Модель защиты многоуровневых коммуникаций

**Человек:** Работа посвящается актуальной проблеме обеспечения безопасности гетерогенных информационных платформ, с применением системы электронной поддержки процессов он-лайн коммуникаций в медицинском учреждении – e-health online communications. Особое внимание автор уделяет таким важным аспектам темы как: безопасность гетерогенных информационных платформ, модель защиты гетерогенных информационных платформ, классификация коммуникаций и механизмы защиты ММК. Рассматриваются тенденции для разработки новых распределённых моделей безопасности. В данной статье представлена модель многоуровневых коммуникаций. Предложена классификация коммуникаций и механизмы защиты для каждого уровня с разными уровнями безопасности, использующими протоколы криптографии. Гибкость обеспечения безопасности может быть предоставлена организациям здравоохранения, используя различные комбинации размеров ключей для защиты данных и каналов. На каждом уровне могут быть обеспечены различные уровни безопасности в зависимости от чувствительности данных. Таким образом, мы пришли к модели ММК как решение проблемы коммуникации в e-health и других крупных организациях с распределённой сетью компьютерных коммуникаций.

**Key words:** защита информации, обнаружение угроз, интеллектуальные системы защиты, многоуровневые коммуникации, гетерогенные информационные платформы, механизмы защиты, системы анализа, алгоритм обнаружения, электронные коммуникации, защита данных

=================================

**FastText\_KMeans\_Clean:** Совершенно секретно. Содержит конфиденциальную информацию: Информация пациента, необходимая для оперативной работы персонала больницы. Согласно Lenstra [17], симметричная система криптографии с n -битным ключом имеет уровень безопасности n , если она может переносить общую атаку (чтобы найти ключ, когда открытый текст и зашифрованный текст известны заранее), используя усилия меньше Исчерпывающий поиск или атака “грубой силы”. Проводная связь: 129-192. 128. Уровень 3 (Защищено). В ММК существует безопасность данных и каналов, предоставляемая пользователям таким образом, что пользователь может выбрать наиболее подходящие процессы безопасности с точки зрения стоимости и эффективности.

**Key words part:** 0.41935483870967744

=================================

**FastText\_KMeans\_Raw/:** Шифр - ключ : E (K, H (P)) pubKr . Согласно Lenstra [17], симметричная система криптографии с n -битным ключом имеет уровень безопасности n , если она может переносить общую атаку (чтобы найти ключ, когда открытый текст и зашифрованный текст известны заранее), используя усилия меньше Исчерпывающий поиск или атака “грубой силы”. Проводная связь: 129-192. 128. Уровень 3 (Защищено). (Совершенно секретно). В ММК существует безопасность данных и каналов, предоставляемая пользователям таким образом, что пользователь может выбрать наиболее подходящие процессы безопасности с точки зрения стоимости и эффективности.

**Key words part:** 0.3870967741935484

=================================

**FastText\_PageRank\_Clean/:** ПарамедикСистемный координатор. Шифр-текст = E (P)K . Проводная связь: 129-192. Упрощённое устройство: 112-192. 128. Уровень 3 (Защищено). Проводная связь: 129-192. Беспроводная связь: 112-192. Уровень 3 (Защищено).

**Key words part:** 0.2903225806451613

=================================

**FastText\_PageRank\_Raw/:** Совершенно секретно. ПарамедикСистемный координатор. D (шифр-текст) К = Р ;. Совершенно секретно. Проводная связь: 129-192. (Высококонфиденциально). Проводная связь: 129-192. Беспроводная связь: 112-192.

**Key words part:** 0.2903225806451613

=================================

**Mixed\_ML\_TR/:** Только для внутреннего использования. Согласно Lenstra [17], симметричная система криптографии с n -битным ключом имеет уровень безопасности n , если она может переносить общую атаку (чтобы найти ключ, когда открытый текст и зашифрованный текст известны заранее), используя усилия меньше Исчерпывающий поиск или атака “грубой силы”. Уровень 1, который защищает информацию “Совершенно секретно”, должен обеспечивать самую высокую доступную безопасность, и поэтому должен быть обеспечен самый надёжный ключ. - 193-бит и более: подходит для уровня 1, для защиты информации “Совершенно секретно”, которая требует наивысшей защиты безопасности;. Проводная связь: 129-192. – Спецификации безопасности в модели ММК. Гибкость обеспечения безопасности может быть предоставлена организациям здравоохранения, используя различные комбинации размеров ключей для защиты данных и каналов. В противном случае можно выбрать более короткую длину ключа с высокой производительностью в соответствии с потребностями.

