Международный союз электросвязи

МСЭ-Т

X. 1376

(01/2021)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги (2) – Безопасность интеллектуальных транспортных систем (ИТС)

Механизм обнаружения относящегося к безопасности ненадлежащего поведения, использующий большие данные, для соединенных транспортных средств

Рекомендация МСЭ-Т X.1376

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	**X.1370–X.1389**
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1376

Механизм обнаружения относящегося к безопасности ненадлежащего поведения, использующий большие данные, для соединенных транспортных средств

Резюме

В Рекомендации МСЭ-Т X.1376 описан механизм обнаружения относящегося к безопасности ненадлежащего поведения для соединенных транспортных средств в помощь заинтересованным сторонам при использовании автомобильных данных для повышения безопасности транспортных средств.

С расширением возможности соединения транспортных средств возрастает количество уязвимостей вследствие развития сложных технологий. Такие уязвимости увеличивают число угроз для соединенных транспортных средств. Для оценки безопасности соединенных транспортных средств весьма полезен анализ большого количества автомобильных данных.

Хронологическая справка

Издание	Рекомендация	Утверждена	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1376	07.01.2021 г.	17-я	11.1002/1000/14448

Ключевые слова

Соединенные транспортные средства; обнаружение ненадлежащего поведения.

* Для доступа к Рекомендации наберите URL http://handle.itu.int/ в вашем веб-браузере, а затем уникальный идентификатор Рекомендации. Например: http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1376

Механизм обнаружения относящегося к безопасности ненадлежащего поведения, использующий большие данные, для соединенных транспортных средств

1 Сфера применения

В настоящей Рекомендации описан механизм обнаружения относящегося к безопасности ненадлежащего поведения для соединенных транспортных средств. Этот механизм выполняет определенные ниже функции.

a) Сбор данных. – Определение типов данных и информации, которые могут быть получены из различных источников, включая автомобили, элементы инфраструктуры, производителей оригинального оборудования (OEM) и поставщиков, в целях обнаружения ненадлежащего поведения. Методы и процедуры сбора данных выходят за рамки настоящей Рекомендации.

b) Обнаружение. –Анализ собранных данных для обнаружения ненадлежащего поведения.

Настоящая Рекомендация применяется к соединенным транспортным средствам для выявления ненадлежащего поведения проектировщиками и поставщиками решений в целях обеспечения безопасности. Методы использования уведомлений выходят за рамки настоящей Рекомендации.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

Отсутствуют.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 ненадлежащее поведение (misbehaviour): Акт предоставления ложных или вводящих в заблуждение данных, направленный на то, чтобы помешать другим получателям услуг или действовать за пределами разрешенной сферы. Ненадлежащее поведение может исходить от внутренних или внешних компонентов системы транспортного средства.

ПРИМЕЧАНИЕ 1. – Основано на [b-ISO/TR 17427-4].

ПРИМЕЧАНИЕ 2. – Ненадлежащее поведение включает в себя подозрительное поведение, преднамеренное или непреднамеренное, например сообщения неправильного типа или нарушение периодичности сообщений, недопустимый вход в систему и несанкционированный доступ, неправильно подписанные или зашифрованные сообщения и т. д.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ADAS Advanced Driver-Assistance Systems Современные системы содействия водителю

ABS	Anti-skid Braking System		Противоскользящая тормозная система
AEB	Autonomous Emergency Braking		Автономное экстренное торможение
API	Application Programming Interface		Интерфейс прикладного программирования
CAN	Controller Area Network		Локальная сеть контроллеров
GNSS	Global Navigation Satellite System	ГНСС	Глобальная навигационная спутниковая система
ITS	Intelligent Transportation System	ИТС	Интеллектуальная транспортная система
IP	Internet Protocol		Протокол Интернет
LiDAR	Light Detection and Ranging	лидар	Датчик лазерного обнаружения и измерения дальности
MCU	Microcontroller Unit		Микроконтроллер
OEM	Original Equipment Manufacturer		Производитель оригинального оборудования
TCU	Telematics Control Unit		Блок управления телематикой
URL	Uniform Resource Locator		Унифицированный указатель ресурса

5 Соглашения

Отсутствуют.

6 Модель механизма обнаружения ненадлежащего поведения

Модель механизма обнаружения ненадлежащего поведения для соединенных транспортных средств представлена на рисунке 1. Работа механизма включает два этапа – сбор данных и обнаружение ненадлежащего поведения, которые реализуются двумя системами.

