ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

А.БАЙТҰРСЫНОВ АТЫНДАҒЫ ҚОСТАНАЙ ӨҢІРЛІК УНИВЕРСИТЕТІ

СҰЛТАНҒАЗИН ОҚУЛАРЫ

«ҚАЗІРГІ БІЛІМ БЕРУДІ ДАМЫТУДЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ»
ХАЛЫҚАРАЛЫҚ
ҒЫЛЫМИ-ПРАКТИКАЛЫҚ
КОНФЕРЕНЦИЯ

МАТЕРИАЛДАРЫ

СУЛТАНГАЗИНСКИЕ ЧТЕНИЯ

МАТЕРИАЛЫ

МЕЖДУНАРОДНОЙ
НАУЧНО-ПРАКТИЧЕСКОЙ
КОНФЕРЕНЦИИ
«АКТУАЛЬНЫЕ ВОПРОСЫ
РАЗВИТИЯ СОВРЕМЕННОГО
ОБРАЗОВАНИЯ»

Қостанай, 2023

УДК 378 (094)
ББК 74.58
Қ 22

Қ 22

«Қазіргі білім беруді дамытудың өзекті мәселелері»: «СҰЛТАНҒАЗИН ОҚУЛАРЫ-2023» Халықаралық ғылыми-тәжірибелік конференцияның материалдары, 2023 жылдың 15 наурызы. Қостанай: А.Байтұрсынов атындағы Қостанай өңірлік университеті, 2023. – 427 б.
«Актуальные вопросы развития современного образования»: Материалы международной научно-практической конференции «СУЛТАНГАЗИНСКИЕ ЧТЕНИЯ-2023», 15 марта 2023 года. Костанай: Костанайский региональный университет имени А.Байтурсынова, 2023. – 427 с.

ISBN 978-601-356-257-5

«Сұлтанғазин оқулары-2023» халықаралық ғылыми-тәжірибелік конференциясының «Заманауи білім беруді дамытудың өзекті мәселелері» жинағында жаратылыстану-ғылыми білім берудің мәселелері мен болашағына арналған ғылыми мақалалар жинақталған, жалпы және кәсіптік білім берудің психологиялық-педагогикалық аспектілері қарастырылған, педагогикалық білім берудің ақпараттандыру және дамытудың қазіргі тенденциялары мен технологиялары мәселелері қозғалады.

Осы жинақтың материалдары ғалымдар мен жоғары оқу орындарының оқытушыларына, магистранттар мен студенттерге пайдалы болуы мүмкін.

В сборнике Международной научно-практической конференции «Султангазинские чтения-2023» «Актуальные вопросы развития современного образования»: представлены научные статьи по проблемам и перспективам естественно-научного образования, рассматриваются психолого-педагогические аспекты общего и профессионального образования, затронуты вопросы информатизации и современных тенденций и технологий развития педагогического образования.

Материалы данного сборника могут быть интересны ученым, преподавателям высших учебных заведений, магистрантам и студентам.

ISBN 978-601-356-257-5

УДК 378 (094)
ББК 74.58

- мультимедийное сопровождение объяснения нового материала (презентации, учебные видеоролики);
- использование виртуальных лаборатории;
- обработка учащимися статистических данных (построение таблиц, графиков).

Проанализировав результаты своей работы за период с 2013-2022гг., могу отметить изменения, повышающие самооценку: повышение качества преподавания предметов, повышение успеваемости и качества знаний учащихся, разработка и проведение уроков с использованием компьютерной технологии, освоение компьютерных технологий, владение текстовыми редакторами, создание электронных презентаций.

Согласившись с высказываниями Э. Фромма о том, что преступники – это затормозившиеся в своём развитии дети, в основном те, кому не посчастливилось встретить в своей жизни мудрого наставника, - педагога, и именно от этой посылки стремлюсь строить свою работу с учащимися - осуждёнными.

