ПОДХОДЫ К ПОИСКУ УЯЗВИМОСТЕЙ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В СЕТЯХ ЦИФРОВОГО ПРОИЗВОДСТВА

Парфёнов Д.И., Торчин В.А., Забродина Л.С., Парфёнов А.И.
Оренбургский государственный университет
parfenovdi@mail.ru

Аннотация: В настоящее время актуальным является проблема обеспечение кибербезопасности сетевой и информационной инфраструктуры критически важных объектов. Особое место в этом занимает безопасность автоматизированные системы управления, являющихся основой индустрии 4.0. При этом основным источником угроз для таких систем является внешняя сеть провайдера телекоммуникационных услуг, через которую осуществляется мониторинг работы удаленных объектов и систем. В рамках настоящего исследования разработан подход к поиску аномального поведения в сетях провайдеров телекоммуникационных услуг, построенный на основе анализа событий в журналах различных систем, в том числе отвечающих за сетевую безопасность. Предложенный подход является развитием системы управления информацией и событиями.

Ключевые слова: критическая информационная инфраструктура, сетевая безопасность, информационно-телекоммуникационные сети, автоматизированные системы управления, кибератаки.

Введение

На сегодняшний день использование компьютерных сетей является неотъемлемой частью повседневной жизни. Однако современные сети выполняют не только передачу данных между пользователями, но и обеспечивают функционирование объектов критической информационной инфраструктуры (КИИ) [1]. При этом транзитную инфраструктуру формируют провайдеры телекоммуникационных услуг, являющиеся ключевым звеном в цепочке информационного взаимодействия. Именно на их плечи ложится ответственность за обеспечение требуемого уровня сервиса (SLA), качества обслуживания (QoS) и безопасности сетей. Одной из масштабных мировых проблем, оказывающих влияние на функционирования сетей связи, является деструктивное воздействие, оказываемое со стороны различных нарушителей. Если в начале развития сетей конечной целью атак являлись простые пользователи, то на сегодняшний день пользователи и их персональные устройства, имеющие доступ к сети, выступают в роли инструментов для проведения атак на объекты КИИ. Только за 2018 год выявлено 4,3 млрд. кибератак на объекты критической информационной инфраструктуры в России [2]. В последние годы с развитием цифровых систем и переходу к индустрии 4.0 изменился и сам вектор атак. Если раньше основную долю атакуемых объектов составляли банковские информационные системы, то тенденцией последних лет стали атаки на промышленные объекты, а именно их автоматизированные системы управления (АСУ) [3]. Вывод из строя или нарушение заданных алгоритмов работы таких систем может повлечь за собой не только тяжелые финансовые потери, но и техногенные и иные негативные последствия.

Для решения обозначенных проблем провайдеры телекоммуникационных услуг для защиты конечных пользователей и объектов КИИ от внешних и внутренних угроз активно внедряют решения, позволяющие обеспечивать сетевую безопасность. На сегодняшний день, в данной области, существует достаточно много технических решений. Однако, основу любого программного комплекса составляет система обнаружения вторжений (IDS), для построения которой применяются SIEM-технологии (Security Information and Event Management). Одной из основных задач данного компонента является сбор и агрегирование данных мониторинга устройств и сервисов, входящих в зону ответственности провайдера телекоммуникационных услуг. Другой не менее важной задачей является анализ полученной информации и выявление инцидентов безопасности или обнаружение аномального поведения. Работа таких систем безопасности, как правило, организована по проактивному принципу – реакция на инциденты осуществляется до того, как ситуация станет критичной. Поэтому для таких систем критически важным является время принятия решений. Это особенно актуально ввиду постоянно изменяющихся векторов атак и методик их обнаружения. Тем не менее, анализ существующих решений показывает, большинство систем на сегодняшний день работают в полуавтоматизированном режиме. Конечное решение остается за администратором сетевой безопасности, осуществляющим контроль и наблюдение за работой данной системы. При этом для принятия решений администратору сетевой безопасности необходимо в сжатые сроки проанализировать множество разнородных факторов. Этот факт

негативно сказывается на результатах реакции на проводимые атаки. Допущенные ошибки могут сказаться на работе АСУ едва ли не хуже самой атаки, проводимой на нее.

