Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

*На правах рукописи*

УДК 004.056.-026.26

Моисеенко
Александр Игоревич

# МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОБИЛЬНОГО ДОСТУПА

**АВТОРЕФЕРАТ**
диссертации на соискание степени
магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии
проектирования электронных систем

Минск 2017

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **МАТЮШКОВ Владимир Егорович,**
доктор технических наук, профессор, главный инженер ОАО «КБТЭМ-ОМО»

Рецензент: **ТОНКОВИЧ Ирина Николаевна,**
кандидат химических наук, доцент, заведующая кафедрой информационных технологий учреждения образования «Минский инновационный университет»

Защита диссертации состоится «22» июня 2017 г. года в $10^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

# ВВЕДЕНИЕ

Под угрозой информационной безопасности принято понимать потенциально возможные действия, явления или процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию.

Среди проблем, связанных с обеспечением информационной безопасности мобильного доступа, значительное внимание продолжает уделяться проблеме обеспечения конфиденциальности данных. Считается, что при ее решении автоматически решается проблема целостности и доступности информации. Однако если среди внешних угроз выделить угрозу деструктивных воздействий на систему разведки и наблюдения, то можно констатировать, что система обеспечения информационной безопасности, выполняя все возложенные на нее функции, будет защищать и искаженную информацию. Это связано с тем, что защита от угрозы нарушения целостности информации на уровне содержания сведений в обычной практике, как правило, не рассматривается.

При изучении процессов информационной безопасности необходимо выделить пять наиболее важных противоречий.

Первое противоречие возникает в связи с необходимостью выполнения требований к качеству информации и недостаточным учетом ряда важных свойств информации в теории информационной безопасности.

Второе противоречие определяется возрастанием роли человеческого фактора и недостаточным набором методов и средств его оценки и защиты от искажения информации обслуживающим персоналом.

Третье противоречие возникает между широким диапазоном потенциальных возможностей практического использования методов и средств информационной безопасности, с одной стороны, и практикой оценки информационного противоборства, с другой стороны. Использующиеся обобщенные оценки эффективности средств и методов информационной безопасности не изменяются весь период эксплуатации, что не в полной мере отвечает содержанию процесса информационного противоборства. Решение задачи оценки безопасности и информационной устойчивости следует искать в использовании такого критерия оценки показателей, который непосредственно связан с качеством принимаемого решения.

Четвертое противоречие связано с тем, что в настоящее время ведутся интенсивные работы по созданию интеллектуальных помех за рубежом. Системный анализ показывает, что требуется новое комплексное решение, направленное на защиту семантической составляющей информации. Решение задач информационной безопасности предлагается осуществлять на основе адекватного описания выявленных законов и закономерностей исследуемых процессов информационного противоборства.

При формировании комплекса типовых механизмов создается необходимое разнообразие средств и методов обеспечения информационной безопасности и позволяет разрешить пятое противоречие – создать механизм оптимального управления процессом информационной безопасности в дина-

мике протекания всех этапов жизненного цикла.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

### Актуальность темы исследования

В настоящее время информация играет более многогранную и значимую роль в жизни современного общества. Одной из наиболее динамически развивающихся базовых инфраструктурных отраслей, обладающих долгосрочным потенциалом роста, является отрасль связи и информатизации. Важное место среди современных информационных телекоммуникационных систем занимают сотовые системы связи, предназначенные для обеспечения мобильной связью огромного количества потребителей на значительных территориях, позволяющие осуществлять передачу данных, а так же речевой информации.

В связи с вышесказанным, актуальность темы методы обеспечения информационной безопасности мобильного доступа довольно высока.

### Степень разработанности проблемы

Теоретической базой при изучении проблемы обеспечения информационной безопасности стали работы российских и белорусских ученых: В. А. Садовничий, В. А. Носов, М.С. Абламейко, С.В. Лазовский, М.С. Соколов, В.М. Арсентьев, В. В. Ященко, В. А. Котельников, а так же зарубежных авторов: К. Шенон, Р. Лидл, А. Шваба, Г. Пильц и др.

Одним из недостатков методов обеспечения информационной безопасности, является их устаревания с каждым днем.

Предложенные методы исследования направлены на усовершенствования существующих методов и способов защиты информации мобильного доступа.

### Цель и задачи исследования

Целью диссертации является оптимизация методов обеспечения информационной безопасности мобильного доступа.

Поставленная цель работы определяет следующие основные задачи:

1. Анализ методов и средств защиты и передачи информации.
2. Оптимизация существующих методов и средств защиты и передачи информации.
3. Реализация метода передачи информации и методов обеспечения информационной безопасности.

