ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1382 (03/2023)

СЕРИЯ X: Сети передачи данных, взаимосвязь открытых систем и безопасность

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

Руководящие указания по обмену информацией об угрозах безопасности для соединенных транспортных средств

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	X.1000-X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	X.1100-X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	X.1200-X.1299
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	X.1300-X.1499
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.1350-X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	**X.1370-X.1399**
Безопасность технологии распределенного реестра (DLT)	X.1400-X.1429
Безопасность приложений (2)	X.1450-X.1459
Безопасность веб-среды (2)	X.1470-X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	X.1500-X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	X.1600-X.1699
КВАНТОВАЯ СВЯЗЬ	X.1700-X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	X.1750-X.1799
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800-X.1819

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

Рекомендация МСЭ-Т X.1382

Руководящие указания по обмену информацией об угрозах безопасности для соединенных транспортных средств

Резюме

По мере стремительного развития соединенных транспортных средств возникают все более серьезные проблемы сетевой безопасности. Информация об угрозах безопасности соединенных транспортных средств, которая составляет неотъемлемую часть обеспечения безопасности соединенных транспортных средств, – это любая информация, которая может помочь организации в идентификации, оценке, мониторинге соединенного транспортного средства и реагировании на него. Организации, которые обмениваются информацией об угрозах для соединенных транспортных средств, могут улучшить свои собственные средства обеспечения безопасности и средства обеспечения безопасности других организаций

В Рекомендации МСЭ-Т X.1382 содержатся руководящие указания по принципам, правилам, методике и процедурам обмена информацией о безопасности для соединенных транспортных средств. Приведено также краткое описание разных областей деятельности, ролей и эффективности различных организаций в процессе их участия в жизненном цикле обмена информацией об угрозах безопасности.

Цель настоящей Рекомендации – помочь организациям поддерживать взаимодействие с сообществом по обмену информацией, относящейся к соединенным транспортным средствам, и участвовать в сборе информации об угрозах, которая будет поддерживать практику обеспечения безопасности соединенных транспортных средств. В целом, настоящая Рекомендация направлена на расширение обмена информацией об угрозах безопасности и смягчение потенциального воздействия кибератак на соединенные транспортные средства.

Хронологическая справка *

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор
1.0	ITU-T X.1382	2023-03-03	17	11.1002/1000/15104

Ключевые слова

Соединенные транспортные средства; обмен информацией об угрозах.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL https://handle.itu.int/ после которого укажите уникальный идентификатор Рекомендации.

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 в целях 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.1382

Руководящие указания по обмену информацией об угрозах безопасности для соединенных транспортных средств

1 Сфера применения

Цель настоящей Рекомендации – предоставить руководящие указания по обмену информацией об угрозах для экосистем соединенных транспортных средств, в том числе о ролях и взаимодействии организаций, а также о сфере и процедурах обмена и требованиях к обмену информацией об угрозах для соединенных транспортных средств.

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 справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1371] Рекомендация МСЭ-Т X.1371 (2020 г.), *Угрозы безопасности для соединенных транспортных средств.*

[NIST SP 800-150] *Guide to Cyber Threat Information Sharing.*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 предупреждение (alert) [NIST SP 800-150]: Краткое, обычно удобное для восприятия человеком техническое уведомление о выявленных уязвимостях, инструментах эксплуатации уязвимости и других проблемах безопасности. Другие варианты термина: информационное сообщение, информационный бюллетень или уведомление об уязвимости.

3.1.2 информация об угрозах безопасности (security threat information) [NIST SP 800-150]: Информация, связанная с угрозами, которая помогает организации защититься от этих угроз или обнаружить действия злоумышленника.

3.1.3 угроза (threat) [b-ISO/IEC 27000]: Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 тактические приемы злоумышленника (actor tactics): Описание технических задач, которые необходимо решить злоумышленнику, чтобы выполнить определенное действие.

3.2.2 методы злоумышленника (actor techniques): Описание способов, с помощью которых злоумышленник решает технические задачи, выполняя определенное действие.

