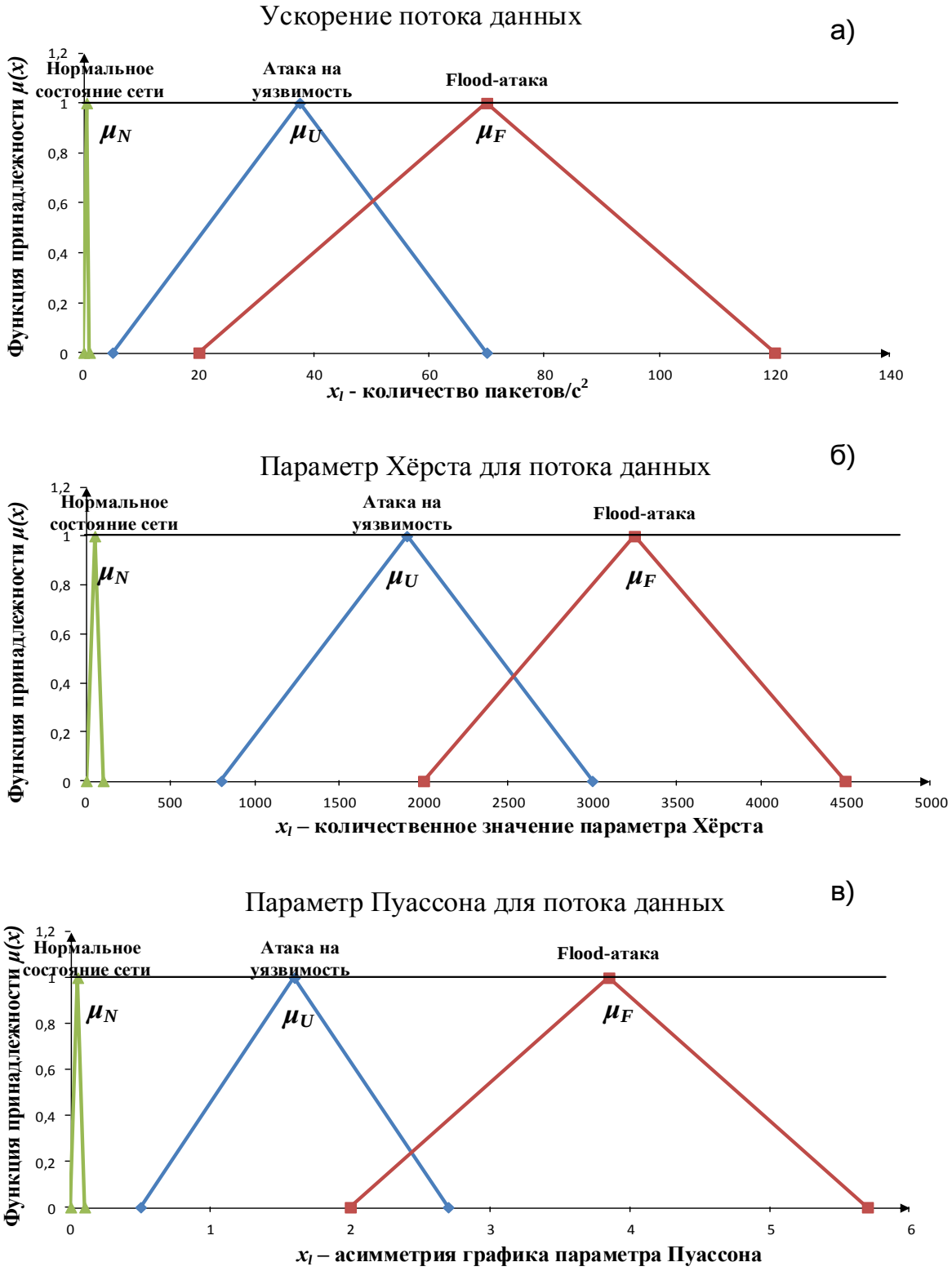


Рисунок 45 - Функция принадлежности $\mu(x)$ для ускорения (а), параметров Хёрста (б) и Пуассона (в) для потока данных

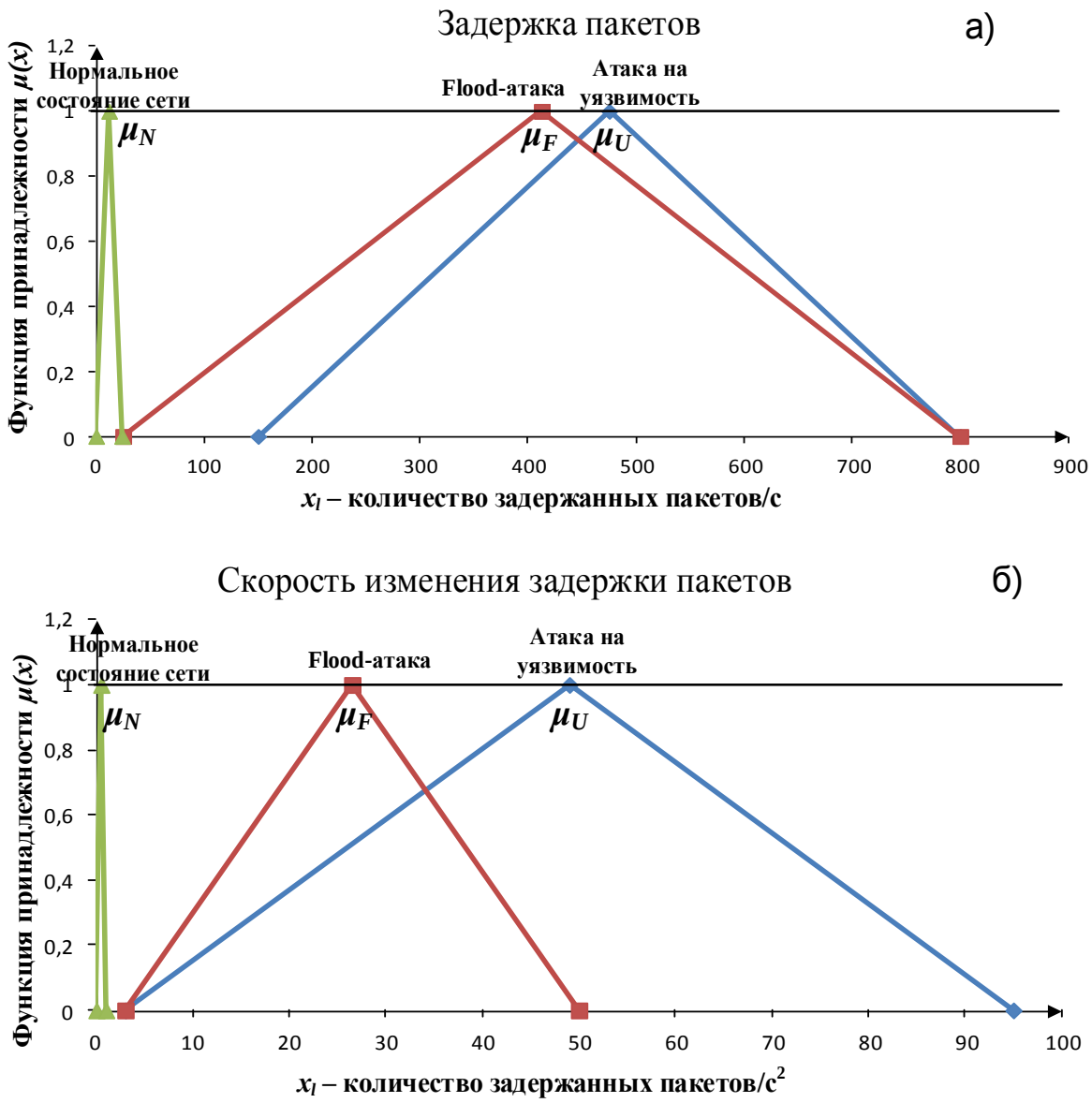


Рисунок 46 - Функция принадлежности $\mu(x)$ для задержки пакетов (а) и скорости изменения задержки пакетов (б)

При определении коэффициента значимости энтропии потока данных в качестве лингвистической переменной x_l используется время, через которое энтропия снизится до нуля. Так как при нормальном состоянии сети энтропия варьируется в некоторых постоянных пределах и не снижается до нуля, в терм-множество «энтропия» не вошла функция принадлежности μ_N определяющая терм «нормальное состояние сети», в остальном определение коэффициента не изменяется (рисунок 47) [132].

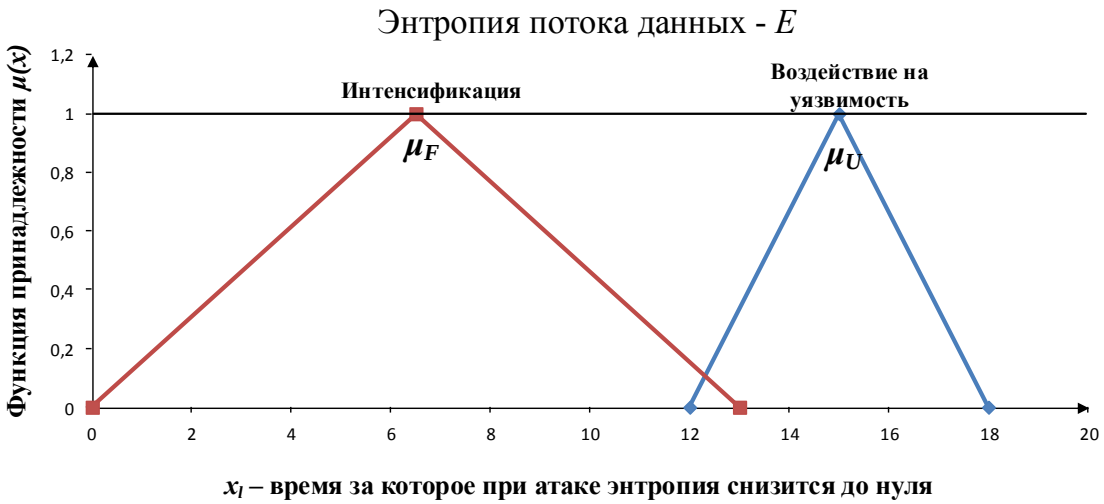


Рисунок 47 - Функция принадлежности $\mu(x)$ для энтропии потоков данных (E)

Полученные коэффициенты значимости для статистических параметров потока данных при воздействии деструктивных потоков данных на уязвимость и интенсификация (K_U, K_f) приведены в таблице 2.

Таблица 2 - Коэффициенты значимости статистических параметров

№	Параметры потока данных	K_U	K_f
1	Скорость потоков данных	0,91	0,96
2	Ускорение потоков данных	0,41	0,66
3	Параметр Хёрста для потоков данных	0,85	0,87
4	Параметр Пуассона	0,91	0,95
5	Энтропия потоков данных	0,95	0,98
6	Задержка пакетов	0,43	0,39
7	Скорость изменения задержки пакетов	0,64	0,30

Для определения вида воздействия необходимо для каждого статистического параметра потока данных вычислить параметры воздействия $A_U = \frac{S_{AU}}{S_U}$; $A_f = \frac{S_{Af}}{S_f}$, где S_{AU} и S_{Af} - площади фигур, образованных термом μ_q «определяемого воздействия» (рисунок 48). Таким образом определяется по два

параметра воздействия для каждого статистического параметра деструктивного потока данных [120].

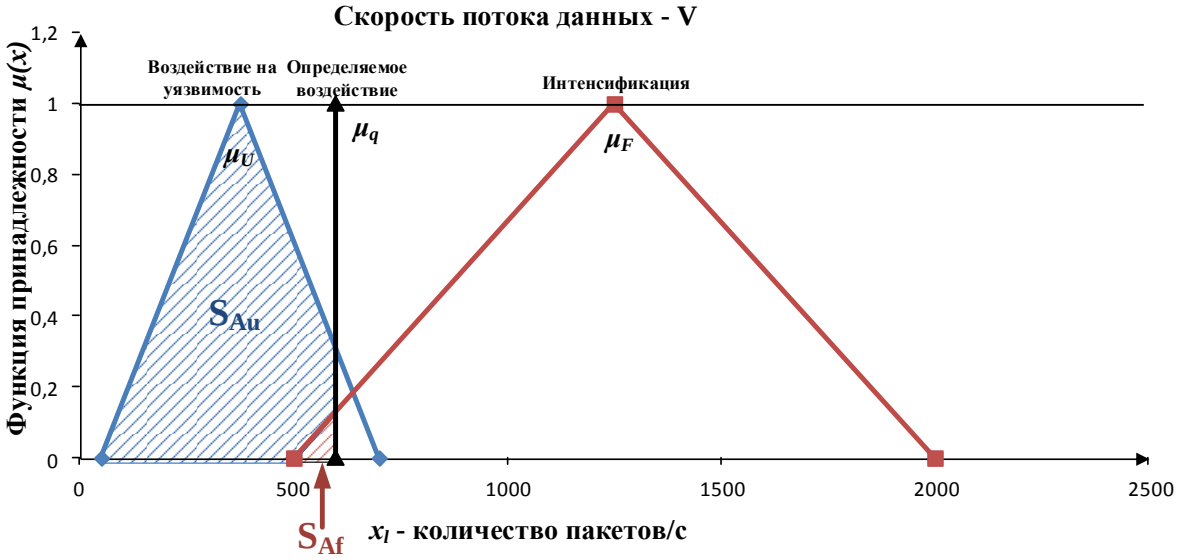


Рисунок 48 - Определение вида воздействия деструктивных потоков данных на управляющие узлы технологической сети

Далее необходимо решить задачу распознавания образа воздействия деструктивных потоков данных, а именно классифицировать ее как деструктивную интенсификацию, если верно:

$$\begin{cases} d_U = \sum_{i=1}^{7} K_{Ui} A_{Ui}, \\ d_f = \sum_{i=1}^{7} K_{fi} A_{fi}, \\ d_U < d_f. \end{cases}$$

И как воздействие на уязвимость если верно:

$$\begin{cases} d_U = \sum_{i=1}^{7} K_{Ui} A_{Ui}, \\ d_f = \sum_{i=1}^{7} K_{fi} A_{fi}, \\ d_U > d_f. \end{cases}$$

Что дает возможность идентифицировать вид воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия на базе установленных взаимосвязей статистических параметров потоков данных.

Пятый уровень модели

На пятом уровне модели представлены уровни модели OSI, на которых может быть реализовано воздействие. В основе архитектуры технологических сетей, несмотря на отличающуюся структуру, функции и реализацию, как и в корпоративных сетях, лежит модель OSI. Вид пакетов, составляющих деструктивный поток данных, зависит от используемого протокола, а, следовательно, от уровня воздействия (Таблица 3).

Таблица 3 - Модель OSI (Open Systems Interconnection basic reference model - базовая эталонная модель взаимодействия открытых систем)

Тип данных	Уровень	Функции	Протоколы
Биты	Физический	Взаимодействие со средой передачи данных, сигналами и двоичными данными	IEEE 802.15 (Bluetooth), IRDA, EIA RS-232, EIA-422, EIA-423, RS-449, RS-485, DSL, ISDN, SONET/SDH, 802.11 Wi-Fi, Etherloop, GSM Um radio interface, ITU и ITU-T, TransferJet[en], ARINC 818, G.hn/G.9960
Кадры	Канальный	Физическая адресация	ARCnet, ATM, CAN, Econet, IEEE 802.3 (Ethernet), EAPS, FDDI, Frame Relay, HDLC, IEEE 802.2, LAPD, IEEE 802.11 wireless LAN, LocalTalk, MPLS, PPP, PPPoE, StarLan, Token ring, UDLD, x.25, ARP.
Пакеты	Сетевой	Определение маршрута и логическая адресация	IP/IPv4/IPv6, IPX, X.25 CLNP, IPsec, Протоколы маршрутизации — RIP, OSPF, BGP

Продолжение табл. 3

Сегменты	Транспортный	Связь между конечными пунктами, надежность доставки	ATP, CUDP, DCCP, FCP, NBF, NCP, SCTP, SPX, SST, TCP, UDP
Данные	Сеансовый	Управление сеансом связи	ADSP, ASP, H.245, ISO-SP (OSI Session Layer Protocol (X.225, ISO 8327)), iSNS, L2F, L2TP, NetBIOS, PAP, PPTP, RPC, RTCP, SMPP, SCP, ZIP, SDP
	Представления	Представление и кодирование	AFP, ICA , LPP , NCP , NDR , XDR , X.25 PAD .
	Прикладной	Доступ к сетевым службам	RDP, HTTP, SMTP, SNMP, POP 3, FTP, XMPP, OSCAR, Modbus, SIP, TELNET и другие

Первый уровень модели OSI является физическим, тип данных передаваемый посредством этого уровня – биты. На этом уровне происходит передача двоичных данных, и любые воздействия на этом уровне сводятся к физическому разрушению или физическому препятствию корректной работе. Для организации воздействия деструктивных потоков данных на управляющие узлы технологических сетей промышленных предприятий данный уровень не используется, и не будет отражен в иерархической модели воздействия [17, 46].

Второй уровень модели OSI является канальным, тип данных передаваемый посредством этого уровня – кадры. На этом уровне производится установка и сопряжение передачи сообщений на физическом уровне (протоколы 802.3б 802.5). При воздействии деструктивных потоков данных на управляющие узлы технологических сетей промышленных предприятий на этом уровне используется MAC-flood для переполнения пакетами данных сетевых коммутаторов. Для уменьшения ущерба от воздействия на этом уровне в корпоративных сетях используются коммутаторы, настроенные на работу только с доверенными MAC-адресами, которые проходят проверку аутентификации, авторизации и учета на сервере (протокол AAA). Использовать подобный подход в технологической сети промешенного предприятия, чаще всего не

представляется возможным, в силу особенностей ее структуры и реализации [17, 46].

Третий уровень модели OSI является сетевым, тип данных передаваемый посредством этого уровня – пакеты. На этом уровне функционируют протоколы маршрутизации и передачи информации между разными сетями или сегментами сети - IP, ICMP, RIP, OSPF, BGP и т.д. При воздействии деструктивных потоков данных на управляющие узлы технологических сетей промышленных предприятий на этом уровне, как и на 4 уровне, используется деструктивный интенсификация, но, в отличии от 4 уровня, целью воздействия на третьем уровне является снижение пропускной способности сети в целом. Уменьшить ущерб можно, ограничив количество обрабатываемых узлом запросов, но это не повлияет на заполнение линий передачи данных вредоносными пакетами [17, 46].