**Область исследования**

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 81 01 «Компьютерные технологии проектирования электронных систем».

**Теоретическая и методологическая основа исследования**

В основу диссертации легли работы белорусских и зарубежных ученых в области информационной безопасности, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

*Информационная база* исследования сформирована на основе литературы, открытой информации, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

**Научная новизна**

*Научная новизна* и значимость полученных результатов работы заключается в разработке методов обеспечения информационной безопасности мобильного доступа.

*Теоретическая значимость* работы заключается в детальном анализе методов информационной безопасности.

*Практическая значимость* диссертации состоит в расчёте параметров передачи информации в сетях *LTE*, которые позволят оптимизировать методы передачи и защиты информации.

**Основные положения, выносимые на защиту**

1. Классификация методов и средств защиты и передачи информации, на примере передачи данных через сеть *LTE* с использованием технических средств, таких как: ноутбук, планшет, смартфон.
2. Оптимизация программных методов защиты информации на основе нового программного обеспечения, аппаратных средств криптографической защиты и метода передачи информации в сетях *LTE*.
3. Реализация метода передачи информации в сетях *LTE* и методов обеспечения информационной безопасности в повседневной жизни.

**Апробация диссертации и информация об использовании ее результатов**

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 53-ой научно-техническая конференции аспирантов, магистрантов и студентов БГУИР (Минск, Беларусь, 2017 г.).

Так же на 21−ой Всероссийской научно-технической конференции студентов, молодых ученых и специалистов РГРТУ (Рязань, Российская федерация, 2016 г.).

### Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 4 печатных работах. В их числе 4 статьи в сборниках материалов научных конференций.

Общий объем публикаций по теме диссертационной работы составляет 0,52 авторских листа.

### Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

**В первой главе** приведен анализ методов и средств защиты информации, а так же анализ методов и средств передачи информации. **Во второй главе** представлена оптимизация программных методов защиты информации на основе нового программного обеспечения, аппаратных средств криптографической защиты и метода передачи информации в сетях *LTE*. **В третьей главе** представлена реализация метода передачи информации в сетях *LTE* и методов обеспечения информационной безопасности в повседневной жизни. **В приложении** представлены публикации автора и акт внедрения.

Общий объем диссертационной работы составляет 88 страницы. Из них 48 страниц основного текста, 11 иллюстраций на 9 страницах, 3 таблицы на 3 страницах, библиографический список из 32 наименований на 2 страницах, список собственных публикаций соискателя из 4 наименований на 1 странице, 3 приложений на 25 страницах.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы обеспечения безопасности информации мобильного доступа, указаны основные направления исследований, проводимых по данной тематике, а также описано обоснование актуальности темы.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

**В первой главе** приведен анализ современных методов и средств защиты информации.

Из анализа следует, что проблема обеспечения информационной безопасности мобильного доступа заключается в усовершенствовании методов и средств несанкционированного доступа к информации, похищения, уничтожения информации. Ее решение позволит улучшить процесс обеспечения информационной безопасности.

Проанализированы особенности используемых методов и средств передачи информации. Выявлено, что для корректного обмена данными между узлами локальной вычислительной сети используют определенные режимы передачи информации: симплексная, полудуплексная и дуплексная передача информации. Основным отличием данных режимов является варьирование параметров очередности передачи информации.

При проведении анализа существующих средств обеспечения информационной безопасности выявлено, что в большинстве случаев их можно разделить на следующие группы: технические (аппаратные); программные и технические средства; смешанные аппаратно программные; организационные средства защиты информации.

**Во второй главе** представлена оптимизация программных методов защиты информации на основе нового программного обеспечения.

Сущность предложенной методики состоит в том, что создание любой компьютерной системы невозможно без разработки и оптимизации алгоритмического обеспечения.

Надежную защиту информации может обеспечить только комплексный подход, подразумевающий одновременное использование аппаратных, программных и криптографических средств (ни одно из этих средств в отдельности не является достаточно надежным). Подобный подход предусматривает анализ и оптимизацию всей системы, а не отдельных ее частей, что позволяет обеспечить баланс характеристик, тогда как улучшение одних параметров нередко приводит к ухудшению других.

Организационные меры, принимаемые при комплексном подходе, являются самостоятельным инструментом и объединяют все используемые методы в единый целостный защитный механизм. Такой подход обеспечивает безопасность данных на всех этапах их обработки. При этом правильно организованная система не создает пользователям серьезных неудобств в процессе работы.