**Key words part:** 0.5483870967741935

=================================

**MultiLingual\_KMeans/:** Только для внутреннего использования. 2. Для того, чтобы отправитель удостоверился, что открытый текст не изменен, хэш-сообщение может быть вычислено из открытого текста и внедрено в сообщение перед отправкой его получателю. Общепринятой практикой является медицинский персонал, который сохраняет конфиденциальную информацию пациента во время её передачи, что указано в нескольких стандартах, таких как, IPPA (http://www.hhs.gov/ocr/hipaa/) и APA (http://www.privacy.gov.au/). Согласно Lenstra [17], симметричная система криптографии с n -битным ключом имеет уровень безопасности n , если она может переносить общую атаку (чтобы найти ключ, когда открытый текст и зашифрованный текст известны заранее), используя усилия меньше Исчерпывающий поиск или атака “грубой силы”. - 129-бит – 192-бит: подходит для уровня 2, для защиты высоко конфиденциальной информации, требующей очень высокой защиты;. Проводная связь: 129-192. – Рекомендуемые размеры ключей для каждого уровне в ММК. – Спецификации безопасности в модели ММК.

**Key words part:** 0.5161290322580645

=================================

**Multilingual\_PageRank/:** В этой связи предлагается разбивать сообщения в e-health на пять уровней от Уровня 1 до Уровня 5, на основе пяти классификаций информации, описанных в п. 3.2. В таблице 1 показаны пять типов сообщений в ММК. – Пять уровней коммуникаций в ММК. Уровень 5: для обмена информацией между пользователями, обменивающимися общедоступной информацией. Ниже описывается процесс шаг за шагом со стороны отправителя и стороны получателя. - в заключении проверяется P путём вычисления нового H(P) от P , и сравнивается с указанным на стадии (а). Существует ещё целый ряд критериев выбора. Для сравнения в таблице также включены рекомендации США [19]. Модель ММК: обоснования и преимущества.

**Key words part:** 0.3870967741935484

=================================

**RuBERT\_KMeans\_Without\_ST/:** В этой связи предлагается разбивать сообщения в e-health на пять уровней от Уровня 1 до Уровня 5, на основе пяти классификаций информации, описанных в п. 3.2. В таблице 1 показаны пять типов сообщений в ММК. 2. Для того, чтобы отправитель удостоверился, что открытый текст не изменен, хэш-сообщение может быть вычислено из открытого текста и внедрено в сообщение перед отправкой его получателю. D (шифр-текст) К = Р ;. В ММК существует безопасность данных и каналов, предоставляемая пользователям таким образом, что пользователь может выбрать наиболее подходящие процессы безопасности с точки зрения стоимости и эффективности.

**Key words part:** 0.3548387096774194

=================================

**RuBERT\_KMeans\_With\_ST/:** Необходимо определить, как классифицировать каждую коммуникацию между пользователями в e-health на основе уровней чувствительности информации, передаваемой во время связи. Совершенно секретно. Безопасность на этом уровне низкая. - простой (незашифрованный) текст, Р , хеш незашифрованного текста, Н (Р );. Обмен ключами : ключ K , должен быть зашифрован и отправлен получателю, так что K может быть использован для расшифровки сообщения на стороне получателя. Чем длиннее ключ, тем выше безопасность, которую он может обеспечить, потому что трудность поиска всех возможных ключей в исчерпывающем поиске прямо пропорциональна количеству используемых битов [18]. Защита данных или канала. (Только для внутреннего использования).

**Key words part:** 0.5483870967741935

=================================

**RUBERT\_page\_rank\_Without\_ST/:** Содержит конфиденциальную информацию:. Существует ещё целый ряд критериев выбора. 128. Уровень 2 (Высококонфиденциально). (Высококонфиденциально). (Только для внутреннего использования).

**Key words part:** 0.3225806451612903

=================================

**RUBERT\_page\_rank\_With\_ST/:** 3,Ниже описаны обозначения, используемые в процессах криптографии:. - цифровая подпись, S . Шифр - ключ : E (K, H (P)) pubKr . D (шифр-текст) К = Р ;. Совершенно секретно.