Четвертый уровень модели OSI является транспортным, на этом уровне функционируют протоколы, обеспечивающие передачу сообщений между узлами. Тип данных передаваемых на этом уровне – сегменты. При воздействии деструктивных потоков данных на управляющие узлы технологических сетей промышленных предприятий на этом уровне поток данных представляет собой различные варианты деструктивной интенсификации, целью организации которой является достижение предела по пропускной способности канала или по количеству допустимых подключений к управляющему узлу. Также могут произойти нарушения в работе оборудования, как устранимые, так и неустранимые. Для предотвращения этих последствий в корпоративных сетях применяют фильтрацию потока данных, что в условиях технологических сетей либо невозможно в силу особенностей реализации, либо повлечет за собой реконфигурацию, усложнение структуры и, как следствие, неоправданное удорожание как реализации, так и дальнейшего обслуживания [17, 46].

Пятый уровень модели OSI является сеансовым, тип данных передаваемый посредством этого уровня – данные, управляющие установкой и завершением соединения, а также синхронизацией сеансов связи через сеть. На этом уровне функционируют протоколы для удаленного управления, а именно:

удаленного вызова процедур RPC, протокол простой проверки подлинности, предусматривающий отправку имени пользователя и пароля на сервер удалённого доступа открытым текстом PAP. При воздействии деструктивных потоков данных на управляющие узлы технологических сетей промышленных предприятий на этом уровне чаще всего производится эксплуатация уязвимости программного обеспечения управляющего узла. Как следствие этих воздействий можно отметить невозможность администрирования узла. Проблема уязвимостей в программном обеспечении управляющих узлов технологических сетей промышленных предприятий на сегодняшний момент или не рассматривается, или ей уделяется крайне небольшое внимание, так как при разработке основная ставка делается на организацию требуемого технологического процесса [17, 46].

Шестой уровень модели OSI является представительским, тип данных, передаваемый посредством этого уровня – данные, транслируемые от источника к получателю. При воздействии деструктивных потоков данных на управляющие узлы технологических сетей промышленных предприятий на этом уровне используются фальшивые запросы, так как проверка шифрованных пакетов очень истощает ресурсы. Как следствие этих воздействий можно отметить прекращение принятия запросов узлом жертвой, или его автоматическую перезагрузку. Для уменьшения ущерба от воздействий на этом уровне в корпоративных сетях применяют распределение шифрующей инфраструктуры с выделением отдельного сервера для шифрования, а также производят мониторинг потока данных приложений на предмет аномалий. В технологических сетях промышленных предприятий усложнение структуры дополнительными управляющими узлами, в функции которых войдет исключительно шифрация данных передаваемых по технологической сети, в большинстве случаев, нереализуема в виду структурной организации сети [17, 46, 90].

Седьмой уровень модели OSI является прикладным, тип данных передаваемый посредством этого уровня это данные приложений. Воздействия деструктивных потоков данных на управляющие узлы технологических сетей промышленных предприятий, использующие этот уровень, имеют характерные

черты, например, к ним можно отнести GET запросы. Как следствие этих воздействий можно отметить чрезмерное потребление ресурсов службами на узлецели. Для выявления такого рода воздействий необходимо постоянно отслеживать состояние программного обеспечения, с использованием алгоритмов и подходов в зависимости от платформы, на которой это ПО установлено. Установить факт воздействия деструктивных потоков данных можно исключительно с помощью технологий, выявляющих уязвимости (0day-уязвимости) программного обеспечения и при постоянном мониторинге состояния сети. При обнаружении уязвимость устраняется, что в последствии предотвращает успешное выполнение воздействие деструктивных потоков данных. Однако ПО, устанавливаемое на управляющих узлах технологических сетей промышленных предприятий, крайне редко обновляется производителями, а сам процесс обновления требует остановки технологического процесса. Кроме того, он бывает не реализуем в силу конфигурации программных и аппаратных средств технологической сети или требует физической замены управляющих узлов на более современные модели [17, 46].

В таблице 4 представлены примеры и последствия воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия согласно уровням модели OSI.

Таблица 4 - Последствия воздействий

Уровень модели OSI	Протоколы уровня	Пример воздействия	Последствия
Прикладной	RDP, HTTP, SMTP, SNMP, POP3, FTP, XMPP,OSCAR ,Modbus, SIP, TELNET и др.	PDF GET запросы, HTTP GET, HTTP POST	Чрезмерное потребление ресурсов службами на узле-цели

Продолжение табл. 4

Представительский	Протоколы сжатия и кодирования данных (ASCII, EBCDIC)	Фальшивые запросы	Прекращение принятия запросов узлом-целью, или его автоматическую перезагрузку
Сеансовый	Протоколы входа/выхода (RPC, PAP)	Эксплуатация уязвимости программного обеспечения, например	Невозможность осуществлять администрирование узла
Транспортный	TCP, UDP	Различные варианты интенсификации	Достижение предела по пропускной способности канала или по количеству допустимых подключений к серверу
Сетевой	IP, ICMP, ARP, RIP, OSPF, BGP и т.д	Различные варианты интенсификации	Снижения пропускной способности сети в целом
Канальный	протоколы 802.3, 802.5	Интенсификация MAC-ответ	Переполнение пакетами данных сетевых коммутаторов
Физический	100BaseT, 1000 Base-X	Не используется	Не используется

Шестой уровень модели

На шестом уровне иерархической модели фиксируется возможное состояние узла-цели *B* после успешного проведения воздействия деструктивных потоков данных. При направленного воздействия может преследоваться одна из

двух целей: истощение канала связи узла B с остальными узлами сети либо истощение вычислительных ресурсов узла B.

3.2 Прогнозирование последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия

Связи между уровнями иерархической модели воздействий деструктивных потоков данных сформированы на основе анализа статистических данных по проводимым воздействиям, а также исходя из специфики работы каналов передачи данных в технологических сетях промышленного предприятия. При этом сформирована иерархическая модель (рисунок 49), которая позволяет спрогнозировать исход того или иного вида воздействий деструктивных потоков данных, а набор связей формируют правила осуществления воздействия. На каждом уровне, за исключением связей с третьим, может быть одна связь в зависимости от характера деструктивных потоков данных [50, 51, 85, 116].

Анализ потоков данных на втором и третьем уровнях иерархической модели позволяет сделать вывод о начале воздействия деструктивных потоков данных и своевременно принять меры по предотвращению последствий воздействий. Основываясь на анализе динамических и статистических параметров, проходящих в технологической сети потоков данных, можно определить начало воздействия. При этом отсутствует необходимость ожидания полноценной эксплуатации уязвимости технологической сети или реализации интенсификации потоков данных и рассмотрения протоколов обмена данными по отношению к уровню модели OSI. В этой связи своевременно принятые меры позволят избежать перехода узла-цели в состояние отказа в обслуживании.

На четвертом–шестом уровнях производится анализ рисковых событий и прогнозирование состояния узла от успешно реализованного направленного

воздействия деструктивных потоков данных в технологических сетях промышленного предприятия [66].

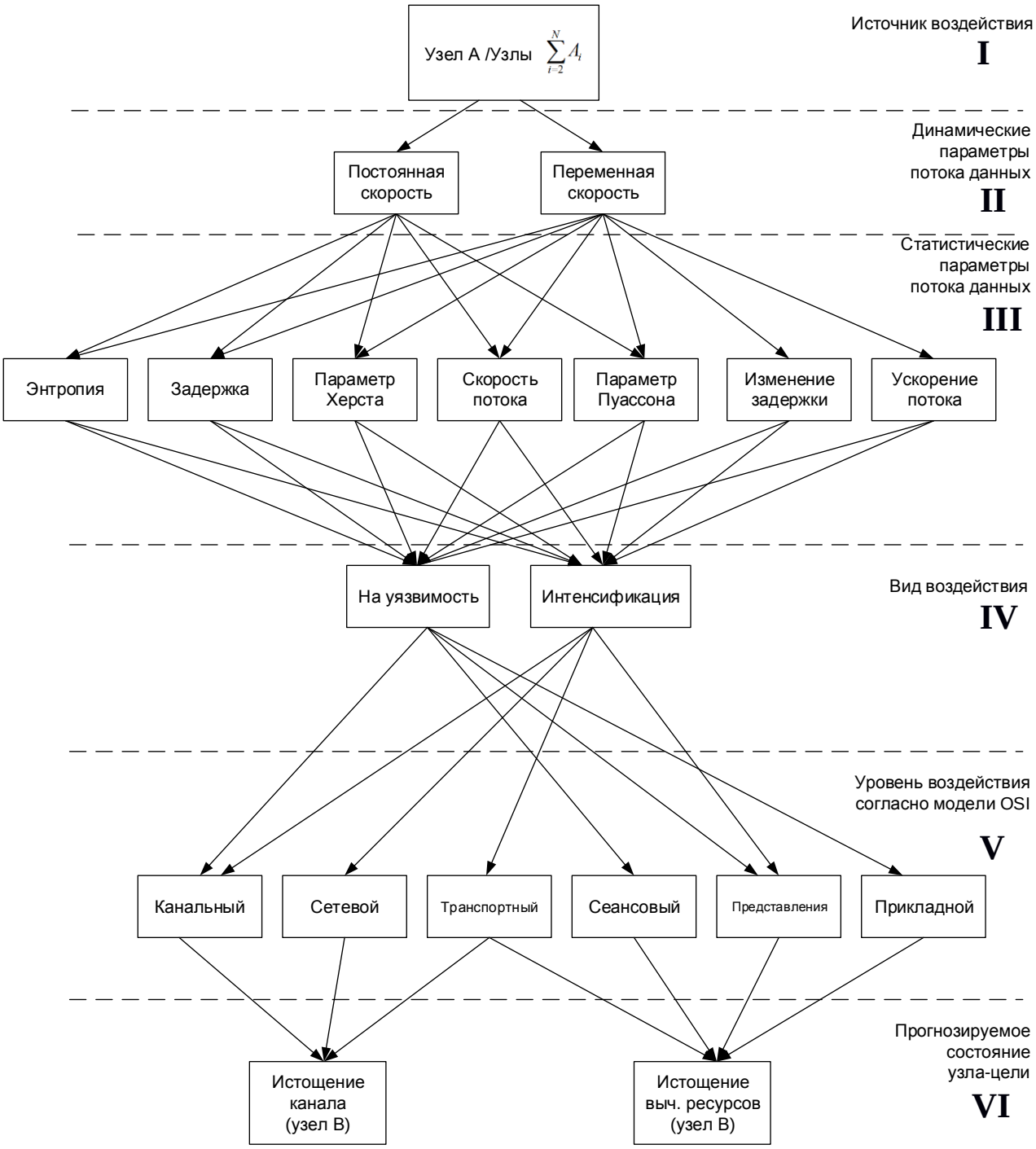
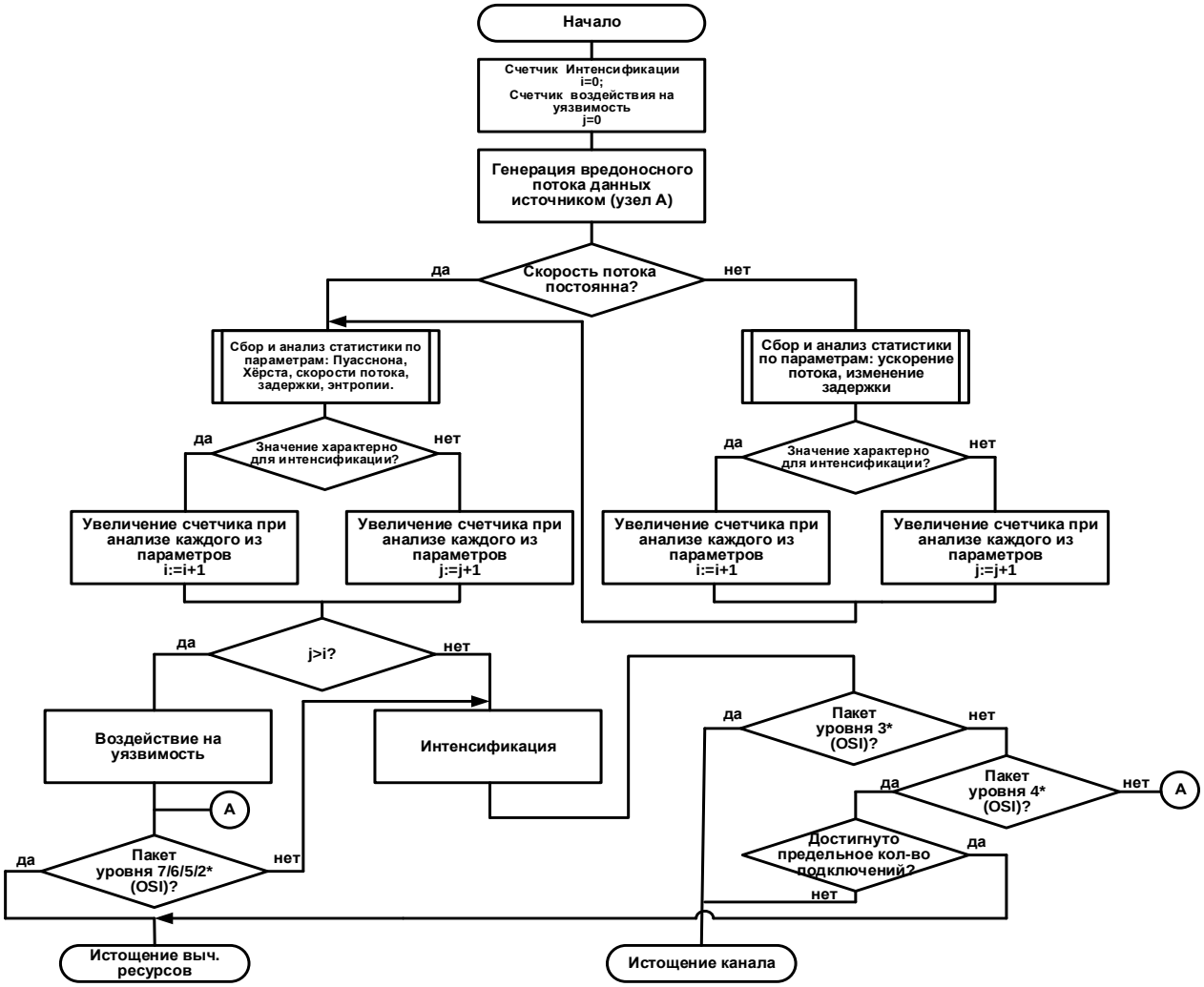


Рисунок 49 - Иерархическая модель воздействия деструктивных потоков данных на управляющие узлы технологической сети

Данная модель универсальна и может применяться для прогнозирования исхода воздействий деструктивных потоков данных на управляющие узлы как в технологических сетях, так и в корпоративных [31, 103, 105].

3.2.1 Разработка алгоритма прогнозирования последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия

На основе системы правил, составленных при построении иерархической модели, был разработан алгоритм прогнозирования последствий воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия (рисунок 50, Б.1, Б.2).



* Уровни модели OSI: 7 - прикладной уровень; 6 – уровень представления; 5 - сеансовый уровень; 4 - транспортный уровень; 3 - сетевой уровень; 2 - канальный уровень; 1 - физический уровень(не рассматривается).

Рисунок 50 - Алгоритм прогнозирования последствий воздействия деструктивных потоков данных на управляющие узлы технологической сети

Пороговые значения статистических параметров, используемые в качестве условий перехода, могут быть определены посредством нагрузочного тестирования [68, 109, 146].

3.2.2 Прогнозирование существующих воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия на основе графовой модели

Для прогнозирования отдельно взятого типа воздействия деструктивных потоков данных иерархическую модель можно представить в виде направленного графа (рисунок 51) [61, 79, 122, 124].