3.2.3 процедуры злоумышленника (actor procedures): Описание процесса реализации злоумышленником определенного метода.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

ACL	Access Control List		Список управления доступом
APP	Application		Приложение
CERT	Computer Emergency Response Team		Группа реагирования на нарушения компьютерной защиты
CSIRT	Computer Security Incident Response Team		Группа реагирования на инциденты в сфере компьютерной безопасности
ECU	Electronic Control Unit	ЭБУ	Электронный блок управления
GSMA	GSM Association		Ассоциация GSM
ISAC	Information Sharing and Analysis Center		Центр обмена информацией и анализа информации
MEC	Multi-access Edge Computing		Периферийные вычисления в режиме множественного доступа
T-BOX	Telematics BOX		Телематический блок
TSP	Telematics Service Provider		Поставщик телематических услуг
TTP	Tactics, Techniques and Procedures		Тактические приемы, методы и процедуры
V2X	Vehicle-to- Everything		Связь транспортного средства с различными объектами

5 Соглашения по терминологии

В настоящей Рекомендации:

ключевое слово "рекомендуется" означает требование, которое рекомендуется, но не является абсолютно необходимым; таким образом, для заявления о соответствии это требование не является обязательным.

6 Обзор

К основным элементам процесса обмена информацией об угрозах для соединенных транспортных средств относятся типы информации об угрозах, принципы обмена информацией, роли, правила, сообщества и процедуры. Как правило, разные организации, имеющие отношение к соединенным транспортным средствам, вырабатывают информацию об угрозах безопасности разного типа. Разные действующие лица играют различные роли в деятельности по обмену информацией об угрозах для соединенных транспортных средств. Организации, участвующие в этой деятельности, должны следовать определенным принципам, правилам и процедурам; при этом результаты использования информации об угрозах могут быть разными. Несколько организаций могут образовать сообщество по обмену информацией, которое будет следовать определенному режиму и использовать определенную платформу обмена информацией.

6.1 Типы информации об угрозах для соединенных транспортных средств

Согласно [NIST SP 800-150], информацию об угрозах для соединенных транспортных средств можно подразделить на индикаторы, тактические приемы, методы и процедуры (TTP), предупреждения безопасности и аналитические отчеты об угрозах.

a) Индикаторы – это наблюдаемые признаки того, что атака готовится или неизбежна. Индикаторы можно использовать для обнаружения потенциальных угроз и противодействия им. Таким индикатором в отношении соединенных транспортных средств может служить, например, принадлежность к организации лиц, подозреваемых в участии в атаках на системы связи транспортных средств с различными объектами (V2X).

b) TTP описывают поведение злоумышленника. TTP могут указывать на склонность злоумышленника к применению определенного варианта вредоносного ПО, инструмента атак, механизма доставки, системы использования уязвимостей или к определенной последовательности действий. Существует множество типов угроз, в том числе угрозы для внутренних серверов и центрального сервера организации, а также угрозы для транспортных средств, нацеленные на их каналы связи. TTP могут включать в себя отличающиеся от традиционных сетевых угроз действия по манипулированию соединениями, используемыми определенными функциями транспортного средства, или по обходу системы контроля.

c) Предупреждения безопасности - это технические уведомления об уязвимостях, инструментах эксплуатации уязвимости, вредоносных программах и других угрозах безопасности. Предупреждения безопасности обычно поступают из авторитетных источников, таких как группы реагирования на нарушения компьютерной защиты (CERT) или группы реагирования на инциденты в сфере компьютерной безопасности (CSIRT). Предупреждения безопасности выдаются, когда могут быть затронуты разнородные соединенные транспортные средства или когда угрозы могут причинить значительный вред.

d) Аналитические отчеты об угрозах содержат углубленный анализ угроз, включая участников события, целевую систему, тип атаки и другую информацию, а также рекомендации по мерам смягчения угроз. В аналитических отчетах об угрозах также могут прогнозироваться будущие тенденции в области угроз. Аналитические отчеты об угрозах играют важную роль в предотвращении новых атак на соединенные транспортные средства.

