Автоматизация и моделирование в проектировании и управлении. 2022. № 4 (18). С. 63-69.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2022. № 4 (18). P. 63-69

Управление в организационных системах

Научная статья
Статья в открытом доступе
УДК 004.056.53
doi: 10.30987/2658-6436-2022-4-63-69

МЕТОДИКА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ТЕЛЕФОННЫХ КОММУНИКАЦИЙ РАБОТНИКОВ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Наталия Михайловна Кузнецова [1], Татьяна Владимировна Карлова [2], Анна Николаевна Запольская [3]

[1] Московский государственный технологический университет «СТАНКИН», Москва, Россия
[2, 3] Институт конструкторско-технологической информатики Российской академии наук
[1] knm87@mail.ru, [2] karlova-t@yandex.ru, [3] zap-ann@yandex.ru

Аннотация. *Целью научной работы является создание методики обеспечения конфиденциальности телефонных коммуникаций работников промышленного предприятия. Статья посвящена разработке комплекса технических и организационных мер обеспечения информационной безопасности переговоров работников, находящихся на изолированной территории предприятия, в том числе с несколькими уровнями конфиденциальности. Также в статье рассмотрен вопрос обеспечения безопасности переговоров работников в условиях территориальной удаленности департаментов предприятия. Новизной работы является предложенная креативная концепция использования беспроводных технологий передачи сигналов с применением методов экранирования и зашумления для построения изолированных телекоммуникационных сетей предприятия. Результатом исследования являются рекомендации по использованию беспроводных персональных и беспроводных локальных сетей, схемы экранирования, схема организации коммуникации между работниками территориально удаленных департаментов предприятия.*

Ключевые слова: автоматизация, защита информации, информационная безопасность, телефонные переговоры, коммуникация, конфиденциальность

Для цитирования: Кузнецова Н.М., Карлова Т.В., Запольская А.Н. Методика обеспечения конфиденциальности телефонных коммуникаций работников промышленного предприятия // Автоматизация и моделирование в проектировании и управлении. 2022. №4 (18). С. 63-69. doi: 10.30987/2658-6436-2022-4-63-69.

Original article

Open Access Article

METHODOLOGY FOR ENSURING THE TELEPHONE COMMUNICATION CONFIDENTIALITY OF INDUSTRIAL ENTERPRISE STAFF

Natalia M. Kuznetsova[1], Tatyana V. Karlova[2], Anna N. Zapolskaya[3]

[1]Moscow State University of Technology «STANKIN», Moscow, Russia
[2,3]Institute for Design-Technological Informatics of the Russian Academy of Sciences, Moscow, Russia

[1]knm87@mail.ru, [2]karlova-t@yandex.ru, [3]zap-ann@yandex.ru

Abstract. *The aim of the paper is to make a methodology for ensuring the telephone communication confidentiality of industrial enterprise staff. The article is devoted to developing a set of technical and organisational measures including those with several levels of confidentiality to ensure the information security of communication between employees located in the enterprise isolated territories. The article also considers security provision of the employees' conversations given that the company departments are distantly locat-*

ed. The novelty of the work is the proposed creative concept of using wireless signal transmission technologies with the application of shielding and noise methods to build isolated telecommunication networks of the enterprise. The study results in recommendations for using wireless personal and local networks, schemes of shielding and organising communication between employees of the enterprise remote departments.

Keywords: automation, information protection, information security, telephone conversations, communication, confidentiality

For citation: Kuznetsova N.M., Karlova T.V., Zapolskaya A.N. Methodology for ensuring the telephone communication confidentiality of industrial enterprise staff. Automation and modeling in design and management, 2022, no. 4 (18). pp. 63-69. doi: 10.30987/2658-6436-2022-4-63-69.