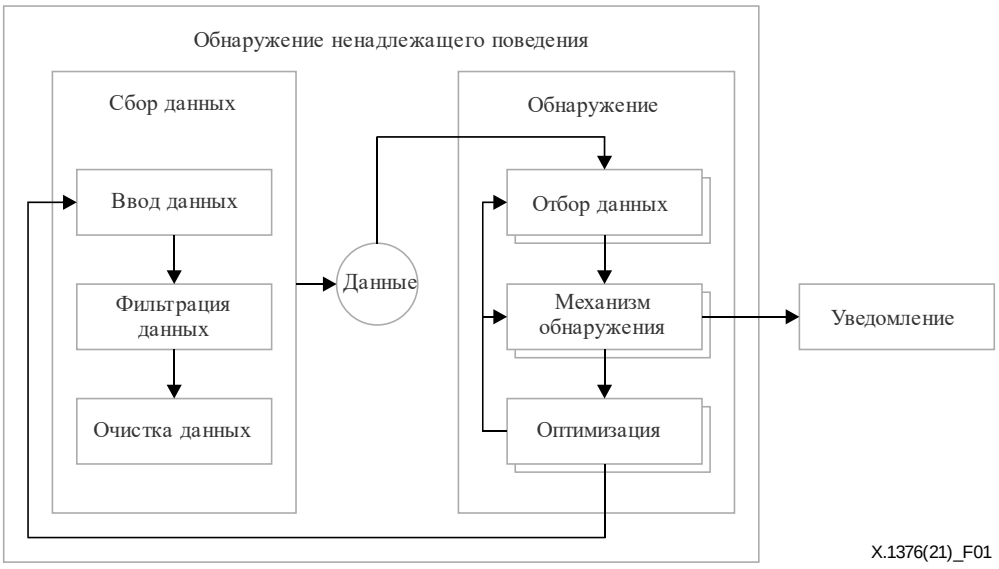

Рисунок 1 − Модель механизма обнаружения ненадлежащего поведения

Поскольку методы и процедуры сбора данных выходят за рамки настоящей Рекомендации, система сбора данных (например, фильтрация данных и очистка данных), представленная на рисунке 1, представляет собой лишь информативный пример практической реализации обнаружения ненадлежащего поведения.

Данные из системы сбора передаются в систему обнаружения, и собранные данные обрабатываются в соответствии с типами, описанными в разделе 7.

Система сбора данных состоит из следующих модулей:

a) модуль сбора данных: собирает данные для системы обнаружения из разных источников, например от поставщиков услуг, из системы кузова и от датчиков;

b) модуль фильтрации данных: фильтрует собранные данные на основе классификации данных;

c) модуль очистки данных: выполняет операции дедупликации и подавления шума в собранных данных.

Система обнаружения состоит из следующих модулей:

a) модуль отбора данных: отбирает наборы данных в соответствии с различными методами обнаружения ненадлежащего поведения, а затем передает их механизму обнаружения;

b) механизм обнаружения: обнаруживает ненадлежащее поведение на основе использования методов обнаружения, а затем передает результаты решений для оптимизации и уведомления в зависимости от ситуации;

c) модуль оптимизации: использует результаты обнаружения, поступившие от механизма обнаружения, для совершенствования механизмов отбора, обнаружения и ввода данных.

Модуль уведомления передает результаты работы механизма обнаружения заинтересованным сторонам. Он не входит в сферу охвата настоящей Рекомендации.

7 Сбор данных

Сбор данных обычно подразумевает ввод, очистку и фильтрацию данных. Ввиду того что методы и процедуры сбора данных выходят за рамки настоящей Рекомендации, здесь приведены только те типы данных, которые используются в процедуре обнаружения. Любые конфиденциальные персональные данные должны быть защищены с помощью соответствующих технологий, таких как обеспечение анонимности, которые выходят за рамки настоящей Рекомендации.

В этом разделе на основе данных и информации, полученных из разных источников, перечислены типы данных, используемые в механизме обнаружения ненадлежащего поведения, а именно данные о состоянии, данные управления и оперативные данные, как показано в таблице 1.

Таблица 1 − Типы данных

Тип	Подтип	Источники данных	Примеры данных
Данные о состоянииа	Данные приложений или служб	Поставщик контента или услуг	Информационно-развлекательные данные
		Данные картографической службы	Навигация, позиционирование
		Данные из мобильного приложения	Данные, связанные с приложением
	Состояние транспортного средства	Система безопасности	Противоскользящая тормозная система (ABS), подушка безопасности, автономное экстренное торможение (AEB), современные системы содействия водителю (ADAS)
		Система кузова	Двери, окна, дворники
		Система шасси	Крутящий момент, угол
		Система двигателя	Скорость, частота вращения, дроссельная заслонка, остановка двигателя
	Датчики состояния окружающей среды	Радар	Радар миллиметрового диапазона
		Датчик лазерного обнаружения и измерения дальности (Лидар)	Облако точек