**Key words part:** 0.2903225806451613

=================================

**RUSBERT\_KMeans\_Without\_ST/:** Строго конфиденциально. Хотя разные организации имеют разные требования безопасности в соответствии с их потребностями, основные требования безопасности должны быть сосредоточены на рассмотрении аспектов конфиденциальности, целостности и доступности [1]. Криптографические протоколы, которые шифруют, дешифруют, осуществляют хеш-функции, цифровую подпись и цифровые сертификаты, должны удовлетворять следующим требованиям безопасности. - публичные и частные ключи получателя (pubKr , privKr );.

**Key words part:** 0.2903225806451613

=================================

**RUSBERT\_KMeans\_With\_ST/:** В предлагаемом подходе используется симметричный ключ шифрования, хэш-функции и цифровая подпись, обеспечивающие безопасность данных. Ключ K является важным компонентом процесса шифрования, поскольку он представляет уровень безопасности, который может предоставить алгоритм. \* мобильные устройства используют только защиту данных. Модель ММК обеспечивает механизмы безопасности для защиты различных типов коммуникаций между различными пользователями в e-health в соответствии с их потребностями.

**Key words part:** 0.5806451612903226

=================================

**RUSBERT\_page\_rank\_Without\_ST/:** Безопасность на этом уровне минимальна. 128. Уровень 3 (Защищено). Уровень 4 (Только для внутреннего использования). Уровень 3 (Защищено). (Только для внутреннего использования).

**Key words part:** 0.2903225806451613

=================================

**RUSBERT\_page\_rank\_With\_ST/:** Чувствительность данных. Строго конфиденциально. Безопасность на этом уровне средняя. 128. Уровень 3 (Защищено). Уровень 3 (Защищено).

**Key words part:** 0.3225806451612903

=================================

**Simple\_PageRank/:** Эта информация должна быть защищена от угроз и потерь и раскрываться только уполномоченным пользователям, таким как врачи, сами пациенты и медсестры. Исходя из этих требований, разрабатывается предлагаемая модель безопасной коммуникации для каждого уровня в ММК, которая может обеспечить гибкие функции защиты. - 193-бит и более: подходит для уровня 1, для защиты информации “Совершенно секретно”, которая требует наивысшей защиты безопасности;. - 80-бит – 111-бит: подходит для уровня 4, для защиты информации только для внутреннего использования, для которой требуется низкая защита безопасности. ММК удовлетворяет существующему технологическому разрыву и ограничениям, как показано в п. 3.1. Используя ММК, пользователи могут общаться с различными типами механизмов безопасности, адекватными их потребностям. Например, организация может выбрать для коммуникаций канал SSL, который обходится дешевле, чем шифрование данных [23], однако с компромиссом негибкой конфигурации безопасности, когда пользователю необходимо перейти на более сильный или более слабый уровень безопасности.

**Key words part:** 0.6129032258064516

=================================

**TextRank/:** Согласно Lenstra [17], симметричная система криптографии с n -битным ключом имеет уровень безопасности n , если она может переносить общую атаку (чтобы найти ключ, когда открытый текст и зашифрованный текст известны заранее), используя усилия меньше Исчерпывающий поиск или атака “грубой силы”. Уровень 1, который защищает информацию “Совершенно секретно”, должен обеспечивать самую высокую доступную безопасность, и поэтому должен быть обеспечен самый надёжный ключ. - 193-бит и более: подходит для уровня 1, для защиты информации “Совершенно секретно”, которая требует наивысшей защиты безопасности;. - 80-бит – 111-бит: подходит для уровня 4, для защиты информации только для внутреннего использования, для которой требуется низкая защита безопасности. Гибкость обеспечения безопасности может быть предоставлена организациям здравоохранения, используя различные комбинации размеров ключей для защиты данных и каналов. Например, организация может выбрать для коммуникаций канал SSL, который обходится дешевле, чем шифрование данных [23], однако с компромиссом негибкой конфигурации безопасности, когда пользователю необходимо перейти на более сильный или более слабый уровень безопасности.

