Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский технологический университет «МИСИС»

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

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

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

Москва – 2023

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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.

Содержание работы

Потоки данных, циркулирующие между узлами внутри технологических и корпоративных сетей промышленного предприятия, могут подвергаться нелегитимным воздействиям со стороны злоумышленников. В частности, воздействие деструктивных потоков данных в виде направленной интенсификации потоков данных между внутренними управляющими узлами приводит к отказу в обслуживании технологического оборудования. В этой связи отказ в обслуживании может привести к внеплановому ремонту или перезагрузке аппаратных средств в составе технологической сети промышленного предприятия, в которой реализованы функции передачи данных, контроля и управления процессами и основными технологическими операциями, а также обработка производственной и технической документации.

Целью реализации атак, направленных на технологические сети, может быть, как нарушение информационной безопасности (нарушение целостности, конфиденциальности и доступности информации), так и причинение ущерба

ресурсам промышленного предприятия. К виду деструктивных воздействий относятся те, при которых один или несколько неисправных программируемых управляющих узлов начинают массово отсылать пакеты/команды управляемым устройствам или узлам, соединенным с ними сетью. В дальнейшем возможен вывод из строя как аналогового, так и цифрового оборудования, составляющего компоненты технологической сети промышленного предприятия. Ввиду того что в обычном режиме к каналам связи не предъявляются требования на высокую пропускную способность, то они в короткий промежуток времени заполняются деструктивными потоками данных и не могут проводить требуемую для выполнения технологического процесса информацию. Воздействие деструктивных потоков данных, направленное на технологические сети, в большинстве случаев таргетировано, выполняются с участием инсайдеров и/или с использованием закладок в новом недавно установленном оборудовании, но может быть и следствием выхода из строя управляющего узла.

При этом нарушение технологического процесса исходя из специфики производства в некоторых случаях может приводить не только к большим финансовым потерям, но и к человеческим жертвам. В этой связи воздействие деструктивных потоков данных нарушает надежность как управляющих узлов, так и объектов управления промышленного предприятия. Основная проблема при разработке метода противодействия воздействию деструктивных потоков данных в технологических сетях заключается в многообразии оборудования и специфике производства на каждом отдельно взятом промышленном предприятии.

Существующие методы, используемые для защиты от атак на отказ в обслуживании в корпоративных сетях, неприменимы для промышленных сетей по следующим основным причинам: необходимость полной реконфигурации промышленной сети; специфичность протоколов связи, используемых для обмена данными на полевом уровне; нелегитимные потоки данных могут распространять легитимные узлы; деструктивный поток данных может содержать стандартные пакеты, которые при интенсификации потоков будут нести соответствующую угрозу.

Для определения параметров воздействия деструктивных потоков данных в работе сформировано исходное множество значимых факторов, характеризующих уровень и состояние воздействия, а именно: источник вздействия; динамические параметры потоков данных; статистические параметры потоков данных; вид воздействия; уровень воздействия согласно модели OSI (англ. Open Systems Interconnection basic reference model – базовая эталонная модель взаимодействия открытых систем); прогнозируемое состояние узла, подвергшегося воздействию.

Для получения статистических данных по выбранным параметрам, определяющим состояние воздействия деструктивных потоков данных, была разработана имитационная модель технологической сети на основе виртуальной машины (рисунок 1). В качестве воспроизводимого оригинала технологической сети выступает абстрактная сеть, состоящая из двух узлов: источника деструктивных потоков данных и цели воздействия.

