МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

К защите допустить
Зав. кафедрой

_____
"___"_____ 2016 г.

Выпускная работа бакалавра

на тему: **ЭВОЛЮЦИЯ АСПЕКТОВ БЕЗОПАСНОСТИ В СОТОВЫХ СИСТЕМАХ СВЯЗИ**

Выпускник _____ Гуламова Ш.Г.
подпись ф.и.о.

Руководитель _____ Алимджанов Х.Ф
подпись ф.и.о.

Рецензент_____ _____
подпись ф.и.о.

Консультант
по БЖД и Э _____ Кадиров Ф.М.
подпись ф.и.о.

Ташкент – 2016

МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Факультет _____ТТ_____ кафедра ____Технологии мобильной связи_____
Направление (специальность)_____5311400_____
_____Мобильные системы связи_____

У Т В Е Р Ж Д А Ю

Зав. кафедрой _____
«_____» _____2016 г.

З А Д А Н И Е

на выпускную квалификационную работу Гуламовой Шахнозы Гайрат кизи
на тему: Эволюция аспектов безопасности в сотовых системах связи

1. Тема утверждена приказом по университету №1267-17 от 02.12.2015 г.

2. Срок сдачи законченной работы 25.05.2016

3. Исходные данные к работе: Характеристики сотовых систем связи стндартов GSM, CDMA, LTE и пр.

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов: Введение; 1. Обзор информационной безопасности в телекоммуникационных системах связи. 2.Эволюция аспектов безопасности в сотовых системах связи; 3. Безопасность жизнедеятельности и экология; Заключение

5. Перечень графического материала _____демонстрационные слайды____

6. Дата выдачи задания _____

Руководитель _____
подпись
Задание принял _____
подпись

7. Консультанты по отдельным разделам выпускной работы

Наименование раздела	Консультант	Подпись, дата	
		Задание выдал	Задание получил
Главы 1-2	Алимджанов. Х.Ф.	12.02.2016 г.	12.02.2016 г.
БЖД и Э	Кадиров Ф.М.	14.04.2016 г.	14.04.2016 г.

8. График выполнения работы

№	Наименование раздела	Срок Выполнения	Подпись руководителя (консультанта)
1.	Обзор информационной безопасности в телекоммуникационных системах связи	16.03.2016 г.	
2.	Эволюция аспектов безопасности в сотовых системах связи	20.04.2016 г.	
3.	Безопасность жизнедеятельности и экология	18.05.2016 г.	

Выпускник _____ «_20_»_____01____2016 г.
подпись

Руководитель _____ «_20_»_____01_____2016 г.
подпись

Ушбу битирув ишда телекоммуникация тармоқларида ахборот хавфсизлиги масалалари кўриб чиқилган. Ҳаракатдаги алоқа тизимларида ахборот хавфсизлигининг ривожланиш тарихи ёритиб берилган, сотали алоқа тизимларининг ҳар бир авлоди учун ахборот хавфсизлигини таъминлаш жараёнининг таҳлили келтирилган.

Шу қаторда ҳаёт фаолияти хавфсизлиги ва экология масалалари кўриб чиқилган.

В данной работе рассматриваются вопросы информационной безопасности в телекоммуникационных системах связи. Приводится обзор истории развития информационной безопасности в подвижных системах связи, выполняется анализ обеспечения информационной безопасности в разных поколениях систем сотовой связи.

Также рассмотрены вопросы безопасности жизнедеятельности и экологии.

In this final qualification work the review of information security in telecommunication system. Provides an overview of history of the development of information security in mobile communication systems, analyses will be carried out about information security in different generations of cellular communication systems.

Safety issues of activity and ecology are also considered.

ОГЛАВЛЕНИЕ

Введение

В современных условиях, в эпоху Интернета и электроники приоритетное значение имеет широкое внедрение современных информационно-коммуникационных технологий в отраслях экономики, кардинальное ускорение создания системы «Электронное правительство».

Весь мировой опыт показывает, что в настоящее время в глобальной экономике все более возрастающую роль и значение приобретает сектор информационно-коммуникационных технологий, включающий в себя производство компьютерных и телекоммуникационных технологий, разработку программного обеспечения и предоставление на их основе широкого спектра интерактивных услуг. Не следует забывать, что развитие ИКТ напрямую влияет на уровень конкурентоспособности страны, позволяет собирать и обобщать огромные массивы информации, открывает широкие возможности для управления на стратегическом уровне [1].

В Республике Узбекистан создана современная и мощная законодательная база в сфере инфокоммуникационных технологий. В республике предусмотрены проведение модернизации, технического и технологического перевооружения предприятий, широкое внедрение современных гибких технологий. Ставится задача ускорения реализации принятых отраслевых программ модернизации, технического и технологического перевооружения производства. Одной из важнейшей задач, которое стоит перед нашим обществом, является обеспечение поступательного и устойчивого развития страны.

Сотовая связь появилась в нашей жизни совсем недавно и за короткий срок успела превратиться из неслыханной роскоши в незаменимое средство связи, развиваясь буквально у нас на глазах. Аналоговым стандартам первого поколения 1G пришли на смену цифровые стандарты второго поколения 2G, которые вскоре эволюционировали в 2.5G, и далее в высокоскоростной 3G, позволяющий передавать даже потоковое видео.

В настоящее время бурными темпами развитваются сети четвертого поколения 4G и рассматриваются концепция сетей следующего пятого поколения 5G.

Столь бурное развитие и огромная популярность отрасли особенно остро поставили перед разработчиками стандартов сотовой связи и оборудования вопросы надежной аутентификации пользователей и безопасности передачи информации. Безопасность была одним из главных аспектов сотовой телефонии с самого ее рождения, как для операторов так и для абонентов. Причем, если операторов в большей мере беспокоила ее часть, связанная с предотвращение мошеннических операций, таких как создание двойников мобильных телефонов или ложная аутентификация, то абонентов кроме этого очень интересовала безопасность передачи конфиденциальной информации.

В данной выпускной работе выполняется анализ вопросов безопасности в сотовых системах связи.

1. ОБЗОР ОСОБЕННОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ СВЯЗИ

1.1.Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена.

На практике важнейшими являются три аспекта информационной безопасности:

Доступность - возможность за разумное время получить требуемую информационную услугу.