Комплексный подход включает детальный анализ внедряемой системы, оценку угроз безопасности, изучение средств, используемых при построении системы, и их возможностей, анализ соотношения внутренних и внешних угроз и оценку возможности внесения изменений в систему.

Таким образом, для обеспечения защиты информации необходимо предпринимать следующие меры:

– формирование политики безопасности и составление соответствующей документации;

– внедрение защитных технических средств.

При разработке нового программного обеспечения необходимо учесть следующие этапы обеспечения безопасности:

1. Тестирования ПО на основе разработки комплексов тестов, подразделяются на конкретные классы программ с возможностью функционального и статистического контроля в широком диапазоне изменения входных и выходных данных;

2. Проведения натурных испытаний программ при экстремальных нагрузках с имитацией воздействия активных дефектов;

3. Осуществления "фильтрации" программных комплексов с целью выявления возможных преднамеренных дефектов определенного назначения на базе создания моделей угроз и соответствующих сканирующих программных средств;

4. Разработки и экспериментальной отработки средств верификации программных изделий;

5. Проведения стендовых испытаний ПО для определения непреднамеренных программных ошибок проектирования и ошибок разработчика, приводящих к невыполнению целевых функций программ, а также выявление потенциально "узких" мест в программных средствах для разрушительного воздействия;

6. Отработки средств защиты от несанкционированного воздействия нарушителей на ПО;

7. Сертификации программных изделий автоматизированные системы управления по требованиям безопасности с выпуском сертификата соответствия этого изделия требованиям технического задания.

Так же в данной главе рассматривалась оптимизация аппаратных средств криптографической защиты.

В последнее время возрос интерес к современным аппаратным средствам криптографической защиты информации (АСКЗИ). Это обусловлено, прежде всего, простотой и оперативностью их внедрения. Для этого достаточно у абонентов на передающей и приемной сторонах иметь аппаратуру АСКЗИ и комплект ключевых документов, чтобы гарантировать конфиденциальность циркулирующей в автоматизированных системах управления (АСУ) информации.

Современные АСКЗИ строятся на модульном принципе, что дает возможность комплектовать структуру АСКЗИ по выбору заказчика.

При разработке современных АСКЗИ приходится учитывать большое количества факторов, влияющих на эффективность их развития, что усложняет нахождение аналитических оценок по выбору обобщенного критерия оптимальности их структуры.

Конечная цель проведения процесса оценки и нейтрализации рисков заключается в наиболее эффективном обеспечении безопасности информации в информационной системе и оказании необходимой помощи пользователям, ответственным за функционирование системы в целом.

При выполнении работ можно использовать модель построения системы защиты информации проиллюстрированной на рисунке 1, основанную на адаптации общих критериев и стандартов. Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности.

Из выше указанного следует, что проводя мероприятия по выявлению рисков в организации, а также дальнейшие процедуры по их снижению и ликвидации, уровень защиты информационных процессов и ресурсов повы-

шается в разы.


**Рисунок 1 – Модель построения системы защиты информации**

Ниже представлена оптимизация метода передачи информации в сетях *LTE*.

В настоящее время интегрированные телекоммуникационные сети, в которых сочетаются различные виды трафика и различные методы доступа являются достаточно эффективным решением для транспортных сетей мегаполиса, позволяя объединить различные виды и сети информационного обмена.

В них особенно рационально использование беспроводных сетей, обеспечивающих доступ мобильных абонентов к ресурсам сетей фиксированной связи.

Современные системы передачи информации (СПИ) представляют собой сложные комплексы, состоящие из различных функционально взаимосвязанных элементов. Эти системы характеризуются не только большим числом элементов, но и иерархичностью структуры, избыточностью, наличием между элементами прямых, обратных и перекрестных связей.

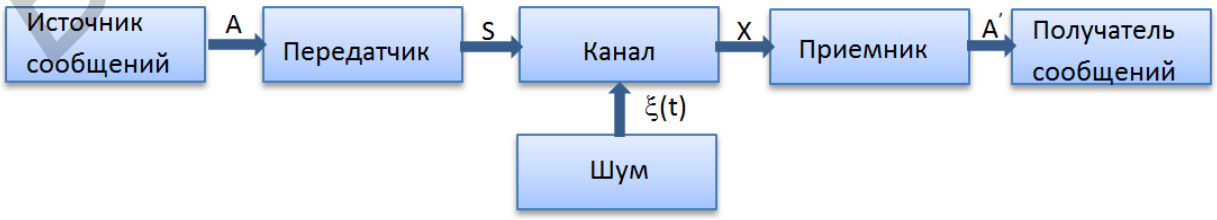


**Рисунок 2 – Обобщенная модель СПИ**

В общем виде решение задачи оптимизации СПИ может оказаться сложным и мало обозримым для принятия решения. Поэтому обычно прибегают к поэтапной процедуре оптимизации. Сначала производится оптимизация по одной группе параметров, а затем по другой. Так, для СПИ сначала осуществляется оптимизация (выбор) по способам передачи (модуляции, кодирования) и приема (обработки) сигналов, а затем оптимизация параметров выбранного варианта системы.