**Key words part:** 0.6129032258064516

=================================

**TF-IDF\_KMeans/:** Уровень 4: для обмена информацией между пользователями, которые обмениваются информацией только для внутреннего использования, которая связана с общей информацией о системе организации и не связанной с медицинской информацией. 2. Для того, чтобы отправитель удостоверился, что открытый текст не изменен, хэш-сообщение может быть вычислено из открытого текста и внедрено в сообщение перед отправкой его получателю. Механизм 3: защита данных и каналов. Размер ключа для шифрования с симметричным ключом. Уровень 1 (Совершенно секретно). \* мобильные устройства используют только защиту данных. На каждом уровне могут быть обеспечены различные уровни безопасности в зависимости от чувствительности данных.

**Key words part:** 0.5806451612903226

=================================

**Текст:** Модель многоуровневых коммуникаций (ММК): классификация коммуникаций.. Необходимо определить, как классифицировать каждую коммуникацию между пользователями в e-health на основе уровней чувствительности информации, передаваемой во время связи. Классификация коммуникаций может обеспечить гибкие механизмы защиты в рамках коммуникации на основе потребностей организации.. В этой связи предлагается разбивать сообщения в e-health на пять уровней от Уровня 1 до Уровня 5, на основе пяти классификаций информации, описанных в п. 3.2. В таблице 1 показаны пять типов сообщений в ММК. Коммуникация Уровня 1 содержит данные с самым высоким уровнем чувствительности (“Совершенно секретно”), тогда как уровень 5 содержит данные с самым низким уровнем чувствительности (“Общедоступная”). Предлагаемая на каждом уровне защита безопасности соответствует безопасности, предусмотренной в ISO 17799:. Уровень 1: для обмена информацией между пользователями, которые обмениваются информацией категории Совершенно секретно, являющейся чрезвычайно чувствительной. Должны применяться механизмы максимальной защиты. Эта информация должна быть защищена от угроз и потерь и раскрываться только уполномоченным пользователям, таким как врачи, сами пациенты и медсестры. Любое раскрытие другим пользователям должны получить согласие пациентов.. . Уровень. Чувствительность данных. Тип данных коммуникаций. Пользователи. Уровень 1. Совершенно секретно. Содержит чрезвычайно чувствительную информацию: Личная информация пациента и подробная медицинская информация.. Доктор Доктор. Доктор Пациент. Доктор Медсестра. Медсестра Пациент. Уровень 2. Строго конфиденциально. Содержит высокочувствительную информацию: Информация о пациенте, не подлежащая публикации, а также информацию от парамедика на месте аварии.. ПарамедикСистемный координатор. Уровень 3. Закрытая. Содержит конфиденциальную информацию: Информация пациента, необходимая для оперативной работы персонала больницы.. Доктор Соц. работник. Медсестра Соц. работник. Пациент Соц. работник. Уровень 4. Только для внутреннего использования. Содержит конфиденциальную информацию:. Любая информация, не одобренная для общего обращения за пределами организации.. Системный администратор Все пользователи. Уровень 5. Общедоступная. Открыть канал: Информация низкой конфиденциальности, такая как общая информация о больнице, информация о здоровье, заболеваниях, часто задаваемые вопросы, годовые отчёты и доступные услуги. Общественность. . . Безопасный открытый канал: Любой пользователь, например, исследователь, который хочет получить доступ или получить контактную информацию к любой анонимной конфиденциальной информации.. . Таблица 1. – Пять уровней коммуникаций в ММК. Уровень 2: для обмена информацией между пользователями, обменивающимися высококонфиденциальной информацией, для которой недопустимо коллективное пользование или общедоступность. Сюда входит информация, поступающая от мобильных устройств в организацию. Безопасность на этом уровне должна быть очень высокой и соответствовать устройствам с ограниченными ресурсами.. Уровень 3: для коммуникации информации между пользователями, обменивающимися частной информацией, необходимой для операционных процедур в больнице. Безопасность на этом уровне средняя.. Уровень 4: для обмена информацией между пользователями, которые обмениваются информацией только для внутреннего использования, которая связана с общей информацией о системе организации и не связанной с медицинской информацией. Безопасность на этом уровне низкая.. Уровень 5: для обмена информацией между пользователями, обменивающимися общедоступной информацией. Этот уровень разделён на два уровня безопасности, называемый безопасным открытым каналом, и без