Поэтому построение интеллектуальных систем защиты и обеспечения безопасности для объектов критической информационной инфраструктуры (КИИ) является актуальным направлением. Базовым компонентом при этом является система мониторинга событий.

1 Обзор исследований

Разработке методов и подходов к выявлению и обнаружению атак, в том числе, сетях передачи данных и системах АСУ посвящено достаточно много исследований.

В работе [4] проводится обзор и систематизация методов и подходов к организации систем безопасности, применяемых для Intrusion Detection in Industrial Control Systems. Авторы отмечают три наиболее эффективных подхода применяемые при использовании Network-Based Intrusion Detection Systems. В их число входят: метод поиска Critical Process Values, метод сканирования Network Packet Reporting Values and метод Network Traffic Pattern Anomalies. В настоящее время все большую популярность набирают методы, основанные на интеллектуальном анализе данных.

В работе исследователей из Peter the Great St. Petersburg Polytechnic University решается задача обнаружения атак на магистральных сетях передачи данных. Авторы предлагают прототип модуля анализа сетевого трафика, позволяющий объединять данные, получаемые из потока трафика во временные ряды и проводить дальнейший математический анализ. В основе предложенного модуля положен иерархический принцип агрегации данных, что существенно сокращает время на анализ данных [5].

В работе [6] авторами исследования разработано приложение для обнаружения атак SysDetect. В основе предложенного подхода по определению критических изменений в состоянии системы используется итеративный алгоритм интеллектуального анализа данных, то есть Apriori. Это позволяет достаточно точно идентифицировать все состояния системы.

В исследовании [7] авторы проводят поиск атак на системы SCADA путем анализа трафика в открытой и закрытой сети на различных промежутках времени. При этом основная задача сводится к поиску аномалий в поведении системы путем оценки самоподобия трафика системы SCADA.

Важной составляющей для разработки эффективной системы обнаружения вторжений на критически важную инфраструктуру является наборы данных, характеризующих различные виды атак. Авторы исследования в своей работе проводят глубокий сравнительный анализа различных шести наборов данных, полученных при мониторинге работы Industrial control systems на различных уровнях. Тем не менее представленные наборы охватывают не полный перечень угроз и как следствие не позволяют достаточно полно обучить интеллектуальную систему обнаружения вторжений [8].

Современные производственные системы в своей работе используют множество датчиков, собирающих информацию о состоянии оборудования и протекающих технологических процессах. В исследовании статье авторы предлагают методологию для разработки систематического подход к анализу набора данных для обнаружения аномалий трафика в сети таких IoT [9].

В работе исследуются атаки на киберфизические системы (CPS). Авторами предложен метод SIDS, направленный на обнаружения аномалий в поведении CPS. Предложенный метод основан на анализе состояний CPS и частоты их изменения. В проведено исследовании авторы отмечают, что метод SIDS позволяет эффективно обнаруживать кибератаки на large I/O CPSs [10].

Иной подход к поиску уязвимостей в сетях критически важной инфраструктуры рассмотрен в исследовании. Авторы предлагают использовать достаточно популярный метод, основанный на использовании системы Honeynet. Полученные данные могут быть использованы для обогащения наборов данных, используемых при обучении интеллектуальной системы обнаружения атак [11].

Таким образом, обзор исследований в области обеспечения безопасности критической информационной инфраструктуры показал, что в настоящее время отсутствует комплексное решение позволяющие выявлять атаки на ранней стадии ввиду отсутствия эффективных методов их обнаружения.

2 Постановка задачи

Рассмотрим постановку задачи мониторинга потоков событий и инцидентов безопасности в сети провайдеров телекоммуникационных услуг. В целом задачу мониторинга сети можно описать следующим образом. Поскольку события, происходящие в сети провайдеров телекоммуникационных услуг, носят случайный характер, то для их анализа наиболее

подходящими являются вероятностные математически модели теории массового обслуживания – теорией марковских цепей. Чаще всего модель сеть провайдера телекоммуникационных услуг представляет собой топологию «дерево» с дополнительными избыточными связями. Неотъемлемой составляющей сети любого оператора связи является система мониторинга событий, собирающая информацию о состоянии устройств и циркулирующих потоках трафика. В качестве сервиса мониторинга чаще всего применяют одну из следующих систем Zabbix/Nagios/Cacti и др. В задачи системы мониторинга входит не только сбор данных, но и их предварительная обработка, а также запуск скриптов оповещений о срабатывании определенных типов событий. Кроме того, по действующему законодательству провайдеры обязаны внедрить в своей сети программно-аппаратный комплекс для сбора, накопления и хранения информации об абонентах операторов связи (СОРМ), а так же обеспечить хранение проходящего трафика пользователей в специализированном хранилище данных. Таким образом, перечисленные системы образуют единую информационную платформу основной целью которой является поиск и выявление сетевых атак.