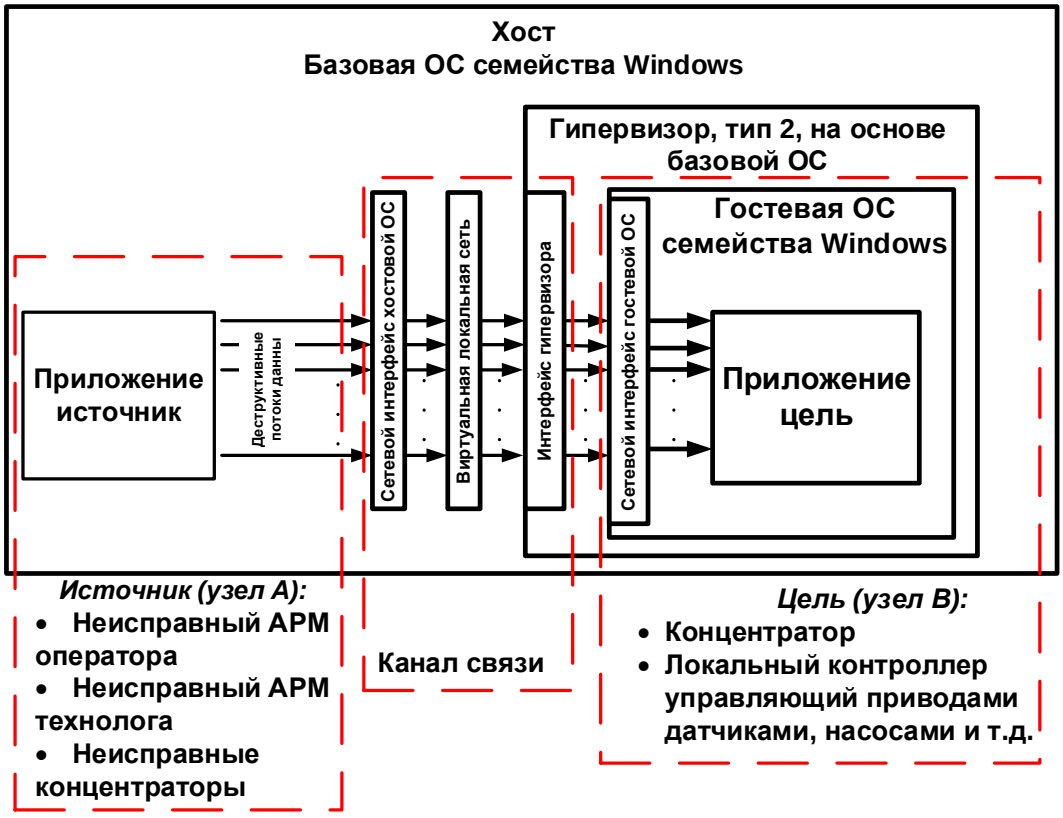


Рисунок 1 – Структурная схема имитационной модели воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия

На компьютер (хост) с базовой операционной системой установлен монитор виртуальных машин, или гипервизор. В имитационной модели используется гипервизор второго типа, а именно компонент, работающий на одном уровне (кольце) с ядром основной операционной системы, т.е. виртуализация производится на базе основной операционной системы. В роли узла источника *A* выступает программное обеспечение, позволяющее воздействовать на заданный узел с определенной интенсивностью. В роли цели, узла, подвергающегося воздействию деструктивных потоков данных, выступает виртуальная машина под управлением гостевой операционной системы семейства Windows с заданными исходя из возможностей моделируемого управляющего узла вычислительными ресурсами. В роли канала связи выступает комплекс из сетевого интерфейса хостовой операционной системы, виртуальной локальной сети и интерфейса гипервизора. Нагрузка на моделируемый узел *B* и канал связи, оказываемая приложением на узле источнике, может варьироваться в зависимости от воспроизводимого типа воздействия.

На основе результатов моделирования были определены пороговые значения перехода из нормального состояния технологической сети в состояние воздействия деструктивных потоков данных на управляющий узел.

Параметры потоков данных, используемые для определения начала и вида воздействия, приведены в таблице 1.

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 $P(k)$; $P(\tau)$	$\begin{cases} P(k) = \frac{(\lambda t)^k}{k!} \cdot e^{-\lambda t}, \\ P(\tau) = \lambda \cdot e^{-\lambda t}, \end{cases}$ где k=0,1,… - число сообщений; λ - интенсивность потоков; t - интервал времени измерения количества запросов; τ - распределение интервала между соседними событиями.

Продолжение табл. 1

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	$\begin{cases} (R/S)_N = \dfrac{\max_{1\le n\le N} \sum_{n=1}^{N}(x-\bar{x}) - \min_{1\le n\le N} \sum_{n=1}^{N}(x-\bar{x})}{\sqrt{\sum_{n=1}^{N}(x-\bar{x})^2 / N}}, \\ (R/S)_N = cN^H, \\ H = \log_N((R/S)_N), \end{cases}$ 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	$Z = t_{запр} - t_{отв}$, $a_z = \dfrac{Z - Z_n}{\Delta t}$, где $t_{запр}$ - время отправки запроса, а $t_{отв}$ - время получения ответа от соседнего узла, $Z - Z_n$ - изменение задержки в промежуток времени.

Результаты имитационного моделирования параметров потоков данных при нормальном и аномальном состояниях функционирования технологической сети приведены на рисунках 2–4.