6.2 Выгоды и проблемы обмена информацией об угрозах для соединенных транспортных средств

Используя обмен информацией об угрозах для соединенных транспортных средств, отраслевые организации могут повысить свой уровень безопасности, активно применяя знания, опыт и возможности партнеров. Обмен информацией об угрозах для соединенных транспортных средств дает следующие выгоды:

a) Повышение степени защищенности организаций в отношении соединенных транспортных средств. Соединенные транспортные средства подвергаются новым угрозам, и обмен информацией может помочь организациям совершенствовать свои средства защиты. В качестве основного инструмента атак часто используются вновь выявленные уязвимости. Обмен информацией об угрозах поможет своевременно справиться с атаками, осуществляемыми через такие уязвимости, и повысить способность организаций противостоять подобным атакам. Соединенные транспортные средства сталкиваются со многими новыми атаками, и обмен информацией об угрозах помогает справляться с новыми угрозами для соединенных транспортных средств и совершенствовать средства защиты.

b) Поддержание здоровой экосистемы соединенных транспортных средств. Обмен информацией об угрозах помогает повысить безопасность экономической среды соединенных транспортных средств и обеспечить экологическую безопасность любых соединенных транспортных средств. Безопасность производственной цепочки в сфере соединенных транспортных средств подразумевает безопасность поставщиков услуг, поставщика телематических услуг (TSP), автопроизводителей, операторов связи, поставщиков автомобильного и портативного оконечного оборудования, поставщиков мобильного интеллектуального оконечного оборудования и т. д.

Хотя обмен информацией об угрозах приносит выгоды, сохраняются и определенные проблемы. В число задач в области обмена информацией, которые предстоит решить, входят:

a) Создание стандартной системы обмена информацией об угрозах для соединенных транспортных средств. Чтобы сохранить здоровую экосистему соединенных транспортных средств, необходимо создать рациональную стандартную систему обмена информацией об угрозах для соединенных транспортных средств. В настоящее время единого международного стандарта системы обмена информацией об угрозах для соединенных транспортных средств не существует. Отсутствие стандартной системы будет препятствовать обмену информацией и в конечном итоге повлияет на его развитие.

ПРИМЕЧАНИЕ. – В ряде руководств, например [ITU-T X.1371] и Руководящие указания GSMA по безопасности IoT [b-GSMA CLP.11], могут быть представлены вопросы безопасности, которые следует рассматривать как возможные передовые методы обмена информацией.

b) Определение объема и содержания информации об угрозах. Производственная цепочка в сфере соединенных транспортных средств состоит из разных звеньев, и каждое звено сталкивается с угрозами разных типов. Необходимо определить информацию об угрозах, передаваемую каждым звеном, и режим обмена информацией между звеньями.

c) Защита конфиденциальной и секретной информации. Обмен информацией об угрозах для соединенных транспортных средств сопряжен с риском раскрытия конфиденциальной информации. Криптографические технологии могут быть скомпрометированы или применяться в недостаточной степени. Применение криптографических технологий в недостаточной степени также может привести к утечке криптографических ключей или учетных данных.

Кроме того, риск утечки информации может возрасти в связи с использованием уже взломанных и устаревших криптографических технологий. Подлежащая защите конфиденциальная информация включает охраняемое авторским правом или проприетарное ПО транспортного средства; личную информацию владельца, например персональные данные, информацию о платежном счете, адресную книгу, информацию о местонахождении и электронный идентификатор транспортного средства; криптографические ключи и т. д. Кроме того, неавторизованным организациям не разрешен доступ к секретной информации. Процесс получения и сохранения разрешений, необходимых организации для постоянного доступа к источникам секретной информации, является дорогостоящим и трудоемким.

7 Принципы обмена информацией об угрозах для соединенных транспортных средств

Для обеспечения эффективности, точности и безопасности процесса обмена и передачи информации об угрозах необходимо, чтобы организации и предприятия придерживались ряда принципов.

7.1 Взаимная выгода

Смысл обмена информацией об угрозах безопасности заключается в усовершенствовании средств защиты безопасности сети, используемой соединенными транспортными средствами, за счет совместных усилий. Рекомендуется, чтобы участники обмена информацией об угрозах безопасности для соединенных транспортных средствах знали права, обязанности и степень ответственности друг друга в процессе деятельности по обмену информацией об угрозах. Помимо получения информации об угрозах, относящейся к их собственной организации, также рекомендуется, чтобы они сами прилагали активные усилия для общего блага и достижения взаимовыгодных результатов.

7.2 Категоризация и классификация

Разные организации играют разные роли в процессе обмена информацией об угрозах безопасности. Значение и важность той или иной информации об угрозах для разных организаций могут быть разными. Организациям рекомендуется распределить по категориям и классифицировать информацию об угрозах для соединенных транспортных средств, а также определить ее эффективный объем и содержание. Рекомендуется создать разные уровни системы управления в соответствии с категориями, классами и объемом и содержанием информации. Рекомендуется применять соответствующие методы шифрования для обеспечения конфиденциальности и целостности информации и/или защиты ее подлинности.