3 Моделирование системы мониторинга уязвимостей и обеспечения безопасности

На начальном этапе моделирования необходимо определить входные данные. В качестве состояний рассматриваемой системы мониторинга сети предлагается рассмотреть события, возникающие в сети провайдера в разрезе трафика, проходящего через телекоммуинкационное оборудование. Данные о произошедших событиях сети хранятся в журнале событий, представляющий собой следующий кортеж:

$$< data\_time,\ src\_ip,\ dst\_ip,\ src\_port,\ dst\_port,\ protocol,\ size >, \quad (1)$$

где: *data_time* – дата и время отправления пакета;
src_ip – IP-адрес отправителя пакета;
dst_ip – IP-адрес получателя пакета;
src_port – порт отправителя пакета;
dst_port – порт получателя пакета;
protocol – сетевой протокол, по которому осуществляется соединение;
size – размер пакета.

Рассмотрим исходные данные, а именно, список записей сформированных проходящим через сеть провайдера трафиком. В рамках исследования из множества характеристик, описывающих сетевые соединения, были выбраны такие характеристики как IP-адреса отправителя и получателя, соответствующие им порты и протокол, по которому осуществляется передача данных. Каждую такую строку представим в виде вектора следующего вида:

$$x_k = \{x_{k1}, x_{k2}, x_{k3}, x_{k4}, x_{k5}, x_{k6}, x_{k7}\}, \quad (2)$$

где: k – номер записи в журнале;
x_{k1} – дата и время отправления пакета;
$x_{k2} \in [0; 2^{32} - 1]$ – IP-адрес отправителя пакета;
$x_{k3} \in [0; 2^{32} - 1]$ – IP-адрес получателя пакета;
$x_{k4} \in [0; 65535]$ – порт отправителя пакета;
$x_{k5} \in [0; 65535]$ – порт получателя пакета;
x_{k6} – сетевой протокол, по которому осуществляется соединение;
x_{k7} – размер пакета.

Список записей о пакетах представим в виде множества следующего вида:

$$X = \{x_k\}, \quad k = \overline{1,n}, \quad (3)$$

где n – длина списка журнала.

Для того, чтобы анализировать состояния узлов в процессе передачи данных в сети установлен сервер Zabbix, который предоставляет данные с системы мониторинга о сетевых устройствах следующего формата:

$$< CPU\_LOAD,\ ping, RAM\_load,\ ch\_speed,\ av\_port,\ port\_speed,\ lp >, \quad (4)$$

где: *CPU_LOAD* - нагрузка на CPU %;

ping - время отклика (мс.);
RAM_load - загрузка памяти %;
ch_speed - пропускная способность канала Мбит/с;
av_port - доступность порта (да/нет);
port_speed - скорость работы порта Мбит/с;
lp - количество потерь пакетов.

Тогда список записей с системы мониторинга о сетевых устройствах можно представить в виде множества следующего вида:

$$(5) \qquad \begin{aligned} Z^s &= \{z_k^s\}, \quad k = \overline{1,m} \\ z_k^s &= \{z_{k1}^s, z_{k2}^s, z_{k3}^s, z_{k4}^s, z_{k5}^s, z_{k6}^s, z_{k7}^s\}, \end{aligned}$$

где *m* – количество сетевых устройств.

Данные Z^I с системы мониторинга о состоянии информационной системы, поддерживающей работу критически важных объектов имеют другой формат:

$$(6) \qquad < time\_work,\ CPU,\ storage,\ stat\_in >,$$

где *time_work* - время выполнения работы мс. (z_{k1}^I);

storage - загрузка памяти % (z_{k2}^I);

CPU - загрузка CPU % (z_{k3}^I);

stat_in={(*ip_*,*numb_in*)} (z_{k4}^I) – статистика входа на ИС с IP-адресов (содержит записи вида: (IP-адрес, среднесуточное количество входов)).