Введение

Современные промышленные предприятия, относящиеся к стратегически важным объектам, используют автоматизированные системы защиты информации. Однако данные системы не обеспечивают комплексной защиты внутренних переговоров работников по телефону. Конфиденциальность переговоров обеспечивается за счёт дополнительного применения технических и организационных мер. В статье предложена методика, позволяющая автоматизировать процессы защиты телефонных коммуникаций работников предприятия за счёт применения комплекса взаимодействующих инструментов.

Постановка задачи обеспечения конфиденциальности телефонных коммуникаций работников предприятия

Работникам предприятия необходимо обеспечение конфиденциальной телефонной коммуникации. Однако использование общей городской, а также мобильной сетей недопустимо в силу наличия возможности реализации атак перехвата информации.

Кроме того, использование общих телекоммуникационных сетей может привести к утечкам по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

С другой стороны, использование дополнительных технических и организационных мер является неудобным для конечных пользователей (работников предприятия).

Таким образом, необходимо создание такого механизма коммуникации работников, при котором будет обеспечен максимально возможный уровень конфиденциальности при сохранении удобства для самих работников.

Обеспечение конфиденциальности телефонных коммуникаций на изолированной территории предприятия

Для обеспечения конфиденциальности внутренних телефонных коммуникаций работников предприятия на изолированной территории необходимо выполнение условий:

– обеспечение полной изоляции сигналов телекоммуникационной сети (далее – ТКС) от внешней среды;

– обеспечение идентификации, аутентификации, авторизации работников при использовании ТКС – для определения списка работников, с которыми можно связаться (в случае, если уровень доступа одинаковый, но для разных проектов предприятия свои списки допущенных лиц), также для дальнейшего проведения расследований;

– обеспечение доступности ТКС всем допущенным абонентам (работникам).

Таким образом, ТКС представляет собой изолированную среду коммуникаций.

Обеспечение полной изоляции сигналов ТКС от внешней среды. С целью полной изоляции сигналов ТКС от внешней среды необходимо использовать беспроводные технологии передачи сигналов, например:

– беспроводные персональные сети – Wireless Personal Area Networks (далее – WPAN): Bluetooth [1];

– беспроводные локальные сети – Wireless Local Area Networks (далее – WLAN): WiFi [2].

При использовании данных технологий необходимо разместить оборудование ТКС таким образом, чтобы отсутствовала физическая возможность перехвата сигнала.

Ввиду совершенствования технологий – сохранения энергоэффективности связи на увеличенном расстоянии – наиболее подходящими способами являются экранирование и зашумление сигналов на границах территории предприятия.

WLAN может быть использован для оповещения всех работников функционального департамента, имеющих одинаковые права доступа (например, для работников отдела кадров).

В отличие от WLAN, технология WPAN может быть рассмотрена, как более гибкий механизм создания ТКС: как относительно времени, так и относительно пространства создания ТКС. Например, для создания ТКС для разработчиков временного проекта [3].

На рис. 1 представлена схема создания нескольких ТКС на территории предприятия.

Рис. 1. Схема создания нескольких ТКС на территории предприятия
Fig. 1. Scheme of creation of some Telecommunication Network on an enterprise area

Согласно рис. 1, на территории предприятия N ТКС. ТКС 1, ТКС i+1, ТКС N реализованы с помощью технологии WLAN; ТКС 2, ТКС i, ТКС N-1 – с помощью технологии WPAN.

Для повышения уровня конфиденциальности переговоров внутри каждой ТКС предприятия необходимо:

– обеспечение разграничения доступа (для каждой ТКС необходимо ведение списка абонентов);

– обеспечение шифрования (для каждой ТКС свой ключ и алгоритм шифрования) [4, 5].

Обеспечение идентификации, аутентификации, авторизации работников. При входе работника на территорию предприятия, где обеспечено функционирование ТКСi, работнику предоставляется телефонный аппарат без физической возможности связи с городской телефонной сетью и сетями мобильных операторов (отсутствие соответствующих антенн и механизмов подключения к сетям).

