Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1454 (09/2023)

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

Безопасные приложения и услуги (2) – Безопасность приложений (2)

Меры безопасности для услуг "умного" офиса с поддержкой определения местоположения

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.1454

Меры безопасности для услуг "умного" офиса с поддержкой определения местоположения

Резюме

Услуги "умного" офиса, объединяющие несколько "умных" приложений, направлены на повышение качества ведения офисной деятельности и эффективности управления. Поскольку основой технологий, применяемых в услугах "умного" офиса, служат информационно-коммуникационные технологии (ИКТ), оператор электросвязи играет важную роль среди систем "умного" офиса.

К типовым услугам "умного" офиса относятся "умная" стоянка автотранспорта, "умное" вождение, "умный" магазин розничной торговли, "умный" офис, "умное" управление конференц-залами, "умное" водоснабжение и "умное" управление энергопотреблением. Одним из ключевых элементов в большинстве реализаций этих типовых услуг "умного" офиса являются данные о местоположении, предоставляемые оператором.

Чтобы обеспечить безопасность услуг "умного" офиса с поддержкой определения местоположения, необходимо проанализировать угрозы безопасности и соответствующие требования безопасности, характерные для услуг с поддержкой определения местоположения, а также установить общие меры безопасности.

В Рекомендации МСЭ-Т X.1454 анализируются типовые сценарии применения услуг "умного" офиса с поддержкой определения местоположения, определяются соответствующие угрозы и требования безопасности, а также устанавливаются меры безопасности, которые должны соблюдаться операторами и основными системами "умного" офиса, чтобы обеспечить защиту услуг с поддержкой определения местоположения.

Хронологическая справка[*]

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор
1.0	МСЭ-Т X.1454	08.09.2023 г.	17-я	11.1002/1000/15111

Ключевые слова

Местоположение, меры безопасности, услуги "умного" офиса.

[*] Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://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/авторскими правами на программное обеспечение, 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 соответствующим базам данных МСЭ-Т, доступным на веб-сайте МСЭ-Т по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1454

Меры безопасности для услуг "умного" офиса с поддержкой определения местоположения

1 Сфера применения

В настоящей Рекомендации анализируются типовые сценарии применения услуг "умного" офиса с поддержкой определения местоположения, определяются соответствующие угрозы и требования безопасности, а также устанавливаются меры безопасности, которые должны соблюдаться операторами и основными системами "умного" офиса, чтобы обеспечить защиту услуг с поддержкой определения местоположения.

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.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

Отсутствуют.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определен следующий термин.

3.2.1 услуга "умного" офиса (smart office service): Услуга, объединяющая несколько "умных" приложений ("умная" стоянка автотранспорта, "умное" водоснабжение, "умный" магазин розничной торговли) и нацеленная на обслуживание и поддержку ведения офисной деятельности, повышение ее качества и эффективности управления, а также создание для сотрудников удобных условий на рабочих местах.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

DDoS	Distributed Denial of Service		Распределенный отказ в обслуживании
GNSS	Global Navigation Satellite System	ГНСС	Глобальная навигационная спутниковая система
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
RNSS	Radio Navigation Satellite System	РНСС	Радионавигационная спутниковая система
SEM	Smart Environmental Monitoring		"Умный" мониторинг окружающей среды
UWB	Ultra-Wide Band	СШП	Сверхширокополосный
WiFi	Wireless Fidelity		Высокая точность беспроводной передачи

5 Соглашения

Ключевое слово "требуется" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящему документу.

6 Обзор услуг "умного" офиса с поддержкой определения местоположения

Согласно представлению об "умных" устойчивых городах, в которых для повышения качества жизни, эффективности деятельности и работы городских служб, а также конкурентоспособности используются информационно-коммуникационные технологии (ИКТ) и другие средства, услуги "умного" офиса становятся типовыми услугами в "умном" устойчивом городе.

Услуги "умного" офиса, объединяющие несколько "умных" приложений ("умная" стоянка автотранспорта, "умное" водоснабжение, "умный" магазин розничной торговли), нацелены на повышение качества предложений офисного бизнеса и эффективности его управления.

Поскольку услуги "умного" офиса объединяют несколько "умных" приложений, основные системы "умного" офиса могут быть разными. Поскольку технологической основой услуг "умного" офиса служат ИКТ, одним из ключевых элементов большинства реализаций типовых услуг подобного рода являются данные о местоположении, предоставляемые оператором.

В число основных систем "умного" офиса с возможностью определения местоположения входят:

– система поставщика услуг "умного" офиса;

– система поставщика данных и услуг по их обработке;

– система поставщика измерительных устройств и инфраструктуры.

– пользователь.