7.3 Безопасность данных

Такие проблемы, как незаконное использование, кража и фальсификация данных об угрозах и несанкционированный доступ пользователей серьезно сказываются на желании участников процесса обмена информацией делиться своими знаниями и снижают уровень безопасности и эффективности обмена оперативной информацией. По этой причине в центре внимания при обмене информацией об угрозах также оказывается управление возникающим при этом риском. В число контрмер входят такие эффективные средства защиты данных, связанных с информацией об угрозах безопасности для соединенных транспортных средств, как шифрование, десенсибилизация предоставляемых данных, выявление и уничтожение данных после обмена и т. д.

8 Организации, их роли и партнерские отношения

8.1 Организации и их роли

8.1.1 Автопроизводители

Автопроизводители играют наиболее важную роль в деятельности по обмену информацией об угрозах для соединенных транспортных средств, поскольку они напрямую взаимодействуют с пользователями и несут ответственность за безопасность своей продукции.

Извлекая данные из собственных производственных систем, бортовых устройств и инфраструктуры для соединенных транспортных средств, автопроизводители собирают, объединяют, создают и анализируют информацию об угрозах безопасности, связанных с соединенными транспортными средствами, и принимают меры для смягчения этих угроз.

8.1.2 Поставщики

Поставщики предоставляют аппаратуру или программное обеспечение для соединенных транспортных средств, в том числе микросхемы, телематические блоки (T-BOX) и внутренние/внешние шлюзы. Поставщики собирают и получают информацию об угрозах безопасности, связанных с их продукцией, и помогают координационной группе, автопроизводителям и другим соответствующим сторонам смягчать угрозы и/или уменьшать количество относящихся к их продукции инцидентов безопасности и предотвращать их.

8.1.3 Сторонние поставщики продуктов и услуг

К сторонним поставщикам продуктов и услуг относятся главным образом организации, предоставляющие отдельные продукты и услуги, связанные с соединенными транспортными средствами, отличные от автопроизводителей и поставщиков запасных частей, такие как TSP, поставщики облачных услуг, поставщики оборудования, производители мобильных терминалов, поставщики услуг страхования транспортных средств, другие операторы сторонних сервисных платформ и т. д.

Сторонние поставщики продуктов и услуг собирают/создают/передают информацию об угрозах безопасности для своих платформ продуктов или услуг, например об угрозах, связанных с неисправностями соединенных транспортных средств, несанкционированным поведением пользователей или дистанционными атаками, и помогают соответствующим сторонам, таким как группы координации соединенных транспортных средств и автопроизводители, смягчать угрозы и/или справляться с инцидентами безопасности, связанными с соединенными транспортными средствами. Поставщики облачных услуг также несут ответственность за обмен информацией, в том числе за неправильную конфигурацию или ошибки, злоупотребление портами управления, ненадлежащее управление учетными данными, утечку облачных данных и т. д.

8.1.4 Координационные группы

Координационные группы в сфере соединенных транспортных средств обычно действуют как независимые структуры, которые занимаются координацией информации об угрозах безопасности и реагированием на инциденты; примером таких структур являются, в частности, CERT/CSIRT и Auto-ISAC.

Они помогают соответствующим сторонам в межорганизационной координации обмена информацией об угрозах безопасности и предоставляют услуги по уведомлению и раннему предупреждению.

8.1.5 Операторы сетей электросвязи

Операторы сетей электросвязи предоставляют базовые услуги электросвязи для соединенных транспортных средств.

Операторы сетей электросвязи обеспечивают безопасность сетевой инфраструктуры электросвязи, такой как базовые сети, базовые станции, платформы MEC и т. д.

ПРИМЕЧАНИЕ. – В качестве примера для операторов электросвязи в контексте соединенных транспортных средств можно рассматривать Руководящие указания GSMA для операторов сетей [b-GSMA CLP.14].

8.1.6 Поставщики средств обеспечения кибербезопасности

Поставщики средств обеспечения кибербезопасности – это компании или организации, связанные с сетевыми технологиями и участвующие в деятельности автопроизводителей и поставщиков продуктов или услуг, относящихся к кибербезопасности.