Таблица 1 − Типы данных

Тип	Подтип	Источники данных	Примеры данных
		Ультразвуковые датчики	Расстояние
		Видеокамера	Изображение окружающей обстановки
		Датчики интеллектуальной транспортной системы (ИТС)	Знак придорожных сооружений
Данные управленияb	Локальное управление	Бортовой контроллер	Открытие дверей, закрытие дверей
	Дистанционное управление	Автоматизация, телематика	Удаленная диагностика
Оперативные данныес	Данные внутренних исследований	Исследование безопасности, результаты испытаний	Уязвимости, ошибки ПО, внутренние события, относящиеся к кибербезопасности
	Оперативные данные из внешних источников	Заказчик, поставщик, сообщество, конференции или литература, интернет	Адрес протокола Интернет (IP), хэш-значения, унифицированный указатель ресурса (URL), доменные имена, общеизвестные уязвимости и незащищенности (CVE) и т. д.

a Данные и информация, относящиеся к состоянию транспортных средств, приложений, услуг, датчиков и других объектов в составе ИТС.

b Данные и информация, используемые для управления транспортными средствами, приложениями, услугами, датчиками и другими объектами в составе ИТС.

c Данные и информация, относящиеся к кибербезопасности, полученные от источников вне ИТС. Предполагается, что источники данных имеют надлежащий уровень целостности.

8 Обнаружение

Модуль обнаружения составляют в основном отбор данных, механизм обнаружения и оптимизация. Механизм обнаружения использует анализ больших данных для выявления ненадлежащего поведения, основываясь на данных и информации из разных источников, как показано на рисунке 2. Модуль оптимизации применяет случаи ненадлежащего поведения для оптимизации отбора данных, а механизм обнаружения делает обнаружение ненадлежащего поведения более точным и эффективным.

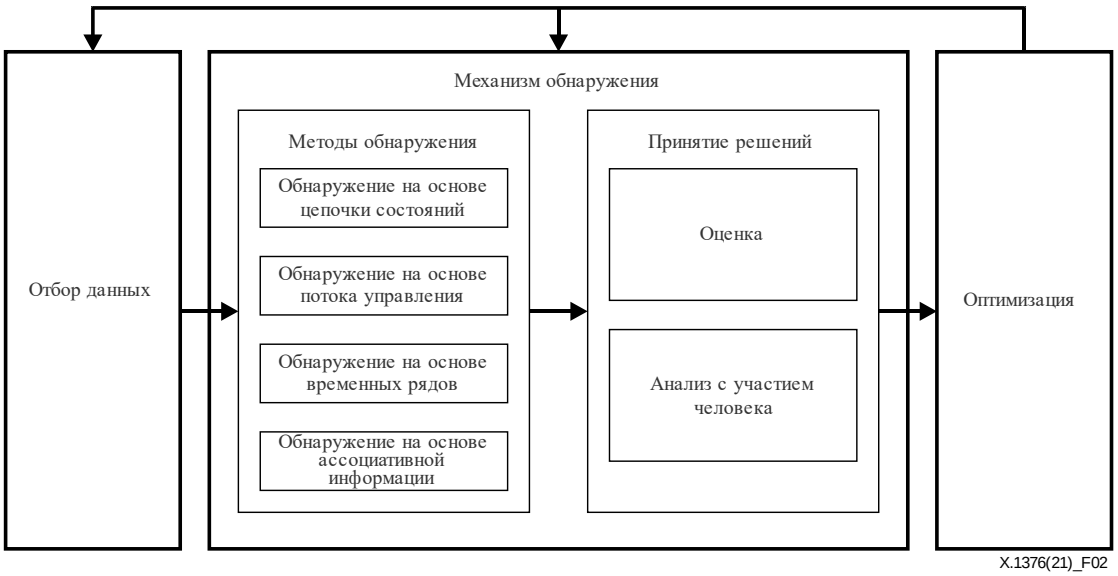

Рисунок 2 − Процедура обнаружения

8.1 Отбор данных

Исходя из требований к данным, обусловливаемых различными методами обнаружения, модуль отбора данных группирует данные по различным наборам данных в соответствии с требованиями механизмов обнаружения, как показано на рисунке 3. Входными данными для модуля отбора данных служат данные из системы сбора данных.