Если (V) - множество вершин, где начальная вершина (V1) - источник воздействия, (V19) и (V20) - конечные вершины - прогнозируемое состояние узла (B) (истощение канала и истощение вычислительных ресурсов соответственно), а (X) - множество ребер (таблица 5), тогда граф будет иметь вид [43, 48, 113, 114]:

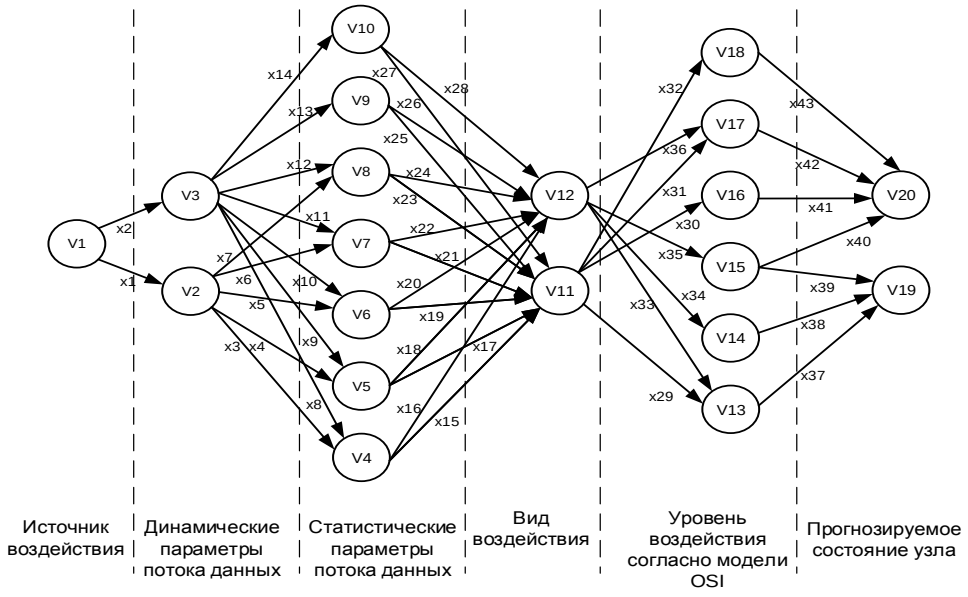


Рисунок 51 - Направленный граф воздействия деструктивных потоков данных на управляющие узлы технологической сети

Каждому уровню иерархической модели воздействия деструктивных

потоков данных на управляющие узлы технологической сети промышленного предприятия соответствует подмножество вершин (L1,L2,L3,L4,L5,L6) принадлежащих множеству (V):

$$L1 = \{V1\}, L1 \subset V;$$
$$L2 = \{V2, V3\}, L2 \subset V;$$
$$L3 = \{V4, V5, V6, V7, V8, V9, V10\}, L3 \subset V;$$
$$L4 = \{V11, V12\}, L4 \subset V;$$
$$L5 = \{V13, V14, V15, V16, V17, V18\}, L5 \subset V;$$
$$L6 = \{V19, V20\}, L6 \subset V.$$

Таблица 5 - Описание графа воздействия деструктивных потоков данных на управляющие узлы технологической сети

Подмнож-во вершин	Вершины	Ребра	
		Входящие	Исходящие
L1 $\subset$ V	V1	-	X1,X2
L2 $\subset$ V	V2 V3	X1 X2	X3,X4, X5,X6,X7 X8,X9,X10,X11,X12, X13,X14
L3 $\subset$ V	V4 V5 V6 V7 V8 V9 V10	X3, X8 X4, X9 X5, X10 X6, X11 X7, X12 X13 X14	X15,X16 X17,X18 X19,X20 X21,X22 X23,X24 X25,X26 X27,X28
L4 $\subset$ V	V11 V12	X15,X17,X19,X21, X23,X25,X27 X16,X18,X20,X22, X24,X26,X28	X29,X30,X31,X32 X33, X34, X35, X36
L5 $\subset$ V	V13 V14 V15 V16 V17 V18	X29, X33 X34 X35 X30 X31,X36 X32	X37 X38 X39, X40 X41 X42 X43
L6 $\subset$ V	V19 V20	X37, X38, X39 X40, X41, X42, X43	- -

Прохождение по ребрам слева направо описывает сценарий воздействия деструктивных потоков данных на управляющие узлы технологической сети и его последствия, и отражает негативное влияние вредоносного потока данных по мере его продвижения от узла-источника *A* к узлу-цели *B*. Граф позволяет описать

воздействие деструктивных потоков подмножеством ребер [35, 39, 115, 127].

Пример воздействия деструктивных потоков данных на управляющие узлы технологической сети (сценарий №1)

Подмножеством ребер {X1,X4,X17,X32,X43} описывается воздействие, при котором источник *A* отправляет деструктивные пакеты с постоянной скоростью, из-за чего прием и отправка легитимных пакетов на управляющем узле *B* существенно снижается (высокая задержка), воздействие оказывается на уязвимость программного обеспечения узла-цели и проводится на прикладном уровне модели OSI, в силу чего, вычислительные ресурсы управляющего узла *B* истощаются [131, 133].

На подмножестве ребер {X1,X4,X17,X32,X43} и вершинах, которым они инцидентны, можно построить порожденный подграф графа, соответствующий заданным параметрам воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия (рисунок 52).

Пример воздействия деструктивных потоков данных на управляющие узлы технологической сети (сценарий №2)

Подмножеством {X2,X14,X28,X33,X37} описывается воздействие, при котором источник *A* отправляет деструктивные пакеты с постоянной скоростью, из-за чего на управляющем узле *B* наблюдается ускорение потока поступающих данных с течением времени, так как деструктивная интенсификация происходит в потоке пакетов протокола канального уровня модели OSI, происходит постепенное истощение канала [139].

На вышеописанном подмножестве ребер {X2,X14,X28,X33,X37} и вершинах, которым они инцидентны, можно построить порожденный подграф графа, соответствующий заданным параметрам воздействия деструктивных потоков данных на управляющие узлы технологической сети (рисунок 53).

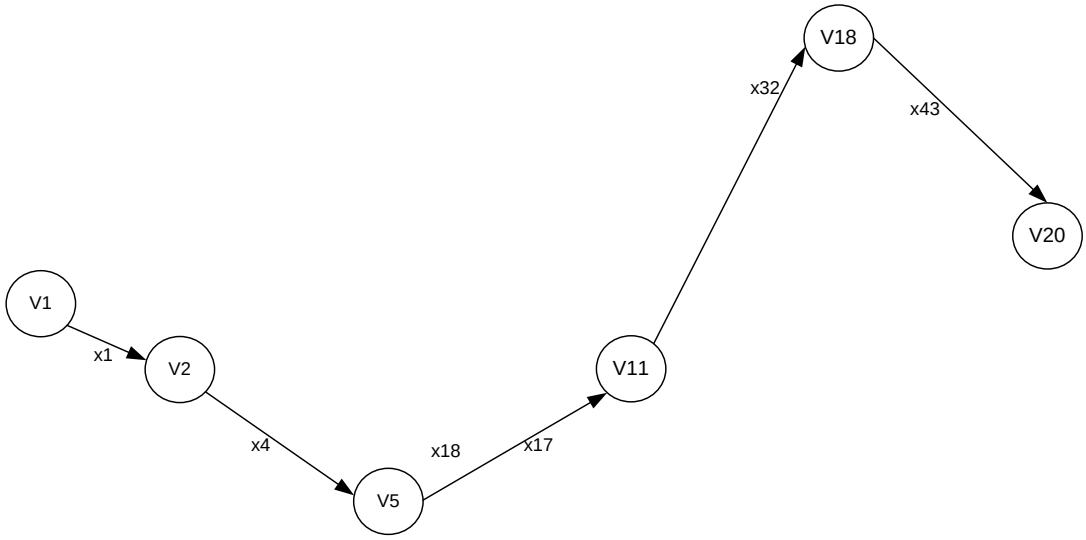


Рисунок 52 - Порожденный подграф графа воздействия деструктивных потоков данных на управляющие узлы технологической сети (сценарий №1)

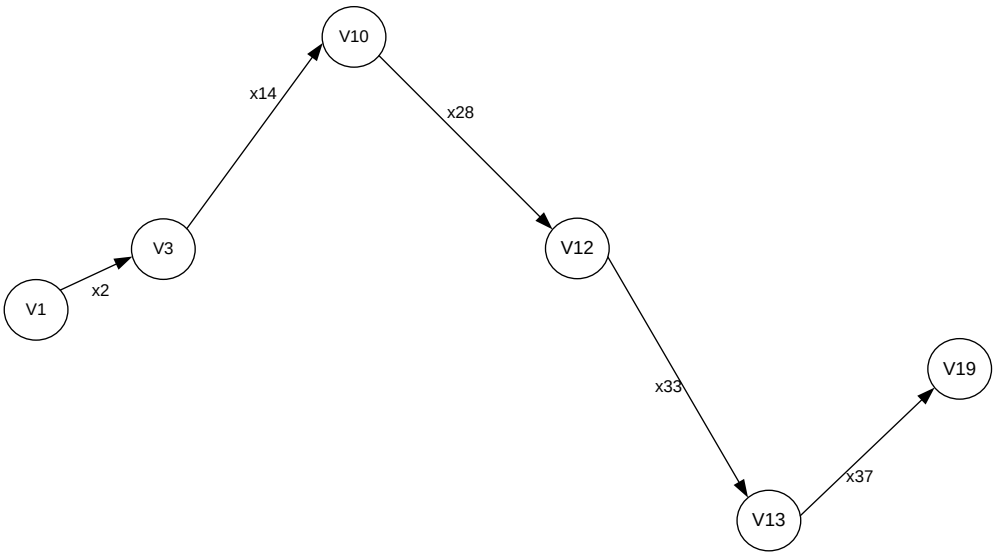


Рисунок 53 - Порожденный подграф графа воздействий деструктивных потоков данных на управляющие узлы технологической сети (сценарий №2)

Граф позволяет прогнозировать исход возможных воздействий деструктивных потоков данных последовательным рассмотрением возможных сочетаний подмножества ребер уровней иерархической модели.

Исследование специфичности возникновения рисковых событий при воздействиях деструктивных потоков данных позволяет прогнозировать состояния узла-цели при успешной реализации воздействия деструктивных потоков данных на управляющие узлы технологической сети [41].

Выводы по главе 3

1. Разработанная шестиуровневая иерархическая модель воздействия деструктивных потоков данных на управляющие узлы учитывает системные связи и закономерности функционирования управляющих узлов технологической сети и позволяет прогнозировать исход воздействий на узлы. Первый уровень характеризует воздействие по виду источника, при разработке иерархической модели на данном уровне отдельное внимание было уделено особенностям работы источника. На втором уровне выделены динамические параметры деструктивных потоков данных, характеризующих воздействие с позиции вариативности скорости поступления вредоносных пакетов. На третьем уровне представлены статистические параметры потока данных, позволяющие на основе выявленных корреляционных взаимосвязей показателей вариации определить начало воздействия деструктивных потоков данных на управляющий узел. На четвертом уровне рассмотрены возможные виды воздействия и решена задача распознавания образа воздействия на базе определения взаимосвязей статистических параметров потоков данных, с целью идентификации вида воздействия деструктивных потоков данных. На пятом уровне воздействие характеризуется по виду вредоносных пакетов, составляющих деструктивный поток данных, а на шестом по прогнозируемым результатам деструктивного воздействия на управляющие узлы технологической сети промышленного предприятия.

2. Разработан алгоритм прогнозирования последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети, проводимых по различным сценариям.

3. Иерархическая модель представлена виде направленного графа, позволяющего прогнозировать последствия воздействий деструктивных потоков данных последовательным рассмотрением возможных сочетаний подмножества ребер согласно выбранному сценарию.

4. ОПРЕДЕЛЕНИЕ УЩЕРБА И ПРЕДОТВРАЩЕНИЕ ПОСЛЕДСТВИЙ ВОЗДЕЙСТВИЙ ДЕСТРУКТИВНЫХ ПОТОКОВ ДАННЫХ НА УПРАВЛЯЮЩИЕ УЗЛЫ ТЕХНОЛОГИЧЕСКИХ СЕТЕЙ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

4.1 Оценка сценариев возможных последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия

Как уже упоминалось, иерархическая модель воздействия деструктивных потоков данных на уровнях с четвертого по шестой позволяет произвести анализ рисковых событий и прогнозирование состояния узла от успешно реализованного воздействия в технологических сетях промышленного предприятия (рисунок 54).

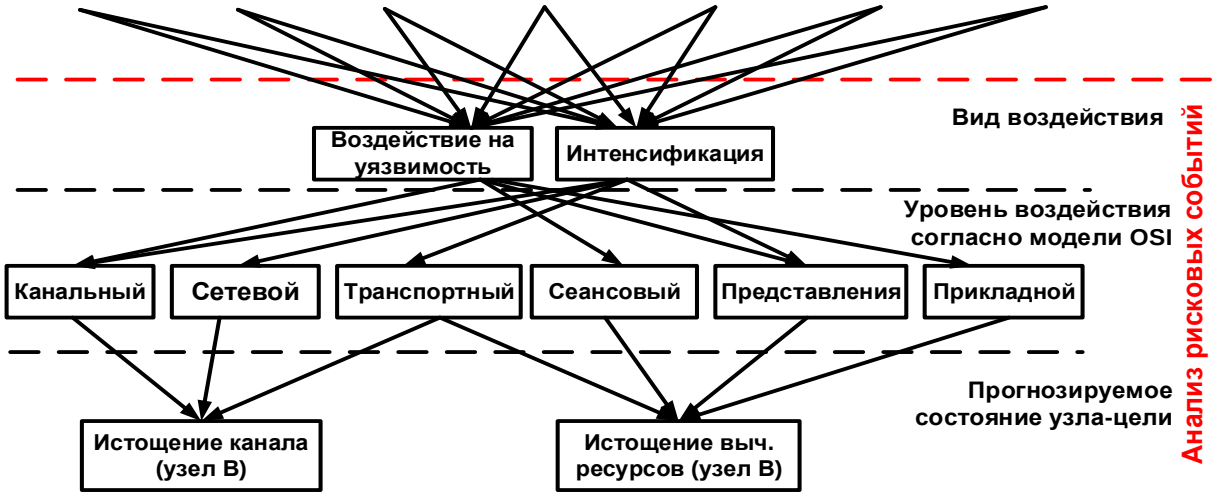


Рисунок 54 - Анализ рисковых событий в иерархической модели воздействия деструктивных потоков данных

Вычислительные ресурсы узла обусловлены совокупностью характеристик аппаратных средств, входящих в его состав. Наиболее важными характеристиками считаются: производительность процессора/микроконтроллера (далее – процессор); объем оперативной памяти; объем хранилища данных. Воздействия деструктивных потоков данных, направленные на истощение

вычислительных ресурсов, имеют своей целью максимально нагрузить процессор узла. Так как помимо прикладных вычислений $F_{прик}$, связанных с обработкой запросов и данных, вычислительные ресурсы процессора тратятся на выполнение служебных команд $F_{служ}$ различного характера, зависящих от архитектуры системы, то количество операций в единицу времени, которые могли бы выполнить простаивающие ресурсы процессора $F_{простой}$, зависит от максимального количества операций, выполняемых процессором в единицу времени $F_{проц}$, и их можно вычислить по формуле: $F_{простой} = F_{проц} - (F_{служ} + F_{прик})$.

Истощение вычислительных ресурсов и канала связи (рисунок 55) влечет за собой не только затраты на покупку и монтаж нового оборудование взамен вышедшего из строя, но и нарушение отдельно взятого технологического процесса на промышленном предприятии, что, в свою очередь, может привести к браку на производстве, выходу из строя дорогостоящей промышленной техники и человеческим жертвам [14, 15, 58].

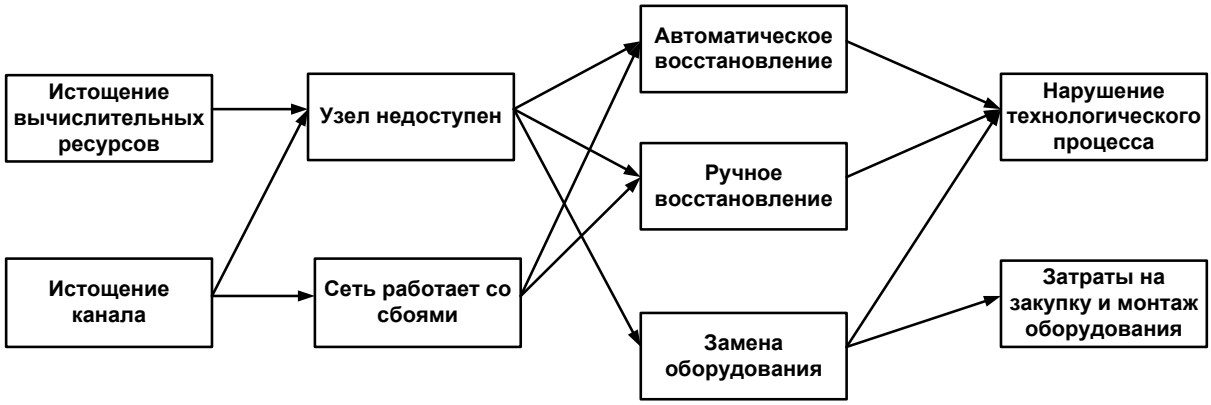


Рисунок 55 - Последствия воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия

Таким образом, если для обслуживания запросов узла/узлов источника деструктивных потоков данных процессору узла B необходимо выполнение операций, равных $F_д$, а время восстановления после прекращения воздействия $T_{вос}$(мин), то можно говорить об успешности воздействия, в том случае, если

$\left(\frac{F_{\text{д}}}{F_{\text{простой}}}\right) > 1 \cup (0{,}5 < \text{T}_{\text{вос}})$. Воздействие неуспешно в том случае, если $\left(\frac{F_{\text{д}}}{F_{\text{простой}}}\right) \leq 1 \cup (0 \leq \text{T}_{\text{вос}} \leq 0{,}5)$.

При этом узлы-цели можно разделить на два типа: веб-ресурс (например, интерфейс для удаленного управления оператором) и локальный узел. На веб-ресурсы проводятся воздействия с использованием протоколов транспортного и прикладного уровней, а также уровня представления данных, которые направлены на истощение вычислительных ресурсов узла. Тогда как на локальные узлы воздействия могут проводиться с использованием протоколов любых уровней – как с целью истощения вычислительных ресурсов узла, так и истощения канала [98].

Любой из сценариев воздействия может иметь следующие последствия для узла.

1) Полная недоступность узла, которая, в свою очередь, включает следующие варианты восстановления:

- сервис восстанавливается автоматически, как только воздействие заблокировано или прекращено (время полного восстановления работоспособности в таких случаях составляет в среднем от 0,5 до 5 мин и зависит от уровня проведения воздействия);
- для восстановления сервиса требуются действия оператора (время полного восстановления в таком случае, при условии своевременной реакции администратора, составляет от 5 до 15 мин, в отдельно взятых ситуациях возможно увеличение времени до 30 мин и зависит от масштабов администрируемой системы);
- сервис невозможно восстановить вообще или за короткий промежуток времени (время полного восстановления в таком случае может составлять промежуток, необходимый для ремонта или полной замены выведенного из строя оборудования).

2) Деградация сервиса, а именно постепенное замедление отправки ответов на запросы. В данном случае восстановление производительности произойдет сразу после блокирования воздействия деструктивных потоков данных.

При проведении сценарного анализа были определены риски от успешно проведенного воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия (таблица 6) [57].