Целостность - ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность - защита от несанкционированного прочтения.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления - производством, транспортом. Менее драматичные, но также весьма неприятные последствия - и материальные, и моральные - может иметь длительная недоступность информационных услуг, которыми

пользуется большое количество людей, например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет.

Доступность - это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными.

Таким образом, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность - гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность - самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем

связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность - гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации (рис.1.1).

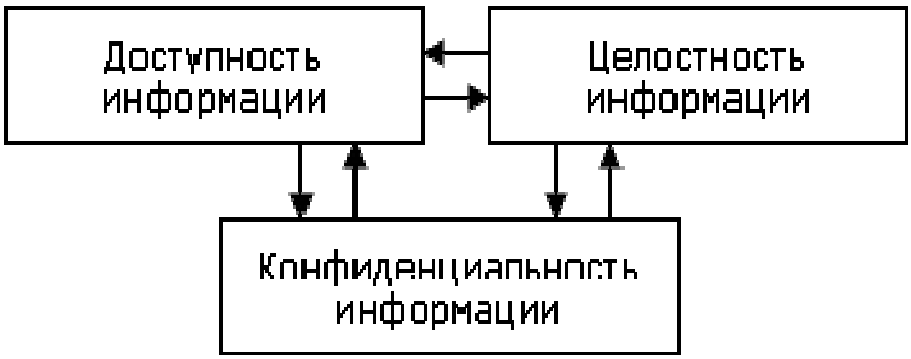

Рис.1.1. Составляющие информационной безопасности

Как уже отмечалось, выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью

реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме этого, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

Обеспечение "информационной безопасности" - не одноразовый акт. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий.

Безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты на всех этапах обработки информации.

Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм – комплексную систему защиты информации (КСЗИ).

На практике выделяют следующие направления информационной безопасности:

– правовая защита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

– организационная защита - это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе исключающая или ослабляющая нанесение какого-либо ущерба исполнителем;

– инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности.

1.2.Угрозы, атаки и каналы утечки информации

Под угрозой безопасности информации будем понимать действие или событие, которое может привести к нарушению достоверности, целостности или конфиденциальности хранящейся, передаваемой или обрабатываемой информации.

Обратим внимание, что мы говорим о защите не только хранящейся в информационной базе информации, но и информации, которая передается по каналам связи или обрабатывается программным обеспечением.

- *Атака* – попытка реализовать угрозу.
- *Злоумышленник* – тот, кто осуществляет атаку.
- *Источник угрозы* – потенциальный злоумышленник.
- *Окно опасности* - промежуток времени от начала возникновения возможности использовать слабое место в защите до момента, когда это слабое место будет ликвидировано.

Угрозы можно разделить по тем компонентам ИС и ее инфраструктуры, на которые непосредственно направлена данная угроза. В этом случае, можно говорить об:

- угрозе непосредственно данным,
- угрозе программному обеспечению ИС,
- угрозе системному программному обеспечению,
- угрозе компьютерной технике и сетевому оборудованию и т.д.

Известно большое количество угроз безопасности информации различного происхождения. В литературных источниках дается множество разнообразных классификаций, где в качестве критериев деления используются источники появления угроз, виды порождаемых опасностей,

степень злого умысла и т.д. Одна из самых простых классификаций приведена на (рис. 1.2)

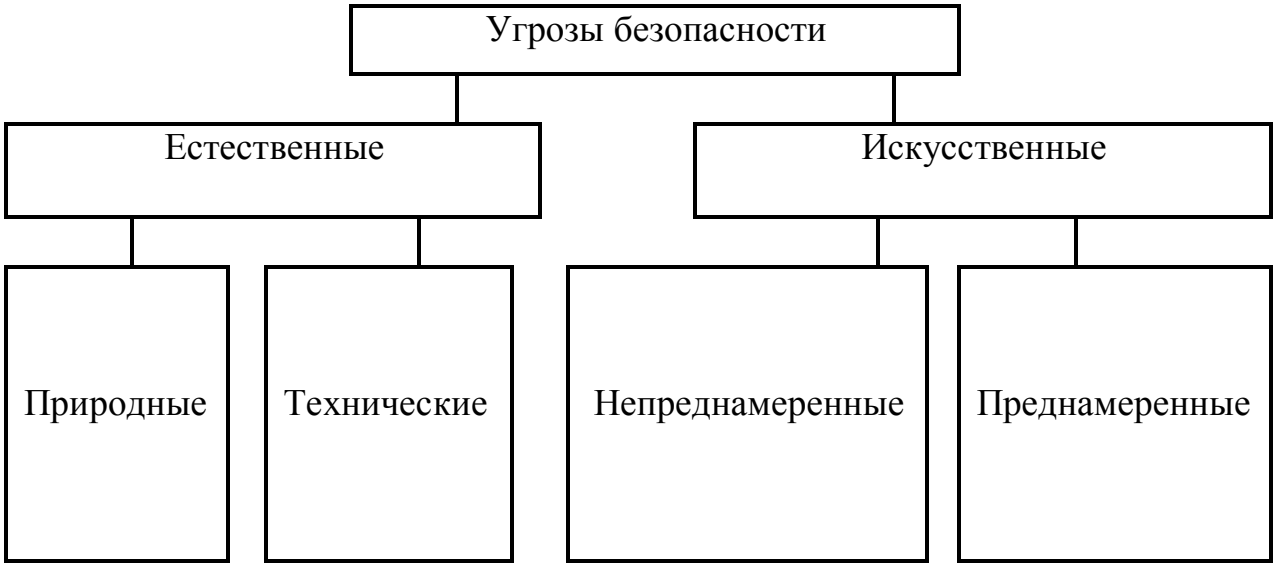

Рис. 1.2. Общая классификация угроз безопасности.

Естественные угрозы - это угрозы, вызванные воздействиями на компьютерную систему и ее элементы каких-либо физических процессов или стихийных природных явлений, которые не зависят от человека. Среди них можно выделить:

- природные - это ураганы, наводнения, землетрясения, цунами, пожары, извержения вулканов, снежные лавины, селевые потоки, радиоактивные излучения, магнитные бури;
- технические - угрозы этой группы связаны с надежностью технических средств обработки информации.