ПРИМЕЧАНИЕ. – Эти ключевые заинтересованные стороны – поставщик услуг "умного" офиса, поставщик данных и услуг по их обработке, а также поставщик измерительных устройств и инфраструктуры в системах "умного" офиса с возможностью определения местоположения – могут быть как отдельными поставщиками, так и поставщиками интегрированных услуг.

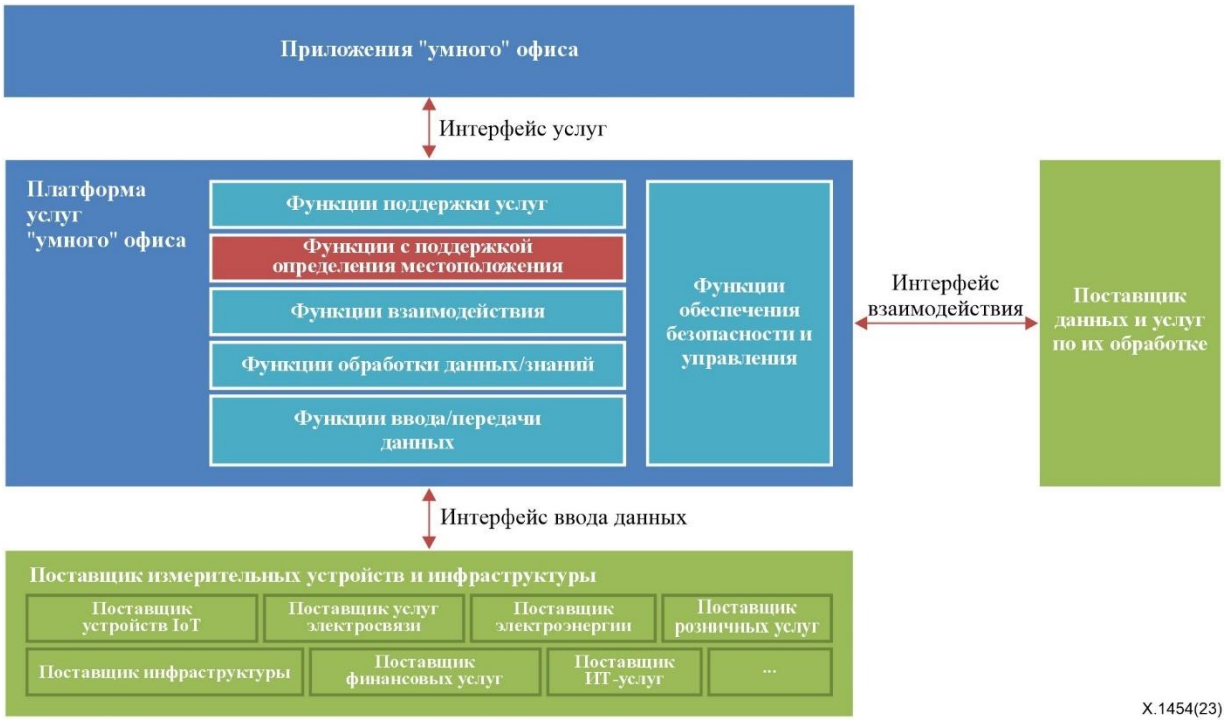

Рисунок 1 – Обзор системы "умного" офиса с поддержкой определения местоположения

Система "умного" офиса с поддержкой определения местоположения обеспечивает выполнение следующих функций:

– **Функции ввода/передачи данных**: обеспечивают механизмы сбора данных из различных источников систем сбора данных.

– **Функции обработки данных/знаний**: обеспечивают обработку данных, их обогащение и преобразование информации в знания.

– **Функции взаимодействия**: обеспечивают доступ к информации на разных уровнях.

– **Функции определения местоположения**: предоставляют данные о местоположении из системы оператора.

– **Функции поддержки услуг**: координируют работу всех возможных служб, участвующих в каждом действии, обеспечивают поддержку функциональной совместимости.

– **Функции обеспечения безопасности и управления**: обеспечивают горизонтальные функции, такие как контроль, мониторинг и обеспечение безопасности.

Интерфейсы обеспечивают связь между функциями:

– **Интерфейс ввода данных**: позволяет собирать информацию от внешних элементов.

– **Интерфейс взаимодействия**: обеспечивает связь с внешними поставщиками данных и сторонними вычислительными системами.

– **Интерфейс услуг**: обеспечивает доступ различных приложений к вспомогательным функциям, предоставляемым платформой услуг "умного" офиса.

