Цуриков Александр Николаевич

КОНЦЕПЦИЯ СИСТЕМЫ ОПОВЕЩЕНИЯ О ПРОИСШЕСТВИЯХ В КОНТРОЛИРУЕМЫХ ПОМЕЩЕНИЯХ НА БАЗЕ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Монография

Новосибирск
2021

УДК 621.39
ББК 32.88
Ц871

Рецензенты:
Шархун С.В., канд. техн. наук, доцент, старший научный сотрудник – начальник научно-исследовательского отделения учебно-научного комплекса обеспечения пожарной безопасности объектов и населенных пунктов Уральского института Государственной противопожарной службы МЧС России, г. Екатеринбург;
Ильичева В.В., канд. техн. наук, доцент, доцент кафедры «Информатика» ФГБОУ ВО «Ростовский государственный университет путей сообщения» (РГУПС), г. Ростов-на-Дону.

Цуриков А.Н.
Ц871 «Концепция системы оповещения о происшествиях в контролируемых помещениях на базе телекоммуникационной сети»: – Монография – Новосибирск: Изд. ООО «СибАК», 2021. – 176 с.

ISBN 978-5-6045789-8-8

Монография посвящена разработке концепции и методики функционирования системы оповещения на базе телекоммуникационной сети. В качестве объекта контроля выбраны серверные комнаты. Описана методика оповещения на базе сетей мобильной GSM-связи и надежных сервисов передачи коротких текстовых сообщений, основанная на обмене алфавитно-цифровыми кодами и их обработке специальным программным и/или аппаратным обеспечением, установленным в мобильные терминалы оповещаемых лиц.

Создан прототип реализовывающего программного приложения для мобильных устройств, обеспечивающий обработку сообщений, привлечение внимания абонента и выдачу ему актуальных уведомлений о происшествии. На указанные решения получены охранные документы (патенты и свидетельства).

Предназначено для научных работников, студентов, магистрантов и аспирантов, а также для специалистов, изучающих информационные технологии.

ББК 32.88

ISBN 978-5-6045789-8-8

СОДЕРЖАНИЕ:

ВВЕДЕНИЕ

Описанное в монографии исследование посвящено разработке концепции и методики функционирования системы оповещения о происшествиях в контролируемых помещениях на базе телекоммуникационной сети.

В процессе работы над монографией был проведен обзор существующих на данный момент в предметной области схожих систем и методик оповещения, а также осуществлен анализ современных технологий и средств разработки для мобильных телекоммуникационных устройств.

Были подробно рассмотрены серверные комнаты как основной объект контроля, а также особенности применения мобильных телекоммуникационных сетей для оповещения о происшествиях, например о незаконном проникновении на территорию. После анализа выявлены основные параметры, которым должна соответствовать разрабатываемая в работе методика оповещения и реализующая ее система.

В работе рассмотрена возможность как программной, так и аппаратной реализации элементов предлагаемой методики оповещения с помощью специально созданного для этих целей мобильного терминала (МТ), выдаваемого ответственным сотрудникам, которые должны получать оповещения о происшествиях и выполнять необходимые экстренные действия.

Разработка прототипа приложения и внедрение предлагаемой методики должны обеспечить повышение оперативности оповещения о происшествиях на объекте и обеспечить скорейшее принятие ответственным лицом решений для реагирования на это событие.

Под оповещением в рамках работы мы будем понимать доведение до абонента, наделенного полномочиями по принятию решений, сигналов о возникновении происшествия, информации о возникшей ситуации и рекомендуемого порядка действий (последнее – опционально).

В качестве контролируемых помещений в нашем исследовании выступают серверные комнаты, оснащенные набором датчиков, обеспечивающих мониторинг обстановки в них. Однако, в качестве таковых в перспективе могут рассматриваться и другие помещения или объекты контроля.

Под происшествиями мы будем понимать внезапно возникшие события, фиксируемые установленными на объекте контроля датчиками и требующие доведения информации о них до уполномоченных лиц, принимающих решения (ЛПР).

В качестве телекоммуникационной сети мы подразумеваем широко развернутые в нашей стране и в мире сети мобильной *GSM*-связи

различных поколений (*2G* и выше). В качестве средства доставки сообщений выбран надежный и проверенный сервис передачи коротких текстовых сообщений *SMS*.