Таблица 6 – Анализ сценариев и оценка рисков от успешно проведенного воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия

№ сценария	Сценарии воздействий деструктивных потоков данных											
	Вид воздействия		Уровень воздействия согласно модели OSI						Состояние цели	Проявление	Восстановление после блокировки воздействия	Риск
	На уязвимость	Интенсификация	Канальный	Сетевой	Транспортный.	Сеансовый	Представительский	Прикладной				
1	v		v						Истощение канала	Сеть работает со сбоями	Автомат.	Нарушение тех.процесса
2	v					v			Истощение выч. ресурсов	Узлы недоступны	Ручное	Нарушение тех.процесса
3	v						v					
4	v							v			Ручное/ замена оборудования	Нарушение тех.процесса/ Затраты на покупку и монтаж оборудования
5		v	v						Истощение канала	Сеть работает со сбоями	Автомат.	Нарушение тех.процесса
6		v		v								
7		v			v				Истощение выч. ресурсов/ истощение канала	Узлы недоступны/ Сеть работает со сбоями	Замена оборудования/ Ручное	Затраты на покупку и монтаж оборудования/ Нарушение тех.процесса
8		v					v		Истощение выч. ресурсов	Узлы недоступны	Автомат.	Нарушение тех.процесса

4.2 Разработка универсальной методики определения ущерба и предотвращения последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия

Решением задач определения величины потенциального ущерба и предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы в технологических сетях промышленного предприятия может стать методика, основанная на статистическом анализе потоков данных и своевременной сигнализации о состоянии воздействия. При этом в технологической сети нет необходимости очистки трафика, а оптимальным решением является своевременное определение и устранение источников вредоносного воздействия деструктивных потоков данных [45, 62, 93, 142].

Минимизацию ущерба от воздействий деструктивных потоков данных предлагается проводить в рамках трех основных этапов:

Первый этап – подготовительный, в который входит:

1) классификация возможных воздействий с учетом специфических особенностей технологической сети промышленного предприятия;
2) реализация процедур имитационного моделирования с последующим анализом полученных данных;
3) построение иерархической модели воздействия деструктивных потоков данных.

Второй этап – технический, предполагает установку всего необходимого программного обеспечения. Третий этап – организационно-правовой, подразумевающий разработку инструкций и управляющих документов, регламентирующих действия персонала при воздействии деструктивных потоков данных, направленного на технологическую сеть промышленного предприятия [5, 27, 99, 100].

На основе анализа сценариев воздействий деструктивных потоков данных на управляющие узлы в технологических сетях промышленного предприятия и

разработанной универсальной методики предотвращения последствий воздействия была создана принципиальная структура модуля защиты (рисунок 56).

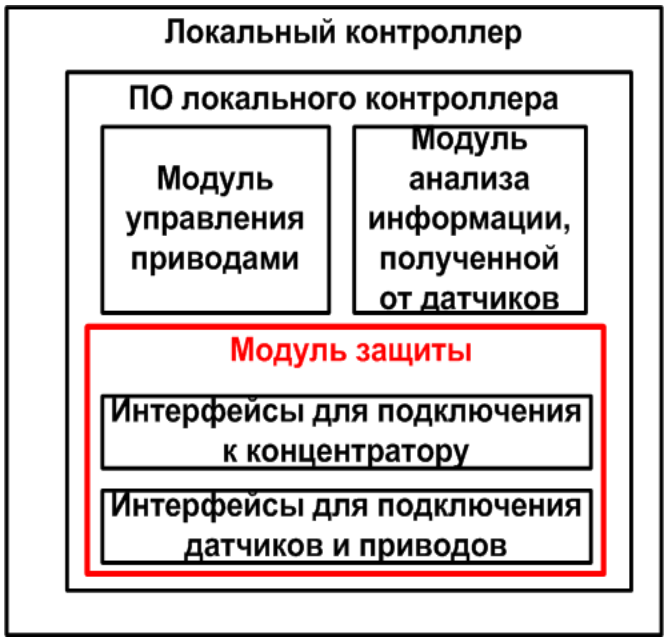


Рисунок 56 - Принципиальная структура модуля защиты

Предлагаемые процедуры необходимо выполнить для максимальной адаптации модуля защиты и оптимизации его работы. В силу ограниченных вычислительных возможностей узлов, на которые устанавливается модуль, избыточность функционала недопустима [63].

Принцип работы модуля защиты заключается в мониторинге статистических параметров потоков данных, выбранных для конкретной технологической сети. Измеренное значение параметров распределяется по категориям и дает возможность определить состояние воздействия $l(x)=(f(x|w_D))/(f(x|w_N))$, где $f(x|w_N)$ – нормальное состояние, $f(x|w_D)$ – нагрузка под воздействием, x – измеренное значение одного из исходного множества параметров. При этом x входит в нормальную категорию w_N, если $l(x) \leq T$; x входит в деструктивную категорию w_D, если $l(x) > T$, где T – порог значений параметров потоков данных (обычно определяется эмпирически, но для низкопроизводительных узлов и узкого канала связи можно принять $T = 1$) [26, 40, 52, 53]

Модули защиты устанавливаются на управляющих узлах технологической сети промышленного предприятия и обеспечивают мониторинг статистических параметров потоков данных, а на АРМ оператора устанавливается модуль сигнализации, сообщающий о начале воздействия деструктивных потоков данных на управляющие узлы (рисунок 57) [70, 97].

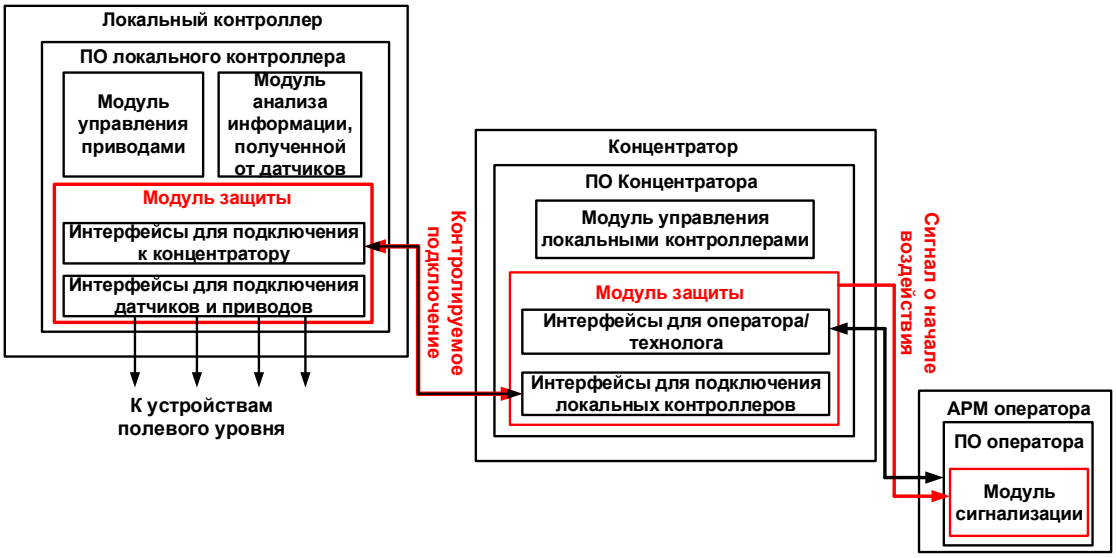


Рисунок 57 - Установка модулей защиты и сигнализации

Таким образом производится развертывание системы защиты, необходимое для реализации второго этапа мер, направленных на минимизацию ущерба от воздействий деструктивных потоков данных.

4.3 Апробация методики определения ущерба и предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы в технологических сетях

В качестве апробации методики определения ущерба и предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы в технологических сетях была рассмотрена система вентиляции промышленного предприятия (рисунок 58, А.2).

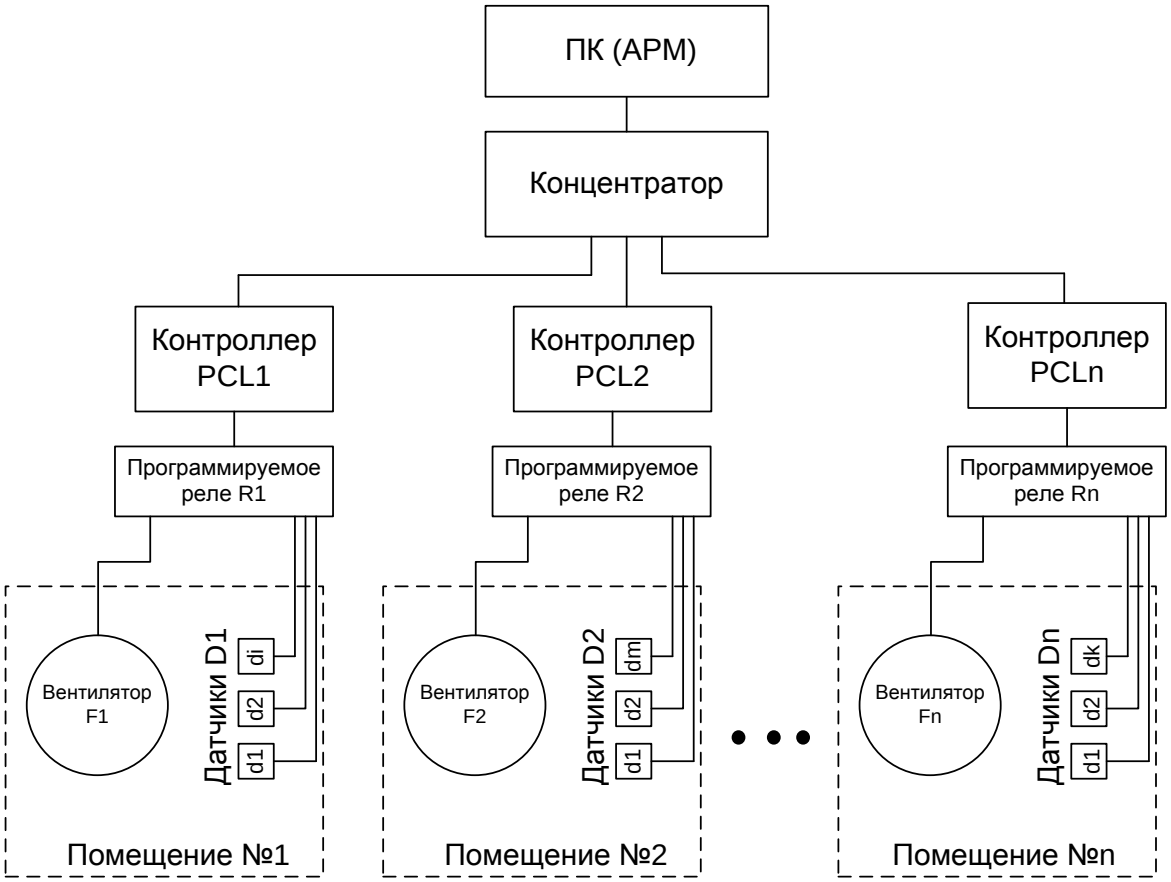


Рисунок 58 - Система вентиляции промышленного предприятия

Рассматриваемая система вентиляции построена с использованием оборудования российской фирмы производителя ОВЕН, относящейся к группе компаний «ЭНЕРГО-СНАБ СПБ».

Системы автоматизации данного производителя базируются на универсальных аппаратных средствах (локальных контроллерах, концентраторах и пр.), которые снабжаются программным обеспечением и полевыми устройствами, необходимыми для конкретной задачи заказчика.

Анализ особенностей системных связей и функционирования управляющих узлов технологической сети произведем по следующим направлениям:

1) Концентратор. Целю воздействия деструктивных потоков данных на данный управляющий узел является нарушение взаимодействия (мониторинг и управление) оператора с технологической сетью, и как следствие невозможность удаленно управлять устройствами полевого уровня, и переход системы в автономный режим.

Для реализации подобного рода воздействия достаточно установить на АРМ оператора нелегитимное программное обеспечение, отсылающее на концентратор постоянные запросы на обработку данных, при этом вычислительные ресурсы концентратора будут постепенно истощаться, вплоть до полного отказа или поломки устройства (рисунок 59).

Воздействие деструктивных потоков данных оказываемое на концентратор, источником которого при этом является АРМ оператора сложно выявить на ранних этапах, поэтому концентратор может длительное время испытывать нагрузку, превышающую показатели характерные для нормального состояния технологической сети [69].

2) Локальный контроллер. Целью воздействия деструктивных потоков данных на данный управляющий узел является нарушение работы устройств полевого уровня (рисунок 60).

Для реализации подобного рода воздействия необходима интеграция нелегитимного модуля в управляющее программное обеспечение на концентраторе, или нарушение работы легитимного программного обеспечения (направленное, или случайное). После чего концентратор начинает генерировать большое количество запросов к локальным контроллерам постепенно истощая их вычислительные ресурсы. Тем самым полностью лишая управления устройства полевого уровня, и они перестают функционировать.

Данное воздействие не может остаться незаметным, в силу прекращения функционирования всех полевых устройств. А при высокой нагрузке на локальные контроллеры они перестают функционировать или выходят из строя и требуют замены. Также полностью останавливается обеспечиваемый ими технологический процесс, что влечет за собой значительные потери и риски в том числе и человеческие жертвы, в случае полного прекращения вентиляции.

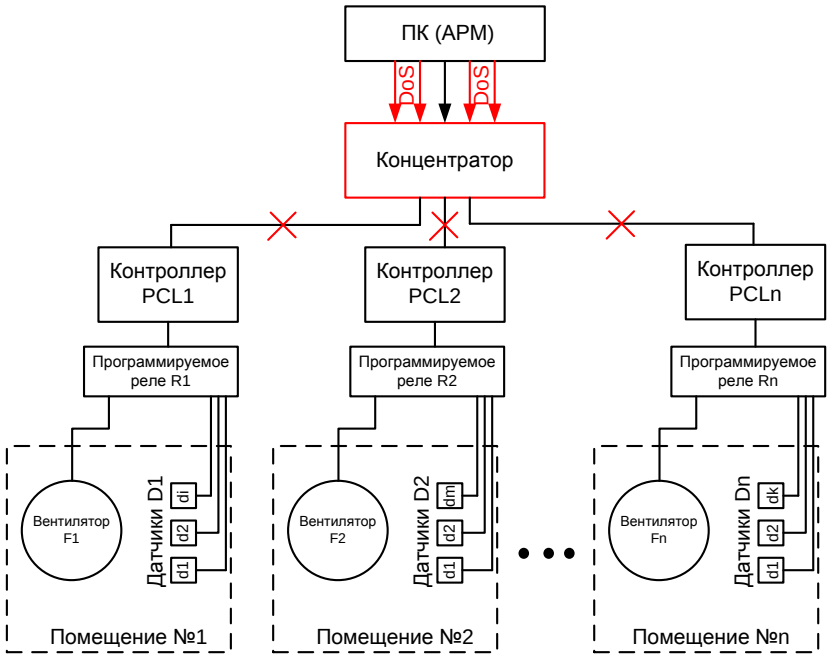


Рисунок 59 - Воздействие деструктивных потоков данных на концентратор

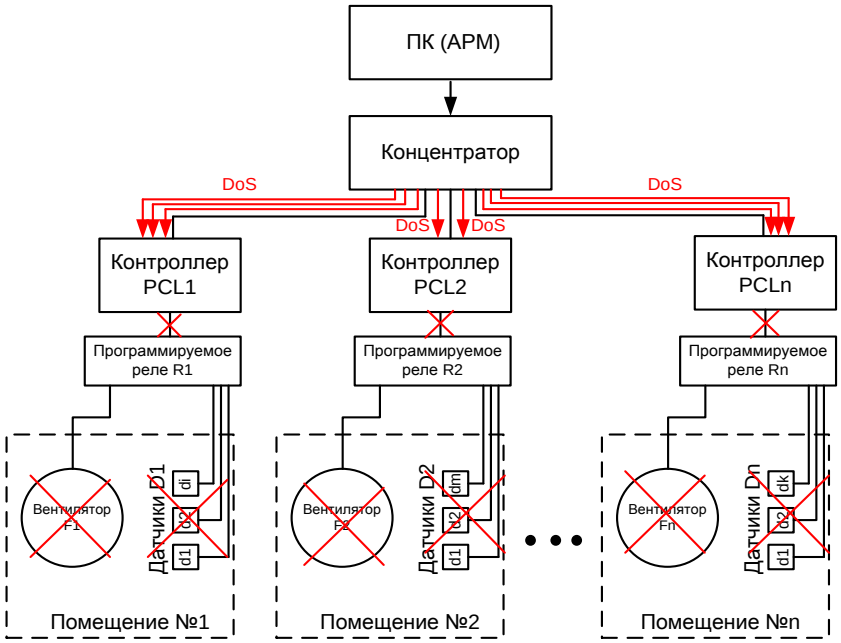


Рисунок 60 - Воздействие деструктивных потоков данных на локальный контроллер

Классификация воздействия деструктивных потоков была произведена с учетом особенностей технологической сети промышленного предприятия и реализации соответствующих процедур имитационного моделирования.

Определение параметров воздействия деструктивных потоков данных по сформированному исходному множеству значимых факторов:

1. Источник воздействия: узел
2. Динамические параметры потока данных: постоянная скорость - исходя из специфики вычислительных средств данной технологической сети.
3. Статистические параметры потока данных: энтропия, параметр Херста, параметр Пуассона, скорость потока данных, задержка; Так как скорость постоянна то ускорение и изменение задержки не учитываются.
4. Вид воздействия: на уязвимость;
5. Уровень воздействия согласно модели OSI: прикладной.
6. Прогнозируемое состояние узла-цели: истощение вычислительных ресурсов.

Данные факторы дают возможность классифицировать воздействие деструктивных потоков данных и реализовать процедуры имитационного моделирования. Для проведения эксперимента по имитации воздействия деструктивных потоков данных на управляющий узел модель настраивается соответствующим образом. Виртуальной машине, имитирующей данный узел, в гипервизоре выделяются ресурсы, приближенные к характеристикам концентратора и локального контроллера, так как относительно высокопроизводительных узлов, таких как например АРМ оператора, их вычислительная мощность близка. Программное обеспечение на имитируемом узле-цели отвечает на запросы в режиме, приближенном к работе сервисов заданной технологической сети. Приложению-источнику задаются параметры согласно типу имитируемого воздействия: постоянная скорость деструктивных потоков данных, состоящих из пакетов прикладного уровня [104, 107].

Далее приведены результаты имитационного моделирования при воспроизведении воздействия деструктивных потоков данных на концентратор технологической сети промышленного предприятия (рисунок 61).