Искусственные угрозы - это угрозы компьютерной системы, которые вызваны деятельностью человека. Среди них можно выделить:

- непреднамеренные угрозы, которые вызваны ошибками людей при проектировании компьютерной системы, а также в процессе ее эксплуатации;
- преднамеренные угрозы, связанные с корыстными

устремлениями людей. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами: недовольство служащего своей карьерой; взятка; любопытство; конкурентная борьба; стремление самоутвердиться любой ценой.

Можно составить предполагаемую модель возможного нарушителя:

- квалификация нарушителя соответствует уровню разработчика данной системы;
- нарушителем может быть как законный пользователь системы, так и постороннее лицо;
- нарушителю известна принципиальная работы системы;
- нарушитель выбирает наиболее слабое звено в защите.

Кроме перечисленных выше признаков, по которым можно классифицировать угрозы информационной безопасности, угрозы можно поделить на прямые и косвенные.

Косвенные угрозы непосредственно не приводят к каким либо нежелательным явлениям в компьютерной системе, но они могут являться источниками новых косвенных или прямых угроз.

Способы нанесения ущерба	Объекты воздействий			
	оборудование	программы	данные	персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование, перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашении, халатность
Потеря целостности информации	Подключение, модификация, спец. вложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала, «маскарад»
Нарушение работоспособности автоматизированной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	

Таб. 1.1. Угрозы безопасности информации

1.3. Классификация методов и средств обеспечения безопасности

Метод (способ) защиты информации: порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации: техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Методами обеспечения защиты информации являются следующие: регламентация, препятствие, маскировка информации, противодействие вирусам, управление доступом, принуждение и побуждение.

Препятствие - это метод, при котором пути злоумышленнику к защищаемой информации преграждаются физически, например, к аппаратуре, носителям информации и т.п.

Регламентация заключается в реализации системы организационных мероприятий, которые определяют все стороны процесса обработки информации. Этот метод создает такие условия автоматизированной обработки, передачи и хранения информации, при которых возможность несанкционированного доступа к ней сводится к минимуму.

Управление доступом – этот метод защиты информации регулирует использование всех ресурсов автоматизированной информационной системы организации (технические, программные, временные и др.) и включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов информационной системы, то есть присваивает каждому объекту персональный идентификатор;
- аутентификацию, то есть устанавливает подлинность объекта или субъекта по предъявленному им идентификатору;
- регистрацию или, говоря другими словами, протоколирование обращений к защищаемым ресурсам;
- проверку полномочий, таких как проверка соответствия дня

недели, времени суток, запрашиваемых ресурсов и процедур в соответствии с установленным регламентом;

- разрешение и создание условий работы в пределах установленного регламента;

- реагирование при попытках несанкционированных действий (сигнализация, отключение, задержка работ, отказ в запросе).

Маскировка информации - метод защиты информации путем ее криптографического закрытия. Механизмы шифрования все шире применяются при обработке и хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности только этот метод является единственно надежным.

Противодействие вирусам (или атакам вредоносных программ) предполагает комплексное использование организационных мер и антивирусных программ. Целью принимаемых мер является уменьшение вероятности инфицирования информационно-вычислительной системы, уменьшение последствий информационных инфекций, локализация или уничтожение вирусов, восстановление информации.

Принуждение - такой метод защиты информации, при котором пользователей и персонал системы вынуждают соблюдать правила обработки, использования и передачи защищаемой информации под угрозой административной, материальной или уголовной ответственности.

Побуждение - такой метод защиты информации, который за счет соблюдения сложившихся моральных и этических норм побуждает пользователей системы не нарушать установленные правила.

Указанные методы обеспечения информационной безопасности реализуются на практике применением различных механизмов защиты, для создания которых используются следующие основные средства: физические, аппаратные, программные, аппаратно-программные, организационные, морально-этические и законодательные.

Физические средства защиты предназначены для внешней охраны

территории объектов, защиты компонентов автоматизированной информационной системы предприятия и включают в себя разнообразные инженерные устройства и сооружения, которые препятствуют проникновению злоумышленников на объекты защиты. Примером физических средств могут служить замки на дверях, средства электронной охранной сигнализации, решетки на окнах и т.д.

Аппаратные средства защиты – это электронные, электромеханические и другие устройства, непосредственно встроенные в вычислительную технику или самостоятельные устройства, которые сопрягаются с ней по стандартному интерфейсу. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д. Такие средства принадлежат к наиболее защищенной части системы. Если есть выбор, то предпочтение следует отдавать аппаратным средствам защиты, так как они исключают вмешательство в их работу непосредственно из сети. Еще одно преимущество аппаратных средств – это их большая производительность по сравнению с программными средствами защиты, особенно, при использовании их в устройствах криптографической защиты.

Недостатком аппаратных средств является их высокая стоимость.

Программные средства защиты – это специальные программы и программные комплексы, предназначенные для защиты информации. Программные средства защиты информации являются наиболее распространенным видом защиты, обладая следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития. Основной их недостаток – это доступность для хакеров, особенно это касается широко распространенных на рынке средств защиты.

Программные средства часто делят на средства, которые реализуются в стандартных операционных системах (ОС) и в специализированных информационных системах.

Криптографические программы основаны на использовании методов шифрования (кодирования) информации. Такие методы очень надежны и значительно повышают безопасность передачи информации в сетях.

Аппаратно-программные средства защиты – средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы. Они совмещают высокую производительность аппаратно реализованных систем и гибкость настройки программных. В качестве примера такого устройства можно привести маршрутизаторы фирмы Cisco, которые допускают их настройку в качестве пакетных фильтров.

Организационные средства – это действия общего характера, предпринимаемые руководством организации. Они регламентируют процессы функционирования и использование ресурсов системы обработки данных, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности, а в случае их реализации снизить размер потерь.

Организационные меры включают в себя:

- мероприятия, осуществляемые при подборе и подготовке персонала;
- мероприятия, осуществляемые при проектировании, строительстве и оборудовании сетей;
- организацию охраны и надежного пропускного режима; разработку политики безопасности;
- распределение реквизитов разграничения доступа; организацию учета, хранения, использования и уничтожения документов и носителей с информацией;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

Организационные меры играют важную роль в обеспечении

безопасности компьютерных систем. Когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности, организационные меры - это единственное, что остается. Но это не означает, что систему защиты необходимо строить исключительно на их основе, так как этим мерам присущи и серьезные недостатки, такие как:

- низкая надежность без соответствующей поддержки физическими, техническими и программными средствами;
- дополнительные неудобства, связанные с большим объемом формальной и рутинной деятельности.