Исследование базируется на опубликованных ранее автором работах по теме оповещения о различных событиях (например [66, 76, 77]), а также вобрало в себя ряд идей, программных и технических решений, предложенных автором и защищенных патентами на изобретение [82], полезную модель [61, 81] и свидетельством о государственной регистрации программы ЭВМ [68]. При подготовке описанного в издании исследования предыдущие разработки были творчески переосмыслены и модифицированы для новой проблемной области – мониторинга серверных комнат.

Результаты данной работы могут найти применение в различных телекоммуникационных предприятиях, вычислительных центрах, осуществляющих обработку информации с помощью серверного оборудования, расположенного в контролируемых помещениях.

Информационная безопасность организации – это состояние сохранности информационных ресурсов предприятия в информационной сфере [9]. Понятие включает в себя защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб элементам информационных отношений [16, 42].

Объекты информационной инфраструктуры могут быть уязвимы, например, в случаях нарушения информационной безопасности, осуществляемых злоумышленниками путем совершения актов незаконного вмешательства на охраняемую территорию или получения несанкционированного доступа к конфиденциальной информации [41].

Стратегией развития многих современных информационных компаний определены основные задачи, стоящие перед ними, с учетом реализации целей поддержания безопасности и работоспособности критически важных элементов, например, серверных комнат. Ставится задача повышения надежности функционирования средств обеспечения безопасности технических средств, входящих в состав объектов инфраструктуры, а также снижение возможного ущерба от происшествий и от незаконных действий злоумышленников.

Важным аспектом информационной безопасности является обнаружение и классификация возможных угроз безопасности. Здесь на помощь могут прийти такие составляющие информационной безопасности, как программно-технические методы и средства обеспечения инфобезопасности [41, 42].

Большинство критически важных объектов уже сегодня оборудованы видеокамерами, различными датчиками и другими средствами слежения [1]. Однако, достаточно надежной методики автоматического обнаружения и оперативного доведения до ЛПР, находящихся вне контролируемого объекта, информации о случаях нарушения информационной безопасности на сегодняшний день не создано [60].

Очевидно, современное распространение высокотехнологичных устройств требует регулярной корректировки действующих правил политики безопасности (*security policy*) – совокупности документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [9, 42].

При возникновении нештатных ситуаций такого рода своевременно принятые управленческие решения по ее ликвидации со стороны лиц, принимающих решения, способствуют минимизации последствий и снижению потерь.

Для оперативного доведения до ЛПР (в том числе тех, которые по каким-то причинам могут не находиться на своих рабочих местах) информации о случаях нарушения информационной безопасности в качестве дублирующей системы предлагается использовать возможности широко развернутых телекоммуникационных сетей мобильной связи.

Сети мобильной беспроводной связи широко развернуты в Российской Федерации и за рубежом [78, 22], повсеместно распространенными являются сети *GSM* (*Global System for Mobile Communications*) и их модификации: *GPRS* (*General Packet Radio Service*), *EDGE* (*Enhanced Data rates for GSM Evolution*), *3G* (*3-rd generation GSM*), *GSM-R* (*GSM-Railway*) и др.

В последнее время среди абонентских устройств значительное распространение получили смартфоны. Они, в частности, отличаются от обычных мобильных телефонов наличием развитой операционной системы, открытой для быстрой разработки дополнительного программного обеспечения.

Установка дополнительных программ позволяет улучшить функциональность смартфонов [76, 78]. Наиболее популярными операционными системами смартфонов на сегодня являются *Google Android*, *Apple iOS*, *Microsoft Windows Phone*. Растет число предлагаемых для установки на смартфоны программ [63] и подключаемых устройств [79], расширяется круг решаемых задач [83, 69].

Комплексное системное использование всех перечисленных средств могло бы значительно повысить эффективности оповещения о случаях нарушения информационной безопасности на объектах информационной инфраструктуры.

Однако удовлетворяющих всем требованиям методик и систем такого оповещения в политике безопасности современных компаний на сегодняшний день практически нет [60]. Это обуславливает актуальность выбранной темы описанного в монографии исследования.

Объект исследования. Информационная безопасность на объектах информационной инфраструктуры предприятий и автоматизированные информационные системы оповещения о происшествиях в контролируемых помещениях.

Цель исследования. Повышение эффективности оповещения о происшествиях на контролируемых объектах информационной инфраструктуры.