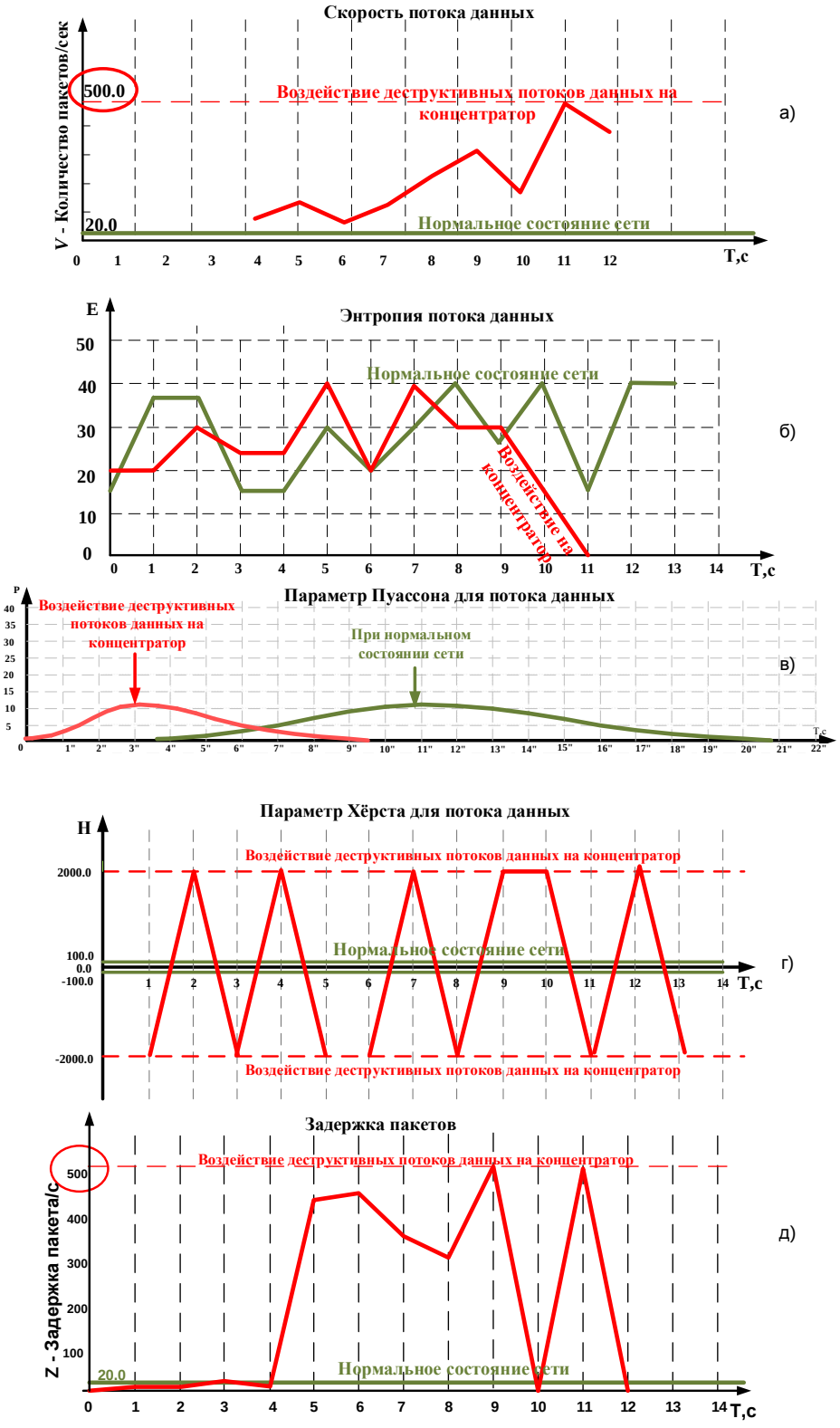


Рисунок 61 - Результаты имитационного моделирования для заданной технологической сети промышленного предприятия (а – скорость потока данных, б – энтропия потока данных, в – параметр Пуассона для потока данных, г – параметр Хёрста для потока данных, д – задержка пакетов данных)

Проведенный анализ послужил основой построения иерархической модели воздействия, отражающей параметры и свойства деструктивных потоков данных для заданной технологической сети, обеспечивающей вентиляцию на промышленном предприятии (рисунок 62).

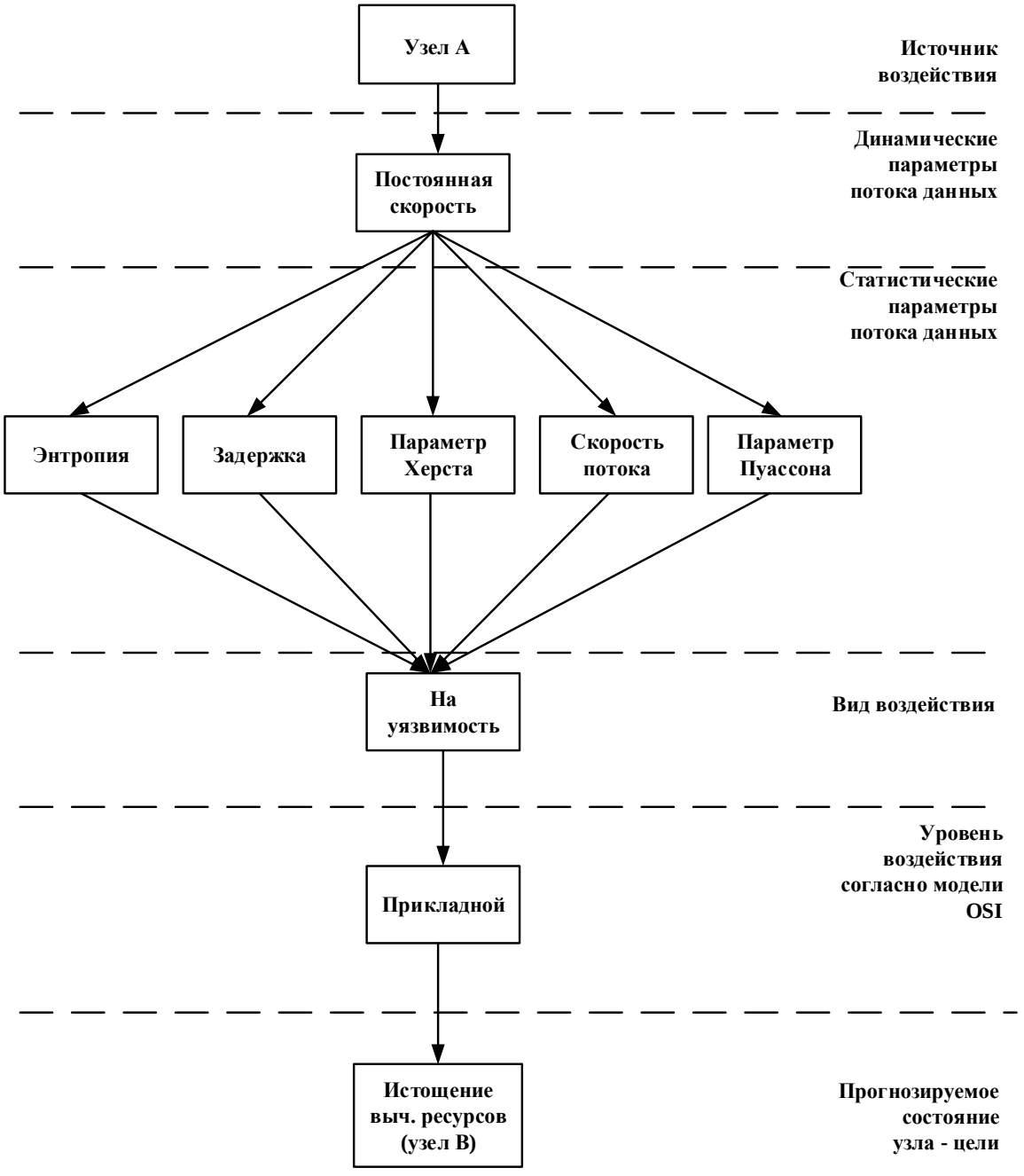


Рисунок 62 - Иерархическая модель заданного воздействия деструктивных потоков данных на управляющий узел технологической сети

Исходя из заданных параметров воздействия на ребрах и вершинах направленного графа, можно построить порожденный подграф (рисунок 63):

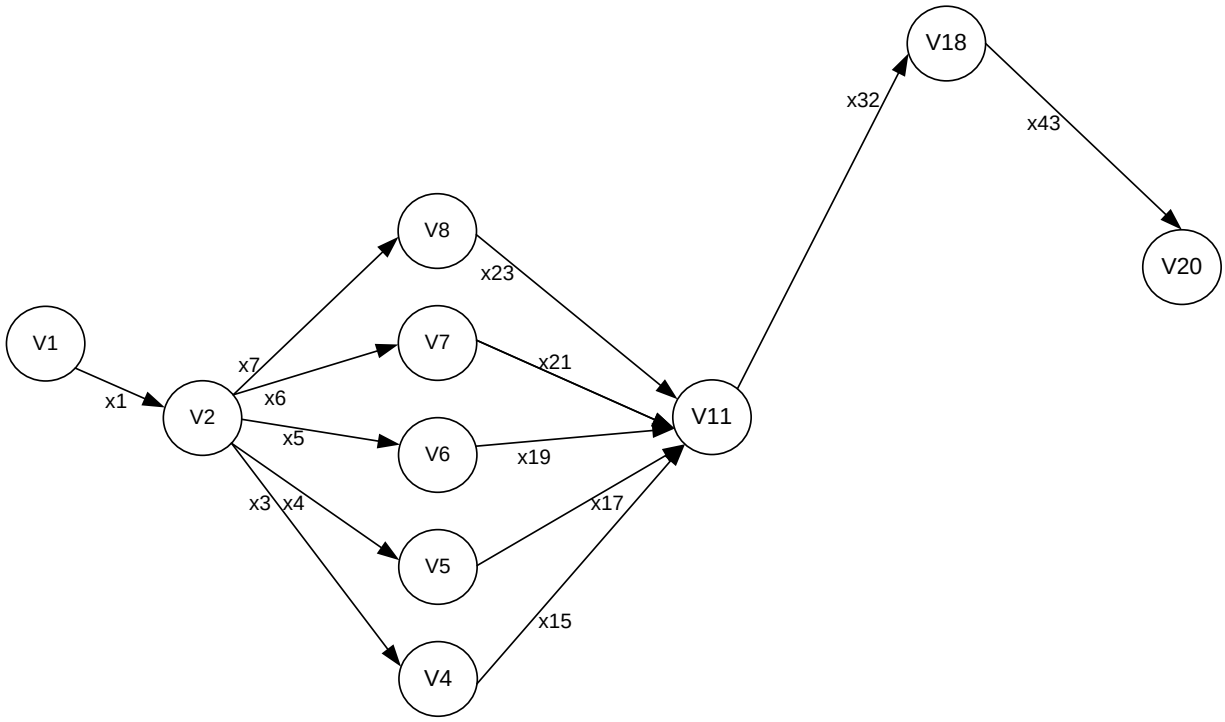


Рисунок 63 - Порожденный подграф графа заданного воздействия деструктивных потоков данных на управляющий узел

Где подмножество вершин Vп = {V1, V2, V4, V5, V6, V7, V8, V11, V18, V20} $\subset$ V, подмножество ребер Xп={X1, X3, X4, X5, X6, X7, X15, X17, X19, X21, X23,X32,X43} $\subset$ X.

4.4 Повышение эффективности функционирования управляющих узлов технологических сетей промышленного предприятия

На основе анализа рисковых событий был построен сценарий воздействия деструктивных потоков данных на управляющий узел технологической сети (таблица 7), который в свою очередь лег в основу определения эффективности разработанной универсальной методики определения ущерба и предотвращения

последствий воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия [16, 42].

Таблица 7 - Сценарии воздействия деструктивных потоков данных

Узел В	Источник	N сценария	Сценарии воздействия деструктивных потоков данных						
			Вид воздействия	Уровень модели OSI	Прогнозируемое состояние узла-цели	Проявление	Восстановление после блокировки воздействия	Риск	Ущерб включая вызов специалиста в среднем (в руб.)
Концентратор	АРМ оператора	1	На уязвимость	Прикладной	Истощение выч. ресурсов	Узлы недоступны	Автомат.	Нарушение тех.процесса	-
		2					Ручное	Нарушение тех.процесса	$Y= S_s$
		3					Замена оборудования	Нарушение тех.процесса/ Затраты на покупку и монтаж оборудования	$Y= S_s + S_в$
Локальный контроллер	Концентратор	4	На уязвимость	Прикладной	Истощение выч. ресурсов	Узлы недоступны	Автомат.	Нарушение тех.процесса	-
		5					Ручное	Нарушение тех.процесса	$Y= S_s$
		6					Замена оборудования	Нарушение тех.процесса / Затраты на покупку и монтаж оборудования	$Y=S_s * d+ S_в * n$
где S_s – стоимость вызова специалиста, $S_в$ – стоимость пострадавшего узла, n – количество вышедших из строя узлов, d– количество дней необходимое для замены оборудования									

Максимальная сумма ущерба включает в себя только покупку и монтаж вышедшего из строя оборудования. В полученную цифру не входят риски, связанные с производством брака и другие последствия отключения вентиляции (таблица 8).

Таблица 8 – Расчет риска от реализации воздействия деструктивных потоков данных

Ущерб от разового воздействия с учетом простоя			Вероятность	Риск реализации воздействия R_1 ($R_1 = Y_1 P_1 t$)	
Мера	Простой 1 раб. день (руб.)	Простой неделя (руб.)		Простой 1 раб. день (руб./год)	Простой неделя (руб./год)
Перепрограммирование узла	510000	3010000	11/365	15369,86	90712,33
Замена 1 узла	540000	3040000	6/365	8876,71	49972,60
Замена сегмента сети	-	3350000	2/365	-	18356,16

При внедрении модуля защиты (таблица 9) на предприятии затраты будут в том числе включать сумму разового вызова специалиста для установки обновления на управляющие узла, а именно программируемый контроллер, концентратор и АРМ оператора.

Таблица 9 – Расчет риска от реализации воздействия при внедрении модуля защиты

Ущерб от разового воздействия с учетом простоя с модулем защиты			Вероятность	Риск реализации воздействия R2 ($R_2 = Y_2 P_2 t$)	
Мера	Простой 1 раб. день (руб.)	Простой неделя (руб.)		Простой 1 раб. день (руб./года)	Простой неделя (руб./год)
Перепрограммирование узла	515000	3015000	4/365	5643,84	33041,10
Замена 1 узла	545000	3045000	2/365	2986,30	16684,93
Замена сегмента сети	-	3355000	1/365	-	9191,78

Исходя из стоимости оборудования $S_в$, которое может выйти из строя при реализации воздействия деструктивных потоков данных, стоимости вызова специалиста S_s, времени простоя предприятия d, т.е. времени, необходимого для монтажа нового или починки вышедшего из строя оборудования, и принимая во

внимание вероятность реализации невправленного воздействия P_i, была определена эффективность модуля защиты $\Delta R = R_1 - R_2$ (рисунок 64), которая, в свою очередь, определяет эффективность и надежность управляющих узлов и всей технологической сети в целом. При этом ущерб определяется как $Y = S_s \times d + S_B \times n$, риск от воздействия деструктивных потоков данных на незащищённую технологическую сеть определяется как $R_1 = Y_1 P_1 t$, а риск от воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия с установленным модулем защиты определяется как $R_2 = Y_2 P_2 t$.

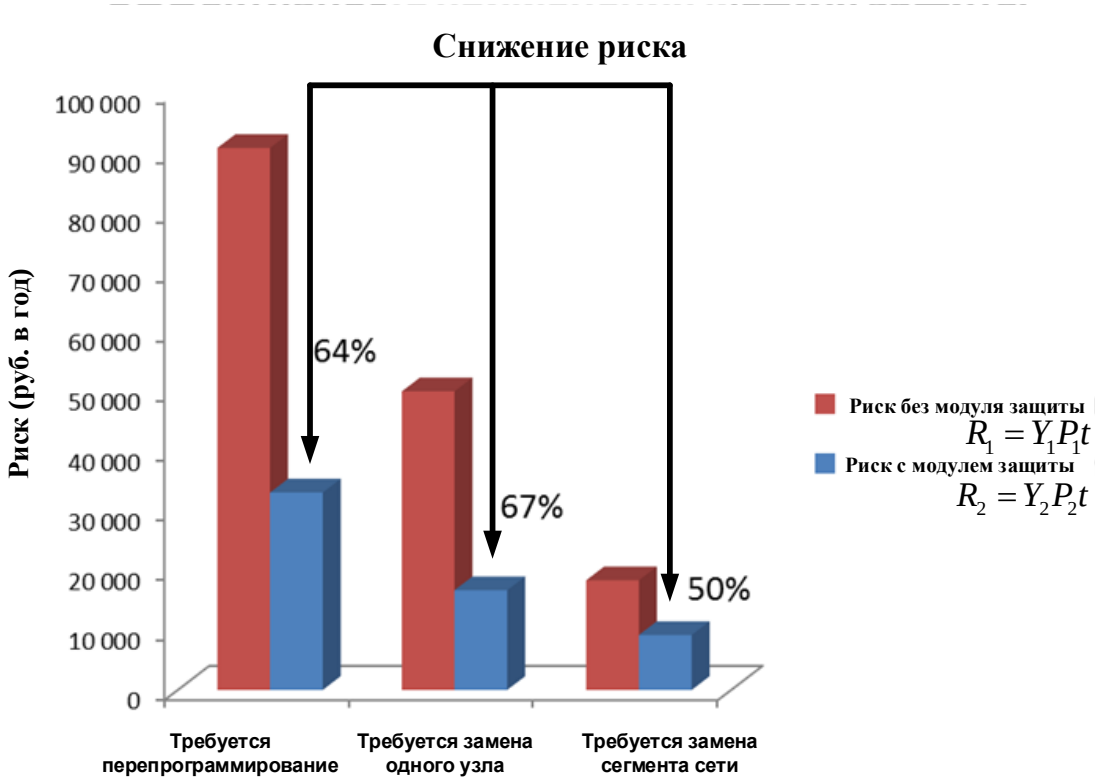


Рисунок 64 - Оценка эффективности применения модуля защиты в системе вентиляции промышленного предприятия

Выводы по главе 4

1. Проведена оценка последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия, выделены характеристики узлов, отражающие успешность воздействия, направленного на истощение вычислительных ресурсов.