Организационные меры нужны для того, чтобы обеспечить эффективное применение других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными техническими и физическими средствами.

Законодательные средства - действующие в стране законы, указы и другие нормативно-правовые акты, которые регламентируют правила обращения с информацией, закрепляют права и обязанности участников информационных отношений, а также устанавливают ответственность за нарушение этих правил. Правовые меры защиты носят преимущественно упреждающий, профилактический характер. Основной целью их является предупреждение и сдерживание потенциальных нарушителей.

Морально-этические средства - всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации. Морально-этические нормы могут быть как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и оформленные в некоторый свод правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах пользователей.

Законодательные и морально-этические меры определяют правила

обращения с информацией и ответственность субъектов информационных отношений за их соблюдение. Они являются универсальными, так как могут применяться для всех каналов проникновения и НСД к информации. В некоторых случаях они могут быть единственно применимыми, как например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией.

Все рассмотренные средства защиты разделяются на формальные (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяемые целенаправленной деятельностью человека либо регламентирующие эту деятельность).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Надежная и безопасная система защиты должна соответствовать следующим требованиям:

- стоимость средств защиты должна быть меньше, чем размеры возможного ущерба;
- каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы;
- защита тем более эффективна, чем проще пользователю с ней работать;
- возможность отключения в экстренных случаях;
- специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать;
- под защитой должна находиться вся система обработки информации;
- разработчики системы защиты, не должны быть в числе тех, кого

эта система будет контролировать;

- система защиты должна предоставлять доказательства корректности своей работы;
- лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность;
- объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других;
- надежная система защиты должна быть полностью протестирована и согласована;
- защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора;
- система защиты должна разрабатываться, исходя из предположения, что пользователи будут совершать серьезные ошибки и, вообще, имеют наихудшие намерения;
- наиболее важные и критические решения должны приниматься человеком;
- существование механизмов защиты должно быть по возможности скрыто от пользователей, работа которых находится под контролем.

У специалистов по защите информации имеется широкий спектр защитных мер: законодательных, морально-этических, административных (организационных), физических и технических (аппаратно-программных) средств. Все эти средства обладают своими достоинствами и недостатками, которые необходимо правильно учитывать при создании систем защиты.

Все известные каналы проникновения и утечки информации должны быть перекрыты с учетом анализа риска, вероятностей реализации угроз безопасности в конкретной прикладной системе и обоснованного рационального уровня затрат на защиту.

Наилучшие результаты достигаются при системном подходе к вопросам безопасности компьютерных систем и комплексном использовании определенных совокупностей различных мер защиты на всех этапах

жизненного цикла системы, начиная с самых ранних стадий ее проектирования.

1.4. Цели и значение защиты информации

Часто цель и задачи защиты информации отождествляют, что неверно.

Цель защиты информации – это то, ради чего она должна защищаться (предполагаемый результат деятельности по защите информации).

Задачи защиты информации - это, что необходимо сделать для реализации цели (результата защиты информации).

Структура целей защиты информации.

Защита информации имеет два уровня целей

Первый уровень – непосредственные цели, которые должны быть привязаны к самой информации как непосредственному объекту защиты.

Цель защиты информации первого уровня – безопасность информации.

Второй уровень – конечные цели (опосредованные), которые должны быть привязаны к субъектам информационных отношений (государству, обществу, личности, конкретному хозяйствующему субъекту).

Цель защиты информации второго уровня – безопасность субъектов информационных отношений.

Защита информации — это деятельность собственника информации или уполномоченных им лиц по:

—обеспечению своих прав на владение, распоряжение и управление защищаемой информацией;

—предотвращению утечки и утраты информации;

—сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки;

—сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

В общем виде цели защиты информации сводятся к режимно-секретному информационному обеспечению деятельности государства, отрасли, предприятия, фирмы.

Задачи защиты информации.

Задачи защиты информации также имеют два уровня:

Первый уровень – задачи общеконцептуального плана:

- на предупреждение угроз. Предупреждение угроз — это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
- на выявление угроз. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
- на обнаружение угроз. Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;
- на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
- на ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

Второй уровень задач защиты информации зависит от конкретного предприятия (прикладные задачи). Они зависят:

- от видов защищаемой на предприятии информации;
- степени ее конфиденциальности;
- состава носителей защищаемой информации.

Защита информации разбивается на решение двух основных групп задач:

1. Своевременное и полное удовлетворение информационных потребностей, возникающих в процессе управленческой, инженерно-технической, маркетинговой и иной деятельности, то есть обеспечение специалистов организаций, предприятий л фирм секретной или конфиденциальной информацией.

2. Ограждение засекреченной информации от несанкционированного доступа к ней соперника, других субъектов в злонамеренных целях.

При решении первой группы задач — обеспечение специалистов информацией — всегда, конечно, учитывается, что специалисты могут использовать как открытую, так и засекреченную информацию. Снабжение специалистов открытой информацией ничем не ограничивается, кроме ее фактического наличия. При снабжении же специалиста засекреченной информацией действуют ограничения: наличие соответствующего допуска (к какой степени секретности информации он допущен) и разрешения на доступ к конкретной информации. В решении проблемы доступа специалиста к соответствующей засекреченной информации всегда существуют противоречия, с одной стороны, — максимально ограничить его доступ к засекреченной информации и тем самым уменьшить вероятность утечки этой информации; с другой стороны, — наиболее полно удовлетворить его потребности в информации, в том числе и засекреченной для обоснованного решения им служебных задач.

В обычных, не режимных условиях, специалист имеет возможность использовать в целях решения стоящей перед ним проблемы разнообразную информацию: ретроспективную, узко- и широкотематическую, отраслевую и межотраслевую, фактографическую и концептуальную. При обеспечении его засекреченной информацией возможности доступа к ней ограничиваются двумя факторами: его служебным положением и решаемой специалистом в настоящее время проблемой.

Вторая группа задач — это ограждение защищаемой информации от несанкционированного доступа к ней соперника, включает такие условия, как:

1. Защита информационного суверенитета страны и расширение возможности государства по укреплению своего могущества за счет формирования и управления развитием своего информационного потенциала.