7 Типовые сценарии применения услуг "умного" офиса с поддержкой определения местоположения

7.1 "Умная" стоянка автотранспорта

"Умная" стоянка автотранспорта обеспечивает эффективное управление парковочными местами организации и координирует их использование с работой других систем (внешней платежной системой, системой парковки с помощью веб-средств/приложений и т. п.).

"Умная" стоянка автотранспорта может выполнять типовые функции, такие как управление парковкой, резервирование парковочных мест, обратный поиск автомобилей, автоматическое управление доступом к автомобилю и самостоятельная оплата. В число функций "умной" парковки с определением местоположения входят:

– **управление парковкой**: информация о местоположении незанятых парковочных мест с поддержкой публикации правил парковки;

– **резервирование парковочных мест**: информация о местоположении помогает находить свободные парковочные места и заблаговременно резервировать их;

– **обратный поиск автомобилей**: информация о местоположении помогает определить, где припаркован автомобиль, если владелец забыл, где он его оставил.

7.2 "Умный" мониторинг окружающей среды

"Умный" мониторинг окружающей среды (SEM) представляет собой приложение для самостоятельного мониторинга состояния и защиты окружающей среды, которое может определять текущее состояние окружающей среды.

В систему "умного" мониторинга окружающей среды могут входить функциональные объекты платформ SEM, устройств SEM и сеть. К функциям "умного" мониторинга окружающей среды с поддержкой определения местоположения относятся:

– **управление параметрами измерения**: информация о местоположении устройства необходима для настройки параметров измерения в соответствии с условиями окружающей среды;

– **представление данных**: необработанные данные по каждому местоположению (одного или нескольких устройств SEM) представляют собой факультативную информацию для представления состояния окружающей среды.

7.3 "Умная" доставка

Для "умной" доставки в сценарии "умного" офиса используются возможности беспилотного автомобиля и робототехнического приложения, позволяющие автоматически доставлять посылки, документы, канцелярские принадлежности и т. д.

К функциям "умной" доставки с поддержкой определения местоположения относятся:

– помощь системе автоматического вождения с возможностью позиционирования с точностью до сантиметра;

– повышение эффективности управления транспортными средствами/роботами путем сопоставления маршрутов доставки с местоположением устройств;

– оптимизация маршрутов доставки и контроль за процессом доставки путем отслеживания местоположения и пути автомобиля/робота в режиме реального времени.

8 Угрозы безопасности услуг "умного" офиса с поддержкой определения местоположения

8.1 Угрозы безопасности данных

8.1.1 Перехват данных о местоположении

Данные о местоположении при предоставлении услуг "умного" офиса могут быть основаны на использовании открытой беспроводной сети, так что злоумышленник может перехватить эти данные, отслеживая беспроводной канал.

8.1.2 Фальсификация данных о местоположении

Злоумышленник может перехватить блок данных о местоположении, передаваемых из сети, и злонамеренно изменить/подделать их в целях осуществления дальнейших атак. В некоторых сценариях, таких как "умная" стоянка автотранспорта, "умное" вождение или аварийно-спасательная служба, измененные/поддельные данные о местоположении могут создавать проблемы безопасности.

8.1.3 Перехват сообщения о местоположении

Злоумышленник может перехватить сообщение с данными о местоположении устройства IoT или помешать его передаче в сеть или на платформу услуг "умного" офиса.

8.1.4 Несанкционированное получение данных о местоположении

При отсутствии механизма аутентификации между приложениями и платформой услуг "умного" офиса злоумышленник может несанкционированно получить данные о местоположении.

8.1.5 Недоступные данные

Неунифицированный формат данных может привести к недоступности приложения в составе "умного" офиса; например, неунифицированный формат данных о местоположении в помещении (включая данные об этаже, кабинете, рабочем месте) может запутать робота при доставке посылки получателю.

8.1.6 Раскрытие информации о поведении

Эта угроза возникает при взломе платформы "умного" офиса или когда злоумышленник выдает себя за систему, имеющую право получать информацию о поведении пользователей (например, об их предпочтениях при планировании маршрутов), в злонамеренных целях, например для перепродажи.

8.1.7 Определение местоположения без согласия пользователя

Эта угроза возникает, когда система определения местоположения собирает данные о местоположении пользователей и без их согласия анализирует информацию, связанную с местоположением, включая область охвата, намерение, способ, результат и стандартная практика.

8.2 Угрозы безопасности устройств

8.2.1 Уязвимость аппаратного и программного обеспечения

В процессе разработки устройств позиционирования могут создаваться уязвимости и угрозы безопасности. Примерами могут служить ненадлежащая защита отладочных портов, применение нестойких алгоритмов шифрования, возможное необновление аппаратного и программного обеспечения и отсутствие своевременной проверки целостности.