**В третьей главе** представлена реализация метода передачи информации в сетях *LTE*, произведен расчёт передачи информации в сетях *LTE*.

Обмен информацией производится по каналам передачи информации.

Каналы передачи информации могут использовать различные физические принципы. Так, при непосредственном общении людей информация передаётся с помощью звуковых волн, а при разговоре по телефону – с помощью электрических сигналов, которые распространяются по линиям связи.

Общая схема передачи информации включает в себя отправителя информации, канал передачи информации и получателя информации.

Основной характеристикой каналов передачи информации является их пропускная способность.

Пропускная способность канала равна количеству информации, которое может передаваться по нему в единицу времени.

Рассмотрим расчет скорости передачи данных в сети *LTE* основные параметры, которые на нее влияют. К таким параметрам относятся следующие :

– ширина канала (*bandwidth*);

– качество канала, то есть в каких радиоусловиях находится абонент;

– загрузка сети (то есть сколько активных пользователей в сети и сколько данных они передают).

Таблица 1 – Зависимость количества ресурсных блоков от ширины канала [29]

| Ширина канала, МГц | 1,4 | 3 | 5 | 10 | 15 | 20 |
|---|---|---|---|---|---|---|
| Количество ресурсных блоков | 6 | 15 | 25 | 50 | 75 | 100 |

Предполагаем, что в нашей сети находится только один абонент, ширина канала у нас 20 МГц и идеальные радио-условия (такие предположения позволяют получить максимальную скорость передачи данных в сети *LTE*), далее количество ресурсных блоков при нашей ширине канала 100.

*MCS Index* = 27 и *TBS* Index = 25

Используя эти числа, получаем TBS = 67500 бит. Скорость передачи:

$$V=67500\times1000=67.5 \text{ Мбит/с}.$$

Предположим, что также используется *MIMO* (*Miltiple input multiple*

*output* – многоканальный вход и многоканальный выход) 2×2. Отсюда получаем

$$V=67.5\times2=135 \text{ Мбит/с}.$$

Продемонстрирована реализация методов обеспечения информационной безопасности в повседневной жизни.

В контексте сферы безопасности под мобильным доступом можно подразумевать инфраструктуру, в которой для получения доступа к материальным или информационным ресурсам в качестве идентификатора используются мобильные устройства, например, мобильные телефоны, с беспроводным интерфейсом передачи данных *NFC* (*near field communication*, связь ближнего действия) и/или *Bluetooth Smart*.


**Рисунок 3 – Пример использование смартфона с NFC**

Используя беспроводную связь *NFC* (технология высокочастотной связи), возможен обмен данными между устройствами, находящимися на расстоянии около 15 сантиметров друг от друга

Безопасность, кроме собственной защиты мобильных идентификаторов, усиливается возможностями самих телефонов - блокировкой экрана и т.д

Рассмотрена применимость методов обеспечения информационной безопасности мобильного доступа.

Как уже отмечалось, в последнее время наметилась тенденция к созданию универсальных многозадачных продуктов. Однако любое универсальное ПО состоит из нескольких модулей-приложений, направленных на «закрытие» специфических проблем информационной безопасности. Одни решают вопросы борьбы со спамом и фишингом, другие ориентированы на мониторинг ИТ-инфраструктуры и поиск сетевых уязвимостей, третьи контролируют отправку факс-сообщений и утечку информации через внешние накопители, архивируют и шифруют документооборот и т.д. Обычно производители программных продуктов предоставляют возможность выбора и компиляции нескольких взаимосвязанных ИТ-решений в группы, исходя из текущих задач компании, что позволяет разумно распорядиться бюджетом.

# ЗАКЛЮЧЕНИЕ

## Основные научные результаты диссертации

1. Произведен анализ методов и средств защиты и передачи информации, на примере передачи данных через сеть *LTE* с использованием технических средств, таких как ноутбук, планшет, смартфон.

2. Произведена оптимизация программных методов и средств защиты информации на основе нового программного обеспечения, аппаратных средств криптографической защиты и метода передачи информации в сетях *LTE*.

3. Произведена реализация метода передачи информации в сетях LTE и методов обеспечения информационной безопасности в повседневной жизни.