2. Разработана универсальная методика определения ущерба и предотвращения последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия. На основе методики и анализа сценариев воздействий деструктивных потоков данных на управляющие узлы в технологических сетях и разработана принципиальная структура модуля защиты.

3.Методика апробирована на технологической сети, обеспечивающей вентиляцию промышленного предприятия, с этой целью проведены анализ особенностей системных связей и функционирования управляющих узлов технологической сети и классификация возможных воздействия. Реализованы процедуры имитационного моделирования с учетом свойств управляющих узлов технологической сети и построена иерархическая модель воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия.

4. Определена эффективность применения модуля защиты для предотвращения последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия. Его внедрение дает возможность повысить эффективность и надежность функционирования управляющих узлов различных уровней технологических сетей промышленного предприятия в условиях угрозы воздействия деструктивных потоков данных.

ЗАКЛЮЧЕНИЕ

В ходе проведенных исследований решена актуальная научно-практическая задача повышения эффективности и надежности функционирования управляющих узлов различных уровней технологических сетей промышленного предприятия в условиях угрозы воздействия деструктивных потоков данных и получены следующие результаты:

1) Сформировано исходное множество критериев оценки деструктивных потоков данных, позволяющих определить начало воздействия на управляющие узлы технологической сети промышленного предприятия.

2) Разработан способ определения вида воздействия деструктивных потоков данных на основе анализа взаимосвязей и закономерностей изменения статистических параметров потоков данных.

3) Разработана иерархическая модель воздействия деструктивных потоков данных на управляющие узлы сложных технических систем, позволяющая определить тип возможных воздействий и прогнозировать определенный исход для конкретной технологической сети промышленного предприятия.

4) Разработан алгоритм прогнозирования последствий воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия.

5) Разработана универсальная методика определения ущерба и предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия. Внедрение методики позволяет оценить уровень риска, а также повысить надежность и эффективность функционирования узлов управления.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Ажмухамедов И.М. Выявление аномалий в вычислительных сетях общего пользования на основе прогнозирования объема сетевого трафика / И.М. Ажмухамедов, А.Н. Марьенков // Проблемы информационной безопасности. Компьютерные системы. – 2012. – № 3. – С. 35-39. – EDN PIMJAF.

2. Андрюхин Е.В., Ридли М.К. Анализ сетевого трафика для выявления критических состояний систем автоматизации в условиях индустриальных промышленных сетей // Безопасность информационных технологий. – 2018. – Т. 25, № 3. – С. 79-87. EDN YODVSH.

3. Астахова Т.Н., Романов А.В., Кривоногов С.В. Анализ моделей и принципов системного моделирования для решения многокритериальной задачи принятия решений / // International Journal of Open Information Technologies. – 2020. – Т. 8, № 8. – С. 17-25. – EDN KJQJKQ.

4. Аханова М.А. Математическое моделирование / М.А. Аханова, С.В. Овчинникова, А.С. Еропкина. – Тюмень : Тюменский индустриальный университет, 2020. – 160 с. – ISBN 978-5-9961-2322-3. – EDN AUTCDD.

5. Ашихмин А.А. Разработка и принятие управленческих решений: Формальные модели и методы выбора / А.А. Ашихмин. – М. : Горная книга, 2011. – 79 с. – ISBN 978-5-98672-247-4. – EDN SURHKH.

6. Беляев П.С., Ху В.Ц., Варепо Л.Г., Усенова А.Ж. К вопросу управления технологическими процессами // Известия Тульского государственного университета. Технические науки. – 2019. – № 9. – С. 618-624. – EDN TSMWZR.

7. Билятдинов К.З., Меняйло В.В., Андрианов В.И. Модель устойчивости автоматизированной системы управления // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – № 4. – С. 43-47. – DOI 10.46418/2079-8199_2020_4_6. – EDN ASDJUY.

8. Благодарный А.И., Пищик Б.Н. Методы защиты команд управления в инструментальной среде для автоматизированных систем управления технологическими процессами // Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2021. – Т. 19, № 4. – С. 5-15. – DOI 10.25205/1818-7900-2021-19-4-5-15. – EDN OSJXBW.

9. Благодатский Г.А., Копысов А.Н., Хворенков В.В., Батурин И.С. Анализ иерархической модели автоматизированной системы управления параметрами радиолиний когнитивной радиосистемы // Наукоемкие технологии в космических исследованиях Земли. – 2018. – Т. 10, № 6. – С. 51-67. – DOI 10.24411/2409-5419-2018-10187. – EDN YTVGEH.

10. Бродский Ю.И. О математическом моделировании поведения сложных систем // Труды Института системного анализа Российской академии наук. – 2018. – Т. 68, № 2. – С. 12-15. – DOI 10.14357/20790279180203. – EDN XRQZPF.

11. Будников К.И., Курочкин А.В. Программное моделирование устройства обработки сетевого трафика в информационной системе // Автометрия. – 2021. – Т. 57, № 3. – С. 66-74. – DOI 10.15372/AUT20210308. – EDN IDETAN.

12. Булатов В.В. Введение в математические методы моделирования сложных систем / В.В. Булатов. – М. : Общество с ограниченной ответственностью "ОнтоПринт", 2018. – 342 с. – ISBN 978-5-00121-030-6. – EDN YRYBMF.

13. Бутов А.А., Волков М.А., Голованов В.Н. и др. Математическое моделирование основных классов стохастических продуктивных систем // Инженерные технологии и системы. – 2019. – Т. 29, № 4. – С. 496-509. – DOI 10.15507/2658-4123.029.201904.496-509. – EDN DWFDJF.

14. Бутырский Е. Ю. Математическое моделирование систем и процессов / Е.Ю. Бутырский, А.В. Матвеев. – СПб. : Информационный издательский учебно-научный центр "Стратегия будущего", 2022. – 733 с. – ISBN 978-5-4268-0064-9. – DOI 10.37468/book_011222. – EDN CCRIRT.

15. Бутырский, Е.Ю. Методы моделирования и оценивания случайных величин и процессов / Е.Ю. Бутырский. – СПб. : Информационный издательский

учебно-научный центр "Стратегия будущего", 2020. – 642 с. – ISBN 978-5-4268-0054-0. – DOI 10.37468/mon_1850. – EDN RIWUKM.

16. Васильев В.И., Вульфин А.М., Кириллова А.Д.Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10, № 2(37). – DOI 10.26102/2310-6018/2022.37.2.022. – EDN FKRMPL.

17. Васильев С.А., Канзитдинов Ш.К., Левичев И.В., Перес А.Д. Построение модели управления пропускной способностью телекоммуникационных сетей // International Journal of Open Information Technologies. – 2023. – Т. 11, № 2. – С. 16-24. – EDN HHJZNJ.

18. Веселова В.А., Коломойцев В.С. Подход к обнаружению аномалий в самоподобном сетевом трафике // Надежность. – 2023. – Т. 23, № 2. – С. 57-63. – DOI 10.21683/1729-2646-2023-23-2-57-63. – EDN KLWDUT.

19. Галяев В.С., Зыкова Е.А., Краснов А.Е. и др. Современные подходы к анализу сетевого трафика для обнаружения его аномальных состояний // Информатизация образования и науки. – 2019. – № 3(43). – С. 22-35. – EDN FZFJNK.

20. Гетьман А.И., Маркин Ю.В., Евстропов Е.Ф., Обыденков Д.О. Обзор задач и методов их решения в области классификации сетевого трафика // Труды Института системного программирования РАН. – 2017. – Т. 29, № 3. – С. 117-150. – DOI 10.15514/ISPRAS-2017-29(3)-8. – EDN YUFLVX.

21. Голева А. И., Стороженко Н.Р., Потапов В.И., Шафеева О.П. Математическое моделирование отказоустойчивости информационных систем // Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2019. – Т. 17, № 4. – С. 33-45. – DOI 10.25205/1818-7900-2019-17-4-5-33-45. – EDN POKCRJ.

22. Грачков И. А. Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты // Безопасность информационных технологий. – 2018. – Т. 25, № 1. – С. 90-98. – EDN YWYPWX.

23. Губкина В.Р. Теоретико-множественная модель для решения задачи системного анализа и синтеза в телекоммуникациях // Вестник СибГУТИ. – 2019. – № 2. – С. 57-67. – EDN CJVVLJ.

24. Данилкин С.В., Карасев П.И., Ефанов М.С., Шамсулдин Х.А. Определение аномалий в сетевом трафике на основе использования его энтропийных характеристик // Приборы и системы. Управление, контроль, диагностика. – 2023. – № 3. – С. 9-14. – DOI 10.25791/pribor.3.2023.1393. – EDN IRIJIF.

25. Доронина Ю.В., Скатков А.В. Каскадно-иерархическое моделирование в задачах анализа динамики ресурсных характеристик сложных систем // Информационно-управляющие системы. – 2020. – № 3(106). – С. 48-58. – DOI 10.31799/1684-8853-2020-3-48-58. – EDN COPTIA.

26. Дорожко И.В., Горохов Г. М., Кириллов И. А. Методический подход к разработке системы поддержки принятия решений оператора автоматизированной системы управления технологическими процессами на основе динамических байесовских сетей // Труды МАИ. – 2022. – № 125. – DOI 10.34759/trd-2022-125-23. – EDN NUMQMM.

27. Емельянов А.Е. Системный анализ и моделирование сетевых систем для повышения качества управления технологическими процессами / А.Е. Емельянов // Системный анализ и моделирование процессов управления качеством в инновационном развитии агропромышленного комплекса : Материалы V Международной научно-практической конференции,в рамках реализации Ассоциации «Технологическая платформа «Технологии пищевой и перерабатываю-щей промышленности АПК – продукты здорового питания», Воронеж, 21 мая 2021 года / Воронеж. гос. ун-т инж. технол.. – Воронеж: Воронежский государственный университет инженерных технологий, 2021. – С. 9-19. – EDN SFOUYF.

28. Ефимов А.Ю. Использование энтропийных характеристик сетевого трафика для определения его аномальности // Программные продукты и системы.

– 2021. – № 1. – С. 83-90. – DOI 10.15827/0236-235X.133.083-090. – EDN MHJVBV.

29. Журавлев С.С., Рудометов С.В., Окольнишников В.В., Шакиров С.Р. Применение модельно-ориентированного проектирования к созданию АСУ ТП опасных промышленных объектов // Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2018. – Т. 16, № 4. – С. 56-67. – DOI 10.25205/1818-7900-2018-16-4-56-67. – EDN YQNXAL.

30. Иваненко В.Г., Иванова Н.Д. Методика анализа стойкости автоматизированных систем управления технологическим процессом энергоблока АЭС к воздействию компьютерных атак // Безопасность информационных технологий. – 2021. – Т. 28, № 4. – С. 52-62. – DOI 10.26583/bit.2021.4.04. – EDN JHDULZ.

31. Иванов А.К., Типикин В.В. Модели взаимовлияния информационных потоков // Автоматизация процессов управления. – 2019. – № 3(57). – С. 73-85. – DOI 10.35752/1991-2927-2019-3-57-73-85. – EDN RWQRNA.

32. Иванов В.К. К вопросу создания комплексной математической модели производственной системы // Автоматизация. Современные технологии. – 2020. – Т. 74, № 5. – С. 199-202. – DOI 10.36652/0869-4931-2020-74-5-199-202. – EDN VEQJFG.

33. Ивахненко А.Г., Юрачковский Ю.П. Моделирование сложных систем по экспериментальным данным. - М. : Радио и связь, 1987. – 123 с.

34. Ильина А.И., Рыбакова Е.А. Изучение состояния информационных потоков // Вестник Самарского университета. Экономика и управление. – 2019. – Т. 10, № 4. – С. 49-58. – EDN KIHLTQ.

35. Инденко О.Н. Математическое моделирование динамических систем со статической нелинейной характеристикой // Актуальные направления научных исследований XXI века: теория и практика. – 2018. – Т. 6, № 6(42). – С. 157-158. – EDN YUDLCX.

36. Исаев А.С., Луценко О.И., Симанович А.А. Обзор методик выявления аномального поведения сетевого трафика в локальной сети // Научно-технический вестник Поволжья. – 2020. – № 4. – С. 87-89. – EDN UJGLMK.

37. Истратова Е.Е., Смирнов А.Е., Глинин Е.В. Разработка программного обеспечения для мониторинга характеристик трафика в корпоративной компьютерной сети // International Journal of Open Information Technologies. – 2021. – Т. 9, № 10. – С. 73-79. – EDN JVLLVY.

38. Карандашев А.А., Оленев В.Л., Бритов Г.С. Моделирование динамики информационных потоков в маршрутах вычислительных сетей // Информационно-управляющие системы. – 2023. – № 3(124). – С. 39-50. – DOI 10.31799/1684-8853-2023-3-39-50. – EDN AUBKNL.

39. Кенетова Р.О. К вопросу математического моделирования на основе теории конфликта // Вестник КРАУНЦ. Физико-математические науки. – 2021. – Т. 36, № 3. – С. 72-79. – DOI 10.26117/2079-6641-2021-36-3-72-79. – EDN PMJQHW.

40. Кини Р.Л. Райфа Х. Принятие решений при многих критериях: Предпочтения и замещения. - М. : Радио и связь, 1981. - 560 с.

41. Кобзев В.В. Математическое моделирование производственных систем / В.В. Кобзев, А.Е. Радаев, А.С. Кривченко. – 2-е издание, переработанное и дополненное. – СПб. : Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого", 2018. – 252 с. – ISBN 978-5-7422-6066-0. – EDN ZFZFHI.

42. Колмогоров А.Н. Основные понятия теории вероятностей. — М. : Наука, 1974. — 119 с.

43. Комолов Д.В., Горшков А.А., Лопатин Д.А. Автоматизация процедур многоагентного планирования в аспекте мультиатрибутивного графового моделирования // Известия Тульского государственного университета. Технические науки. – 2021. – № 9. – С. 340-345. – DOI 10.24412/2071-6168-2021-9-340-345. – EDN VHDNKE.

44. Кондаков С.Е., Рудь И.С. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий // Вопросы кибербезопасности. – 2021. – № 5(45). – С. 12-20. – DOI 10.21681/2311-3456-2021-5-12-20. – EDN EWLLIJ.

45. Костогрызов А.И. К методам системной инженерии: вероятностные подходы к анализу процесса управления качеством системы // Современные информационные технологии и ИТ-образование. – 2022. – Т. 18, № 2. – С. 227-240. – DOI 10.25559/SITITO.18.202202.227-240. – EDN CBAGRX.

46. Котляров А.С., Левин И.И. Обработка сетевых потоков данных в реконфигурируемых вычислительных системах // Известия ЮФУ. Технические науки. – 2019. – № 2(204). – С. 48-56. – DOI 10.23683/2311-3103-2019-2-48-56. – EDN SWNLFM.

47. Крамер Г. Математические методы статистики / Г. Крамер. — М. : Мир, 1975. — 648 с.

48. Кузьмин В.Н. Шуваев Ф.Л., Розганов М.В. Сравнительный анализ моделей случайных графов // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. – 2022. – № 58. – С. 23-34. – DOI 10.17223/19988605/58/3. – EDN DTLKHF.

49. Купреев О., Бадовская Е., Гутников А. DDoS-атаки в первом квартале 2019 года. // Securelist, Kaspersky. - 2019. URL: https://securelist.ru/ddos-report-q1-2019/93890/ (дата обращения: 07.04.2019).

50. Лебедев С.В. Модель-ориентированный подход к построению связанных данных на основе разнородных источников // Онтология проектирования. – 2019. – Т. 9, № 1(31). – С. 101-116. – DOI 10.18287/2223-9537-2019-9-1-101-116. – EDN PDUJRG.

51. Лубенцов А.В. Синтез модели получения характеристик эффективности комплексной системы безопасности на базе метода анализа иерархий // Моделирование, оптимизация и информационные технологии. – 2023. – Т. 11, № 1(40). – С. 12-13. – DOI 10.26102/2310-6018/2023.40.1.030. – EDN ENDMMS.

52. Лукина С. В. Формирование инструментов принятия решений на основе граф-моделей / С.В. Лукина, В.В. Макаров, О.Е. Зимовец. – Курск : Закрытое акционерное общество "Университетская книга", 2021. – 122 с. – ISBN 978-5-907555-14-3. – EDN HAJTSO.

53. Макаров А.М., Виноградская Т.Н. и др. Теория выбора и принятия решений. –М : Наука, 1982.- 328с.

54. Манита А.Д. Теория вероятностей и математическая статистика / А.Д. Манита. — М. : Изд-во Моек, ун-та, 2001. — 120 с.

55. Макшанова Л.М., Тонхоноева А.А., Цыбикова Т.С. Разработка математической модели анализа трафика с использованием метрики Хаусдорфа // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2020. – № 4. – С. 93-96. – DOI 10.37882/2223-2966.2020.04.27. – EDN IBFYOQ.

56. Марков Г.А. Применение модели неокортекса для выявления контекстуальных аномалий в сетевом трафике промышленного Интернета вещей // Проблемы информационной безопасности. Компьютерные системы. – 2023. – № 2(54). – С. 140-149. – DOI 10.48612/jisp/b5fk-dug5-3g37. – EDN YWOMVT.

57. Матвеев, А.В. Методы моделирования и прогнозирования / А.В. Матвеев. – Санкт-Петербург: Санкт-Петербургский университет Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева, 2022. – 230 с. – ISBN 978-5-907116-73-3. – EDN IMLKWS.

58. Математическое моделирование процессов и систем: по материалам пленарных докладов VIII Международной молодежной научно-практической конференции / Башкирский государственный университет; Ответственный редактор - С.А. Мустафина. Том Часть I. – Стерлитамак: Башкирский государственный университет, 2018. – 296 с. – ISBN 978-5-7477-4722-7. – EDN YVAYDB.

59. Мосолов А.С., Краснов А.Е., Урбан Н.А. О применении метода анализа уязвимостей технологического процесса производственного объекта для обеспечения информационной безопасности АСУ ТП с учётом взаимосвязи компонентов // Безопасность информационных технологий. – 2022. – Т. 29, № 3. – С. 38-52. – DOI 10.26583/bit.2022.3.03. – EDN VDEBLC.