Предмет исследования. Методики и средства организации оповещения о случаях нарушения информационной безопасности в автоматизированных информационных системах на базе телекоммуникационных сетей.

Научная задача исследования. Разработка концепции системы и методики оповещения, использующей развернутые телекоммуникационные сети мобильной связи *GSM* и надежные сервисы передачи коротких сообщений (*SMS*), обеспечивающей повышение эффективности оповещения о случаях нарушения информационной безопасности на объектах информационной инфраструктуры.

Наиболее существенные результаты исследования:

1 Методика оповещения о случаях нарушения информационной безопасности на базе телекоммуникационных сетей мобильной связи *GSM* и надежных сервисов передачи коротких сообщений, основанная на передаче алфавитно-цифровых кодов, их приеме и обработке специальным программным и/или аппаратным обеспечением, установленным в мобильные терминалы ЛПР.

2 Методика автоматизированного пополнения баланса мобильных номеров системы оповещения о случаях нарушения информационной безопасности, обеспечивающая бесперебойное поддержание работоспособности *GSM*-устройств системы оповещения, путем предотвращения их финансовой блокировки оператором связи.

3 Прототип реализовывающего программного приложения для мобильных устройств под управлением операционной системы *Android*, обеспечивающий обработку получаемых сообщений от системы оповещения их обработку, привлечение внимания абонента (ЛПР) и выдачу ему актуальных уведомлений о проникновении на охраняемый объект информационной инфраструктуры (в серверную комнату), а также структура возможной аппаратной реализации приложения.

4 Целостная концепция системы оповещения о происшествиях в контролируемых помещениях на базе телекоммуникационной сети, обеспечивающая эффективное функционирование всех описанных ранее частей.

Наиболее существенный новый научный результат. Методика оповещения о случаях нарушения информационной безопасности на базе телекоммуникационной сети, реализуемая передачей алфавитно-цифровых кодов по сети мобильной связи *GSM* и их приеме, отличающаяся от известных методом обработки входящих сообщений.

Теоретическая значимость исследования заключается в разработанных оригинальных методиках автоматизированного пополнения баланса и оповещения о нарушениях информационной безопасности на базе телекоммуникационной сети связи *GSM* и надежных сервисов передачи коротких сообщений (*SMS*), включающих в себя генерацию и обработку входящих сообщений.

Практическая значимость основных результатов выполненного исследования состоит в возможности повышении эффективности оперативного доведения актуальной информации до ЛПР о случаях нарушения информационной безопасности на контролируемых объектах информационной инфраструктуры.

Возможность реализации результатов работы подтверждается (Приложение Б) полученными патентами на изобретение RU 2598294, на полезные модели RU 137441, RU 147524, а также регистрацией реализующей компьютерной программы (свидетельство о регистрации программы ЭВМ RUS 2014611447).

Публикации и апробация результатов. Основные научные результаты исследования опубликованы в рецензируемых научных журналах из списка ВАК РФ [74, 76, 77, 78] и в изданиях, индексируемых в РИНЦ [70, 72]. Основные научные результаты докладывались, обсуждались и были одобрены на ряде международных и всероссийских научных конференций с изданием тезисов докладов в соответствующих сборниках конференций [12, 62, 66, 83]. Выходные данные публикаций приведены в библиографическом списке монографии.

Монография предназначена для научных работников, студентов, магистрантов и аспирантов, изучающих информационные технологии. Рассмотренные задачи могут использоваться в учебном процессе, в курсовом и дипломном проектировании. Монография может быть полезна большинству современных специалистов, вне зависимости от направления подготовки.

Цуриков Александр Николаевич

Монография

КОНЦЕПЦИЯ СИСТЕМЫ ОПОВЕЩЕНИЯ О ПРОИСШЕСТВИЯХ В КОНТРОЛИРУЕМЫХ ПОМЕЩЕНИЯХ НА БАЗЕ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Подписано в печать 12.04.21. Формат бумаги 60x84/16.
Бумага офсет №1. Гарнитура Times. Печать цифровая.
Усл. печ. л. 11. Тираж 550 экз.

Издательство ООО «СибАК»
630049, г. Новосибирск, Красный проспект, 165, оф. 4.
E-mail: mail@sibac.info

Отпечатано в полном соответствии с качеством предоставленного
оригинал-макета в типографии «Allprint»
630004, г. Новосибирск, Вокзальная магистраль, 3.
16+