8.2.2 Манипулирование устройством позиционирования

Злоумышленник может производить манипуляции с устройством позиционирования, вмешиваясь в системы измерения и инфраструктуру, что ведет к неточному результату определения местоположения.

8.3 Угрозы безопасности интерфейсов

8.3.1 Интерфейс ввода данных

Интерфейс между поставщиком измерительных устройств и инфраструктуры и платформой услуг "умного" офиса уязвим в отношении следующих видов угроз:

– **Перехват данных**. При отсутствии механизмов аутентификации и авторизации между платформой услуг "умного" офиса и поставщиком измерительных устройств и инфраструктуры злоумышленник может выдать себя за платформу услуг "умного" офиса и перехватывать данные, поступающие от измерительных устройств и инфраструктуры.

– **Отказ в обслуживании**. Злоумышленник может инициировать распределенную атаку типа "отказ в обслуживании" (DDoS), изменив стратегию сбора данных (например, опрашивая измерительные устройства и инфраструктуру с высокой частотой в течение очень короткого времени).

– **Утечка информации**. Мобильные устройства периодически передают данные услуг, особенно данные о местоположении, на платформу услуг "умного" офиса через интерфейс ввода данных; если злоумышленнику удастся перехватить данные услуг и данные о местоположении, он может изучить режим дня пользователя.

8.3.2 Интерфейс взаимодействия

Интерфейс между платформой услуг "умного" офиса и поставщиком данных или услуг по их обработке уязвим в отношении следующих видов угроз:

– **Несанкционированный доступ к данным**: при отсутствии механизмов аутентификации и авторизации между платформой услуг "умного" офиса и поставщиком данных или услуг по их обработке злоумышленник может изменить интерфейс функционального взаимодействия и получить доступ к данным услуг, данным о местоположении и данным профиля пользователя.

– **Фальсификация данных**: при отсутствии механизмов аутентификации и авторизации между платформой услуг "умного" офиса и поставщиком данных или услуг по их обработке злоумышленник может внести изменения в интерфейс взаимодействия в целях фальсификации данных услуг, данных о местоположении и данных профиля пользователя. Это может привести к утечке информации, неправильной работе платформы и некорректному выставлению счетов поставщику данных или услуг по их обработке.

8.3.3 Интерфейс услуг

Интерфейс между платформой услуг "умного" офиса и приложениями "умного" офиса уязвим в отношении следующих видов угроз:

– **Несанкционированный доступ к данным**: при отсутствии механизмов аутентификации и авторизации между платформой услуг "умного" офиса и приложениями "умного" офиса злоумышленник может внести изменения в интерфейс услуг в целях получения доступа к данным услуг, данным о местоположении и данным профиля пользователя.

– **Фальсификация данных**: при отсутствии механизмов аутентификации и авторизации между платформой услуг "умного" офиса и приложениями "умного" офиса злоумышленник может внести изменения в интерфейс услуг в целях фальсификации данных услуг, данных о местоположении и данных профиля пользователя. Это может привести к некорректному выставлению счетов клиентам.

8.4 Угрозы безопасности платформы

8.4.1 Уязвимость гибридных технологий определения местоположения

Будучи одним из основных функциональных объектов на уровне платформы, функция определения местоположения может нуждаться в объединении гибридных технологий определения местоположения, основанных на нескольких системах беспроводных сетей, таких как ГНСС, РНСС, Bluetooth, Wi-Fi, сотовые сети и сверхширокополосная (СШП) связь. Реализация этих гибридных технологий определения местоположения предполагает извлечение информации, расчет параметров позиционирования и фильтрацию, и уязвимости процесса и алгоритма агрегации могут привести к неточному результату определения местоположения.

8.4.2 Представление функциональных возможностей

Платформа "умного" офиса предоставляет "умным" приложениям информацию о местоположении и других функциональных возможностях услуг, так что неавторизованная система может добавить, изменить или удалить права на использование таких возможностей. В роли неавторизованной системы может выступать человек, программа или устройство. Такие атаки происходят, когда злоумышленник добавляет данные к существующему соединению с использованием возможностей, предоставляемых услугой, путем перехвата соединения или злонамеренной передачи данных конфигурации. Это позволит ему организовать атаку типа "отказ в обслуживании" или осуществить перехват сервисных данных.

8.5 Угрозы безопасности "умного" приложения

8.5.1 Несанкционированное использование

Эта угроза возникает, когда неавторизованное "умное" приложение получает доступ к функциональным возможностям услуг, предлагаемых платформой "умного" офиса, маскируясь под авторизованную систему.