При этом работник «не привязан» к конкретному телефонному аппарату – при входе на территорию ТКСi ему может быть выделен любой телефонный аппарат из набора ТКСi.

Далее работнику предприятия необходимо последовательно пройти процедуры идентификации и аутентификации. Аутентификация может быть организована несколькими способами:

– на основе пароля;

– на основе владения материальным носителем (брелок для телефонного аппарата);

– на основе биометрических данных (биометрические считыватели, установленные на телефонном аппарате) [6].

Также аутентификация работника может быть многофакторной. При этом важно соблюдать правило: чем выше уровень секретности, тем больше факторов аутентификации следует применять.

Далее работнику присваиваются права (процедура авторизации): список абонентов, с которыми работник может осуществлять коммуникацию в рамках ТКСi.

Также важно, чтобы работник, находясь на территории ТКСi, не терял телефонный аппарат, на котором им был совершен вход в ТКСi. Для повышения уровня информационной

безопасности целесообразно производить автоматический «выход» работника из ТКС*i*, если работник не производил коммуникацию в течение определенного промежутка времени (промежуток времени настраивается офицером безопасности). В случае поступления входящего вызова по истечении данного промежутка времени работнику необходимо пройти процедуры аутентификации и авторизации повторно прежде чем принять входящий вызов.

При выходе работника с территории функционирования ТКС*i* он должен произвести «выход» их ТКС*i* и сдать телефонный аппарат.

Программно-аппаратная реализация. Для обеспечения мониторинга и ведения журнала действий работников следует использовать клиент-серверную архитектуру. При использовании технологии WLAN серверная часть является стационарной. При использовании WPAN серверная часть формируется динамически при создании соответствующей ТКС.

В связи с тем, что мониторинг и ведение журнала аудита не требуют больших объемов вычислительных ресурсов, серверная часть может быть организована с помощью персонального компьютера (при использовании технологии WLAN), либо с помощью переносного устройства, например, планшета (при использовании технологии WPAN).

Важно отметить, что доступ к серверной части должны иметь только офицеры безопасности.

Сторону клиента составляют выдаваемые работникам телефонные аппараты. Данные аппараты содержат клиентскую часть программного обеспечения (ПО) идентификации, аутентификации, авторизации и мониторинга.

В случае, если работник умышленно или непреднамеренно вынес с территории предприятия телефонный аппарат, данный аппарат превращается в «кирпич»: какая-либо информация о коммуникации работника на аппарате отсутствует. В случае попадания аппарата в руки злоумышленника вероятность реализации угрозы утечки информации стремится к нулю.

Обеспечение конфиденциальности телефонных коммуникаций с несколькими уровнями секретности на изолированной территории предприятия

При наличии нескольких уровней конфиденциальности на предприятии можно организовывать несколько уровней экранирования. При этом при увеличении уровня конфиденциальности также необходимо увеличивать количество факторов аутентификации.

Пример схемы экранирования ТКС на предприятии представлен на рис. 2.