2. Создание условий эффективного использования информационных ресурсов общества, отрасли, предприятия, фирмы, структурного подразделения, индивида.

3. Обеспечение безопасности защищаемой информации: пред отвращение хищения, утраты, несанкционированного уничтожения, модификации, блокирования информации и т.п., вмешательства в информацию и информационные системы.

4. Сохранение секретности или конфиденциальности засекреченной информации в соответствии с установленными правилами ее защиты, в том числе предупреждения ее утечки и несанкционированного доступа к ее носителям, предотвращению ее копирования, фотографирования и др.

5. Сохранение полноты, достоверности, целостности информации и ее массивов и программ обработки, установленных собственником информации или уполномоченными им лицами.

6. Обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальной персональной информации, в том числе накапливаемой в банках данных.

7. Недопущение безнаказанного растаскивания и незаконного использования интеллектуальной собственности, принадлежащей государству, предприятиям и фирмам, частным лицам.

Значение защиты информации определяется не только в системе информационной безопасности, но и в системе национальной безопасности. Цели защиты информации для государства, общества и отдельных личностей различна. Они в конечном итоге дополняют друг друга и каждый из субъектов объективно заинтересован в защите информации других субъектов. В различных сферах деятельности политической, экономической, военной, социальной интересы всех субъектов должны или совпадать или дополнять друг друга. С учетом этого значения защиту информации следует рассматривать с привязкой не к субъектам, а к сферам деятельности независимо от того ко всем или одному субъекту относится эти сферы

деятельности. При этом значение защиты информации целесообразно определить через те последствия (положительные или отрицательные), которые наступают в результате защиты или при ее отсутствии:

1. В области внешней политики обеспечивает свои внешне - политические интересы, т. е. иметь преимущества над другими государствами. Достигаются с помощью секретно - сепаратных договоров о военно-политическом сотрудничестве. Защита информации повышает политический уровень такого государства и его международный авторитет. Защита информации может давать и отрицательный результат : если предоставить очень большой объем закрытой информации, во внешней политике это может привести к осложнению в области международной политики.

2. В военной области защита информации позволяет сохранить в тайне от потенциального противника сведения о составе военной техники, ее количестве, тактики, технических данных о разработке новых систем оружия и военной технике, об организации обороны подготовке на случай войны. С другой стороны чрезмерная закрытость информации о вооружении вызывает сомнения других государств, приводит к гонке вооружений. Неоправданный объем защищенной информации в этой области сокращает возможность использования научно-технических достижений в гражданских областях экономики.

3. В экономической сфере деятельности защита информации дает возможность иметь высокие доходы, сохранять приоритет, заключать выгодные контракты, добиваться преимущества над конкурентами, избегать экономического ущерба. Излишняя засекреченность в экономике снижает доверие к ее отраслям или предприятиям со стороны потенциальных партнеров и потребителей продукции, тормозит инвестиции и подрывает престиж предприятия.

4. В социальной сфере - в политических, экономических, правовых и других областях, определяющих общественную и частную жизнь человека

защита информации направлена на улучшения морального и материального благосостояния человека.

Меры обеспечения сохранности и защиты информации в государственной организации, на предприятии или фирме различаются по своим масштабам и формам. Они зависят от производственных, финансовых и других возможностей фирмы, от количества охраняемых на нем секретов и их значимости. При этом выбор таких мер необходимо осуществлять по принципу экономической целесообразности, придерживаясь в финансовых расчетах «золотой середины», поскольку чрезмерное закрытие информации, так же как и халатное отношение к ее сохранению, могут вызвать потерю определенной доли прибыли или привести к непоправимым убыткам. Отсутствие у руководителей предприятий четкого представления об условиях, способствующих утечке конфиденциальной информации, приводят к ее несанкционированному распространению.

Наличие большого количества уязвимых мест на любом современном предприятии или фирме, широкий спектр угроз и довольно высокая техническая оснащенность злоумышленников требует обоснованного выбора специальных решений по защите информации.

2. ЭВОЛЮЦИЯ АСПЕКТОВ БЕЗОПАСНОСТИ В СОТОВЫХ СИСТЕМАХ СВЯЗИ

2.1. Информационная безопасность в сотовых системах связи

В современной действительности непрерывно происходят процессы эволюционного развития систем сотовой подвижной связи (СПС) в направлении высоких технологий, использования интеллектуальных ресурсов, разработки и внедрения механизмов обеспечения информационной безопасности. Исторический опыт показывает, что эволюционный путь развития является более прагматичным, по сравнению с революционным, более надежным и стабильным. Эволюционный подход подразумевает изучение плюсов и минусов того, что было, с последующим усилением позитивных аспектов и исключением негативных факторов.

Развитие сетей СПС представляет собой динамически развивающийся рынок связи, если можно так выразиться, развитие мобильных систем связи намного прогрессивнее стационарной связи и это вызвано рядом причин. Расширение зоны покрытия сетей и межсетевой роуминг обеспечивает комфорт и избавляет абонента сети от лишних забот. Не менее важным является и расширение сервисов обслуживания абонентов сети и интенсивное внедрение новых услуг.

Перечисленные преимущества сетей СПС базируются именно на эволюционном принципе развития. Переход от аналоговых сетей связи с достаточно с небольшой зоной покрытия к цифровым сетям связи современного состояния происходило не скачкообразно, а плавно, с использованием ресурсов прежних сетей и развитие на их основе принципиально новых сетей связи. Но на этом развитие систем сотовой связи не останавливается, т.к. растущие с каждым годом потребности пользователей в услугах СПС приводят к необходимости производить

операторами улучшение качественных и количественных характеристик сети, внедрение новых услуг и, как следствие, новых технологий.

Следующим этапом развития СПС будет полномасштабное внедрение сетей UMTS. В идеологию развития сетей UMTS заложен тот же принцип эволюционности. Сети UMTS будут внедряться постепенно и будут функционировать одновременно с существующими сетями GSM\GPRS до момента их полного вытеснения с рынка мобильной связи. С учетом существующих тенденций на рынке радиодоступа можно определить следующие пути развития систем сотовой связи в объединении с другими технологиями доступа. Для операторов связи, использующих сети второго поколения:

– внедрение и эксплуатация сетей на основе технологии EDGE, а также модернизация существующих сетей;

– внедрение WiMAX-сетей с целью расширения возможностей сетей GPRS/EDGE.