Используя такие источники, как защитные устройства, программное обеспечение терминалов и интернет, поставщики средств обеспечения кибербезопасности помогают соответствующим организациям собирать, интегрировать и анализировать информацию об угрозах безопасности для соединенных транспортных средств, а также обеспечивать поддержку и предоставлять услуги в области безопасности для предотвращения и сокращения количества инцидентов безопасности.

8.2 Сфера охвата деятельности организаций по обмену информацией

Организациям рекомендуется определить сферу охвата своей деятельности по обмену информацией об угрозах, включая определение типов информации, которой можно делиться, обстоятельств, при которых разрешен обмен информацией об угрозах, и порядка приоритетности при обмене информацией об угрозах для соединенных транспортных средств.

Масштабы деятельности по обмену информацией варьируются в зависимости от ресурсов и возможностей организации. В разных типах организаций сфера охвата деятельности по обмену информацией об угрозах для соединенных транспортных средств будет различной. Например, для поставщиков средств обеспечения кибербезопасности сфера охвата будет иной, чем для автопроизводителей, поставщиков оборудования V2X, поставщиков оборудования связи, операторов связи и т. д. Поставщикам информации об угрозах для соединенных транспортных средств, обладающих ограниченными ресурсами, рекомендуется сосредоточиться на меньшем наборе мер по созданию/сбору информации об угрозах, ограничившись сведениями об угрозах, наиболее ценными для организации и ее партнеров по обмену информацией. Организация может расширить сферу охвата деятельности по обмену информацией об угрозах за счет дополнительных возможностей и ресурсов. Организация, обладающая бóльшими ресурсами и более широкими возможностями, может изначально обеспечить более широкую сферу охвата деятельности по обмену информацией об угрозах для достижения своих целей и решения поставленных задач.

В таблице 1 показано, какие организации могут подвергаться угрозам каждого типа, определенным в [ITU-T X.1371].

Таблица 1 − Организации, подверженные воздействию угроз каждого типа для соединенных транспортных средств

Тип угроз	Организации, участвующие в обмене информацией об угрозах					
	Автопроизводители	Поставщики	Сторонние поставщики продуктов и услуг	Координационная группа	Операторы связи	Поставщики услуг кибербезопасности
Угрозы для внутренних серверов	✓		✓	✓		✓
Угрозы для транспортных средств, связанные с каналами связи	✓	✓	✓	✓	✓	✓
Угрозы, связанные с процедурами обновления ПО на транспортных средствах	✓		✓	✓		✓
Непреднамеренные действия человека как угроза для транспортных средств	✓	✓	✓			

Таблица 1 − Организации, подверженные воздействию угроз каждого типа для соединенных транспортных средств

Тип угроз	Организации, участвующие в обмене информацией об угрозах					
	Автопроизводители	**Поставщики**	**Сторонние поставщики продуктов и услуг**	**Координационная группа**	**Операторы связи**	**Поставщики услуг кибербезопасности**
Угрозы для транспортных средств, связанные с возможностями взаимодействия и соединениями с внешними объектами	✓	✓	✓	✓	✓	✓
Потенциальные цели или причины атаки	✓	✓	✓	✓		✓
Потенциальные уязвимости	✓	✓	✓	✓	✓	✓

8.3 Правила обмена информацией между организациями

Основываясь на характеристиках и классификации информации об угрозах для соединенных транспортных средств, можно предложить следующие правила обмена информацией об угрозах между организациями.

a) Рекомендуется, чтобы организации обменивались информацией об угрозах для соединенных транспортных средств.

b) Обмен информацией об угрозах для соединенных транспортных средств часто происходит на платформах управления соединенными транспортными средствами или через поставщиков общих транспортных услуг, автопроизводителей, поставщиков оборудования V2X, поставщиков оборудования связи либо операторов связи.

c) Многие организации, такие как автопроизводители и поставщики средств обеспечения кибербезопасности, выступают как в роли источников, так и в роли потребителей информации об угрозах.

d) Рекомендуется, чтобы источники информации об угрозах были профессиональными.

e) Рекомендуется предъявлять требования по управлению информацией об угрозах, такие как требование фильтрации информации и проверки наличия подписки.