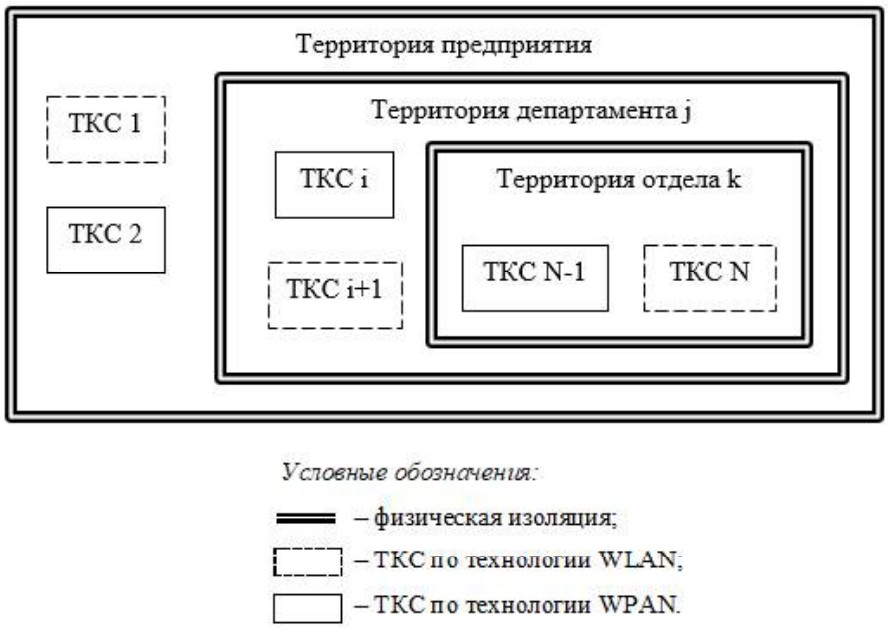

Рис. 2. Пример схемы экранирования ТКС на предприятии с несколькими уровнями конфиденциальности
Fig. 2. Example of shielding scheme of Telecommunication Network on an enterprise with several confidence levels

Согласно рис. 2, на территории предприятия существует три уровня конфиденциальности и для каждого уровня предусмотрена физическая изоляция. На каждом уровне возможно использование технологии как WLAN, так и WPAN.

При этом физическая изоляция организована таким образом, чтобы сигналы от ТКС из территории с высшим уровнем конфиденциальности не поступали на территорию с меньшим уровнем конфиденциальности.

При переходе от одного уровня конфиденциальности к другому, работники предприятия должны пользоваться разными наборами телефонных аппаратов и каждый раз проходить процедуры идентификации, аутентификации и авторизации.

Для удобства телефонные аппараты, предназначенные для разных уровней конфиденциальности, могут иметь разные цвета корпусов.

Обеспечение конфиденциальности телефонных коммуникаций в условиях территориальной удаленности департаментов предприятия

На рис. 3 представлена схема организации коммуникации работников, находящихся в удаленных друг от друга департаментах предприятия.