60. Муллин А.А., Захаров А.А. Выявление аномалий трафика сетевой инфраструктуры АСУ ТП на основе статистических данных // Безопасность информационного пространства : сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных, Челябинск, 26–28 ноября 2014 года / Министерство образования и науки Российской Федерации, Южно-Уральский государственный университет, Кафедра «Безопасность информационных систем». – Челябинск : Издательский центр ЮУрГУ, 2015. – С. 31-34. – EDN ZUGORH.

61. Мунтян Е.Р. Представление знаний в граф-моделях сложных технических систем / Е.Р. Мунтян // Информатизация и связь. – 2020. – № 3. – С. 12-16. – DOI 10.34219/2078-8320-2020-11-3-12-16. – EDN DHDAXZ.

62. Мушик Э., Мюллер П. Методы принятия технических решений /пер. с нем. Н.В. Васильченко, В.А. Душского. - М. : Мир, 1990.- 204 с.

63. Николаев А.А. Теория автоматического управления / А.А. Николаев, А.Б. Лымарь, Е.Я. Омельченко. – Магнитогорск : Магнитогорский государственный технический университет им. Г.И. Носова, 2020. – 187 с. – ISBN 978-5-9967-1936-5. – EDN RWRRHJ.

64. Никонов А.И., Кусакина Н.М. Статистический анализ сетевого трафика и выявление аномалий // Актуальные проблемы информационной безопасности. Теория и практика использования программно аппаратных средств: Материалы X Всероссийской научно-технической конференции, Самара, 21–22 марта 2017 года. – Самара : Самарский государственный технический университет, 2017. – С. 55-56. – EDN ZMTXGT.

65. Нуйкин, Д.А., Кулакова Е.С. Эффективность работы моделей надежности отказоустойчивой автоматизированной системы управления //

Электротехнические и информационные комплексы и системы. – 2021. – Т. 17, № 1. – С. 113-119. – DOI 10.17122/1999-5458-2021-17-1-113-119. – EDN JJDDAX.

66. Орлов Ю.Н., Панкратов А.С. К разработке модели эволюции структуры сетевого графа // Препринты ИПМ им. М.В. Келдыша. – 2021. – № 24. – С. 1-16. – DOI 10.20948/prepr-2021-24. – EDN FTIHGP.

67. Орловский С.А. Проблемы принятия решений при нечеткой исходной информации. М. : Наука, 1981.- 318с.

68. Осипова В.А., Дубинина К.С. Применение алгоритмов теории графов к упрощенному методу анализа иерархий // Моделирование и анализ данных. – 2019. – № 3. – С. 24-31. – EDN WGTKVM.

69. Павленко Е.Ю. Модель функционирования адаптивной сетевой топологии крупномасштабных систем на основе динамической теории графов // Проблемы информационной безопасности. Компьютерные системы. – 2022. – № 3. – С. 68-79. – DOI 10.48612/jisp/tn56-xvah-7tf1. – EDN WUDQXX.

70. Певнева А.Г., Зимовец А.И., Санжаревский Г.А. Системный анализ и моделирование критической нагрузки на информационные ресурсы // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2020. – № 1. – С. 105-111. – DOI 10.25586/RNU.V9187.20.01.P.105. – EDN QITJJR.

71. Перов Р.А., Лаута О.С., Крибель А.М., Федулов Ю.В. Метод выявления аномалий в сетевом трафике // Наукоемкие технологии в космических исследованиях Земли. – 2022. – Т. 14, № 3. – С. 25-31. – DOI 10.36724/2409-5419-2022-14-3-25-31. – EDN QSBJKM.

72. Плохов И.В., Егоров О.А., Создание экспертной системы для анализа функционирования АСУ ТП тепловой электростанции // Научно-технический вестник Поволжья. – 2022. – № 11. – С. 128-131. – EDN MBPFRY.

73. Пугач А.В., Степанова Д.С., Гаипов К.Э. Анализ статистических закономерностей информационных потоков в IP сетях // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические

науки. – 2022. – № 2-2. – С. 89-97. – DOI 10.37882/2223-2966.2022.02.28. – EDN ASYIKY.

74. Пырьев М.С., Коллеров А.С. Средства анализа сетевого трафика локальной вычислительной сети в ретроспективе // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 4(34). – С. 58-62. – DOI 10.14529/secur190407. – EDN HPPACS.

75. Рева И.Л., Иванов А.В., Медведев М.А., Огнев И.А. Сравнительный анализ современных трендов в области моделей трафика сетей передачи данных // Системы анализа и обработки данных. – 2022. – № 2(86). – С. 55-68. – DOI 10.17212/2782-2001-2022-2-55-68. – EDN GAHCGS.

76. Репин Д.С., Филаретов Г.Ф., Червова А.А. Исследование фрактальных характеристик сетевого трафика // Информатизация образования и науки. – 2019. – № 2(42). – С. 48-67. – EDN ZAWXFR.

77. Саенко И.Б., Старков А.М. Подход к моделированию виртуальных локальных вычислительных сетей в корпоративных информационных системах // Наукоемкие технологии в космических исследованиях Земли. – 2019. – Т. 11, № 1. – С. 66-77. – DOI 10.24411/2409-5419-2018-10226. – EDN ZAJITZ.

78. Самарин М.А., Максимов А.В. Архитектура информационной системы анализа закономерностей в информационных потоках // Научно-аналитический журнал "Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России". – 2023. – № 2. – С. 177-185. – EDN HGMAMI.

79. Сафаров И.М., Валеев З.Н., Шумаев Т.А. Проектирование автоматизированных систем управления технологическими процессами с применением методов теории графов // Инженерный вестник Дона. – 2018. – № 4(51). – С. 149. – EDN RBVUIF.

80. Симанков В.С., Дубенко Ю.В. Системный анализ в иерархических интеллектуальных многоагентных системах // Вестник компьютерных и информационных технологий. – 2021. – Т. 18, № 3(201). – С. 33-46. – DOI 10.14489/vkit.2021.03.pp.033-046. – EDN EOXOPX.

81. Слесарчик К.Ф. Метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности // Вопросы кибербезопасности. – 2018. – № 1(25). – С. 19-27. – DOI 10.21681/2311-3456-2018-1-19-27. – EDN OSZMCD.

82. Смелянский Р.Л. Иерархические периферийные вычисления // Моделирование и анализ информационных систем. – 2019. – Т. 26, № 1(79). – С. 146-169. – DOI 10.18255/1818-1015-2019-1-146-169. – EDN YYYVBR.

83. Современные автоматизированные системы управления в промышленности: теория, методы и средства: Сборник научных трудов кафедры «Автоматизация и управление». – Грозный: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Грозненский государственный нефтяной технический университет имени академика М.Д.Миллионщикова", 2012. – 72 с. – ISBN 978-5-9904148-1-5. – EDN RUQMZH.

84. Сухарева А.В., Воронцов К.В. Построение полного набора тем вероятностных тематических моделей // Интеллектуальные системы. Теория и приложения. – 2019. – Т. 23, № 4. – С. 7-23. – EDN CWOGHS.

85. Сухинов А.И., Чистяков А.Е., Проценко Е.А., Проценко С.В. Моделирование сложных систем // Том Часть 1. – Ростов-на Дону : Донской государственный технический университет, 2019. – 241 с. – ISBN 978-5-6042240-5-2. – EDN YXZPQT.

86. Сухих Я.А., Правиков Д.И., Кузичкин А.А. Разработка защищенных архитектур автоматизированных систем управления технологическими процессами // Безопасность информационных технологий. – 2020. – Т. 27, № 2. – С. 97-117. – DOI 10.26583/bit.2020.2.08. – EDN IOKYSW.

87. Суходолов А.П. Системный анализ, моделирование. Математическое моделирование / А.П. Суходолов, В.А. Маренко. – Иркутск : Байкальский государственный университет, 2018. – 144 с. – ISBN 978-5-7253-2966-7. – EDN YMTPPF.

88. Татарникова Т.М., Вольский А.В. Оценка вероятностно-временных характеристик сетевых узлов с дифференциацией трафика // Информационно-управляющие системы. – 2018. – № 3(94). – С. 54-60. – DOI 10.15217/issn1684-8853.2018.3.54. – EDN XQLJOH.

89. Татарникова Т.М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. – 2018. – № 5(96). – С. 35-43. – DOI 10.31799/1684-8853-2018-5-35-43. – EDN YLFXZZ.

90. Терехина И.Ю. Выявление аномалий с использованием построенной модели процессов в виде ациклического ориентированного графа // Программная инженерия. – 2023. – Т. 14, № 6. – С. 285-291. – DOI 10.17587/prin.14.285-291. – EDN EWLRJR.

91. Терновой О.С. Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности при DDoS-атаках: специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность": автореферат диссертации на соискание ученой степени кандидата технических наук / Терновой Олег Степанович. – Барнаул, 2016. – 22 с. – EDN ZQIPIH.

92. Тиханычев О.В. Об организации применения современных технологий информационного обследования // Программные системы и вычислительные методы. – 2021. – № 1. – С. 63-76. – DOI 10.7256/2454-0714.2021.1.31229. – EDN EZTOJK.

93. Трайнев В.А., Филалеев Ю.А. Моделирование решений и его информационное обеспечение на основе системы параметров // Информационные и телекоммуникационные технологии. – 2021. – № 51. – С. 14-19. – EDN DDGOBK.

94. Тырсин А.Н. Энтропийное моделирование сетевых структур // Автоматика и телемеханика. – 2022. – № 10. – С. 144-155. – DOI 10.31857/S0005231022100130. – EDN ALLDVU.

95. Феллер В. Введение в теорию вероятностей и ее приложения / В. Феллер, О.В. Прохоров ; В. Феллер ; пер. со второго англ. изд. и предисл. Ю. В.

Прохорова. – 2-е изд.. – М. : URSS, 2009. – 22 с. – ISBN 978-5-397-01036-8. – EDN QJVXJL.

96. Фишер Р.А. Статистические методы для исследователей / Р.А. Фишер. — М. : Госстатиздат, 1958. — 267 с.

97. Флегонтов А.В. Моделирование задач принятия решений при нечетких исходных данных : монография / А.В. Флегонтов, В.Б. Вилков, А.К. Черных. – СПб. : Издательство "Лань", 2020. – 328 с. – (Учебники для вузов. Специальная литература). – ISBN 978-5-8114-4402-1. – EDN TFEFLF.

98. Хмара В.В., Хасцаев Б.Д., Кабышев А.М. и др. Особенности информационно-технического обеспечения автоматов Мили единой разветвленной системы автоматизированного управления непрерывным технологическим процессом // Вестник ГГНТУ. Технические науки. – 2022. – Т. 18, № 2(28). – С. 41-52. – DOI 10.34708/GSTOU.2022.60.58.002. – EDN KEXODW.

99. Царькова Е.Г. Оптимальное управление и моделирование систем / Е.Г. Царькова. – Пенза : Общество с ограниченной ответственностью "Наука и Просвещение", 2019. – 126 с. – ISBN 978-5-6042209-1-7. – EDN VVSFFO.

100. Чернов Д.В., Сычугов А.А. О выборе мер обеспечения информационной безопасности автоматизированных систем управления технологическими процессами // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9, № 2(33). – DOI 10.26102/2310-6018/2021.33.2.016. – EDN NHJJLX.

101. Чернов Д.В., Сычугов А.А. Современные подходы к обеспечению информационной безопасности АСУ ТП // Известия Тульского государственного университета. Технические науки. – 2018. – № 10. – С. 58-64. – EDN AUTLJL.

102. Чернов Д.В., Сычугов А.А. Формализация модели нарушителя информационной безопасности АСУ ТП // Известия Тульского государственного университета. Технические науки. – 2018. – № 10. – С. 22-27. – EDN YRBGZF.

103. Чижикова Л.А. Системный подход к математическому моделированию и выбору режима работы подсистемы сложной системы //

International Journal of Open Information Technologies. – 2022. – Т. 10, № 6. – С. 109-114. – EDN EXVZTX.

104. Шайтура С.В., Жиделев М.А., Федоров Д.Ю. Системный анализ технологий компьютерных систем и систем связи / С. В. Шайтура, // Известия Тульского государственного университета. Технические науки. – 2023. – № 3. – С. 290-296. – DOI 10.24412/2071-6168-2023-3-290-296. – EDN HTIZEG.

105. Шуваев Ф.Л., Татарка М.В. Анализ математических моделей случайных графов, применяемых в имитационном моделировании информационно-коммуникационных сетей // Научно-аналитический журнал "Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России". – 2020. – № 2. – С. 67-77. – EDN ZDGGKL.

106. Яркова О.Н. Импутация данных методами статистического моделирования // Инженерный вестник Дона. – 2023. – № 6(102). – С. 160-177. – EDN IPHPLT.

107. Ясинский С.А. Сравнительный анализ базовых типовых структур для построения кабельных локальных вычислительных, телекоммуникационных сетей и сетей доступа // Информация и космос. – 2020. – № 4. – С. 32-38. – EDN ODGAAA.

108. Ageev S.A., Ageeva N.S., Karetnikov V.V. et al. Algorithm for Online Detection of Traffic Anomalies in High-Speed Enterprise Multiservice Communication Networks // Automatic Control and Computer Sciences. – 2021. – Vol. 55, No. 8. – P. 1068-1079. – DOI 10.3103/S0146411621080022. – EDN ZILBYA.

109. Aliev A.R. About one mathematical model of reliability and safety of complex systems / A.R. Aliev, V.M. Mamedov, M.I. Seyidov // Advances in Intelligent Systems and Computing. – 2020. – Vol. 1095. – P. 712-719. – DOI 10.1007/978-3-030-35249-3_92. – EDN HRCTYM.

110. Bikmukhamedov R.F. Generative transformer framework for network traffic generation and classification / R. F. Bikmukhamedov, A. F. Nadeev // T-Comm.

– 2020. – Vol. 14, No. 11. – P. 64-71. – DOI 10.36724/2072-8735-2020-14-11-64-71. – EDN GLXOLK.

111. Bulygin M. Anomaly Detection Method for Aggregated Cellular Operator Data / M. Bulygin, D. Namiot // Conference of Open Innovations Association, FRUCT. – 2021. – No. 28. – P. 41-47. – EDN SZCCCB.

112. Cannady J. The detection of temporally distributed network attacks using an adaptive hierarchical neural network 2013 World Congress on Nature and Biologically Inspired Computing. – 2013. – P. 5-9.

113. Dudas A. Decision Trees in Proper Edge k-coloring of Cubic Graphs / A. Dudas, B. Modrovicova // Conference of Open Innovations Association, FRUCT. – 2023. – No. 33. – P. 21-29. – EDN RUMCEO.

114. Emel'yanov D. Algebras of Binary Isolating Formulas for Theories of Root Products of Graphs / D. Emel'yanov // The Bulletin of Irkutsk State University. Series: Mathematics. – 2021. – Vol. 37. – P. 93-103. – DOI 10.26516/1997-7670.2021.37.93. – EDN LTAPCB.

115. Evtushevsky V.Y. Enumeration of Paths in the Young–Fibonacci Graph / V. Y. Evtushevsky // Journal of Mathematical Sciences. – 2020. – Vol. 247, No. 5. – P. 663-679. – DOI 10.1007/s10958-020-04829-7. – EDN SXJJNX.

116. Geyda A. Conceptual Modeling of Information Quality for System Actions / A. Geyda // Conference of Open Innovations Association, FRUCT. – 2023. – No. 33. – P. 38-45. – EDN AHQPVE.

117. Gordon G. System Simulation, Second Ed. Englewood Cliffs, N.J.: Prentice-Hall, 1978.

118. Gülay Ö., Georgios L. A Denial of Service Detector based on Maximum Likelihood Detection and the Random Neural Network // Electrical and Electronic Engineering, Imperial College, Exhibition Road, London, SW7 2BT, UK, 2007.

119. Hu L. Reliability Assessment of Random Uncertain Multi-State Systems / L. Hu, D. Yue, G. Zhao // IEEE Access. – 2019. – Vol. 7. – P. 22781-22789. – DOI 10.1109/ACCESS.2019.2898912. – EDN PFYREA.

120. Huang G. Risk evaluation model for failure mode and effect analysis using intuitionistic fuzzy rough number approach / G. Huang, L. Xiao, G. Zhang // Soft Computing - A Fusion of Foundations, Methodologies and Applications. – 2021. – Vol. 25, No. 6. – P. 4875-4897. – DOI 10.1007/s00500-020-05497-0. – EDN IZHYIE.

121. Jing H. Detection of DDoS Attack within Industrial IoT Devices Based on Clustering and Graph Structure Features / H. Jing, J. Wang // Security and Communication Networks. – 2022. – Vol. 2022. – P. 1401683. – DOI 10.1155/2022/1401683. – EDN UXNAOP.

122. Karpov D.V. On Plane Drawings of 2-Planar Graphs / D.V. Karpov // Journal of Mathematical Sciences. – 2021. – Vol. 255, No. 1. – P. 28-38. – DOI 10.1007/s10958-021-05347-w. – EDN DNBJVX.

123. Korshunov G., Frolova E., Nazarevich S., Smirnov V. Fuzzy models and system technical condition estimation criteria // Advances in Intelligent Systems and Computing. – 2020. – Vol. 1041. – P. 179-189. – DOI 10.1007/978-981-15-0637-6_15. – EDN IBCORM.

124. Krinkin K., Kulikov I., Vodyaho A., Zhukova N. Architecture of a Telecommunications Network Monitoring System Based on a Knowledge Graph // Conference of Open Innovations Association, FRUCT. – 2020. – No. 26. – P. 231-239. – EDN KOKHQF.

125. Kumar A. Modeling and Fuzzy Availability Analysis of Computer Networks: A Case Study / A. Kumar, O. Dahiya, M. Saini // Smart Innovation, Systems and Technologies. – 2021. – Vol. 195. – P. 1-10. – DOI 10.1007/978-981-15-7078-0_1. – EDN XCIIQT.

126. Lande D., Dmytrenko O., Andriichuk O. et al. Building of directed weighted networks of terms for decision-making support during information operations recognition // Advances in Intelligent Systems and Computing. – 2021. – Vol. 1265. – P. 197-208. – DOI 10.1007/978-3-030-58124-4_19. – EDN IZPISR.