8.5.2 Заражение трояном или вирусом

Это происходит, когда злоумышленник выдает себя за легальное "умное" приложение и внедряет в "умное" приложение троянскую программу или вирус; это причинит ущерб и в дальнейшем даже позволит провести атаки на платформу "умного" офиса.

8.6 Связь между угрозами безопасности и основными системами "умного" офиса

Связь между угрозами безопасности и основными системами "умного" офиса с поддержкой определения местоположения показана в таблице 1.

"Да" в ячейке таблицы 1 указывает на то, что данная угроза безопасности имеет отношение к конкретной системе.

Таблица 1 − Связь угроз безопасности и основных систем

Ключевая заинтересованная сторона / Угрозы	Поставщик услуг "умного" офиса	Поставщик данных и услуг по их обработке	Поставщик измерительных устройств и инфраструктуры	Пользователь
Перехват данных о местоположении	Да		Да	Да
Фальсификация данных о местоположении	Да		Да	Да
Перехват сообщения о местоположении	Да		Да	Да
Несанкционированное получение данных о местоположении	Да		Да	Да
Недоступные данные	Да	Да		
Раскрытие информации о поведении	Да	Да	Да	Да
Определение местоположения без согласия пользователя	Да		Да	Да
Перехват данных	Да		Да	Да
Отказ в обслуживании	Да		Да	
Утечка информации	Да		Да	Да
Несанкционированный доступ к данным	Да	Да	Да	Да
Фальсификация данных	Да	Да	Да	Да
Уязвимость гибридных технологий определения местоположения			Да	
Представление функциональных возможностей	Да			
Уязвимость аппаратного и программного обеспечения			Да	
Манипулирование устройством позиционирования			Да	
Несанкционированное использование	Да			
Заражение трояном или вирусом	Да			

9 Требования безопасности услуг "умного" офиса с поддержкой определения местоположения

9.1 Требования безопасности в отношении данных

– R-01: Требуется, чтобы поставщик услуг "умного" офиса, поставщик данных и услуг по их обработке, а также поставщик измерительных устройств и инфраструктуры предоставляли функциональные возможности для обеспечения конфиденциальности данных, прежде всего данных о местоположении.

– R-02: Требуется, чтобы поставщик услуг "умного" офиса, поставщик данных и услуг по их обработке, а также поставщик измерительных устройств и инфраструктуры предоставляли функциональные возможности для обеспечения целостности данных, прежде всего данных о местоположении.

– R-03: Требуется, чтобы поставщик услуг "умного" офиса, поставщик данных и услуг по их обработке, а также поставщик измерительных устройств и инфраструктуры гарантировали, что доступ к данным, прежде всего к данным о местоположении, разрешен только авторизованным пользователям или устройствам.

– R-04: Требуется, чтобы поставщик услуг "умного" офиса, поставщик данных и услуг по их обработке, а также поставщик измерительных устройств и инфраструктуры подтверждали идентичность объектов и предотвращали попытки злоумышленников замаскироваться под авторизованный объект.

– R-05: Требуется, чтобы поставщик услуг "умного" офиса предоставлял функциональные возможности, гарантирующие, что доступ к офисной среде разрешен только авторизованным устройствам или приложениям.

– R-06: Требуется, чтобы поставщик услуг "умного" офиса, поставщик данных и услуг по их обработке, а также поставщик измерительных устройств и инфраструктуры ввели в действие механизм сотрудничества для унификации формата данных.

– R-07: Требуется, чтобы поставщик услуг "умного" офиса, поставщик данных и услуг по их обработке, а также поставщик измерительных устройств и инфраструктуры имели авторизацию пользователя в виде его выраженного согласия на сбор персональных данных пользователя, прежде всего данных о местоположении. Согласие пользователя включает в себя согласие на получение напоминаний, их отображение и краткое разъяснение пользователю процесса сбора персональных данных.

Что касается данных для услуг "умного" офиса с поддержкой определения местоположения, то в таблице 2 показаны требования безопасности и угрозы безопасности, являющиеся источником соответствующих требований.

Таблица 2 – Таблица сопоставления требований безопасности в отношении данных и угроз безопасности

Угрозы безопасности	Требования безопасности
Перехват данных о местоположении	R-01, R-02, R-03, R-04
Фальсификация данных о местоположении	R-03, R-04
Перехват сообщения о местоположении	R-03, R-04
Несанкционированное получение данных о местоположении	R-03, R-04, R-05
Недоступные данные	R-06
Раскрытие информации о поведении	R-01, R-03, R-04
Определение местоположения без согласия пользователя	R-07

9.2 Требования безопасности в отношении устройства

– R-08: Требуется, чтобы поставщик услуг "умного" офиса, поставщик данных и услуг по их обработке, а также поставщик измерительных устройств и инфраструктуры следовали процедуре реагирования на инциденты при обнаружении вредоносных программ, обеспечивали профилактическое развертывание механизмов безопасности в ответ на атаку и своевременного реагирования на нее.