Список записей о состоянии информационной системы в этом случае имеет вид:

$$(7) \qquad \begin{aligned} Z^I &= \{z_k^I\}, \quad k = \overline{1,p} \\ z_k^I &= \{z_{k1}^I, z_{k2}^I, z_{k3}^I, z_{k4}^I\} \end{aligned}$$

где *p* – количество информационных систем.

Для получения реальной возможности оперирования имеющейся информацией для расследования инцидентов, введем структуру данных следующего вида:

$$(8) \qquad < id,\ name,\ adj\_matrix,\ id\_ch,\ cond,\ pid >,$$

где *id* – идентификатор подсистемы, введенный для возможности ссылаться на подсистему; *name* – название подсистемы;

adj_matrix – матрица смежности элементов системы/подсистемы;

id_ch – вектор идентификаторов составляющих системы/подсистемы, в случае если рассматривается узел, матрица смежности не включается, а этот параметр будет являться IP-адресом;

cond – вектор характеристик, описывающих текущее состояние подсистемы;

pid – идентификатор предка подсистемы.

На основе построенной модели в рамках настоящего исследования разработан подход, позволяющий скорелировать данные двух взаимосвязанных систем: мониторинга состояний сети и обнаружения вторжений.

Для этого опешим множество возможных состояний

- S_0 – отсутствие неисправностей;
- S_1 – перегрузка сети;
- S_2 – снижение пропускной способности;
- S_3 – недопустимость порта;
- S_4 – физическая недопустимость устройства;
- S_5 – фрагментация пакета;
- S_6 – полный отказ системы.

Отметим что каждый вектор атак, характеризуется собственным графом переходов из состояния S_i в состояние S_j. Кроме того сама смена состояний характеризуется определенной частотой и распределена по времени. Еще одной не менее важной характеристикой является набор событий, генерируемый элементами информационной системы, входящей в состав объекта критической информационной инфраструктуры. Этот набор данных так же позволяет охарактеризовать поведение системы в заданный момент времени. Эти и другие характеристики

позволяют сформировать набор данных позволяющих построить профиль типового поведения каждого компонента системы и как следствие идентифицировать атаки на целевые системы.

Алгоритм действий, иллюстрирующий предлагаемое решение представлен на рисунке 1.

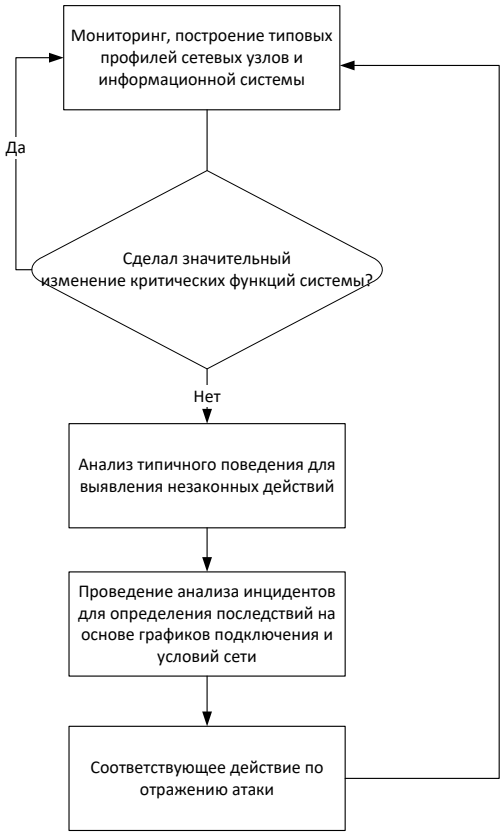

Рис. 1. Блок-схема алгоритма выявления аномального поведения объектов критической информационной инфраструктуры

Предлагаемое решение позволяет обнаруживать аномальное поведение объектов критической информационной инфраструктуры и реагировать на них с опережением по времени.