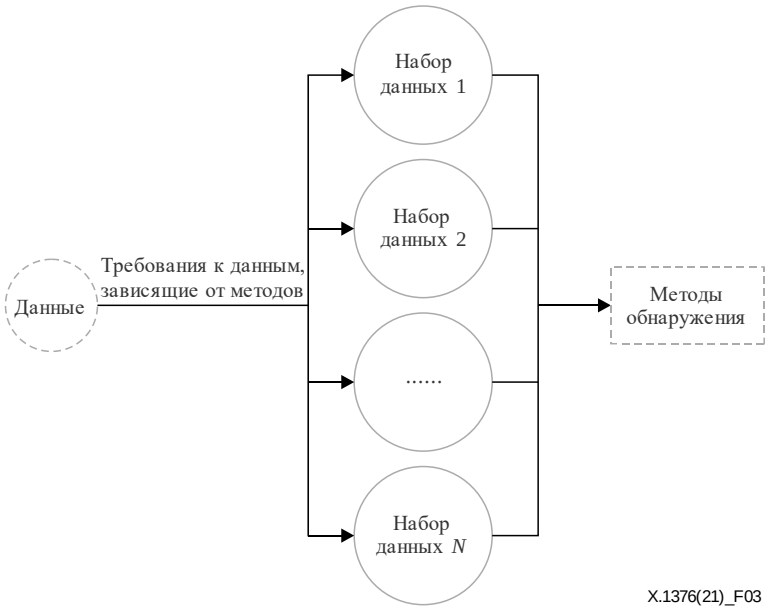

Рисунок 3 − Процедура отбора данных

8.2 Механизм обнаружения

Механизм обнаружения состоит из двух подмодулей: подмодуля методов обнаружения и подмодуля принятия решений. Когда наборы данных поступают в подмодуль методов обнаружения, он преобразует их в признаки поведения. Затем подмодуль принятия решений принимает решение на основе этих признаков поведения. Результаты принятия решений включают три различных типа: запрещено, подозрительно и разрешено. Результат "запрещено" означает аномалию, результат "подозрительно" означает, что невозможно определить, являются ли данные запрещенными или безопасными, а результат "разрешено" означает, что данные безопасны.

8.2.1 Методы обнаружения

Подмодуль методов обнаружения представляет собой набор различных методов обнаружения. На основе типов данных, перечисленных в разделе 7, разработаны четыре метода обнаружения ненадлежащего поведения с использованием этих данных.

8.2.1.1 Обнаружение на основе цепочки состояний

Цепочка состояний содержит ряд коррелированных данных о состоянии. Изменение одного элемента данных в цепочке состояний вызывает одновременное изменение других данных.

Ниже приведены некоторые характеристики цепочки состояний:

a) узел: служба или приложение в составе ИТС, имеющие отношение к действию;

b) поток: направление и траектория изменения данных в результате действия.

Данные о состоянии генерируются в ИТС, и возможно создание контекста, содержащего эти данные. Значение данных также соответствует определенной закономерности и колеблется в пределах определенного диапазона.

По существу, цепочку состояний можно отнести к одной из двух моделей: линейной или древовидной. Эти модели определяются следующим образом:

1) линейная модель: для каждого узла имеется только один узел, принимающий его сигнал;

2) древовидная модель: один узел создает два или более элемента данных о состоянии одновременно и передает их разным узлам.

В линейной модели цепочки состояний узлы имеют только однонаправленные связи (см. рисунок 4).

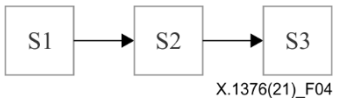

Рисунок 4 − Линейная модель цепочки состояний
S: статус

В древовидной модели цепочки состояний узлы можно подразделить на две или более релевантные линейные модели (см. рисунок 5).

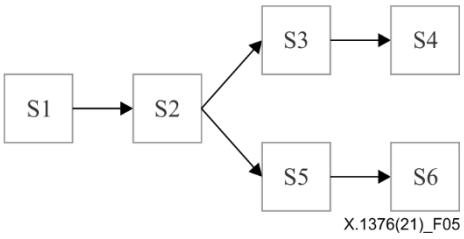

Рисунок 5 − Древовидная модель цепочки состояний

Таким образом, каждый узел описывается следующими признаками:

i) контекст в цепочке состояний;

ii) значение и закономерность поведения каждого узла.

Из узлов в цепочке состояний эти признаки передаются в функцию оценки.

8.2.1.2 Обнаружение на основе потока управления

Поток управления содержит серию коррелированных данных управления. В потоке управления одна команда управления может состоять из нескольких подкоманд управления и влиять на несколько систем.

Ниже приведены некоторые характеристики потока управления для описания выполнения команд управления:

a) узел: служба или приложение в составе ИТС, имеющие отношение к действию;

b) поток: направление и траектория изменения данных в результате действия.

При выполнении действий по управлению управляющие данные проходят через управляющие узлы, образуя поток управления.