Список литературы:

1. Крючкова О. Г. Использование информационных технологий в обучении людей со специальными образовательными потребностями. Обзор терминологии и типов программного обеспечения. Издательский дом «Первое сентября», 2003 – 2009.
2. Кукушкина О. И. Применение информационных технологий в специальном образовании // Тематическое приложение к журналу “Вестник образования”. – 2003. – № 3. – С. 67-76.
3. Полат Е.С. Новые педагогические и информационные технологии в системе образования. – М.: Академия, 2007.
4. Ефименко, А.А., Румбешта, Е.А. Особенности обучения физике учащихся вечерней школы / А.А. Ефименко // Вестник ТГПУ. Выпуск 10 (88). Серия: Методика обучения. – Томск: ТГПУ, 2009. – С. 129 – 133.

УДК 004.056.55

ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ

Әбубәкіров Асхат Мүсілімұлы, бакалавр технических наук, Евразийский национальный университет имени Л. Н. Гумилёва, г.Астана, Казахстан, E-mail: askhat.aks@gmail.com

Аңдатпа

Бұл зерттеу ақпараттық қауіпсіздік мәселесін және осы мәселені шешудің маңызды әдістерін қарастырады. Ақпаратты қорғаудың негізгі механизмдері сипатталған. Қолданыстағы ұялы байланыс стандарттарының тиімділігіне талдау жасалынды.

Кілт сөздер: Ақпараттық қауіпсіздік; Шифрлау; ұялы байланыс жүйелері; алгоритм; GSM.

Аннотация

Данное исследование рассматривает проблему информационной безопасности и наиболее значимые способы решения данного вопроса. Описаны основные механизмы защиты информации. Проведен анализ эффективности существующих стандартов сотовой связи.

Ключевые слова: Информационная безопасность; Шифрование; Системы мобильной связи; алгоритм; GSM.

Abstract

This research examines the problem of information security and the most significant ways to solve this issue. The main mechanisms of information protection are described. The analysis of the effectiveness of existing cellular communication standards is carried out.

Keywords: Information security; Encryption; Mobile communication systems; algorithm; GSM.

Прежде коммуникация между абонентами, осуществлялась только примитивными способами и не отличалась качеством и скоростью передачи информации. Существующие, в настоящее время, технологии, позволяют поддерживать качественную связь, не только между неподвижными, но и между передвигающимися пользователями в режиме реального времени, а обеспечивают ее системы мобильной связи**.** На данный момент мобильные системы связи стали неотъемлемой частью нашего общества. Но у мобильной связи есть один существенный недостаток: передача данных происходит в радиоэфире, где эта информация может быть перехвачена. В связи с этим встает вопрос устранения угрозы информационной безопасности. Под угрозой информационной безопасности подразумевается действие, которое может привезти к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, передаваемую и обрабатываемую информацию.

Современные мобильные устройства перерабатывают все больше и больше цифровых данных, в следствие чего в сети мобильной связи попадает большое количество банковской, персональной и просто конфиденциальной информации. Защита информации в системах мобильной связи стала жесткой необходимостью. [1]

Сложность обеспечения информационной безопасности в системах мобильной связи, обуславливается разнообразием видов ее физического представления в этих системах, что предопределяет наличие различных возможных каналов перехвата информации. Утечка информации, циркулирующей по каналам связи между объектами систем мобильной связи, возможна как при передаче ее по линиям, использующим излучающие средства радиосвязи, так и при передаче по проводным линиям. Это создает необходимость построения многоплановой в физическом и функциональном отношении системы защиты.

Обеспечение информационной безопасности первых аналоговых мобильных сетей было на очень низком уровне. По мере перехода от аналоговых к цифровым системам GSM и DAMPS механизм обеспечения безопасности информации совершенствовался, появились новые методы защиты, основные из которых и описаны в этой статье.