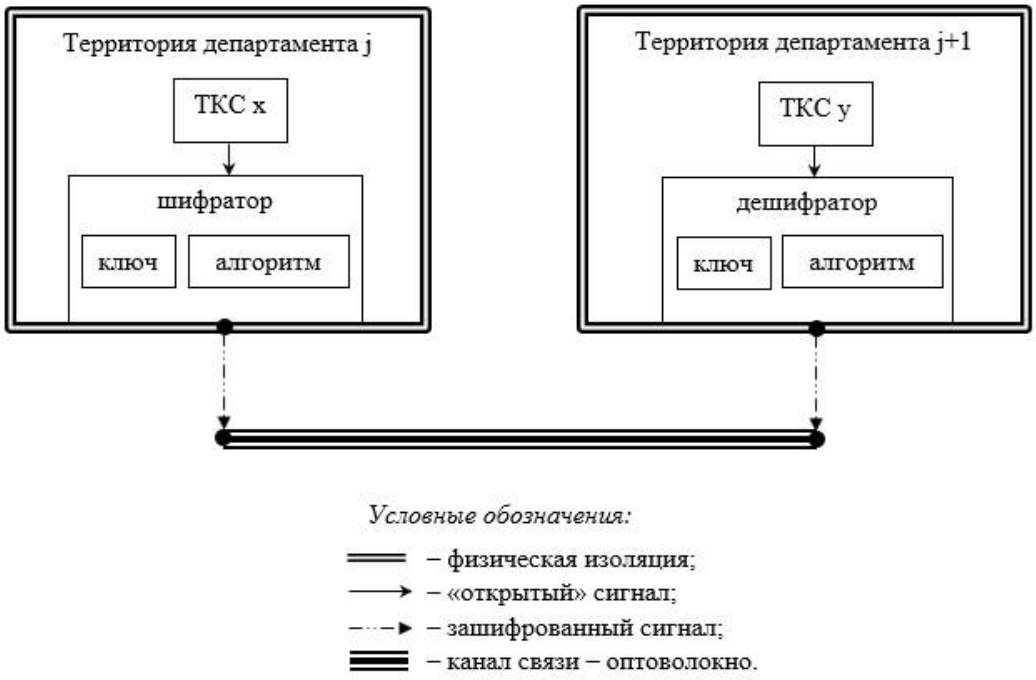

Рис. 3. Схема организации коммуникации работников, находящихся в удаленных друг от друга департаментах
Fig. 3. Scheme of communication creation of staff located in remoted departments

При условии территориальной удаленности департаментов предприятия необходимо обеспечить конфиденциальность телефонных переговоров при передаче данных. Для этого необходимо использовать криптографические методы при трансляции информации из одного департамента предприятия в другой. Кроме того, желательно использовать разные алгоритмы и ключи шифрования для каждой коммуникации работников. При этом наиболее подходящим каналом связи является оптоволокно.

Особенности использования методики обеспечения конфиденциальности телефонных коммуникаций

Основным недостатком применения методики обеспечения конфиденциальности телефонных коммуникаций работников является отрицательное влияние на здоровье вследствие частого применения технологии WPAN, WLAN [7]. Повышенный уровень электромагнитного излучения на территории предприятия может негативно влиять на жизненно важные системы человеческого организма, приводить к:

– расстройствам сердечно-сосудистой системы;
– ослаблению иммунной системы;
– ухудшению зрительной активности;
– нарушениям нервной системы и т.д.

Помимо прямого вреда здоровью, также необходимо рассматривать влияние применения данной методики на психику человека.

К основным факторам, влияющим на психическое здоровье человека, можно отнести:
– отсутствие связи с «внешним миром»;
– постоянное психологическое напряжение;
– превышение полномочий работниками, которые обеспечивают организационные меры защиты.

Мощности антенн оборудования и частота его использования должны быть минимизированы для сокращения влияния на здоровье (в том числе психическое) работников предприятия.

Уменьшение мощности антенн также повысит уровень информационной безопасности, т.к. уменьшит энергоэффективность связи на большом расстоянии. Данный сигнал сложнее перехватить.

Минимизировать количество случаев злоупотребления полномочиями работниками, которые обеспечивают организационные меры защиты, позволит ряд мер:
– создание механизма обратной связи (рекламаций);
– выполнение заранее определенных и установленных проверок здоровья психики данных работников при приеме на работу;
– проведение периодических проверок психического здоровья данных работников.

Также недостатком методики является тот факт, что она не содержит механизмов защиты информации от внутреннего злоумышленника. Частичным решением данной проблемы является отсутствие какой-либо конфиденциальной информации о переговорах в телефонном аппарате за счет применения клиент-серверной архитектуры.

Заключение

Для обеспечения конфиденциальности телефонных коммуникаций работников промышленного предприятия необходимо применение методики рационального использования беспроводных сетей WLAN и WPAN, механизмов экранирования и зашумления. При применении беспроводных сетей WLAN и WPAN должны быть обеспечены процедуры идентификации, аутентификации и авторизации работников для возможных дальнейших расследований инцидентов информационной безопасности. В зависимости от уровней конфиденциальности, а также от территориальной удаленности департаментов предприятиях должны быть применены соответствующие схемы экранирования и зашумления – физической изоляции ТКС.