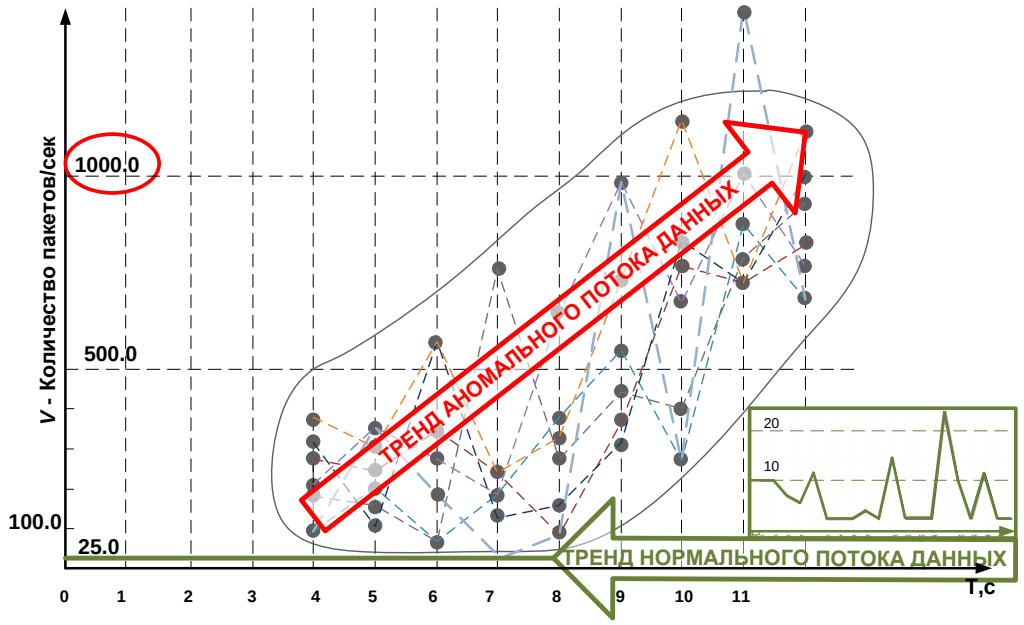


Рисунок 2 – Результаты имитационного моделирования скорости потоков данных нормального и аномального потоков данных

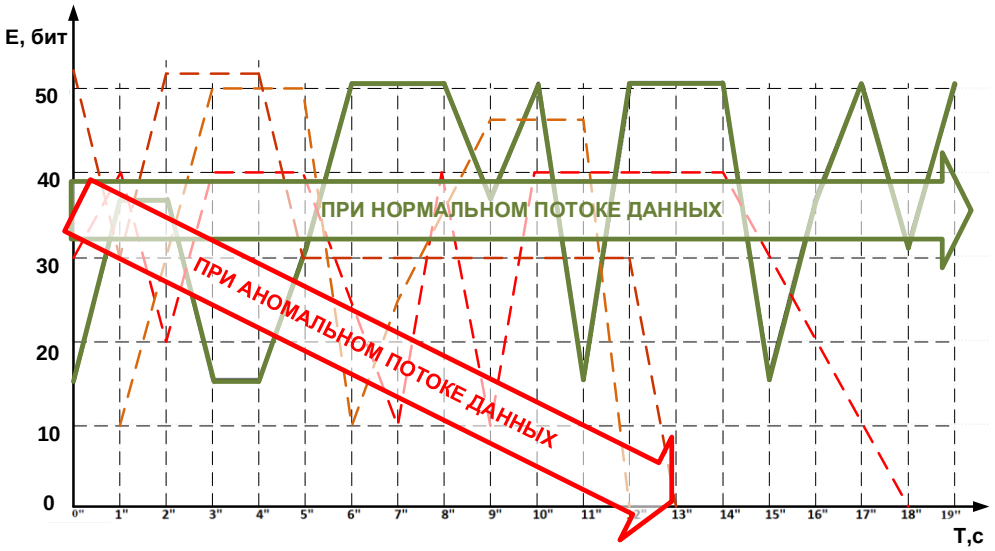


Рисунок 3 – Результаты имитационного моделирования энтропии нормального и аномального потоков данных

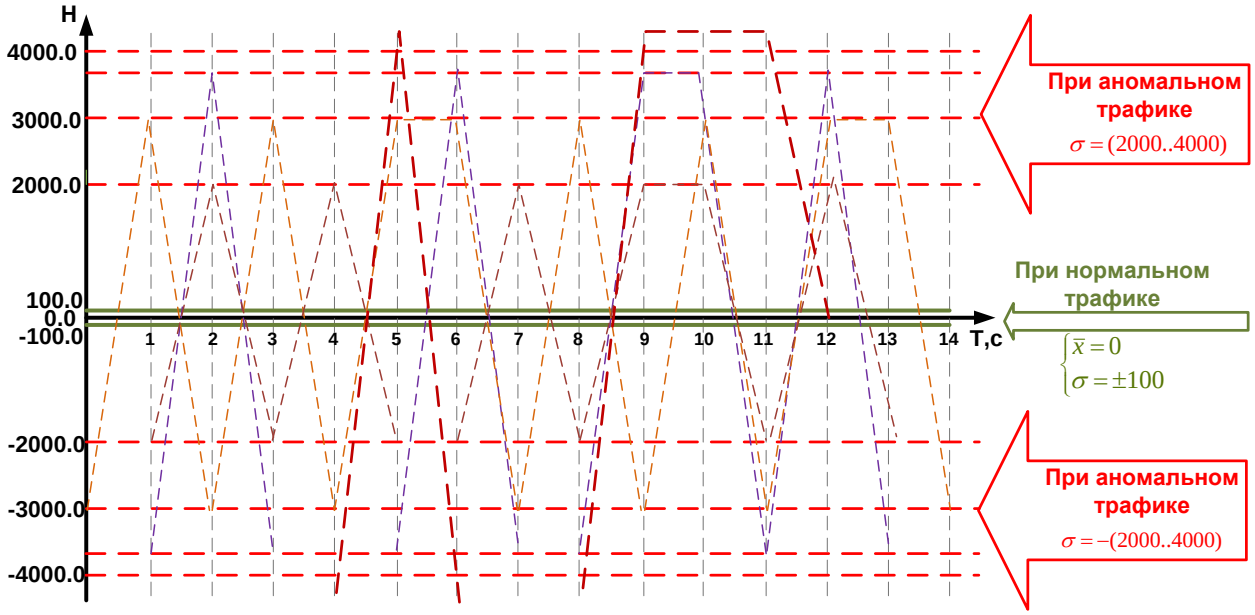


Рисунок 4 – Результаты имитационного моделирования параметра Хёрста нормального и аномального потоков данных