обеспечения безопасности, называемый публичным открытым каналом. Безопасность на этом уровне минимальна.. На данном этапе были предложена классификация коммуникаций и определено, какие типы конфиденциальной информации передаются на каждом уровне. Также было определено, до какого уровня безопасность должна быть применена. Далее рассмотрим предлагаемые механизмы защиты на каждом уровне с разными уровнями безопасности, использующие протоколы криптографии.. Требования безопасности для защищенной среды коммуникаций e-health.. Требования безопасности выводятся из потребностей организации и отличаются от одной организации к другой. Согласно Bleumer [9], требования к системам e-health включают аутентификацию для входа в систему, конфиденциальность с целью предотвращения раскрытия информации и анонимности (например, для получения анонимной консультации от экспертной системы). Rodriguez и др. [10] добавили такие требования как целостность при хранении данных, контроль доступа к защищенной медицинской информации, отказоустойчивость всех информационных потоков, обнаружение атак, а также аудит безопасности. Blobel и Roger-France [11] создали общую модель безопасности, основанную на коммуникационных аспектах приложения. Элементами, необходимыми для обеспечения связи, были идентификация, аутентификация, контроль доступа, целостность, конфиденциальность и доступность.. Хотя разные организации имеют разные требования безопасности в соответствии с их потребностями, основные требования безопасности должны быть сосредоточены на рассмотрении аспектов конфиденциальности, целостности и доступности [1]. Данное исследование ориентировано на защиту обмена сообщениями между двумя точками, находящимися между отправителем и получателем в разных средах обмена данными. Оба пользователя хотели бы убедиться, что отправленное или полученное сообщение защищено от несанкционированного доступа (конфиденциальность), не изменено (целостность), и оригинальность сообщения гарантирована (отказоустойчивость).. Отправитель также хочет удостовериться, что он может проверить, что сообщение от него (отказоустойчивость). Получатель хотел бы убедиться, что он может получить доступ к сообщению всякий раз, когда ему необходимо (доступность). Эти требования часто решаются с использованием криптографии [12-16]. Криптографические протоколы, которые шифруют, дешифруют, осуществляют хеш-функции, цифровую подпись и цифровые сертификаты, должны удовлетворять следующим требованиям безопасности.. 1. Конфиденциальность часто ассоциируется с шифрованием / расшифровкой открытого текста. Шифрование преобразует открытый текст в зашифрованный текст (и, наоборот, для расшифровки), используя общий симметричный ключ, таким образом, чтобы третьему лицу не удалось восстановить фактический текст из открытого текста. Гарантируя, что только предполагаемый получатель может восстановить открытый текст, доступность также включена. 2. Для того, чтобы отправитель удостоверился, что открытый текст не изменен, хэш-сообщение может быть вычислено из открытого текста и внедрено в сообщение перед отправкой его получателю. Получатель может проверить хеш-сообщение, повторно вычисляя новое сообщение хэша из открытого текста.. 3. Отправитель может представить доказательство того, что он отправляет сообщение с использованием цифровой подписи, путём шифрования частей сообщения своим личным ключом, чтобы получатель мог проверить его, используя открытый ключ отправителя.. 4. Открытый ключ получателя можно систематически обрабатывать с помощью цифровых сертификатов, которые связывают пользователя с его открытым ключом.. Исходя из этих требований, разрабатывается предлагаемая модель безопасной коммуникации для каждого уровня в ММК, которая может обеспечить гибкие функции защиты.. ММК: Предлагаемые механизмы защиты.. Как рассматривалось в п 3.1, более чувствительные данные имеют большую степень потери или потенциального ущерба по сравнению с менее чувствительными данными. Общепринятой практикой является медицинский персонал, который сохраняет конфиденциальную информацию пациента во время её передачи, что указано в нескольких стандартах, таких как, IPPA (http://www.hhs.gov/ocr/hipaa/) и APA (http://www.privacy.gov.au/). Однако в этих стандартах не указывается, каким образом следует внедрять механизм безопасности для защиты информации.. Предлагаемые механизмы защиты в ММК основаны на требованиях безопасности, описанных выше, в которых используются криптографические протоколы. ММК принимает во внимание обеспечение гибкой защиты безопасности в целях удовлетворения потребностей в безопасности e-health. ММК