– R-09: Требуется, чтобы поставщик измерительных устройств и инфраструктуры гарантировал, что злоумышленник не сможет получить доступ к данным, даже если оборудование будет захвачено, что включает в себя следующее:

  • проверку подлинности и целостности программного обеспечения устройства с использованием криптографически сгенерированных цифровых подписей [b-ISO/IEC 9796-3];

  • контроль трафика, завершающегося в устройстве, с помощью межсетевого экрана, системы обнаружения вторжений и системы защиты от вторжений.

– R-10: Требуется, чтобы поставщик услуг "умного" офиса, поставщик данных и услуг по их обработке, а также поставщик измерительных устройств и инфраструктуры использовали соответствующие алгоритмы шифрования, гарантирующие конфиденциальность данных, прежде всего данных о местоположении.

– R-11: Требуется, чтобы поставщик измерительных устройств и инфраструктуры обеспечивал функциональные возможности для подтверждения идентичности объектов и предотвращения любых попыток злоумышленника замаскироваться под авторизованный объект.

Что касается устройств для услуг "умного" офиса с поддержкой определения местоположения, то в таблице 3 показаны требования безопасности и угрозы безопасности, являющиеся источником соответствующих требований.

Таблица 3 − Таблица сопоставления требований безопасности в отношении устройства и угроз безопасности

Угрозы безопасности	Требования безопасности
Уязвимость аппаратного и программного обеспечения	R-08, R-09, R-10
Манипулирование устройством позиционирования	R-09, R-11

9.3 Требования безопасности в отношении интерфейса

– R-12: Требуется, чтобы поставщик услуг "умного" офиса и поставщик измерительных устройств и инфраструктуры предоставляли функциональные возможности, гарантирующие, что доступ к данным измерительных устройств и инфраструктуры через интерфейсы разрешен только авторизованным пользователям или устройствам.

– R-13: Требуется, чтобы поставщик услуг "умного" офиса и поставщик измерительных устройств и инфраструктуры предоставляли функциональные возможности для подтверждения идентичности объектов и предотвращения попыток злоумышленника замаскироваться под авторизованный объект.

– R-14: Требуется, чтобы поставщик услуг "умного" офиса и поставщик измерительных устройств и инфраструктуры предоставляли функциональные возможности, гарантирующие конфиденциальность данных, прежде всего данных о местоположении.

– R-15: Требуется, чтобы поставщик услуг "умного" офиса и поставщик данных и услуг по их обработке предоставляли функциональные возможности, гарантирующие, что доступ к сервисным данным, данным о местоположении и данным профилей разрешен только авторизованным пользователям.

– R-16: Требуется, чтобы поставщик услуг "умного" офиса и поставщик данных и услуг по их обработке предоставляли функциональные возможности для подтверждения идентичности объектов и предотвращения любых попыток злоумышленника замаскироваться под авторизованный объект.

– R-17: Требуется, чтобы поставщик услуг "умного" офиса и поставщик данных и услуг по их обработке предоставляли функциональные возможности, гарантирующие целостность сервисных данных, данных о местоположении и данных профилей.

Что касается интерфейса для услуг "умного" офиса с поддержкой определения местоположения, то в таблице 4 показаны требования безопасности и угрозы безопасности, являющиеся источником соответствующих требований.

Таблица 4 – Таблица сопоставления требований безопасности в отношении интерфейса и угроз безопасности

Угрозы безопасности	Требования безопасности
Перехват данных	R-12, R-13
Отказ в обслуживании	R-13
Утечка информации	R-13, R-14
Несанкционированный доступ к данным	R-15, R-16
Фальсификация данных	R-17

9.4 Требования безопасности в отношении платформы

– R-18: Требуется, чтобы поставщик измерительных устройств и инфраструктуры предоставлял функциональные возможности для проверки точности и целостности алгоритма(ов) гибридной локализации.

– R-19: Требуется, чтобы поставщик услуг "умного" офиса предоставлял функциональные возможности, гарантирующие, что доступ к услуге "умного" офиса с поддержкой определения местоположения разрешен только авторизованным устройствам или приложениям.

– R-20: Требуется, чтобы поставщик услуг "умного" офиса предоставлял функциональные возможности для подтверждения идентичности объектов и предотвращения любых попыток злоумышленника замаскироваться под авторизованный объект.

Что касается платформы для услуг "умного" офиса с поддержкой определения местоположения, то в таблице 5 показаны требования безопасности и угрозы безопасности, являющиеся источником соответствующих требований.