Каждый управляющий узел в ИТС работает стабильно и регулярно. Когда много узлов работают сообща, поток управления также ведет себя стабильно благодаря заданному периоду, определенному типами и количеством сообщений.

По существу, поток управления можно отнести к одной из двух моделей: линейной или древовидной. Эти модели определяются следующим образом:

1) линейная модель: для каждого узла имеется только один узел, принимающий его сигнал;

2) древовидная модель: один узел создает два или более элемента данных управления одновременно и передает их разным узлам.

В линейной модели потока управления узлы имеют только однонаправленное соединение (см. рисунок 6).

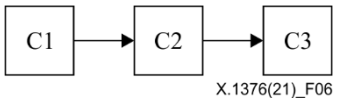

Рисунок 6 − Линейная модель потока управления
C: управление

В древовидной модели потока управления узлы можно подразделить на две или более релевантные линейные модели (см. рисунок 7).

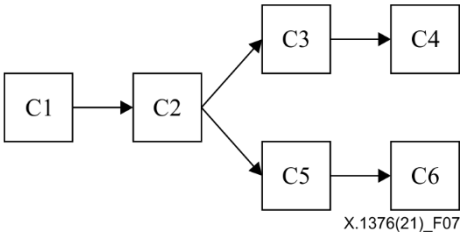

Рисунок 7 − Древовидная модель потока управления

8.2.1.3 Обнаружение на основе временных рядов

Временной ряд используется для описания данных, которые изменяются в зависимости от их типа. Если данные соответствуют типам, можно использовать обнаружение на основе временных рядов.

Закономерности изменения данных временных рядов подразделяются на четыре типа:

a) тенденция: данные изменяются со временем или по независимым переменным, демонстрируя относительно медленную и долгосрочную тенденцию непрерывного роста, сокращения или сохранения своего значения одной и той же природы, но диапазон изменения может быть разным;

b) периодическое изменение: параметр постепенно демонстрирует характеристики, повторяющиеся с течением времени, с пиками и спадами;

c) случайное изменение: данные изменяются случайным образом, но в целом ситуация сохраняется;

d) суперпозиция: фактическое изменение представляет собой суперпозицию или комбинацию нескольких изменений.

Ниже приведены некоторые характеристики поведения временных рядов:

1) узел: служба или приложение в составе ИТС, имеющие отношение к данным временных рядов;

2) поток: указывает время в хронологическом порядке.

Многие данные относятся к данным временных рядов, например сообщения локальной сети контроллеров (CAN). Модель данных для обнаружения ненадлежащего поведения может содержать один или несколько типов данных (см. рисунок 8).

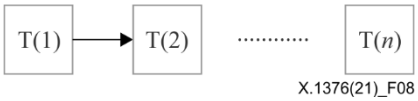

Рисунок 8 − Линейная модель временных рядов
T: время

8.2.1.4 Обнаружение на основе ассоциативной информации

При использовании метода обнаружения с применением ассоциативной информации ненадлежащее поведение может обнаруживаться прямо или косвенно. Таким образом, ассоциативную информацию можно разделить на две категории: прямую и косвенную.

Прямая ассоциативная информация: ненадлежащее поведение обнаруживается непосредственно на основе предоставленной оперативной информации, такой как сторонний отчет об уязвимостях, внутреннее исследование кибербезопасности или публикуемые сведения об общеизвестных уязвимостях.

Косвенная ассоциативная информация: ненадлежащее поведение не обнаруживается на основе этой информации напрямую, поскольку она используется для описания "нормальных" событий, таких как исправление ошибок, выпуск новых функций, обновление программного обеспечения и замена микросхем. Ненадлежащее поведение можно обнаружить, комбинируя косвенную ассоциативную информацию с другими собранными данными.

8.2.2 Принятие решений

В этом разделе представлена процедура принятия решений, показанная на рисунке 9.