В рамках исследования развернут виртуальный стенд, эмулирующий работу сети провайдера, предоставляющего подключение к АСУ. Для этого в экспериментальной сети развернутой на базе облачной платформы OpenNebula развернуто три сегмента сети. В состав первого сегмента сети входят 6 вычислительных узлов, эмулирующие работу системы АСУ. В состав второго сегмента входят 8 вычислительных узлов, эмулирующих работу основных компонентов сети провайдера телекоммуникационных услуг, в том числе системы безопасности, обнаружения вторжений и хранения данных об инцидентах. В состав третьего сегмента входят 16 вычислительных узлов, эмулирующих работу легитимных пользователей и злоумышлиников. Для чистоты экспериментов роли узлов в третьем сегменте сети назначались случайным образом. Также стоит

В качестве базовой системы для организации интеллектуальной обработки данных выбран Apache Spark. В качестве хранилища данных использована Cassandra. Для генерации механизмов атак в качестве исходных наборов данных выбраны публичные Dataset: KDD99 CUP, NSL-KDD, UNSW-NB15. Для исследования перечисленных наборов данных в качестве целевых угроз выбраны следующие векторы атак: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode и Worms. Для классификации по принципу атака-обычный трафик использовалась библиотека для машинного обучения MLLib, входящая в состав Apache Spark.

Вычислительный эксперимент состоял из двух этапов. На первом этапе на целевую систему АСУ генерировались потоки трафика согласно выбранного вектора атаки. При этом в исследуемой системе АСУ собирались данные о событиях возникающих как в самой сети первого сегмента, так и непосредственно в АСУ. Полученные данные агрегировались системой мониторинга и загружались в хранилище данных для последующей обработки. После нормализации и обработки этих данных был сформирован dataset IS_LOG, характеризующий каждый из векторов атак. На основании полученных данных сформированы гибридные наборы данных <name_dataset>+IS_LOG.

На втором этапе экспериментального исследования каждый исходный и гибридный набор данных разделен на два фрагмента: тестовое и обучающее множество. При этом объем каждого тестового множества составляет 10% от общего исследуемого объема данных. В качестве классификатора в рамках второго этапа экспериментального исследования выбрана логистическая регрессия так как этот метод является достаточно эффективным для задач большого размера. В основе логистической регрессии лежит статистическая модель, используемая для прогнозирования вероятности событий путем подгонки данных к логистической кривой.

Для оценки эффективности использования типовых профилей атак при выявлении подозрительной сетевой активности в сети провайдеров телекоммуникационных услуг проведем ROC-анализ, используемый для анализа результатов бинарной классификации. Процесс классификации действий на атаки различного типа представляет собой бинарную классификацию атака/неатака. При этом выделяют класс с положительными исходами (верно классифицированные события), а также с отрицательными исходами (неверно классифицированные события). ROC-кривая показывает зависимость истинно положительных примеров от ложно отрицательных примеров.

Введем следующие обозначения:

TP (True Positives) – истинно положительные случаи;

TN (True Negatives) – истинно отрицательные случаи;

FN (False Negatives) – положительные примеры, классифицированные как отрицательные (ошибка I рода, ложно отрицательные случаи);

FP (False Positives) – отрицательные примеры, классифицированные как положительные (ошибка II рода, ложно положительные случаи).

При анализе чаще оперируют относительными показателями (долями):

Доля истинно положительных примеров (True Positives Rate):

$$TP \cdot 100\% / (TP + FN) \quad (9)$$

Доля ложно положительных примеров (False Positives Rate):

$$FPR = FP \cdot 100\% / \left(TN + FP\right) \quad (10)$$

Важно отметить, что объективная ценность бинарного классификатора отражается в его чувствительности и специфичности.

Чувствительность (Sensitivity) –доля истинно положительных случаев:

$$Se = TPR = TP \cdot 100\% / \left(TP + FN\right) \quad (11)$$

Специфичность (Specificity) – доля истинно отрицательных случаев, которые были верно идентифицированы моделью:

$$Sp = TN \cdot 100\% / \left(TN + FP\right) \quad (12)$$

Выделим для прогностической модели идентификации атак ложно положительные (False Positive) и истинно положительные (True Positive) случаи (таблица 1).