предоставляет три типа механизмов безопасности, которые представляют собой защиту данных, безопасность канала, а также защиту данных и каналов. Безопасность данных использует криптографические протоколы, такие как симметричное шифрование / дешифрование, хеш-функция и цифровую подпись, тогда как безопасность канала использует протокол SSL. Каждый из механизмов безопасности ММК будет подробно рассмотрен.. Механизм 1: защита данных. Рассмотрим две точки коммуникаций (отправитель и получатель), изображенные на рисунке 1. Отправитель хочет отправить открытый текст получателю. Оба они нуждаются в криптографических протоколах для обеспечения (и восстановления) открытого текста.. . Узел отправителя. Узел получателя. . . . . . . . . . . . . Рисунок 1. - Защита данных между двумя точками. 3,Ниже описаны обозначения, используемые в процессах криптографии:. - публичные и частные ключи получателя (pubKr , privKr );. - открытые и закрытые ключи отправителя: (pubKs , privKs );. - симметричные ключи K;. - простой (незашифрованный) текст, Р , хеш незашифрованного текста, Н (Р );. - цифровая подпись, S .. В предлагаемом подходе используется симметричный ключ шифрования, хэш-функции и цифровая подпись, обеспечивающие безопасность данных. Ниже описывается процесс шаг за шагом со стороны отправителя и стороны получателя.. . А. Протокол криптографии со стороны отправителя. (а). Симметричное шифрование : шифрует открытый текст в зашифрованный текст с помощью ключа K . Процесс шифрования обеспечивает конфиденциальность открытого текста.. Шифр-текст = E (P)K .. (б). Хэш-функция : вычисляет хэш-значение из открытого текста, H(P) . Значение хэш-функции будет использоваться получателем для проверки целостности открытого текста и проверки того, не нарушен ли открытый текст. Получатель пересчитывает хеш-значение из открытого текста, полученного из зашифрованного текста, и сравнивает его с отправленным отправителем. Если они совпадают, тогда открытый текст является подлинным и проверяется целостность открытого текста.. (в). Обмен ключами : ключ K , должен быть зашифрован и отправлен получателю, так что K может быть использован для расшифровки сообщения на стороне получателя. Для того чтобы отправитель убедился, что только получатель может восстановить ключ, K будет зашифрован с открытым ключом получателя, pubKr . Чтобы избежать третьей стороны, пытающейся украсть и удалить H(P) , вычисленный ранее, он может быть зашифрован вместе с K с помощью pubKr , обозначая результат шифрования как шифр-ключ .. Шифр - ключ : E (K, H (P)) pubKr .. (г). Цифровая подпись : для того, чтобы отправитель мог доказать, что ключ шифрования является его признаком, он использует свой личный ключ (privKs) , чтобы произвести подпись S .. S = E ( шифр - ключ ) privKs .. (д). Отправить сообщение : После этого отправитель может отправить шифр-текст, шифр-ключи подпись S получателю. В предлагаемом подходе используется протокол HTTP для передачи сообщения по проводной сети, таким образом, что протокол SSL может быть использован для защиты канала. Для передачи сообщения по беспроводной сети используется глобальная система мобильной связи (GSM) сети или беспроводные ЛВС (WiFi).. Б. Протокол криптография на стороне получателя:. (а). Чтобы проверить, действительно ли ключ шифрованияполучен от отправителя, S проверяется на соответствие шифр-ключу.. (б). Если шифр-ключ действителен, то выполняется следующее:. - использовать privKr для расшифровки шифр-ключа;. D ( шифр-ключ) privKr = K , H ( P ) ;. - затем, используя K для расшифровки зашифрованного текста. D (шифр-текст) К = Р ;. - в заключении проверяется P путём вычисления нового H(P) от P , и сравнивается с указанным на стадии (а). Если доказано, надо сохранить P.. Механизм 2: защита канала. В безопасном канале отправитель и получатель обмениваются сертификатами, а затем конечный пользователь устанавливает канал SSL на стороне получателя и просто передаёт открытый текст. Сертификаты можно получить через администратора безопасности в организации, которой поручается создание идентификатора (ID) и пароля для учётных записей пользователей.. Механизм 3: защита данных и каналов. При использовании опции защиты данных и каналов отправитель отправляет всё: Шифр-текст, Шифр-ключ и Подпись S получателю по каналу SSL.. Размер ключа для шифрования с симметричным ключом.. Ключ K является важным компонентом процесса шифрования, поскольку он представляет уровень безопасности, который может предоставить алгоритм. Согласно Lenstra [17], симметричная система криптографии с n -битным ключом имеет уровень безопасности n , если она может