В первую очередь рассмотрим использование широко известного метода аутентификации – PIN-кода. PIN-код один из наиболее простых методов, с низкой степенью защиты (чтобы получить доступ - достаточно услышать персональный код всего лишь один раз). GSM использует PIN-код в сочетании с SIM-картой (Subscriber Identify Module): PIN-код проверяется SIM-картой без передачи в эфир. Также GSM использует более сложный способ, состоящий в использовании случайного числа, на которое может ответить только соответствующее абонентское оборудование (SIM-карта). Смысл этого метода в том, что существует огромное множество подобных чисел и поэтому вероятность того, что одно и то же число будет использовано дважды, крайне низкая. Результатом вычисления является SRES (Signed RESult – подписанный результат), в форме содержащей секретный параметр Ki. Секретность Ki - основа любого механизма безопасности, – свой Ki не знает даже сам абонент. SIM полностью защищает Ki от чтения. Технология чиповых карт, внедренная за некоторое время до того, как GSM приступила к производству этих миниатюрных электронных сейфов, идеально подходила для этой цели. Единственный доступ к Ki происходит во время первоначальной фазы персонализации SIM. Мобильные станций возлагают на SIM большинство функций безопасности. SIM хранит Ki, вычисляет зависимые от оператора алгоритмы и хранит “бездействующий” ключ Кс. [2]

Существование SIM как физической единицы отдельно от мобильного оборудования является одним из элементов, допускающих гибкость в выборе алгоритмов. Производителям мобильного оборудования нет необходимости знать спецификации этих алгоритмов, предназначенных для операторов. С другой стороны, производители SIM обязаны внедрять потенциально разные алгоритмы для каждого из своих заказчиков-операторов, но проблемы конкуренции, массового производства и распределения являются принципиально иными в сравнении с проблемами рынка мобильного оборудования. Защита систем мобильной связи стандарта GSM обеспечивается тремя секретными алгоритмами: A3, A5 и A8. [3]

Алгоритм A3 применяется при аутентификации пользователя и защищает его от клонирования; A3 является однонаправленной функцией. Это значит, что вычисление SRES при известном Ki должно быть простым, а обратное действие – вычисление Ki при известном SRES – максимально затруднено. Именно это в конечном итоге и позволяет добиться необходимого уровня безопасности, Значение, вычисляемое по алгоритму A3, должно иметь длину 32 бита. Параметр Ki может иметь любую длину и формат.

Криптографические методы защиты информации позволяют при помощи относительно простых средств добиться высокого уровня безопасности. В GSM применяются единые методы защиты данных, будь то пользовательская информация: передача сигналов, связанных с пользователем (к примеру, сообщений, содержащих номера вызываемых телефонов), или даже передача системных сигналов (к примеру, сообщений, которые содержат результаты радиоизмерений для подготовки к передаче). Необходимо различать только два случая: либо связь является защищенной (в этом случае всю информацию можно отправлять в зашифрованном виде), либо связь оказывается незащищенной (в таком случае вся информация отправляется в виде незашифрованной цифровой последовательности). И шифрование и дешифрование выполняется с использованием операции “исключающее или” к 114 “кодированным” битам радиопакета и 114-битовой последовательности шифрования, которую генерирует специальный алгоритм шифрования голосового трафика - A5. Чтобы узнать последовательность шифрования для каждого пакета, алгоритм A5 производит вычисление, используя два ввода: номер кадра и ключ Кс, который известен лишь мобильной станции и сети. И в том и другом пакете по две последовательности, но используются они по разному: в первом случае одна последовательность применяется для шифрования в мобильной станции, а другая для дешифрования на базовой станции (BTS), во втором же случае последовательности используются для шифрования в базовой станции (BTS) и дешифрования в мобильной станции.

Обычно Алгоритм А5 устанавливается на международном уровне, так как для обеспечения MS-роуминга он должен быть реализован в рамках каждой базовой станции (как и в любом мобильном оборудовании). В настоящее время во всех странах установлен один-единственный алгоритм А5. Алгоритм вычисляет последовательность шифрования из 114 бит отдельно для каждого пакета, с учетом номера кадра и шифровального ключа Кс. Номер кадра, как правило, изменяется от пакета к пакету для всех типов радиоканалов, а ключ Кс, в свою очередь, при каждом сообщении. Поскольку ключ Кс так часто меняется, он не требует столь сильных средств защиты, как например, ключ Ki. Ключ Кс свободно читается в SIM-карте.