## Рекомендации по практическому использованию результатов

Полученные результаты внедрены в учебный процесс на кафедре проектирования информационно−компьютерных систем учреждения образования “Белорусский государственный университет информатики и радиоэлектроники в учебный курс “Методы и средства защиты информации”.

# СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

*Статьи в сборниках научных трудов*

1. Анализ противоречий при обеспечении информационной безопасности мобильного доступа / А.И. Моисеенко, В.Е.Матюшков. // материалы 21−ой Всероссийской научно-технической конференции студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях», Рязань, Российская федерация, 16 -18 ноября 2016 г. / УО «РГРТУ». – Рязань, 2016. – С.123–125.

2. Подходы к качеству передачи данных при мобильном доступе / А.И. Моисеенко, В.Е.Матюшков. // материалы 21−ой Всероссийской научно-технической конференции студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях», Рязань, Российская федерация, 16 -18 ноября 2016 г. / УО «РГРТУ». – Рязань, 2016. – С.122–123.

3. Мобильный доступ / А.И. Моисеенко, В.Е.Матюшков, В.Ф. Алексеев. // материалы 53−ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно−компьютерных систем», Минск, Респ. Беларусь, 02–06 мая 2017 г. / УО «БГУИР». – Минск, 2017. – Принято в печать.

4. Информационная безопасность / А.И. Моисеенко, В.Е.Матюшков, В.Ф. Алексеев. // материалы 53−ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно−компьютерных систем», Минск, Респ. Беларусь, 02–06 мая 2017 г. / УО «БГУИР». – Минск, 2017. – Принято в печать.

## РЭЗЮМЭ

**Врабій Эдуард Міхайлавіч**

**Методыка забеспячэння функцыянальнай надзейнасці электронных модуляў на базе мікракантролераў пры ўздзеянні разрадаў статычнага электрычнасці**

***Ключавыя словы***: абарона інфармацыі, бяспека.

***Мэта працы:*** з'яўляецца аптымізацыя метадаў забеспячэння інфармацыйнай бяспекі мабільнага доступу.

***Атрыманыя вынікі і іх навізна:*** выкананы аналіз метадаў і сродкаў абароны і перадачы інфармацыі. Выяўлена, што ў цяперашні час пытанне па абароне інфармацыі найбольш актуальны; праведзена аптымізацыя існуючых метадаў і сродкаў абароны і перадачы інфармацыі; праведзена рэалізацыя метаду перадачы інфармацыі і метадаў забеспячэння інфармацыйнай бяспекі.

***Ступень выкарыстання:*** вынікі ўкаранёны ў навучальны працэс на кафедре праектавання інфармацыйна-камп'ютэрных сістэм ўстановы обра¬зования "Беларускі дзяржаўны універсітэт інфарматыкі і радиоэлек¬троники ў навучальны курс" Метады і сродкі абароны інфармацыі".

***Вобласць ужывання:*** інфармацыйныя тэхналогіі, IT - індустрыя..

**РЕЗЮМЕ**

**Моисеенко Александр Игоревич**

**Методы обеспечения информационной безопасности**

***Ключевые слова*:** защита информации, безопасность.

***Цель работы*:** является оптимизация методов обеспечения информационной безопасности мобильного доступа.

***Полученные результаты и их новизна*:** выполнен анализ методов и средств защиты и передачи информации. Выявлено, что в настоящее время вопрос по защите информации наиболее актуален; произведена оптимизация существующих методов и средств защиты и передачи информации; произведена реализация метода передачи информации и методов обеспечения информационной безопасности.

***Степень использования*:** результаты внедрены в учебный процесс на кафедре проектирования информационно−компьютерных систем учреждения образования "Белорусский государственный университет информатики и радиоэлектроники в учебный курс "Методы и средства защиты информации".

***Область применения*:** информационные технологии, IT - индустрия.

**SUMMARY**

**Vrabii Edward Mihailovich**

**The method for ensuring the functional reliability of electronic modules based on microcontrollers when exposed to static discharges electricity**

***Keywords*:** information security, security.

***The object of study*:** is the optimization of methods to ensure the information security of mobile access.

***The results and novelty*:** an analysis of the methods and means of protection and transmission of information. It was revealed that at present the issue of the protection of information, the most relevant; Optimization of existing methods and means of protection and transmission of information; made implementation of the method of information transmission and information security techniques.

***Degree of use*:** the results are implemented in the educational process on the design of information and computer systems for the establishment of education "Belarusian State University of Informatics and Radioelectronics in the course" Methods and Means of Information Protection ".

***Sphere of application***: information technology, IT industry.