Для операторов связи, имеющих лицензии на эксплуатацию сетей 3G:

– запуск и развитие сетей на основе технологии EDGE;

– внедрение сетей UMTS/HSDPA с целью предоставления услуг мобильной связи, связанных с высокоскоростной передачей данных;

– расширение зоны покрытия для сетей UMTS/HSDPA;

– внедрение WiMAX-сетей как расширение сетей 3G.

Таким образом, видно, что одним из направлений развития сетей СПС третьего поколения является интеграционный процесс, включающий в себя объединение различных технологий, процессов и физических сетей.

В рамках рассматриваемой проблематики можно выделить следующие вопросы, представляющие особый интерес при развитии сетей третьего поколения:

– определение рисков для сетей СПС третьего поколения с учетом уязвимостей сопряженных сетей;

– порядок аутентификации абонента при подключении к ресурсам сети UMTS через внешнюю сеть передачи данных;

– безопасность в процессе взаимодействия базовой сети UMTS и сетей контент-провайдеров и внешних сетей.

Аналитические исследования в области ИБ сетей СПС и сетей передачи данных показали, что в этих сетях существует ряд уязвимостей и рисков нарушения ИБ . Уязвимости, угрозы и риски ИБ носят специфический характер, все зависит от среды передачи данных, структуры сети связи, передаваемых данных, назначения сети и т.д. Однако, очевидно, что в рамках процесса объединения различных сетей и расширения области их взаимодействия растет и риск преемственности одной сетью уязвимостей другой. При этом в объединенной сети будут присутствовать одновременно все специфические угрозы ИБ для каждой сети в отдельности, входящей в общую инфраструктуру.

В ракурсе этого вопроса немаловажным становится проблематика изучения и исследования направления – информационной безопасности при интеграционных процессах сетей СПС. О безопасности в сетях СПС можно говорить как об определенном процессе, непосредственно связанном с функционированием сети СПС. Эволюционные процессы, протекающие в рамках общего развития сетей СПС, отразились и на механизмах и принципах реализации ИБ в сетях СПС.

Вопросы обеспечения ИБ в сетях СПС с каждым новым этапом развития расширяются и включают в себя все больше механизмов обеспечения ИБ. При этом стоит отметить, что механизмы, зарекомендовавшие себя в предыдущих поколениях, учитываются при развитии сетей последующих поколений. Эти механизмы могут реализовываться в сетях нового поколения без изменений, а могут модернизироваться с учетом новых угроз ИБ.

Таким образом, из всего вышесказанного можно сделать следующие выводы:

– в развитии сетей СПС наблюдается эволюционное развитие;
– явным образом прослеживаются интеграционные процессы;
– преемственность уязвимостей при объединении различных сетей;
– расширение спектра реализуемых механизмов ИБ в сетях СПС.

2.2. Эволюция систем безопасности сетей сотовой связи разных поколений

Безопасность сотовой связи непосредственно связана с историей развития технологий и средств радиодоступа, используемых в системах связи различных поколений. К настоящему времени в зависимости от скорости передачи данных и количества предоставляемых услуг и сервиса можно выделить четыре поколения сетей сотовой связи (рис.2.1.)

Поколение	1G	2G	2.5G	3G	3.5G	4G
Реализация	1984	1991	1999	2002	2006—2007	2008—2010
Скорость передачи	1,9 кбит/с	14,4 кбит/с	384 кбит/с	2 Мбит/с	3-14 Мбит/с	1 Гбит/с
Стандарты	AMPS, TACS, NMT	TDMA, CDMA, GSM, PDC	GPRS, EDGE, 1xRTT	WCDMA, CDMA2000, UMTS	HSDPA	единый стандарт

Рис.2.1. Эволюция сетей сотовой связи

Каждое из поколений характеризуется особенностями реализации механизмов обеспечения безопасности в функциональной структуре сетей сотовой связи. На начальном этапе развития сетей сотовой связи (технологии

AMPS/ D-AMPS, NMT-450) защита от несанкционированного доступа осуществлялась на основе совместного использования двух, присваиваемых каждому мобильному терминалу (MS), идентификационных номеров:

- ESN – электронный серийный номер, присваивался фирмой изготовителем;
- MIN – мобильный идентификационный номер, присваивался оператором сети.

Механизм идентификации был основан на приёме базовой станцией (BS) на определённой частоте идентификаторов ESN и MIN. Однако простота перехвата в эфире с помощью перестраиваемого приёмника – сканера и достаточно не сложная расшифровка этих сигналов привели к массовому клонированию мобильных терминалов. Так, например, к середине 90-ых годов прошлого века убытки операторов стремительно развивающихся аналоговых сетей сотовой связи от клонирования MS и сотового мошенничества достигали 40% от доходов. Следствием этого явилось внедрение сетевых средств защиты с использованием специальных криптографических технологий аутентификации пользователей A-KEY и SIS (рис.2.2.).