На данный момент базовые станции поддерживают три основных варианта алгоритма А5:

-А5/1 – Используются сложные криптографические методы защиты данных. Алгоритм применяется в большинстве стран;

- А5/2 – Используются упрощенные криптографические методы защиты данных, применяется в странах, в которых использование сложной криптографии нежелательно;

- А5/0 – Криптографические методы защиты данных не используются.

В Казахстане применяется алгоритм А5/1, являющийся собственностью компаний GSM MoU. Из соображений безопасности описание алгоритма не придается публичной огласке. Но все же внешние спецификации А5/1 известны: длина принимающего параметра - 22 бита, параметр, создающий 114-битные последовательности длиной в 64 бита. Также как и в случае с алгоритмом аутентификации А3, степень защиты, предлагаемая алгоритмом А5, определяется сложностью обратного вычисления - определения Кс при двух известных 114-битовых последовательностях шифрования и номера кадра. Ключ Кс вычисляется во время процесса аутентификации и согласовывается между мобильной станцией и сетью до начала шифрования. Затем ключ вводится в энергонезависимую память SIM-карты и хранится там даже после того, как сеанс связи завершен. Также Кс сохраняется в сети и ключа, который берет результат работы А3 и превращает его в сеансовый ключ А5. Алгоритм используется для шифрования.

А8 – алгоритм генерации аутентификации А8 используется для вычисления Кс из случайного числа RAND и ключа Ki. Фактически алгоритмы А3 и А8 можно было бы реализовать в форме единого алгоритма, выходные данные которого состоят из 96 бит (64 бита для образования ключа шифрования Кс, а 32 бита для образования подписанного результата SRES). Иногда длина значимой части ключа Кс может быть меньше 64 бит. В таком случае значимые биты дополняются нулями.Каждый раз, когда какая-либо мобильная станция проходит аутентификацию, она также использует алгоритм А8, вычисляя с его помощью Кс, с теми же самыми вводными данными RAND и Ki, что используются для вычисления SRES посредством алгоритма А3.

Шифрование весьма эффективно для защиты конфиденциальности, но не подходит для защиты отдельно взятого обмена информацией по радиоканалу. Шифрование с помощью Кс применимо только в тех случаях, когда сети известна личность абонента. Шифрование не применяется для общих каналов, принимаемых одновременно всеми мобильными станциями как в данной сотовой ячейке, так и в соседних. Если шифрование применялось бы с использованием ключа, который известен всем мобильным станциям это лишило бы его смысла как механизма безопасности. Когда мобильная станция перемещается на какой-либо специальный канал, шифрование сообщения невозможно, так-как какое-то время выполняется “начальная загрузка”, в течение которой сеть не может установить личность абонента. Поэтому при обмене сигнальными сообщениями, несущими сведения о личности неопределенного абонента, шифрование не выполняется и на данной стадии возможна утечка информации. В тех случаях, когда это возможно, конфиденциальность также обеспечивается путем использования временного идентификатора мобильного абонента - TMSI, используемого вместо международного идентификатора мобильного абонента IMSI. Так же, как и Ключ Кс, временной идентификатор заранее согласовывается с мобильной станцией и сетью.

Цифровые стандарты мобильной связи второго поколения обеспечивают очень высокий уровень информационной безопасности. Но прогресс не стоит на месте, мощность вычислительных средств возрастает с каждым днем, поэтому для повышения качества обеспечения информационной безопасности разрабатываются и внедряются все новые стандарты. Недавно на свет появился алгоритм шифрования информации, получивший индекс А5/3. Внедрение этого алгоритма поднимет защищенность мобильной связи стандарта GSM на ступень выше. Новый стандарт был разработан с учетом всех изменений стандарта GSM произошедших за последние годы. Он поддерживает шифрование голоса и данных в сетях GPRS и EDGE (стандарт сотовой связи III поколения). Предполагается, что стандарт А5/3 будет немедленно внедрен в эксплуатацию. Принятие нового стандарта А5/3 еще более остро поставило вопрос о текущей защищенности систем мобильной связи. Официально в мире нет оборудования, которое позволяет в реальном режиме времени производить перехвата трафика GSM-сетей. Однако существующие сведения заставляют сомневаться в этой информации. В англоязычном сегменте интернета ряд компаний предлагает оборудование для перехвата и раскодировки GSM-переговоров. Реклама данных технологий ведется