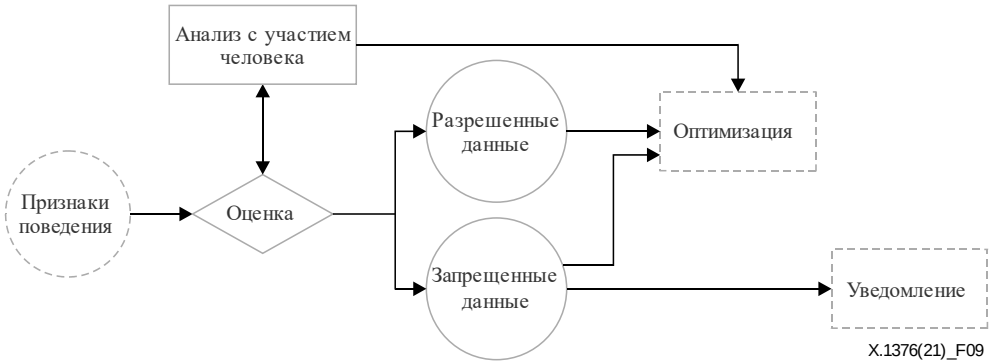

Рисунок 9 − Процедура принятия решений

Для определения результатов применения методов обнаружения используется подмодуль принятия решений. Он выполняет две функции: оценку и анализ с участием человека. Функция оценки определяет тип данных по признакам поведения, а затем оценивает его. Если имеет место ненадлежащее поведение, такое как перехват сеанса или подделка информации, она отклоняется от базового уровня стабильности. Если результат оценки не соответствует пороговому значению разрешенного или запрещенного, он классифицируется как подозрительный. Тогда вмешаются специалисты-аналитики и помогут принять решение, пока оценка не достигнет заданного порогового значения разрешенного или запрещенного.

8.3 Оптимизация

Модуль оптимизации – это модуль обратной связи, который получает данные от механизма обнаружения и использует их для оптимизации (см. рисунок 10).

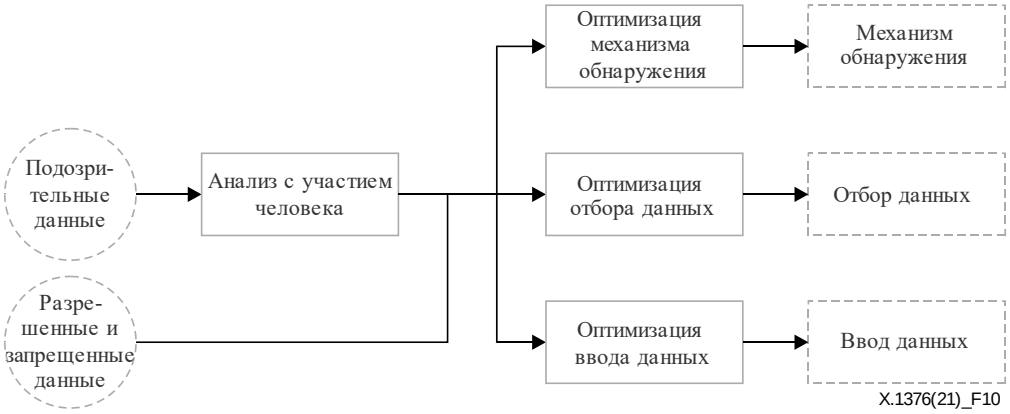

Рисунок 10 − Процедура оптимизации

8.3.1 Оптимизация механизма обнаружения

Признак – это ключевое значение каждого элемента данных в потоке. В начале процесса обнаружения ненадлежащего поведения генерируются базовые уровни стабильности на основе нормальных признаков при нормальных условиях. Инициализируется функция оценки.

Механизм обнаружения оптимизируется по его выходным данным. Методы обнаружения добавляются, изменяются или удаляются в целях повышения эффективности обнаружения; функция оценки также оптимизируется за счет добавления новых знаний, полученных в результате анализа с участием человека.

8.3.2 Оптимизация отбора данных

Наборы данных добавляются, изменяются или удаляются в целях повышения точности обнаружения.

8.3.3 Оптимизация ввода данных

Вводимые данные добавляются, изменяются или удаляются в целях повышения точности обнаружения.

Дополнение I

Примеры использования различных методов обнаружения

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящем Дополнении представлены примеры использования различных методов обнаружения ненадлежащего поведения, указанных в пункте 8.2.1.

I.1 Пример цепочки состояний

Это пример обнаружения на основе цепочки состояний, иллюстрирующий пункт 8.2.1.1.

В автомобиле имеется модуль связи для доступа в интернет, называемый блоком управления телематикой (TCU). TCU работает не постоянно, поэтому после остановки двигателя он переключается в режим пониженного энергопотребления для экономии энергии. Перед переходом в режим пониженного энергопотребления он передает сообщение о состоянии транспортного средства в его шлюз (серверную службу), который синхронизирует это состояние с буфером состояния TCU. Затем командная служба извлекает это состояние из буфера состояния TCU. Когда пользователь подает своему автомобилю команду, командная служба реагирует в соответствии с состоянием TCU. Если TCU находится в режиме пониженного энергопотребления, командная служба подает запрос в службу, инициирующую перевод в режим с увеличенным энергопотреблением (службу пробуждения), которая затем "пробуждает" TCU. Нормальное поведение иллюстрируется на рисунке I.1. В таблице I.1 указаны данные о состоянии, связанные с таким нормальным поведением.