переносить общую атаку (чтобы найти ключ, когда открытый текст и зашифрованный текст известны заранее), используя усилия меньше Исчерпывающий поиск или атака “грубой силы”. Выбор размера ключа зависит от уровня безопасности, необходимого для криптографической системы. Чем длиннее ключ, тем выше безопасность, которую он может обеспечить, потому что трудность поиска всех возможных ключей в исчерпывающем поиске прямо пропорциональна количеству используемых битов [18]. Это объясняет, почему более короткие размеры ключей могут обеспечить только низкую безопасность, так как поиск ключа с использованием исчерпывающего поиска займет меньше времени, по сравнению с более длинными ключами.. Модель ММК предоставляет разные размеры симметричных ключей для каждого слоя. Уровень 1, который защищает информацию “Совершенно секретно”, должен обеспечивать самую высокую доступную безопасность, и поэтому должен быть обеспечен самый надёжный ключ. Уровень 2, который защищает высоко конфиденциальную информацию, должен обеспечивать очень высокую безопасность, уровень 3, который защищает конфиденциальную информацию, должен обеспечивать высокую безопасность, а уровень 4, который защищает информацию только внутреннего использования, должен обеспечивать низкую безопасность.. В частности, политика правительства США предусматривает рекомендации по размерам симметричных ключей для защиты секретной информации, а именно – Совершенно секретно, Секретно и Конфиденциальная информация [19]. Для этой цели выбирается передовой стандарт шифрования (Advanced Encryption Standard) или алгоритм AES [20]. AES-192 bit или AES-256 bit выбираются для защиты информации “Совершенно секретно”, а AES-128 bit выбирается для защиты как секретной, так и конфиденциальной информации.. В отношении выбора размеров симметричных ключей для криптографической системы нет единого мнения. Процесс выбора часто основывается на количестве времени, которое потребуется злоумышленнику на атаку ключа и сколько ресурсов (издержек) потребуется, чтобы добиться успеха. В случае мобильных устройств учитывается энергопотребление. Существует ещё целый ряд критериев выбора. Обобщая результаты исследований различных авторов, в частности [17-19, 21, 22], в контексте данной работы значение размера симметричных ключей для каждого слоя в модели ММК предоставлялось в следующих диапазонах:. - 193-бит и более: подходит для уровня 1, для защиты информации “Совершенно секретно”, которая требует наивысшей защиты безопасности;. - 129-бит – 192-бит: подходит для уровня 2, для защиты высоко конфиденциальной информации, требующей очень высокой защиты;. - 112-бит – 128-бит: подходит для уровня 3, для защиты конфиденциальной информации, требующей высокой степени защиты среды. - 80-бит – 111-бит: подходит для уровня 4, для защиты информации только для внутреннего использования, для которой требуется низкая защита безопасности.. В таблице 2 описаны рекомендуемые размеры ключей в каждом слое в ММК. Для сравнения в таблице также включены рекомендации США [19].. . Политика США. Длина ключа (бит). ММК. Длина ключа (бит). Совершенно секретно. 192/256. Уровень 1 (Совершенно секретно). 193 и выше. Секретно. 128. Уровень 2 (Высококонфиденциально). Проводная связь: 129-192. Упрощённое устройство: 112-192. Конфиденциально. 128. Уровень 3 (Защищено). 112-128. . . Уровень 4 (Только для внутреннего использования). 80-111. Таблица 2. – Рекомендуемые размеры ключей для каждого уровне в ММК. В этой таблице показано, что размеры ключей уровня 1 и уровня 2 согласуются с размерами секретных ключей США (192-бит для уровня 2, 193-бит и более для уровня 1). Уровень 2 поддерживает безопасность мобильных устройств, поэтому длина ключа до 112-бит поддерживается низким энергопотреблением устройства. Для уровня 3 выбирается ключ от 112 до 128 бит, чтобы обеспечить среднюю безопасность, что также соответствует размерам секретных ключей США. Для уровня 4 ключ с размером от 80 бит до 111 бит выбран для обеспечения низкой безопасности. Предоставляя значения длины ключей в определённых диапазонах, можно предложить более широкий диапазон размеров ключей для каждого слоя.. Исходя из этого принимается решение в отношении механизма безопасности в модели ММК, который включает в себя защиту данных и каналов, как показано в таблице 3.. . Уровни. Механизмы защиты. Длины ключа для защищённых данных (бит). Уровень 1. (Совершенно секретно). Защита данных и канала. 193 и выше. Уровень 2. (Высококонфиденциально). Защита данных или канала. \* мобильные устройства используют только защиту данных. Проводная связь: 129-192. Беспроводная связь: 112-192. Уровень 3 (Защищено). Защита данных или канала. 