СПИСОК ИСТОЧНИКОВ

1. Bluetooth Technology. – URL: https://www.tutorial-reports. com / wireless /bluetooth (дата обращения: 15.06.2022). – Текст.: электронный.
2. Хороши й Wi-Fi для предприятия: от А до Я. Беспроводные технологии. Сетевое оборудование. – URL: habr.com/ru/post/570452 (дата обращения: 15.06.2022). – Текст.: электронный.
3. Хьюстон-Эдвардс К. Математика создания связей. В мире науки. 2021. №5-6. С. 4-13.
4. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Совершенствование симметричного шифрования за счёт внедрения блока информации об используемых алгоритмах в ключ. Вестник Брянского государственного технического университета. 2015. №4 (48). С. 121.
5. Кузнецова Н.М., Карлова Т.В., Шептунов С.А. Криптоанализ сообщений в автоматизированных системах предотвращения утечек информации по каналам связи с применением теории графов. Ученые записки Комсомольского-на-Амуре государственного технического университета. 2015. Т. 1. № 4 (24). С. 33-37.

References:

1. Bluetooth technology [Internet] [cited 2022 Jun 15]. Available from: https://www.tutorial-reports.com/ wireless/bluetooth
2. Good Wi-Fi for the Enterprise: from A to Z. Wireless Technologies. Network Hardware. [Internet] [cited 2022 Jun 15]. Available from: habr.com/ru/ post/570452.
3. Houston-Edwards K. Mathematics of Creating Connections. Scientific American. 2021;5-6:4-13.
4. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Symmetric Encryption Update by Introduction of Information Block on Used Algorithms in Key. Bulletin of Bryansk State Technical University. 2015;4(48):121.
5. Kuznetsova N.M., Karlova T.V., Sheptunov S.A. Cryptoanalysis of Messages in Auto-mated Systems for Preventing Information Leaks through Communication Channels Using Graph Theory. Scientific Notes of Komsomolsk-on-Amur State Technical University. 2015;1-4(24):33-37.

6. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Анализ и применение методов биометрической аутентификации в автоматизированной системе защиты ресурсов промышленного предприятия. Вестник Брянского государственного технического университета. 2020. № 8 (93). С. 47-52.
7. О влиянии на здоровье электромагнитных полей, создаваемых базовыми и подвижными станциями сухопутной подвижной радиосвязи. Управление Федеральной службы по надзору в сфере прав потребителей и благополучия человека. – URL:https://www.rospotrebnadzor.ru (дата обращения: 28.07.2022). – Текст.: электронный.

6. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Analysis and Application of Biometric Authentication Methods in Automated System of Industrial Enterprise Resource Protection. Bulletin of Bryansk State Technical University. 2020;8(93):47-52.

7. On the Health Impact of Electromagnetic Fields Generated by Base and Mobile Stations of Land Mobile Radio Communications. Administration of the Federal Service for Supervision of Consumer Rights and Human Welfare [Internet] [cited 2022 Jul 28]. Available from: https://www.rospotrebnadzor.ru.

Информация об авторах:

Наталия Михайловна Кузнецова
Кандидат технических наук, доцент Московского государственного технологического университета «СТАНКИН».
Татьяна Владимировна Карлова
Доктор социологических наук, кандидат технических наук, профессор Институт конструкторско-технологической информатики Российской академии наук .

Анна Николаевна Запольская
Кандидат социологических наук, старший научный сотрудник, ученый секретарь Института конструкторско-технологической информатики Российской академии наук .

Information about authors:

Natalia Mikhailovna Kuznetsova
Candidate of Technical Sciences, Associate Professor of Moscow State University of Technology «STANKIN».

Tatyana Vladimirovna Karlova
Doctor of Sociological Sciences, Candidate of Technical Sciences, Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences.
Anna Nikolaevna Zapolskaya
Candidate of Sociological Sciences, Senior Research Fellow, Academic Secretary of the Institute for Design-Technological Informatics of the Russian Academy of Sciences.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 29.07.2022; одобрена после рецензирования 05.09.2022; принята к публикации 09.09.2022.
The article was submitted 29.07.2022; approved after reviewing 05.09.2022; accepted for publication 09.09.2022.

Рецензент – Рытов М.Ю., кандидат технических наук, доцент, Брянский государственный технический университет.
Reviewer – Rytov M. Yu., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.