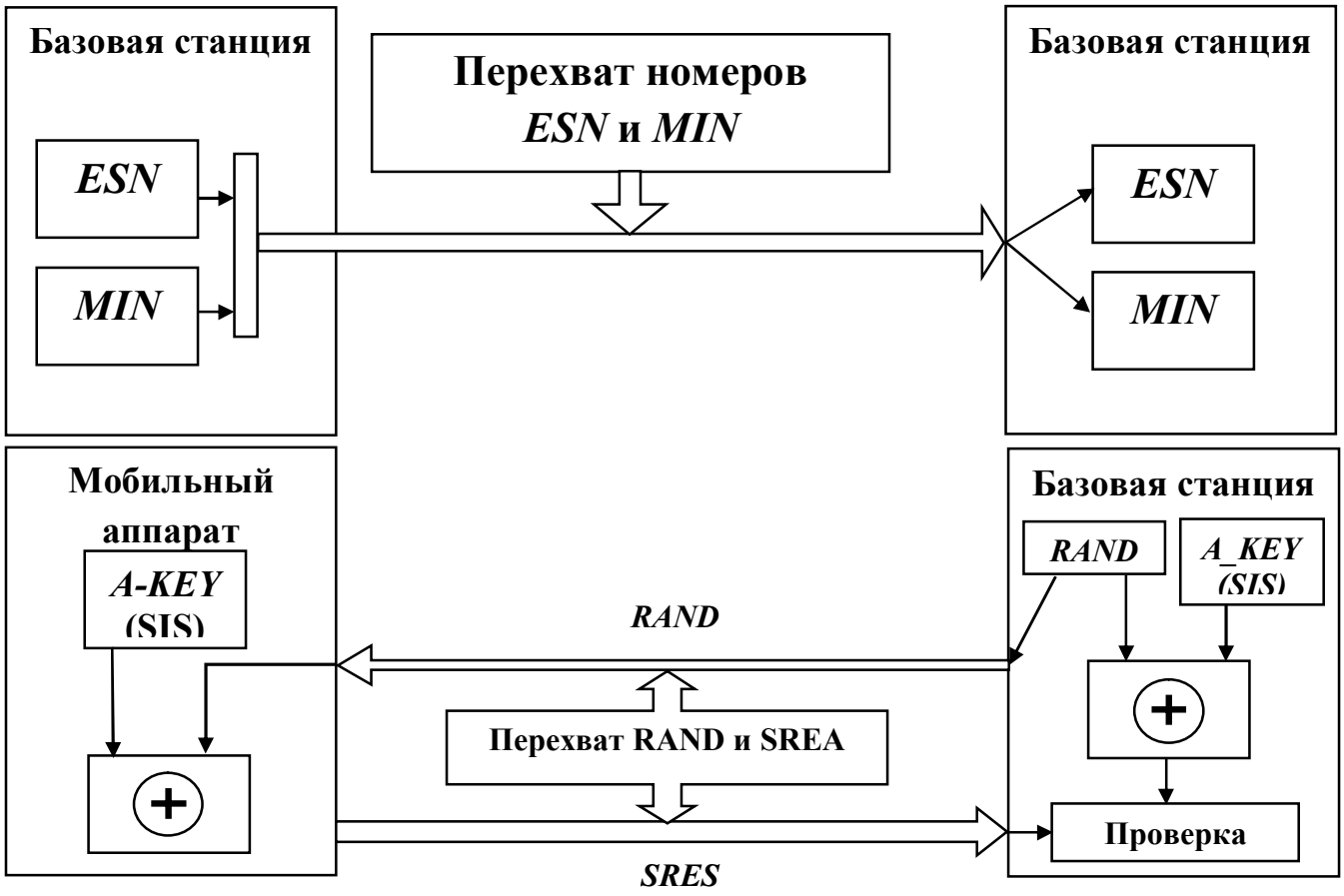

Рис.2.2. Процедуры аутентификации пользователей в аналоговых сетях (1G)

Обе они основаны на методе запрос/ответ, при котором BS посылает запрос, а сотовый телефон обрабатывает его и выдаёт шифрованный ответ. BS сравнивает присланный и ожидаемый ответ и, при их совпадении, допускает пользователя в сеть. Для формирования верного ответа требуется секретный 64-битный ключ, являющийся индивидуальным для каждого телефона и хранящийся как в его памяти, так и на BS. Поскольку ключ не передаётся в эфир, перехватить его нельзя, и следовательно, телефон защищён от клонирования. Введение данных технологий в аналоговых сетях сотовой связи (1G) позволило, ограничить угрозы, связанные с массовым клонированием мобильных трубок, хотя полностью избавиться от клонирования телефонов так и не удалось. Кроме криптографической аутентификации в аналоговых сетях предусматривалось шифрование

информации о набираемом номере. В то же время обеспечение конфиденциальности связи исключается, так как сигналы в эфире передаются с использованием частотной модуляции и прослушиваются в эфире с помощью обычного ЧМ-приёмника.

При проектировании сетей второго поколения термин “безопасность” понимался разработчиками в аспектах как исключение несанкционированного пользования услугами сети так и обеспечения конфиденциальности переговоров подвижных абонентов. Принцип аутентификации, используемый в сетях 2G (GSM) аналогичен реализованному в технологиях A-KEY и SIS и основан на механизме аутентификации «запрос-ответ» с использованием шифрования. Главное отличие заключается в том, что параметры аутентификации не пристроены в мобильное устройство, а хранятся в отдельном аутентификационном модуле – SIM-карты (Subscriber Identify Module). На SIM-карте хранится секретный ключ аутентификации KI (128 бит), алгоритмы шифрования (A3 и A8) и идентификационные параметры абонента. Уровень защиты в сетях GSM (рис.2.3.) существенно выше, чем в аналоговых сетях сотовой связи за счёт использования структурированной системы безопасности, обеспечивающей следующие процедуры:

- аутентификацию абонента к SIM-карте;
- идентификацию абонента;
- аутентификацию абонента к сети;
- генерацию и использование сессионного ключа шифрования ;
- потоковое шифрование данных разговорного трафика и сигналов управления.