достаточно открыто, однако доступ на сайты этих компаний ограничен. В казахстанском же сегменте на электронных платформах достаточно часто встречаются записи объявлений о продаже соответствующего оборудования, причем по довольно низкой цене. Все это говорит о том, что защищенность GSM-сетей несколько преувеличена. [4]

Конечно, представленный в данной статье материал не может охватить абсолютную полноту раскрытия проблемы информационной безопасности в мобильных системах связи, но в нём представлены наиболее значимые аспекты и способы решения данного вопроса.

Список литературы:

1. А.В. Заряев, В.А. Минаев, С.В. Скрыль, В.Ю. Карпычев. Защита информации в мобильных системах связи. Воронеж: Воронежский ин-т МВД России, 2004. 138 с.)
2. А.А. Чекалин, А.В. Заряев, С.В. Скрыль, В.А. Вохминцев. Защита информации в системах мобильной связи. М.: Горячая линия - Телеком, 2005. 171 с.
3. Сетевой ресурс https://detsys.ru/article/bezopasnost_gsm
4. Сетевой ресурс https://www.bibliofond.ru/view.aspx?id=651120

УДК 004.056.2

АҚПАРАТТЫҚ ҚАУІПСІЗДІК МАҢЫЗДЫЛЫҒЫ ЖӘНЕ АЛДЫН АЛУ ШАРАЛАРЫНЫҢ ҚАЖЕТТІЛІГІ

Әлім Әлішер, 2 курс магистранты, Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан, E-mail: alim.alisher@gmail.com

Аңдатпа

Өзектілігі: Ақпараттық қауіпсіздік – бұл ақпаратты, сондай-ақ оның маңызды элементтерін, соның ішінде осы ақпаратты пайдалануға, сақтауға және беруге арналған жүйелер мен жабдықтарды сақтау және қорғау.

Мақсаты: Ақпараттық қауіпсіздікті қамтамасыз ету-ақпараттық деректерді және қолдау инфрақұрылымын кездейсоқ немесе қасақана араласудан қорғау, бұл деректердің жоғалуына немесе олардың рұқсатсыз өзгеруіне әкелуі мүмкін.

Түйінді сөздер: Ақпараттық қауіпсіздік, қолжетімділік, құпиялылық, тұтастық, ақпараттық қауіпсіздік саясаты.

Аннотация

Актуальность: Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации.

Цель: Обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения.

Ключевые слова: Информационная безопасность, доступность, конфиденциальность, целостность, политика информационной безопасности.

Abstract

Relevance: Information security is the preservation and protection of information, as well as its most important elements, including systems and equipment designed to use, save and transmit this information.

Goal:Information security – to protect information data and supporting infrastructure from accidental or intentional interference, which may cause data loss or unauthorized modification.

Keywords: Information security, accessibility, confidentiality, integrity, information security policy.

Ақпараттық қауіпсіздік(ағылш. *Ақпараттық қауіпсіздік*, сонымен қатар-ағылш. InfoSec) - ақпаратқа рұқсатсыз қол жеткізуді, пайдалануды, ашуды, бұрмалауды, Өзгертуді, зерттеуді, жазуды немесе жоюды болдырмау тәжірибесі. Бұл әмбебап ұғым деректер қабылдай алатын формаға қарамастан қолданылады (электронды немесе, мысалы, физикалық). Ақпараттық қауіпсіздіктің негізгі міндеті-қолданудың орындылығын ескере отырып және ұйымның жұмысына ешқандай зиян келтірместен деректердің құпиялылығын, тұтастығын және қол жетімділігін теңдестірілген қорғау. Бұған, негізінен, негізгі құралдар мен материалдық емес активтерді, қауіп көздерін, осалдықтарды, ықтимал әсер ету дәрежесін және тәуекелдерді басқару мүмкіндіктерін анықтауға мүмкіндік беретін