Разработанный подход позволяет определить факт воздействия деструктивных потоков данных по рассчитанным параметрам и визуализируемым графикам, построенным на основе анализа статистических данных за определенный промежуток времени. Следовательно, на основе проведенного анализа можно сделать вывод о том, что статистические параметры потоков данных позволяют определить состояние воздействия на ранних стадиях его возникновения.

Таким образом, разработанная модель позволяет имитировать воздействие деструктивных потоков данных, а выбранные для определения состояния воздействия статистические параметры отражают его ход и могут быть использованы для определения начала воздействия деструктивных потоков данных на малопроизводительном узле.

Проведенный статистический анализ параметров потоков данных послужил основой построения иерархической модели воздействия, 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.

На первом уровне иерархической модели воздействия 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. Объем деструктивных потоков данных $M_{\text{ген}} = N_{\text{ген}} \cdot T_{\text{ген}}$, отправляемых в сторону узла-цели B, также можно назвать эффективностью источника.

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. При этом $M_{\text{Ц}} = M_{\text{ген}} - \Delta M$, а при $\Delta M \to 0$ в сравнении с $M_{\text{ген}}$, можно говорить о том, что $M_{\text{Ц}} \cong M_{\text{ген}}$.

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 $\vec{p} = M_{Ц} \cdot \vec{V}_T$.

На втором уровне иерархической модели 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. Программное обеспечение, управляющее источником, генерирует пакеты с определенной периодичностью и интенсивностью поступления. Данный процесс можно описать, используя функции распределения количества пакетов N в единицу времени t.

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

1) воздействие с постоянной скоростью используются для заполнения канала деструктивным потоком данных и, как следствие, имеют либо затруднение, либо полную блокировку доступа к узлу B в зависимости от характера функции;

2) воздействие деструктивных потоков данных с непостоянной скоростью характеризуются изменением скорости поступления вредоносных пакетов с течением времени. Их можно классифицировать по динамике изменения скорости на воздействия с возрастающей скоростью и воздействия с переменной скоростью, в которых скорость может регулярно падать, вплоть до полного исчезновения вредоносных пакетов из среды передачи данных. Именно такой тип воздействия наиболее сложно поддается идентификации.

Воздействия деструктивных потоков данных с переменной скоростью в зависимости от характера функции тренда можно разделить на простые пульсирующие и пульсирующие с возрастающей скоростью. Для пульсирующего воздействия характерна высокая периодичность и наличие трендовой составляющей $\xi(t)$. Для воздействия деструктивных потоков данных с

переменной увеличивающейся скоростью характерна высокая периодичность и возрастающий тренд.

На третьем уровне иерархической модели 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.

На четвертом уровне иерархической модели 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. В случае если воздействие не имеет характерных особенностей, а представляет собой массовую отсылку пакетов узлу-цели, то имеет место деструктивная интенсификация (далее «интенсификация»). 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 организации интенсификации потока предварительное исследование узла B не проводится, а эффективность воздействия напрямую зависит от эффективности источника деструктивных потоков данных.

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 5 представлены функции принадлежности μ*(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.

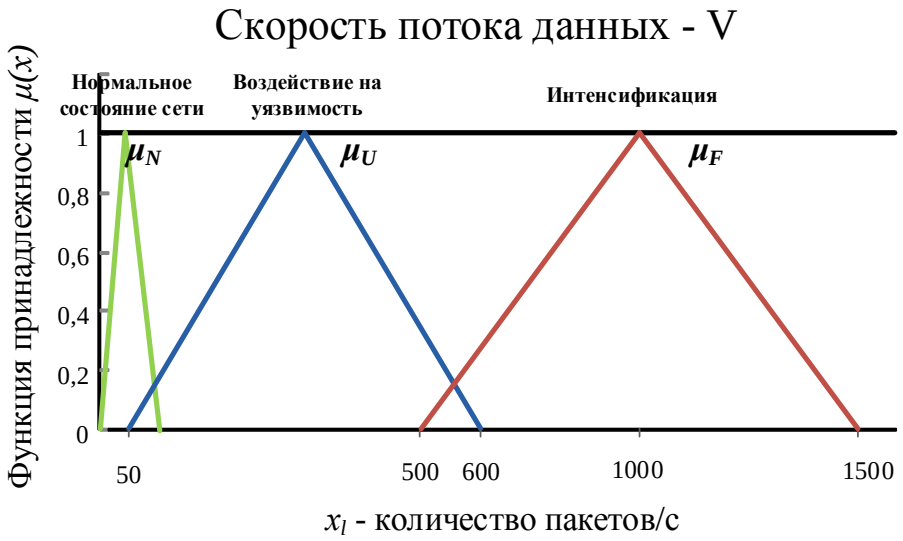


Рисунок 5 – Функция принадлежности μ*(x)* для скорости потока данных *V*

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 μ*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_u, 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.