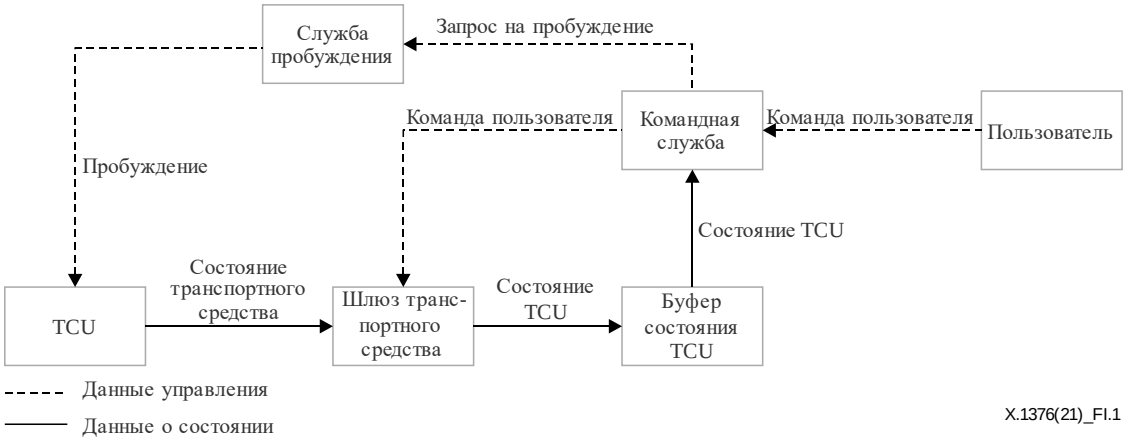

Рисунок I.1 − Нормальное поведение цепочки состояний

Когда злоумышленники захотят взломать эту процедуру, они попытаются изменить состояние TCU, чтобы увидеть, как изменится поведение командной службы. Тогда возникнет разница между содержимым буфера состояния TCU и шлюза транспортного средства.

В рассматриваемом примере функция обнаружения на основе цепочки состояний обнаружит ненадлежащее поведение, сравнив информацию о состоянии транспортного средства в его шлюзе с информацией о состоянии TCU в буфере состояния TCU. Если эти состояния различаются, имеет место ненадлежащее поведение. Во время движения автомобиля TCU не может находиться в режиме пониженного энергопотребления.

Таблица I.1 − Данные о состоянии транспортного средства

Узел	Данные
Шлюз транспортного средства	Состояние транспортного средства
Буфер состояния TCU	Состояние TCU
Командная служба	Состояние TCU

I.2 Пример потока управления

Это пример обнаружения на основе потока управления, иллюстрирующий пункт 8.2.1.2.

Когда пользователь желает управлять автомобилем удаленно, он применяет для запуска этой функции приложение, установленное на его смартфоне. Это приложение создает журнал регистрации операций. Затем оно направляет запрос серверной службе интерфейса прикладного программирования (API), которая регистрирует его в журнале регистрации доступа. После этого служба API предварительно обрабатывает запрос и передает его в конечную точку транспортного средства, например в TCU. TCU обращается к микроконтроллеру (MCU) через приемопередатчик и подает команду соответствующему исполнительному механизму. Наконец, исполнительный механизм выполняет команду управления, поступившую от пользователя (см. рисунок I.2). В таблице I.2 указаны данные управления, связанные с таким нормальным поведением.

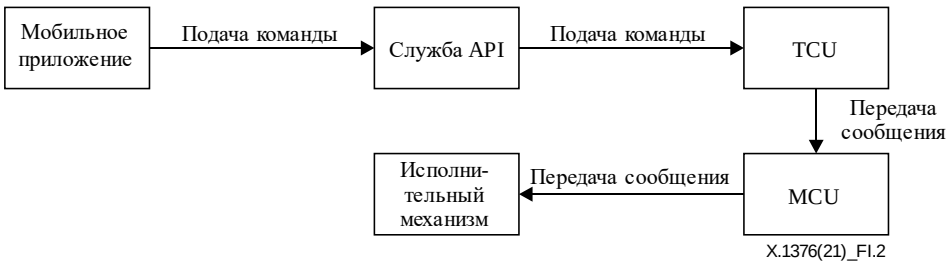

Рисунок I.2 − Нормальное поведение потока управления

В рассматриваемом примере TCU передает сообщения MCU только по запросу службы API. Если MCU вызывается по аномальному пути, в мобильном приложении и в службе API будут отсутствовать журналы регистрации операций. Таким образом, обнаруживается ненадлежащее поведение.