112-128. Уровень 4. (Только для внутреннего использования). Защита данных или канала. 80-111. Уровень 5. (Общедоступный). -. ID и пароль (для защищённого открытого канала). Таблица 3. – Спецификации безопасности в модели ММК. Для защиты канала могут использоваться шифрсьюты (cipher suites) от любого имеющегося провайдера.. Для уровня 1 защита данных и каналов используется для обеспечения самого высокого механизма защиты. Длина ключа для шифрования данных составляет от 193 бит и выше. Уровень 2 использует только защиту данных или канала. Для обеспечения безопасности данных в проводной сети используются 129-бит – 192-битные ключи, а для беспроводной сети выбраны 112-бит – 192-бит ключей. Уровни 3 и 4 также предоставляют два варианта защиты данных или каналов, с длиной ключа от 112 до 128 бит и от 80 до 111 бит соответственно. Для уровня 5, который предназначен для публичного использования, следует использовать только ID и пароль для поддержки безопасного открытого канала, как показано в таблице 1.. Модель ММК: обоснования и преимущества. Модель ММК обеспечивает механизмы безопасности для защиты различных типов коммуникаций между различными пользователями в e-health в соответствии с их потребностями. Например, медсестра может общаться по связи, которая безопасна или менее безопасна в зависимости от ситуации. Медсестра может общаться через самый высокий уровень безопасности при коммуникации с врачами или пациентами. В качестве альтернативы, она может использовать средний уровень безопасности при общении с социальным работником или минимальный уровень безопасности при общении с системным администратором (см. таблицу 1).. Гибкость обеспечения безопасности может быть предоставлена организациям здравоохранения, используя различные комбинации размеров ключей для защиты данных и каналов. На каждом уровне могут быть обеспечены различные уровни безопасности в зависимости от чувствительности данных. Чрезвычайно секретная информация может быть защищена с использованием самых высоких механизмов безопасности, а конфиденциальная информация низкого уровня может быть обеспечена с помощью механизмов минимальной безопасности. Поэтому можно избежать любого избыточного уровня безопасности, применяемого в коммуникации, когда он не нужен. ММК удовлетворяет существующему технологическому разрыву и ограничениям, как показано в п. 3.1. Используя ММК, пользователи могут общаться с различными типами механизмов безопасности, адекватными их потребностям.. Для обеспечения безопасности уровней может быть выбран набор алгоритмов шифрования, которые являются надёжными экспертами. Выбор алгоритмов может быть сделан или определён Администратором безопасности в конкретной организации. В ММК существует безопасность данных и каналов, предоставляемая пользователям таким образом, что пользователь может выбрать наиболее подходящие процессы безопасности с точки зрения стоимости и эффективности. Например, организация может выбрать для коммуникаций канал SSL, который обходится дешевле, чем шифрование данных [23], однако с компромиссом негибкой конфигурации безопасности, когда пользователю необходимо перейти на более сильный или более слабый уровень безопасности. В качестве альтернативы организация может выбрать применение только защиты данных с использованием ключей шифрования подходящих размеров, как показано в таблице 3. В то же время, когда особенно важна избыточная безопасность для чрезвычайно важной связи, организация может выбрать защиту данных и каналов.. Кроме того, коммуникации с устройствами с низкой вычислительной мощностью, например, карманными компьютерами и смартфонами, обеспечивается соответствующей защитой данных с размерами ключей, доступными из 112-битного ключа. Организация может экономить ресурсы, такие как мощность обработки ЦП для лёгких устройств, используя соответствующие длины ключей, чтобы повысить эффективность коммуникаций.. Однако всегда существует компромисс между надёжной безопасностью и производительностью. Чем длиннее длина ключа, тем медленнее производительность процессов безопасности. Более длинная длина ключа обеспечивает лучшую защиту, так как атакующим требуется больше усилий, чтобы найти ключ. Поэтому, если важна безопасность, можно выбрать более сильные алгоритмы с низкой производительностью. В противном случае можно выбрать более короткую длину ключа с высокой производительностью в соответствии с потребностями.. Таким образом, мы пришли к модели ММК как решение проблемы коммуникации в e-health и других крупных организациях с распределённой сетью компьютерных коммуникаций..