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.

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*.

Связи между уровнями сформированы на основе анализа статистических данных по проводимым воздействиям деструктивных потоков данных, а также исходя из специфики работы каналов передачи данных в технологических сетях промышленного предприятия. При этом сформирована иерархическая модель, которая позволяет спрогнозировать исход того или иного вида воздействий, а набор связей формируют правила осуществления воздействия деструктивных потоков данных (рисунок 6).

Анализ потоков данных на втором и третьем уровне 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.

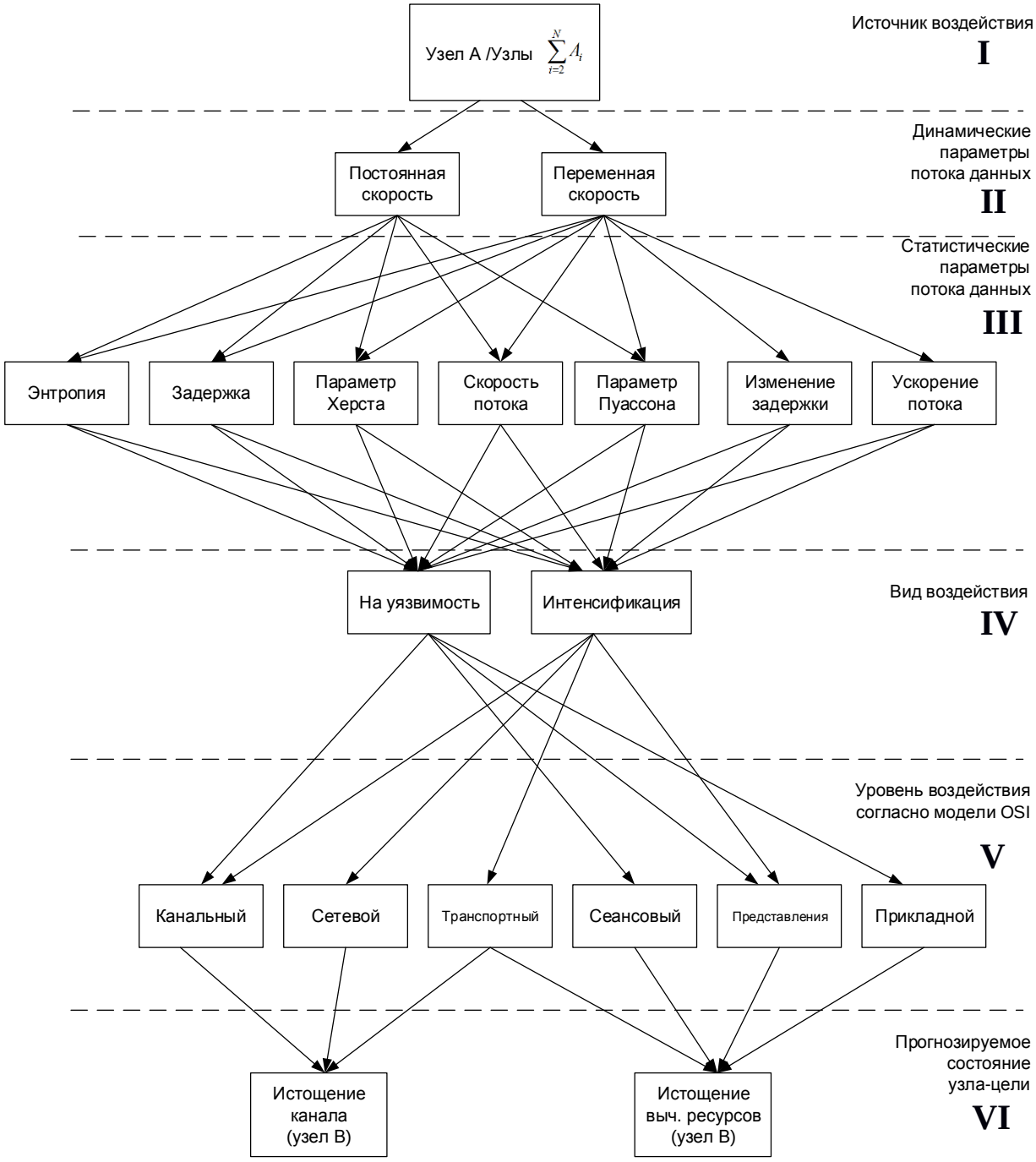
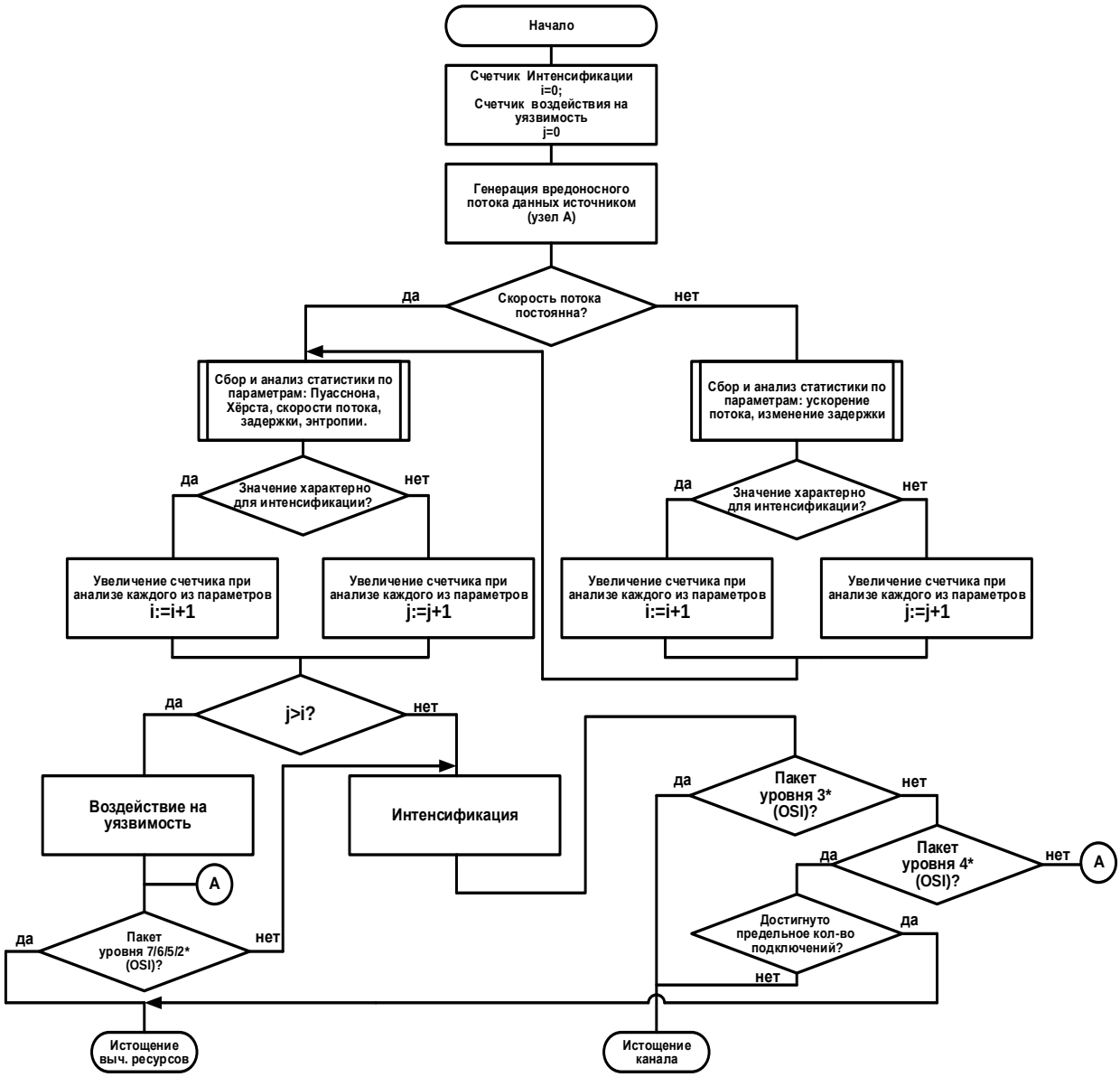