Таблица I.2 − Данные управления телематикой

Узел	Данные
Мобильное приложение	Журнал регистрации операций
Служба API	Журнал регистрации доступа
TCU	Полученные данные
MCU	Вызов журнала
Исполнительный механизм	Журнал исполнительного механизма

I.3 Пример временных рядов

Это пример обнаружения на основе временных рядов, иллюстрирующий пункт 8.2.1.3.

В этом случае TCU периодически передает в серверную службу информацию о местоположении транспортного средства (см. рисунок I.3).

Latitude (°)	Interval (s)
39.9544	10.4015592431
39.9566	10.2439587253
39.9594	10.5735141799
39.9502	10.3234362303
39.9528	10.0973092011
39.9538	10.5066656864
39.9558	10.4945798327
39.9556	10.1209659368
39.9506	10.2163646279
39.9551	10.1042228459

Рисунок I.3 − Нормальные временные ряды позиционирования

Если датчик глобальной навигационной спутниковой системы (ГНСС) подвергся спуфинг-атаке, информация о местоположении и интервал будут явно отличаться от предыдущих данных (см. рисунок I.4).

Latitude (°)	Interval (s)
39.9503	10.4741553595
39.9595	10.2682504585
39.9597	10.2750387130
39.9568	10.4752930715
39.9520	10.6371744699
45.1525	5.4110037357
39.9597	5.5768263688
39.9508	10.4367481108
39.9550	10.0731090275
39.9529	10.5550728359
39.9518	10.5853553005
39.9554	10.1983262711

Рисунок I.4 − Аномальные временные ряды позиционирования

В таблице I.3 указаны стандартные данные временных рядов, используемых в автомобиле.

Таблица I.3 − Данные временных рядов автоматических датчиков

Узел	Данные
Серверная служба	Широта, интервал

I.4 Пример обнаружения на основе ассоциативной информации

В пункте 8.2.1.4 описываются два сценария обнаружения с применением ассоциативной информации, поэтому здесь приведены два примера использования этого метода, по одному для каждого сценария.

I.4.1 Пример обнаружения на основе прямой ассоциативной информации

Обнаружение ненадлежащего поведения на основе прямой ассоциативной информации – более простой способ для соединенного автомобиля. Все формы прямой ассоциативной информации непосредственно указывают на ненадлежащее поведение: IP-адрес, доменное имя, URL-адрес, внутреннее исследование кибербезопасности и сторонние отчеты об уязвимостях. Любые из этих данных содержат абсолютный признак ненадлежащего поведения.

Стандартные виды прямой ассоциативной информации в ИТС указаны в таблице I.4.

Таблица I.4 − Данные для обнаружения на основе прямой ассоциативной информации

Узел	Данные
Бортовая информационно-развлекательная система	IP-адрес URL Доменное имя
База данных ассоциативной информации	Сторонний отчет об уязвимостях Внутреннее исследование кибербезопасности

I.4.2 Пример обнаружения на основе косвенной ассоциативной информации

Косвенную ассоциативную информацию нельзя использовать в качестве самостоятельного средства обнаружения ненадлежащего поведения, но можно сочетать с информацией из других источников. В некоторых случаях единственной уязвимости недостаточно, но злоумышленник может попытаться использовать несколько уязвимостей, чтобы выстроить последовательность операций в целях взлома, поскольку не все производители устраняют уязвимости, предотвращая возможность их использования. Когда механизм обнаружения получает новый технический отчет о такой последовательности, атаки на уязвимости, указанные в [b-CVE-2017-11906] и [b-CVE-2017-11907], могут привести к выполнению произвольного кода; для обнаружения ненадлежащего поведения вводится номер версии браузера бортовой информационно-развлекательной системы, который используется в сочетании с ассоциативной информацией.

Стандартные виды косвенной ассоциативной информации в ИТС указаны в таблице I.5.

Таблица I.5 − Данные для обнаружения на основе косвенной ассоциативной информации

Узел	Данные
База данных ассоциативной информации	Бортовая информационно-развлекательная система Сторонний технический отчет

Библиография

[b-ISO/TR 17427-4] ISO/TR 17427-4:2015, *Intelligent transport systems – Cooperative ITS – Part 4: Minimum system requirements and behaviour for core systems*

[b-CVE-2017-11906] Общеизвестные уязвимости и незащищенности, CVE-2017-11906 (2017 г.). *Internet Explorer information disclosure vulnerability*. Bedford, MA: Mitre Corporation. Доступно [по состоянию на 21 февраля 2021 г.] по адресу: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11906

[b-CVE-2017-11907] Общеизвестные уязвимости и незащищенности, CVE-2017-11907 (2017 г.). *Scripting engine memory corruption vulnerability*. Bedford, MA: Mitre Corporation. Доступно [по состоянию на 21 февраля 2021 г.] по адресу: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11907

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2021 год