8.4 Создание сообщества по обмену информацией

Рекомендуется создать сообщество по обмену информацией об угрозах для соединенных транспортных средств и анализу такой информации. Могут использоваться модели обмена информацией об угрозах на основе одноранговой топологии, источников и подписки или звездообразной топологии [b-OASIS TAXII]. Сообщество позволит организациям получать сведения о сетевых угрозах и уязвимости соединенных транспортных средств в режиме реального времени. В качестве примера можно привести сообщество Auto-ISAC, созданное автопроизводителями в 2015 году. Это сообщество главным образом решает задачу обмена информацией с растущим числом интеллектуальных транспортных средств. Портал Auto-ISAC позволяет участникам анонимно передавать и получать информацию и помогает им эффективнее противостоять сетевым угрозам. Auto-ISAC активно расширяет сотрудничество и обмен информацией между поставщиками, автотранспортными компаниями и автопроизводителями в области сетевой безопасности транспортных средств. В Дополнении I содержится описание деятельности Auto-ISAC по обмену информацией об угрозах.

Сообщество по обмену информацией может включать в себя несколько подсообществ, и организации могут присоединиться к одному или нескольким подсообществам, связанным с соединенными транспортными средствами. Рекомендуется, чтобы сообщество по обмену информацией представляло собой открытое сообщество, позволяющее различным организациям свободно присоединяться к нему и выходить из него в порядке добровольного сотрудничества. Рекомендуется, чтобы при присоединении к подсообществу организация выбирала сообщество с комплементарными информационными ресурсами об угрозах для соединенных транспортных средств. Каждая организация добровольно публикует в сообществе по обмену информацию об угрозах для соединенных транспортных средств и несет ответственность за уместность предоставляемой сообществу информации об угрозах.

9 Процедуры и рекомендации по обмену информацией об угрозах для соединенных транспортных средств

9.1 Введение

Угрозы для соединенных транспортных средств определены и описаны в [ITU-T X.1371]. Организации могут выявлять, анализировать и устранять угрозы безопасности с помощью внутренних ресурсов, а также обмениваться информацией об угрозах, создав межорганизационную структуру для такого обмена. В рамках процедуры межорганизационного обмена организации могут:

a) получать и использовать информацию о внешних угрозах для предотвращения и смягчения угроз для соединенных транспортных средств;

b) создавать и предоставлять другим организациям информацию об угрозах для соединенных транспортных средств, чтобы повысить безопасность экосистемы транспортных средств.

В зависимости от направления передачи информации об угрозах организации можно разделить на два типа: потребители и источники информации. Многие организации, такие как автопроизводители и поставщики средств обеспечения кибербезопасности, обычно выступают как в роли источников, так и в роли потребителей информации об угрозах.

9.2 Процедуры обмена информацией об угрозах

Потребители информации – это потенциальные жертвы угроз для соединенных транспортных средств. Получая и используя информацию об угрозах, потребители могут быстро определить затрагиваемые системы и принять необходимые контрмеры для смягчения угроз. Основными потребителями информации об угрозах среди всех соответствующих организаций являются автопроизводители. Последовательность действий потребителей включает следующие пять этапов:

a) подготовка – разработка соответствующих механизмов для подготовки к участию в мероприятиях по обмену информацией об угрозах;

b) получение – получение информации о внешних угрозах;

c) анализ – выполнение анализа полученной информации об угрозах;

d) смягчение – принятие мер по смягчению угроз по результатам анализа;

e) профилактика – меры по предотвращению возникновения угроз в будущем.

Источники информации – это организации, обладающие техническими возможностями, аналитическими средствами и общим намерением обмениваться информацией в экосистеме транспортных средств. Как правило, источники информации также и потребляют информацию об угрозах безопасности, потому что для создания/сбора информации об угрозах требуется несколько источников, в число которых входят внешние источники информации об угрозах. Последовательность действий источников информации включает следующие три этапа:

a) подготовка – разработка соответствующих механизмов для подготовки к участию в мероприятиях по обмену информацией об угрозах;

b) анализ – выполнение анализа для получения высококачественной информации об угрозах;

c) передача – передача полученной информации об угрозах заинтересованным сторонам.

9.3 Руководящие указания по каждому этапу процедуры

9.3.1 Руководящие указания для организаций – потребителей информации

9.3.1.1 Руководящие указания по деятельности на этапе подготовки

Организациям рекомендуется разработать политику в отношении информации об угрозах безопасности для соединенных транспортных средств, включая постановку задач, определение объема и содержания информации и разработку процесса принятия решений.