Рисунок 6 – Иерархическая модель воздействия деструктивных потоков данных на управляющие узлы технологической сети

На четвертом–шестом уровне производится анализ рисковых событий и прогнозирование состояния узла от успешно реализованного направленного воздействия в технологических сетях 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 7). Пороговые значения статистических параметров, используемые в качестве условий перехода, могут быть определены посредством нагрузочного тестирования.



* 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 7 – Алгоритм прогнозирования последствий воздействия деструктивных потоков данных на управляющие узлы технологической сети

Для прогнозирования отдельно взятого типа воздействия деструктивных

потоков данных иерархическую модель можно представить в виде направленного графа (рисунок 8).

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

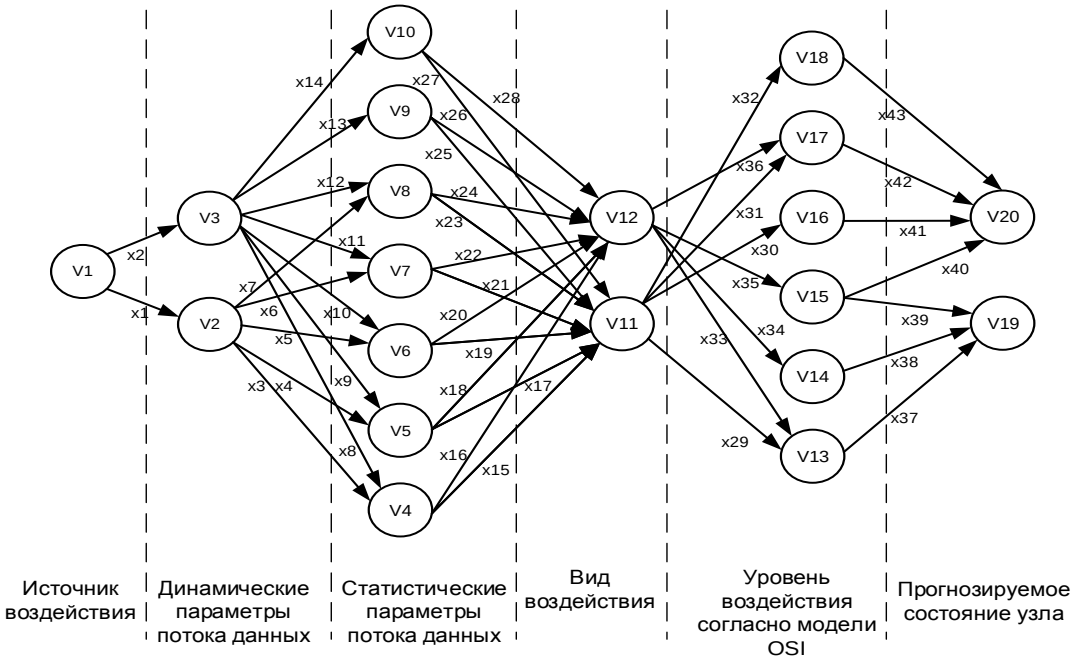


Рисунок 8 – Направленный граф воздействия деструктивных потоков данных на управляющие узлы технологической сети

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.

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 $F_{\text{служ}}$ различного характера, зависящих от архитектуры системы, то количество операций в единицу времени, которые могли бы выполнить простаивающие ресурсы процессора $F_{\text{простой}}$, зависит от максимального количества операций, выполняемых процессором в единицу времени $F_{\text{проц}}$, и их можно вычислить по формуле: $F_{\text{простой}} = F_{\text{проц}} - (F_{\text{служ}} + F_{прик})$.

Истощение вычислительных ресурсов и канала связи (рисунок 9) 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.

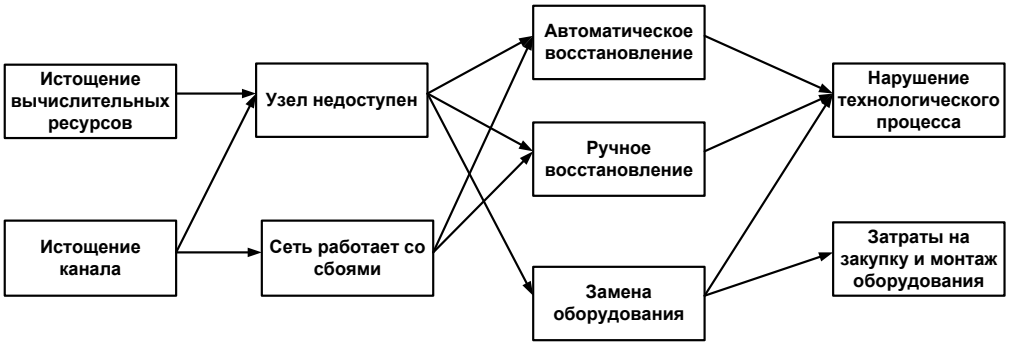


Рисунок 9 – Последствия воздействий деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия

Таким образом, если для обслуживания запросов узла/узлов источника деструктивных потоков данных процессору узла B необходимо выполнение операций, равных $F_{\text{д}}$, а время восстановления после прекращения воздействия $T_{\text{вос}}$(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.

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.

Решением задач определения величины потенциального ущерба и предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы в технологических сетях промышленного предприятия стала методика, основанная на статистическом анализе потоков данных для своевременной сигнализации о факте воздействия. При этом в технологической

сети нет необходимости очистки трафика, а оптимальным решением является своевременное определение и устранение источников вредоносного воздействия деструктивных потоков данных.

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.

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.

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 $T = 1$).

В качестве объекта апробации методики определения ущерба Y и предотвращения последствий воздействия деструктивных потоков данных на управляющие узлы в технологических сетях была рассмотрена система вентиляции промышленного предприятия (рисунок 10).