127. Lavrova D.S. The Analysis of Artificial Neural Network Structure Recovery Possibilities Based on the Theory of Graphs / D.S. Lavrova, A.A. Shtyrkina //

Automatic Control and Computer Sciences. – 2020. – Vol. 54, No. 8. – P. 977-982. – DOI 10.3103/S0146411620080222. – EDN MAUUYE.

128. Liu P., Hendiani S., Bagherpour M., et al. Utility-Numbers Theory // IEEE Access. – 2019. – Vol. 7. – P. 56994-57008. – DOI 10.1109/ACCESS.2019.2912922. – EDN OYXLEI.

129. Martyshov M.I. Preprocessing of system monitoring data for workload analysis of HPC systems / M.I. Martyshov, D.A. Nikitenko // Numerical Methods and Programming. – 2021. – Vol. 22, No. 3. – P. 230-238. – DOI 10.26089/NumMet.v22r314. – EDN XDKDCU.

130. Matsuura K. Hierarchical Model. In: Bayesian Statistical Modeling with Stan, R, and Python. Springer, Singapore. – 2022. – https://doi.org/10.1007/978-981-19-4755-1_8

131. Nikitin P. The Absolute of the Comb Graph / P. Nikitin // Journal of Mathematical Sciences. – 2020. – Vol. 247, No. 5. – P. 723-730. – DOI 10.1007/s10958-020-04834-w. – EDN IBZNPN.

132. Saini M. Modeling and availability analysis of data center: a fuzzy approach / M. Saini, O. Dahiya, A. Kumar // International Journal of Information Technology (Singapore). – 2020. – DOI 10.1007/s41870-020-00532-7. – EDN KWRBET.

133. Samoilov V.S. An Upper Bound on the Number of Edges of a Graph Whose kth Power Has a Connected Complement / V.S. Samoilov // Journal of Mathematical Sciences. – 2018. – Vol. 232, No. 1. – P. 84-97. – DOI 10.1007/s10958-018-3860-7. – EDN MPFSZW.

134. Sheluhin O.I. Network Traffic Anomalies Detection Using a Fixing Method of Multifractal Dimension Jumps in a Real-Time Mode / O.I. Sheluhin, I.Y. Lukin // Automatic Control and Computer Sciences. – 2018. – Vol. 52, No. 5. – P. 421-430. – DOI 10.3103/S0146411618050115. – EDN OJQHKD.

135. Smirnov A.V. The Shortest Path Problem for a Multiple Graph / A.V. Smirnov // Automatic Control and Computer Sciences. – 2018. – Vol. 52, No. 7. – P. 625-633. – DOI 10.3103/S0146411618070234. – EDN WUUAFA.

136. Sukhoparov M.E., Semenov V.V., Salakhutdinova K.I., Lebedev I.S. Identification of Anomalies in the Operation of Telecommunication Devices Based on Local Signal Spectra // Automatic Control and Computer Sciences. – 2020. – Vol. 54, No. 8. – P. 1001-1006. – DOI 10.3103/S0146411620080337. – EDN IBJFEE.

137. Vasil'eva K.V. Detecting Anomalies in Cyber-Physical Systems Using Graph Neural Networks / K.V. Vasil'eva, D.S. Lavrova // Automatic Control and Computer Sciences. – 2021. – Vol. 55, No. 8. – P. 1051-1060. – DOI 10.3103/S0146411621080320. – EDN DFNFBV.

138. Vlasova N.Y. On Contractible 5-Vertex Subgraphs of a 3-Connected Graph / N.Y. Vlasova // Journal of Mathematical Sciences. – 2020. – Vol. 247, No. 3. – P. 394-405. – DOI 10.1007/s10958-020-04809-x. – EDN BMEFQV.

139. Zaitseva E.A. Use of Graph Representation and Case Analysis to Assess the Security of Computer Systems / E.A. Zaitseva, D.P. Zegzhda, M.A. Poltavtseva // Automatic Control and Computer Sciences. – 2019. – Vol. 53, No. 8. – P. 937-947. – DOI 10.3103/S0146411619080327. – EDN HDICTF.

Основные положения диссертационной работы изложены в следующих опубликованных работах

В перечне, рекомендованном ВАК Минобрнауки России

140. Жарова О.Ю. Разработка критериев оценки внешнего воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2020. – № 3(55). – С. 4-16. – DOI 10.21685/2072-3059-2020-3-1.

141. Жарова О.Ю. Разработка иерархической модели оценки внешнего воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2020. – № 2. – С. 152-158. – DOI 10.25586/RNU.V9187.20.02.P.152.

142. Жарова О.Ю. Разработка мер по уменьшению количества широковещательного трафика в локальной сети / О.Ю. Жарова, С.А. Глебов, П.А. Чувак // Вопросы радиоэлектроники. – 2017. – № 11. – С. 15-20. – https://elibrary.ru/item.asp?id=30383218

143. Жарова О.Ю., Федорова В.А. Метод определения типа атаки по статистическим параметрам сетевого трафика // Вопросы радиоэлектроники. – 2016. – № 10. – С. 39-43. – https://elibrary.ru/item.asp?id=26696420

В других изданиях:

144. Жарова О.Ю. Применение системы анализа сетевой нагрузки для выявления начала DDoS-атаки // Вопросы радиоэлектроники. – 2018. – № 11. – С. 48-52. – https://elibrary.ru/item.asp?id=36351559

145. Жарова О.Ю. Разработка алгоритма повышения надежности управляющих узлов в сложных технических системах промышленных предприятий // Приоритетные направления инновационной деятельности в промышленности: Сборник научных статей по итогам одиннадцатой международной научной конференции, Казань, 29–30 ноября 2020 года. Том Часть 1. Казань: Общество с ограниченной ответственностью "КОНВЕРТ", 2020. – С. 108-110. – https://elibrary.ru/item.asp?id=44569710

146. Жарова О.Ю., Федорова В.А. Повышение эффективности гибридной системы противодействующей DDOS-атакам // Вопросы радиоэлектроники. – 2015. – № 8. – С. 126-132. (https://elibrary.ru/item.asp?id=26696420)

147. Жарова, О.Ю., Чевычелов А.В. Использование методов машинного обучения для классификации вредоносного ПО // Электронный журнал: наука, техника и образование. – 2018. – № 4(22). – С. 32-39. – https://elibrary.ru/item.asp?id=36815530

ПРИЛОЖЕНИЕ А

(обязательное)

Рисунок А.1 - Работа механизмов поведенческого анализа

Рисунок А.2 – Пример структуры технологической сети

ПРИЛОЖЕНИЕ Б

(обязательное)

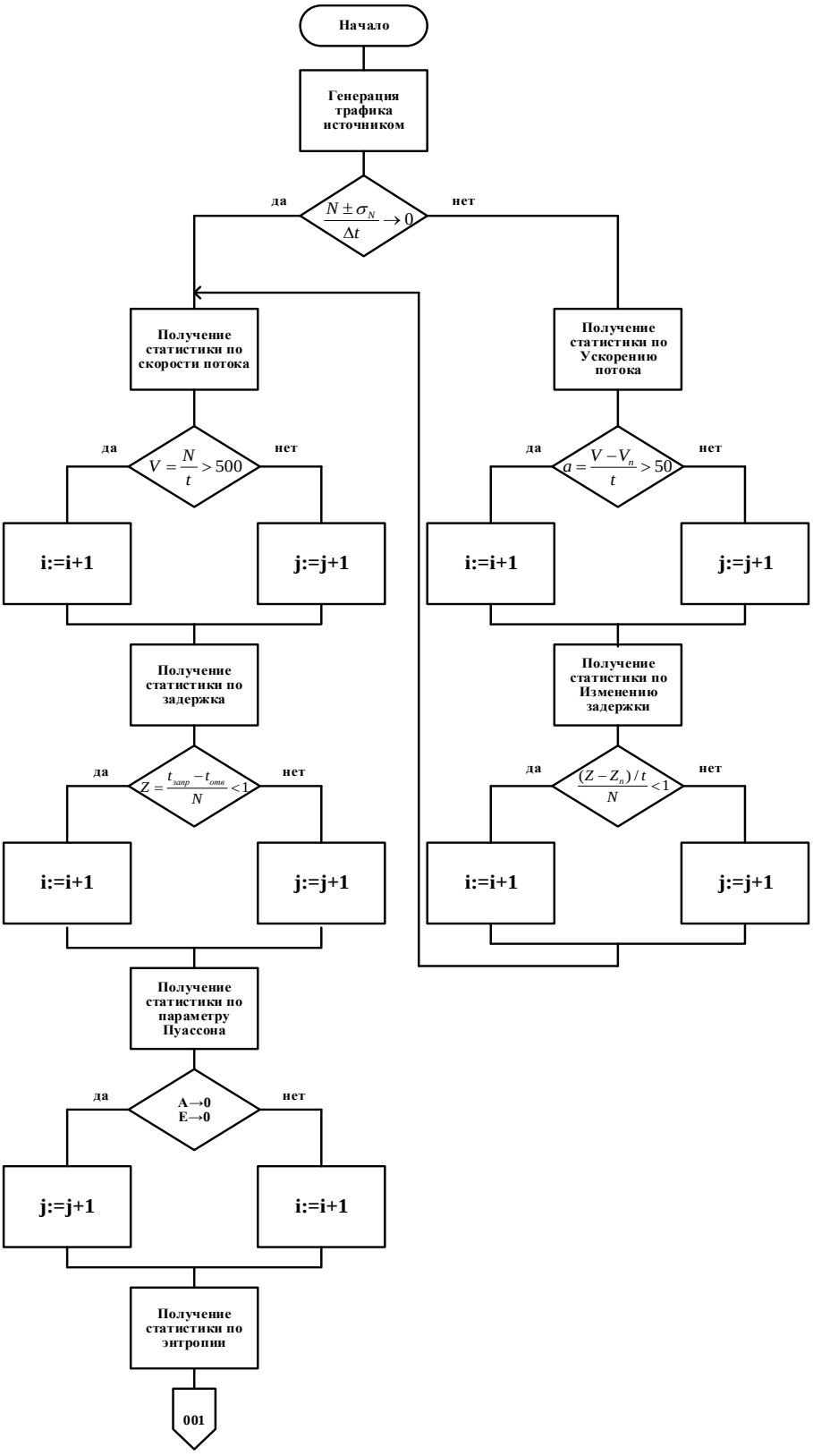


Рисунок Б.1 – Расширенный алгоритм прогнозирования последствий воздействия деструктивных потоков данных (часть 1)

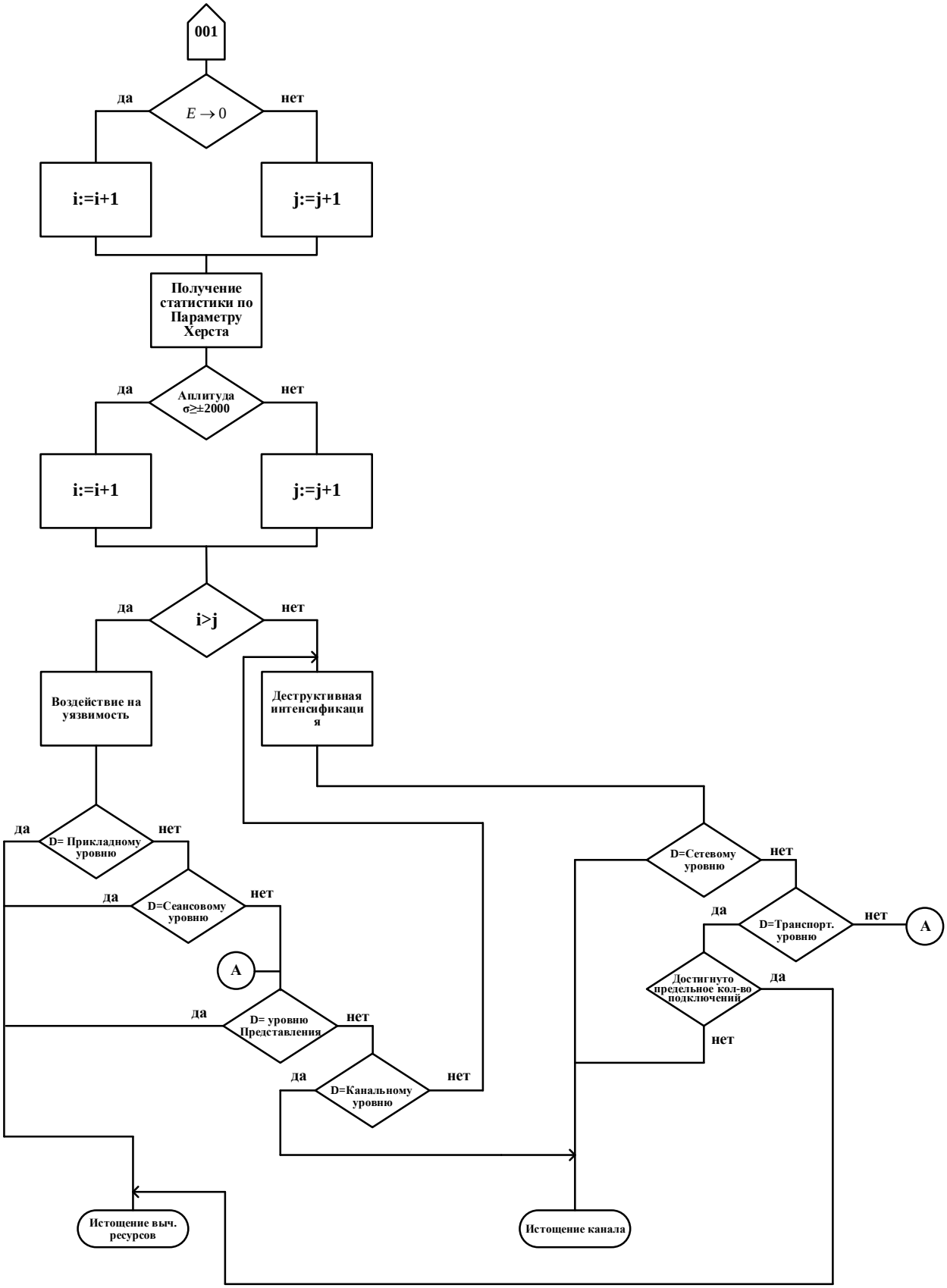


Рисунок Б.2 – Расширенный алгоритм прогнозирования последствий воздействия деструктивных потоков данных (часть 2)

ПРИЛОЖЕНИЕ В

(обязательное)

Акты внедрения результатов исследования

Re:Crypt

г. Калуга, ул. Никитина, д. 41, офис 317
https://re-crypt.com

АКТ
об использовании результатов научных исследований, проведенных Жаровой О.Ю. в диссертационной работе «Моделирование параметров воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия»

В рамках одного из направлений деятельности ООО «Рекрипт», заключающегося в проектировании и эксплуатации технологических сетей промышленных предприятий, была произведена апробация алгоритма прогнозирования исходов воздействий и иерархической модели воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия.

Использование алгоритма позволило оценить с высокой степенью достоверности основные параметры базовых факторов деструктивных воздействий.

Иерархическая модель позволила спрогнозировать исход и сформировать правила осуществления определенного вида воздействия деструктивных потоков данных. Анализ потоков данных на второй и третьей ступени иерархической модели позволил сделать вывод о начале воздействия деструктивных потоков данных и своевременно принять меры по предотвращению последствий воздействий. Основываясь на анализе динамических и статистических параметров, проходящих в технологической сети потоков данных, было определено начало воздействия. При этом не было необходимости ожидать полноценной эксплуатации уязвимости технологической сети или реализации интенсификации потоков данных, а также, не проводилось рассмотрение протоколов обмена данными по отношению к уровню модели OSI, а своевременно принятые меры позволили избежать перехода узла-цели в состояние отказа в обслуживании. На четвертой–шестой ступенях иерархической модели воздействия деструктивных потоков данных производился анализ рисковых событий и прогнозирование состояния узла от успешно реализованного направленного воздействия в технологических сетях промышленного предприятия. Пороговые значения статистических параметров, используемые в качестве условий перехода, были определены посредством нагрузочного тестирования. Разработанные в диссертации алгоритм и иерархическая модель приняты к использованию в ООО «Рекрипт», при построении технологических сетей промышленных предприятий.

Генеральный директор Щелкунов Д.А.\

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ ИНН 4027114002 «Рекрипт» ОГРН 1134027001808 РОССИЯ * г. КАЛУГА *

Общество с ограниченной ответственностью
НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ ЛАБОРАТОРИЯ
АЭРОКОСМИЧЕСКОЙ ТЕХНИКИ ДОСААФ
(ООО «НИЛАКТ ДОСААФ»)
248018, г. Калуга, ул. Баррикад, д.174, оф. 311 Тел/факс (4842) 55-81-74

Исх. № 473 *« 20 » 09 20 23 года*

АКТ

об использовании результатов научных исследований

Проведенные Жаровой О.Ю. научные исследования, изложенные в диссертационной работе «Моделирование параметров воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия» позволили не только разработать универсальную методику предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы в сложных технических системах промышленного предприятия, но и модернизировать программное обеспечение программируемых контроллеров, повысить их эффективность и надежность функционирования в условиях воздействия деструктивных потоков данных. Методика состоит из ряда основных этапов.

Первый этап (подготовительный): классификация возможных воздействий с учетом специфических особенностей технологической сети промышленного предприятия; реализация процедур имитационного моделирования с последующим анализом полученных данных; построение иерархической модели воздействия деструктивных потоков данных.

Второй этап (технический): предполагает установку всего необходимого программного обеспечения.

Третий этап (организационно-правовой): подразумевает разработку инструкций и управляющих документов, регламентирующих действия персонала при воздействии деструктивных потоков данных, направленного на технологическую сеть промышленного предприятия.

Приведенные процедуры основных этапов разработанной методики были использованы при реализации модуля защиты и мониторинга статистических параметров потоков данных технологической сети промышленного предприятия.

Разработанная в диссертации универсальная методика предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы в сложных технических системах принята к использованию в ООО «НИЛАКТ ДОСААФ» при проектировании, производстве и эксплуатации контрольно-проверочной аппаратуры и аппаратуры наземных станций управления космических аппаратов.

Директор, главный конструктор А.П. Папков

(Исп. Краснопеев С.В., +7-910-915-71-90)