Таблица 1. Результаты экспериментального исследования

Набор данных	Точность определения атаки	TP	TN	FP	FN
KDD99 CUP	92%	95%	92%	3.0%	6.0%
KDD99 CUP + IS_LOG	94%	97,2%	93%	2.0%	5.8%
NSL-KDD	95%	94%	92%	2.0%	5.7%
NSL-KDD + IS_LOG	96,6%	95,1%	93,8%	1.8%	4.3%
UNSW-NB15	96%	95%	94%	1.0%	4.3%
UNSW-NB15 + IS_LOG	97.9%	97.51%	99.48%	0.51%	2.48%

Таким образом, исследование показало, что предложенный подход к идентификации атак на основе расширенного за счет анализа событий в журналах различных информационных систем гибридного набора данных, позволяет более точно определять вторжения в сетях провайдеров телекоммуникационных услуг.

Заключение

В ходе исследования были решены следующие задачи:

1) Рассмотрены основные угрозы безопасности и типы атак, актуальные для объектов критической информационной инфраструктуры индустрии 4.0.

2) Разработана модель мониторинга событий и обнаружения сетевых атак на основе методов интеллектуального анализа данных.

3) Проанализированы наборы данных сетевого трафика, пригодные для моделирования трафика промышленной сети предприятий: KDD99 CUP, NSL-KDD, UNSW-NB15 для задачи обнаружения сетевых атак, а так же предложено расширение существующих наборов данных за счет анализа событий в журналах различных информационных систем.

4) Проведен вычислительный эксперимент по построению классификатора атак на основе гибридного набора данных на основе логистической регрессии. Доказана эффективность предложенного решения.

Работа выполнена при финансовой поддержке РФФИ проект № 18-07-01446, гранта Президента Российской Федерации для государственной поддержки молодых российских ученых - кандидатов наук (МК-860.2019.9), а так же Министерства образования Оренбургской области (Соглашение №12).

Литература

1. Зегжда Д. П. и др. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации //Вопросы кибербезопасности. – 2018. – №. 2 (26). – С. 2-15.
2. Бабаев Д.И., Полетыкин А.Г., Промыслов В.Г., Тимофеев М.Ю. Управление архитектурой кибербезопасности АСУТП атомных электростанций ///Проблемы управления. – 2018. – №. 3. – С. 47-55.
3. Bolodurina I. P. et al. Development and Research of Model for Ensuring Reliability of Operation of Network Infrastructure Objects in Cyber-physical System Located in the Cloud Platform //2018 Global Smart Industry Conference (GloSIC). – IEEE, 2018. – P. 1-7.
4. Koh P. et al. Intrusion Detection Methodology for SCADA system environment based on traffic self-similarity property //Journal of the Korea Institute of Information Security and Cryptology. – 2012. – Т. 22. – №. 2. – P. 267-281.
5. Poltavtseva M. A., Zegzhda P. D., Pankov I. D. The Hierarchial Data Aggregation Method in Backbone Traffic Streaming Analyzing to Ensure Digital Systems Information Security //2018 Eleventh International Conference" Management of large-scale system development"(MLSD. – IEEE, 2018. – P. 1-5.
6. Khalili A., Sami A. SysDetect: a systematic approach to critical state determination for Industrial Intrusion Detection Systems using Apriori algorithm //Journal of Process Control. – 2015. – Т. 32. – P. 154-160.
7. Cherdantseva Y. et al. A review of cyber security risk assessment methods for SCADA systems //Computers & security. – 2016. – Т. 56. – P. 1-27.
8. Choi S., Yun J. H., Kim S. K. A Comparison of ICS Datasets for Security Research Based on Attack Paths //International Conference on Critical Information Infrastructures Security. – Springer, Cham, 2018. – P. 154-166.
9. Sherasiya T., Upadhyay H., Patel H. B. A survey: Intrusion detection system for internet of things //International Journal of Computer Science and Engineering (IJCSE). – 2016. – Т. 5. – №. 2.
10. Khalili A. et al. SIDS: State-based intrusion detection for stage-based cyber physical systems //International Journal of Critical Infrastructure Protection. – 2018. – Т. 22. – P. 113-124.
11. Serbanescu A. V., Obermeier S., Yu D. Y. ICS threat analysis using a large-scale honeynet //Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research. – BCS Learning & Development Ltd., 2015. – P. 20-30.