Рекомендации:

a) Постановка задач – организации должны учитывать, что они имеют дело с угрозами безопасности. Рекомендуется, чтобы организации, основываясь на анализе угроз безопасности, определили свои задачи в области безопасности для усиления возможностей защиты.

b) Определение объема и содержания – рекомендуется, чтобы организации определили объем и содержание необходимой информации об угрозах в сочетании со своими целями по обеспечению безопасности, техническими возможностями, бюджетом и потенциальным воздействием различных угроз; кроме того, рекомендуется определить приоритеты.

c) Разработка процесса принятия решений – рекомендуется определить сроки принятия решений в соответствии с типом и приоритетностью информации об угрозах, необходимой организации, во избежание влияния длительного процесса принятия решений на своевременность предоставления информации об угрозах.

9.3.1.2 Руководящие указания по деятельности на этапе получения информации

Организациям рекомендуется:

a) хранить подлежащую обмену информацию об угрозах безопасности надлежащим образом;

b) принять меры по обеспечению безопасности хранения информации об угрозах;

c) удалять устаревшую и бесполезную информацию об угрозах.

9.3.1.3 Руководящие указания по деятельности на этапе анализа

Организациям рекомендуется:

a) определить ценность информации об угрозах. В Дополнении II приведена эталонная методика определения ценности информации об угрозах. Рекомендуется автоматическая оценка;

b) выполнять проверку и анализ для оценки потенциального ущерба своим продуктам и услугам;

c) анализировать контекст для выявления такой информации, как источники атак, TTP и цели атак;

d) выявлять затрагиваемые ресурсы, такие как серверы, домен(ы), электронные блоки управления (ЭБУ), системы и т. д.;

e) выполнять фильтрацию, проверку и анализ в безопасной среде во избежание воздействия на их критические системы.

9.3.1.4 Руководящие указания по деятельности на этапе смягчения последствий

Организациям рекомендуется:

a) разработать решения для противодействия угрозам и осуществлять соответствующие процессы на основе информации об угрозах и результатов анализа. Это могут быть решения об изолировании затронутого аппаратного оборудования, установке исправлений, обновлению программного обеспечения, изменению конфигурации и т. д.;

b) обращаться за помощью к координационной группе по соединенным транспортным средствам, если организации не хватает ресурсов для противодействия угрозам;

c) применять полученные индикаторы угроз в устройствах для обеспечения кибербезопасности;

d) немедленно анализировать угрозы безопасности, создаваемые легитимными пользователями путем изменения конфигурации и распространения вредоносных программ, и укреплять функций управления. Организации могут исправлять и устранять уязвимости, дефекты и ошибки конфигурации сети, используя информацию об угрозах, включая способы их устранения.

9.3.1.5 Руководящие указания по деятельности на этапе профилактики

Организациям рекомендуется продолжать наблюдение за своими продуктами и услугами.

9.3.2 Руководящие указания для организаций – источников информации

9.3.2.1 Руководящие указания по деятельности на этапе подготовки

Организациям рекомендуется разработать собственную политику, включая постановку задач, определение объема и содержания информации и разработку процесса принятия решений.

Организациям рекомендуется:

a) разработать процесс управления реагированием на инциденты для предотвращения утечки важных данных;

b) развернуть необходимые ресурсы и инструменты для создания индикаторов и другой информации об угрозах;

c) находить, оценивать и классифицировать данные об угрозах из разнообразных сетей и источников, чтобы гарантировать наличие полного описания всей актуальной информации, связанной с угрозами, в любой момент времени;

d) создать сообщество по обмену информацией или присоединиться к нему, получать данные, покупая/получая неопубликованную оперативную информацию и собирая общедоступные данные, анализировать эти данные в соответствии с определенными прикладными сценариями и бизнес-требованиями, а затем вырабатывать соответствующие знания об угрозах. В системе обмена информацией об угрозах сообщество объединяет информацию, собранную всеми участниками в соответствии с фактическими потребностями, чтобы получить более сконцентрированные, полные и точные знания об угрозах и распространять их безвозмездно или за плату в зависимости от типа и ценности этих знаний;

e) определить сферу охвата деятельности по обмену информацией об угрозах, включая определение самой информации, подлежащей обмену, и формата обмена.