Таблица 5 − Таблица сопоставления требований безопасности в отношении платформы и угроз безопасности

Угрозы безопасности	Требования безопасности
Уязвимость гибридных технологий определения местоположения	R-18
Представление функциональных возможностей	R-19, R-20

9.5 Требования безопасности в отношении "умного" приложения

– R-21: Требуется, чтобы поставщик услуг "умного" офиса предоставлял функциональные возможности, гарантирующие, что доступ к данным, прежде всего к данным о местоположении, разрешен только авторизованным пользователям или устройствам.

– R-22: Требуется, чтобы поставщик услуг "умного" офиса предоставлял функциональные возможности, гарантирующие, что доступ к услуге "умного" офиса разрешен только авторизованным устройствам или приложениям.

– R-23: Требуется, чтобы поставщик услуг "умного" офиса предоставлял функциональные возможности, гарантирующие, что доступ к услуге "умного" офиса с поддержкой определения местоположения разрешен только авторизованным пользователям или устройствам.

– R-24: Требуется, чтобы поставщик услуг "умного" офиса предоставлял функциональные возможности для выполнения процедуры реагирования на инциденты при обнаружении вредоносных программ, а также обеспечения профилактического развертывания механизмов безопасности в ответ на атаку и своевременного реагирования на нее.

Что касается "умных" приложений для услуг "умного" офиса с поддержкой определения местоположения, то в таблице 6 показаны требования безопасности и угрозы безопасности, являющиеся источником соответствующих требований.

Таблица 6 − Таблица сопоставления требований безопасности в отношении "умного" приложения и угроз безопасности

Угрозы безопасности	Требования безопасности
Несанкционированное использование	R-21, R-22
Заражение трояном или вирусом	R-23, R-24

10 Функции безопасности

Для выполнения требований безопасности для услуг "умного" офиса с поддержкой определения местоположения существует несколько функций безопасности, которые включают, в частности, следующие:

– шифрование данных и управление ключами;
– управление определением идентичности и контроль доступа;
– проверку целостности;
– контроль безопасности и реагирование на события безопасности;
– напоминания для пользователя.

10.1 Шифрование данных и управление ключами

Шифрование и управление ключами – основополагающие механизмы защиты конфиденциальности данных в процессе предоставления услуг "умного" офиса. Шифрование позволяет защищать ресурсы, а управление ключами обеспечивает контроль над ключами шифрования.

Шифрование должно соответствовать применимым отраслевым и государственным стандартам. В него входят, в частности, следующие элементы:

– шифрование динамических данных в процессах услуг;
– шифрование статических данных в базе данных;
– шифрование данных в файле резервной копии.

К управлению ключами относятся функции создания, распространения, передачи, замены и отзыва ключей шифрования для обеспечения конфиденциальности данных и аутентификации. Управление является залогом безопасности услуг и включает, в частности, следующие функции:

– **защита информации ключей**: информация ключей должна быть защищена так же, как конфиденциальные данные, и надежнее другой информации;
– **резервное копирование и восстановление**: поскольку потенциальный инцидент может привести к потере определенного ключа и прекращению предоставления услуг, важно установить систему резервного копирования и восстановления ключей.

10.2 Управление определением идентичности и контроль доступа

Необходимо обеспечивать управление определением идентичности объектов услуг "умного" офиса, которые могут представлять собой необработанные данные контроля доступа, авторизации и аудита.

– Следует обеспечить поддержку управления жизненным циклом идентичности на всем его протяжении, включая реестр идентификационных данных, назначение ролей и привилегий, изменение привилегий и удаление идентификационных данных. При этом следует установить порядок, согласно которому регистрация и изменение идентификационных данных утверждаются администратором.
– Следует обеспечить поддержку управления паролями объектов, в том числе единых наборов стратегий управления паролями на основе правил безопасности клиентов, определяющих такие параметры, как алгоритмы шифрования, длина пароля, сложность пароля и длительность цикла смены паролей. При этом можно предусмотреть поддержку паролей различных типов – графических, звуковых и т. п. Кроме того, следует обеспечить поддержку функций синхронизации паролей и сброса пароля.
– К сфере политики управления определением идентичности относятся политика наименования идентификационных учетных записей и политика их применения.

Должен быть обеспечен контроль доступа для управления доступом объектов к услугам "умного" офиса с применением установления идентичности объектов или их способности определять и устанавливать права доступа. Функция контроля доступа может отклонять попытки несанкционированного или неправомерного доступа и сообщать о них, подавая сигнал тревоги или делая запись в журнале безопасности, включающую:

– аутентификационную информацию (например, пароли), владение и последующее представление которой является доказательством авторизации осуществляющего доступ объекта;
– метку безопасности, созданную в соответствии со стратегией безопасности организации;
– время попытки доступа;

– информацию о маршруте попытки доступа;
– информацию о продолжительности доступа;
– информацию о физическом местоположении попытки доступа.