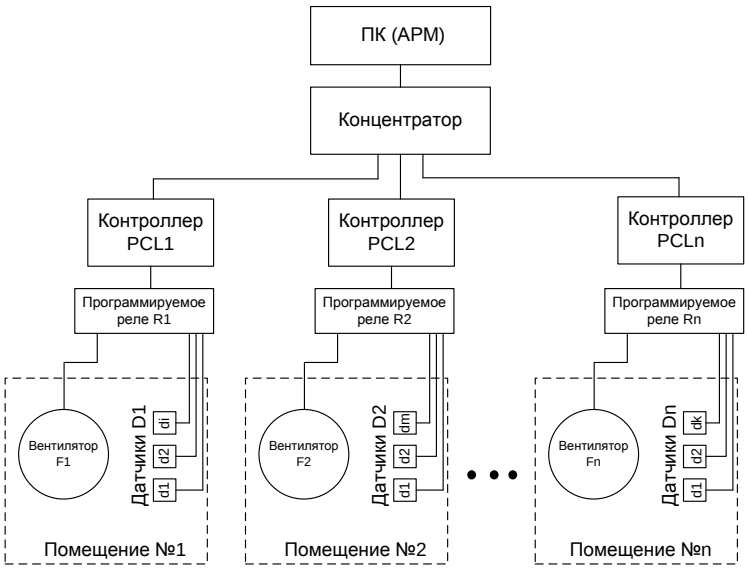


Рисунок 10 – Система вентиляции промышленного предприятия

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 11), 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 $R_2 = Y_2 P_2 t$.

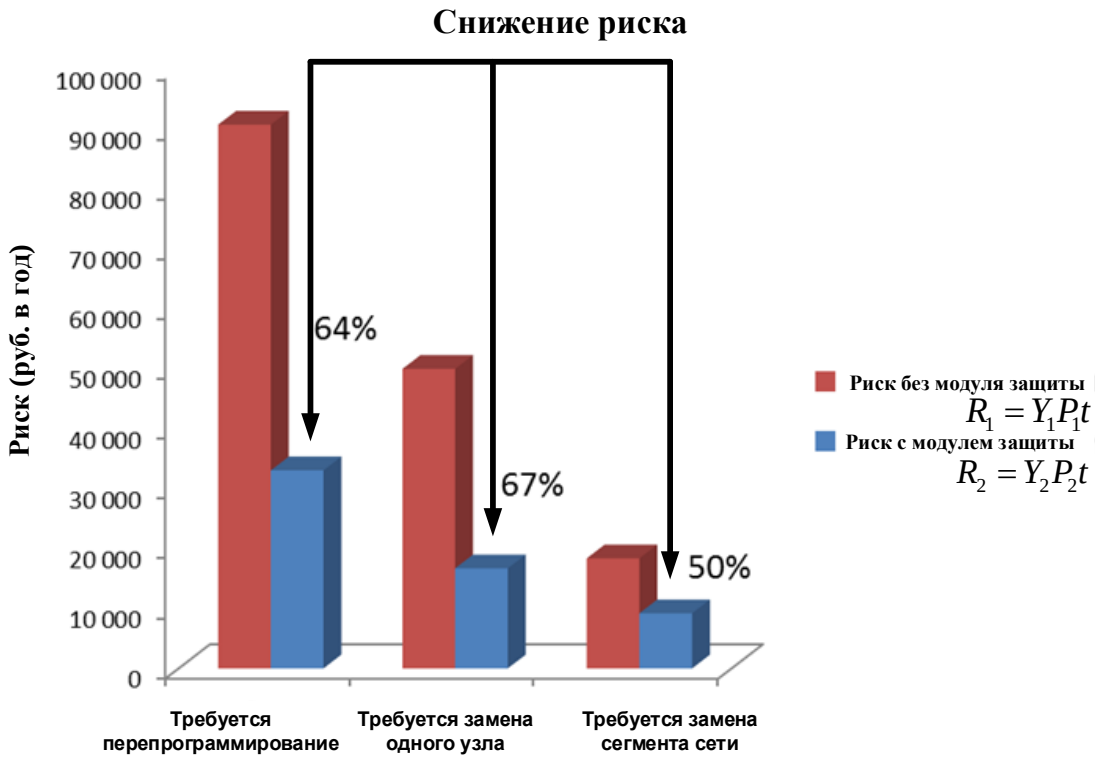


Рисунок 11 – Оценка эффективности применения модуля защиты

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 публикаций по теме диссертации в перечне, рекомендованном ВАК РФ:

1) 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. С. 4-16.

2) 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.

3) Жарова О.Ю., Глебов С.А., Чувак П.А. Разработка мер по уменьшению количества широковещательного трафика в локальной сети // Вопросы радиоэлектроники. 2017. №11. С. 15-20.

4) Жарова О.Ю., Федорова В.А. Метод определения типа атаки по статистическим параметрам сетевого трафика // Вопросы радиоэлектроники. 2016. №10. С. 39-43.

В других изданиях:

5) Жарова О.Ю. Применение системы анализа сетевой нагрузки для выявления начала DDoS-атаки // Вопросы радиоэлектроники. 2018. №11. С. 48-52.

6) Жарова О.Ю., Федорова В.А. Повышение эффективности гибридной системы, противодействующей DDoS-атакам // Вопросы радиоэлектроники. 2015. №8. С. 126-132.

7) 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.

8) 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.