9.3.2.2 Руководящие указания по деятельности на этапе анализа

Организациям рекомендуется:

a) автоматически или вручную фильтровать журналы регистрации аварийных сигналов, удаляя бесполезные или даже ложные сигналы;

b) оценивать важность информации и определить сферу охвата своей деятельности по обмену информацией;

c) определить вероятность обнаружения различных сценариев сетевых угроз и связанных с ними метаданных, а затем проанализировать и обработать результаты сравнения характерных индикаторов этих угроз.

9.3.2.3 Руководящие указания по деятельности на этапе обмена информацией

Организациям рекомендуется:

a) обеспечить обмен информацией об угрозах в соответствии с установленной сферой охвата;

b) представлять информацию об угрозах безопасности в стандартном формате;

c) предоставлять больше справочной информации;

d) создать модель и механизмы обмена, а также решить вопросы достоверности информации и точности операций по обмену;

e) создать платформу обмена информацией об угрозах для соединенных транспортных средств с учетом требований развития отрасли;

f) создать механизм контроля для управления данными об угрозах, включая десенсибилизацию, аутентификацию данных и их уничтожение после обмена;

g) при наличии возможности подготовить информацию об угрозах для соединенных транспортных средств – делиться этой информацией с организациями, имеющими хорошую репутацию.

Дополнение I

Передовой опыт Auto-ISAC по обмену информацией об угрозах

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В 2019 году Центр обмена информацией и анализа информации в сфере автомобильной промышленности [b-AUTO-ISAC] выпустил издание 1.3 справочника "Сотрудничество и взаимодействие с соответствующими сторонними организациями" (Collaboration and engagement with appropriate third parties). В этом справочнике по передовому опыту Auto-ISAC дает рекомендации по обмену информацией, в том числе о соответствующих сторонних организациях, уровне открытости, содержании подходящей для обмена информации, процессах обмена информацией и т. д.

В целях повышения кибербезопасности транспортных средств организации могут сотрудничать и взаимодействовать с несколькими типами сторонних организаций в экосистеме соединенных транспортных средств. К соответствующим сторонним организациям относятся партнеры из отрасли, отраслевые организации, государственные учреждения, учебные заведения, научно-исследовательские институты и СМИ.

Организации могут определить подходящий уровень открытости на основе своих индивидуальных целей в области кибербезопасности транспортных средств и своей уникальной картины рисков. Степень открытости может быть ограниченной, умеренной и широкой.

В число ключевых процессов обмена информацией между различными заинтересованными сторонами входят:

a) определение содержания подходящей для обмена информации;

b) привлечение внутренних заинтересованных сторон;

c) разработка процессов получения и обработки предлагаемой информации;

d) разработка процессов передачи информации внешним сторонним организациям;

e) приобретение соответствующих инструментов и технологий.

Дополнение II

Методика определения ценности информации об угрозах

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Организации могут определять ценность информации об угрозах по пяти следующим признакам:

a) репутация источника – источники информации об угрозах могут иметь разную репутацию. Из источников с высокой степенью достоверности поступает более ценная информация об угрозах;

b) сроки – информация об угрозах чувствительна ко времени. Более раннее поступление информации поможет организациям предотвратить атаки и защитить свои системы;

c) полнота описания – обычно более ценной считается информация об угрозах, сопровождаемая более подробным описанием и контекстуальными сведениями;

d) актуальность и важность для организации – некоторые сведения об угрозах важны для определенной отрасли, продукции или даже для конкретных компаний. Особо ценится информация об угрозах, важная для организации;

e) значимость информации об угрозах – информация об угрозах из разных источников может дублироваться и не совпадать. Объединение схожих угроз и определение подлинности информации об угрозах повышают ее значимость для организации.

Библиография

[b-AUTO-ISAC] *Collaboration and Engagement with Appropriate Third Parties Best Practice Guide, Version 1.3, 2019*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-GSMA CLP.11] GSMA CLP.11 (2020), *IoT Security Guidelines Overview Document, Version 2.2*.

[b-GSMA CLP.14] GSMA CLP.14 (2020), *IoT Security Guidelines for Network Operators, Version 2.2*.

[b-OASIS TAXII] *OASIS Committee Specification, TAXII™ Version 2.1*.

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, 2023 г.