10.3 Проверка целостности

Проверка целостности данных имеет два уровня.

– **Уровень отдельных блоков или полей данных**: определение целостности отдельного блока данных включает два процесса: один на передающем объекте и один на принимающем. Передающий объект добавляет к блоку данных величину, которая является функцией самих данных. Принимающий объект генерирует соответствующую величину и сравнивает ее с принятой величиной, для того чтобы определить, не были ли данные изменены при передаче.
– **Уровень потоков блоков или полей данных**: для проверки на уровне потока блоков данных требуется добавление некоторой формы явного упорядочения, например порядкового номера, отметки времени или криптографической цепочки.

Проверка целостности данных с использованием механизма предварительного развертывания для верификации формата данных и механизма криптографической цифровой подписи в целях проверки того, что данные не фальсифицированы.

10.4 Проверка целостности программного обеспечения и алгоритма(ов) осуществляется с использованием криптографически сгенерированных цифровых подписей − Контроль безопасности и реагирование на события безопасности

Контроль безопасности помогает администраторам услуг проверять отсутствие ошибок и качество услуг. В частности, такой контроль предусматривает следующие операции:

– **Контроль состояния**: включает сбор и отображение записей в журнале событий безопасности, информации об уязвимостях, изменений конфигурации устройств безопасности, качества и рабочего состояния услуг. Это помогает администраторам быть в курсе общей работоспособности услуг.
– **Обнаружение аномального поведения**: включает обнаружение несанкционированного входа в систему, несанкционированного доступа и нарушения правил доступа к определенным услугам, а также аномальных изменений физического устройства.
– **Мониторинг физической безопасности**: включает мониторинг системы регулирования микроклимата, системы видеонаблюдения (CCTV), пропускного пункта, системы противопожарной защиты, кондиционера, системы энергоснабжения и системы наблюдения.

Реагирование на событие безопасности связано с обращением к таким механизмам, как функции обработки событий и управления обработкой, и заключается в выполнении восстановительных операций на основе применения набора правил.

10.5 Напоминания для пользователя

Напоминание для пользователя является механизмом, гарантирующим, что данные, собранные с измерительного устройства, будут использоваться по получении авторизации пользователя услуг "умного" офиса с поддержкой определения местоположения.

Смысл в том, что та или иная услуга "умного" офиса с поддержкой определения местоположения, которой необходимо собирать пользовательские данные, должна отправить пользователю напоминание, отобразить его и кратко разъяснить пользователю. Напоминания для пользователя могут содержать информацию о том, планируется ли сбор данных и какие данные будут собираться. Пользователь также будет проинформирован о том, как данные будут обрабатываться и работа с какими данными будет вестись.

10.6 Связь функций безопасности и требований безопасности

В таблице 7 представлены функции безопасности для удовлетворения соответствующих требований безопасности для услуги "умного" офиса с поддержкой определения местоположения.

Таблица 7 − Таблица сопоставления требований безопасности для "умного" приложения и угроз безопасности

Функции безопасности	**Требования безопасности**	
Шифрование данных и управление ключами	Для данных: R-01	
	Требования безопасности в отношении устройства	R-09, R-10, R-11
	Требования безопасности в отношении интерфейсов	R-14
Управление определением идентичности и контроль доступа	Требования безопасности в отношении данных	R-03, R-04, R-05
	Требования безопасности в отношении интерфейсов	R-12, R-13, R-15, R-16
	Требования безопасности в отношении платформы	R-19, R-20
	Требования безопасности в отношении "умного" приложения	R-21, R-22, R-23
Проверка целостности	Требования безопасности в отношении данных	R-02, R-06
	Требования безопасности в отношении интерфейсов	R-17
	Требования безопасности в отношении платформы	R-18
Контроль безопасности и реагирование на события безопасности	Требования безопасности в отношении устройства	R-08, R-09
	Требования безопасности в отношении "умного" приложения	R-24
Напоминания для пользователя	Требования безопасности в отношении данных	R-07

Библиография

[ITU-T X.1121] Рекомендация МСЭ-Т X.1121 (2004 г.), *Структура технологий безопасности для подвижной передачи данных от конца до конца.*

[b-ISO/IEC 22624] ISO/IEC 22624:2020, *Information technology – Cloud computing – Taxonomy based data handling for cloud services.*

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, 2024 г.