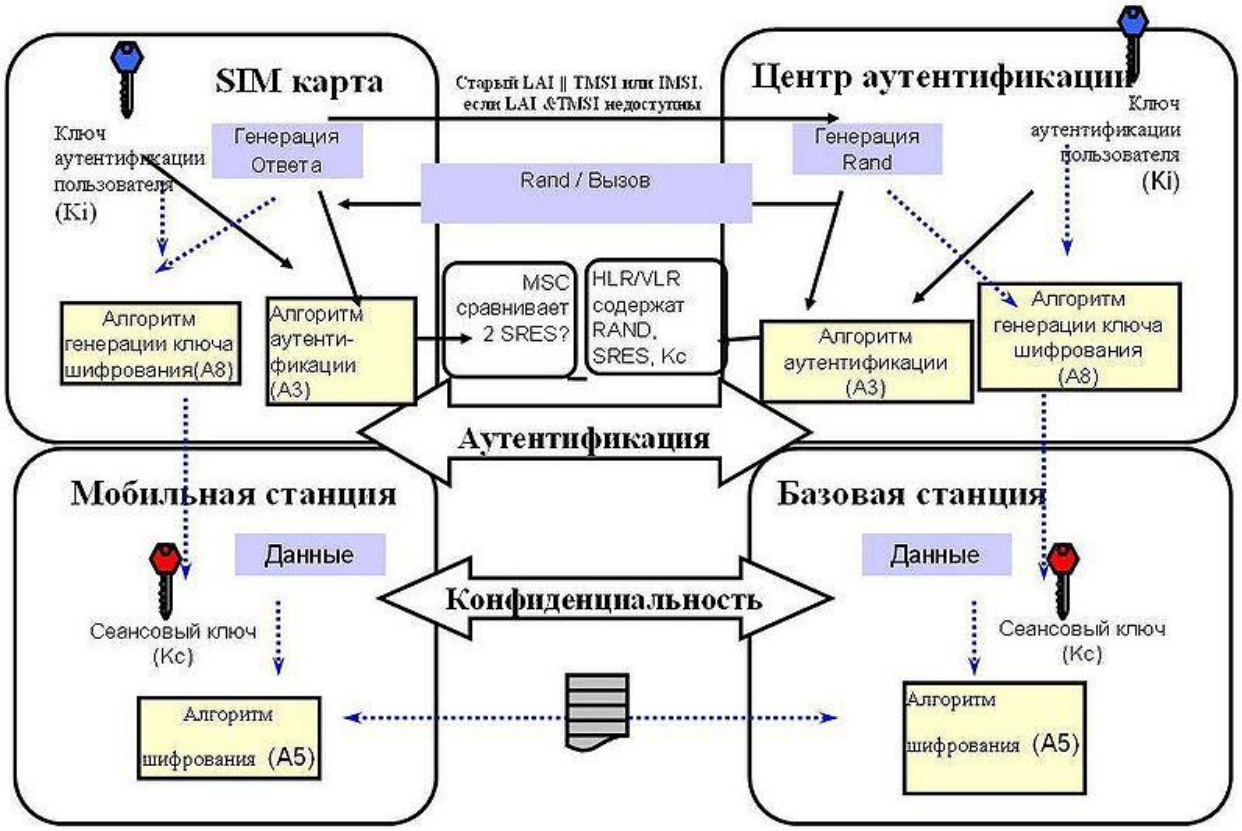

Рис. 2.3. Архитектура системы безопасности сети 2G (GSM)

Процедура аутентификации пользователя к SIM-карте производится путём предъявления PIN-кода. Эта операция может быть пропущена введением блокировки предъявления PIN-кода, если пользователю не требуется этот уровень защиты. Функция идентификации пользователя осуществляется MS путём передачи IMSI-уникального в сетях GSM номера, который хранится на SIM-карте и может быть считан в MS только после предъявления PIN-кода. MS также передаёт свой уникальный номер IMEI, используемый рядом операторов для поиска и отключения украденных телефонов.

Процессы аутентификации и генерации сессионного ключа реализуются алгоритмами A3 и A8. При корректной аутентификации полученный сессионный ключ Kc используется совместно MS и сетью для потокового шифрования данных с помощью алгоритма A5.

Защита MS от клонирования в сетях GSM обеспечивается за счёт алгоритма A3. С его помощью осуществляется вычисление отклика SRES на основании принятого по эфиру случайного числа RAND и индивидуального секретного ключа Ki. SRES=[Ki](A3)[RAND]. Основой механизмов безопасности является секретность Ki, который не может знать даже абонент. При этом процедуры аутентификации и вычисления сессионного ключа шифрования Кс=[Ki](A8)[RAND] проводятся в программной среде SIM-карты, что гарантирует их секретность.

В целом, в сетях поколения 2G реализована успешно основная задача систем безопасности сотовой связи, состоящая в обеспечении аутентификации пользователя и конфиденциальность информационного обмена в радиоканале. Однако детальный анализ 2G-сетей позволяет выявить ряд существенно уязвимых мест подсистемы безопасности, в частности:

1. Криптографическая защита не распространяется на проводную опорную сеть и радиорелейные линии, в результате чего абонентский трафик, потоки служебной информации и сигнализация передаются по ним в незашифрованном виде.

2. Процедура аутентификации и шифрования основана на использовании криптографических ключей малой длины и вскрытых на данный момент алгоритмах. Помимо этого в архитектуре безопасности заложена команда отключения режима шифрования, что открывает сети для различного рода мошенничества.

3. Не предусмотрена взаимная аутентификация, в результате чего абонент не может проверить подлинность базовой станции.

4. Отсутствуют процедуры, позволяющие базовой сетевой инфраструктуре отслеживать параметры абонентов при роуминге.

5. Система безопасности сетей 2G не обладает необходимой функциональной гибкостью и не позволяет наращивать криптостойкость и осуществлять модернизацию.

При переходе к сетям стандарта GPRS, позиционируемых в качестве сетей сотовой связи промежуточного поколения (2.5G) впервые была реализована система безопасности, обеспечивующая защиту каждой из точек сети от внешних атак. При этом учитывались следующие уровни безопасности:

1. Безопасность мобильной станции (MS)
2. Безопасность соединения меж MS и узлом SGSN
3. Безопасность трафика в сети одного оператора (между узлами SGSN)
4. Безопасность данных в процессе их передачи между различными операторами GPRS
5. Безопасность при взаимодействии с внешними сетями (Интернет и др.)

В отличие от GSM, где шифрование обеспечивается только на участке между MS и BS, в GPRS передаваемые IP-пакеты защищены от перехвата на всём пути следования от MS до узла SGSN

В сетях GPRS могут использоваться алгоритмы семейства GPRS-A5, более стойкие по сравнению с алгоритмами A5/1, A/2, A5/3, применяемыми в GSM. Помимо этого ключи шифрования жёстко не закреплены и могут выбираться абонентами в процессе аутентификации на основе согласованного использования общей версии алгоритма GPRS-A5. Если согласие не достигнуто и общая версия не выбрана, происходит отказ в доступе сеть.

Ещё одной особенностью безопасности GPRS-сетей является передача информации при хэндовере (перемещение MS в другую зону) от старого узла SGSN в новый и, связанное с ним изменение ключа шифрования Кс, для повышения уровня безопасности.

Переход к мобильной связи третьего поколения 3G обеспечивает не только качественно новые возможности и сервисы для пользователей, но также влечёт за собой новые серьёзные угрозы и сценарии нарушения

нормального режима работы сети. Архитектура безопасности сетей 3G сохраняет преемственность с сетями 2.5G, однако функции всех сетевых элементов защиты существенно расширяются (рис.2.4.). При этом устраиваются известные слабые места в защите GSM/GPRS-систем с учётом сохранения возможности глобального роуминга и доведения защиты каждой из подсистем сети до максимально возможного уровня.

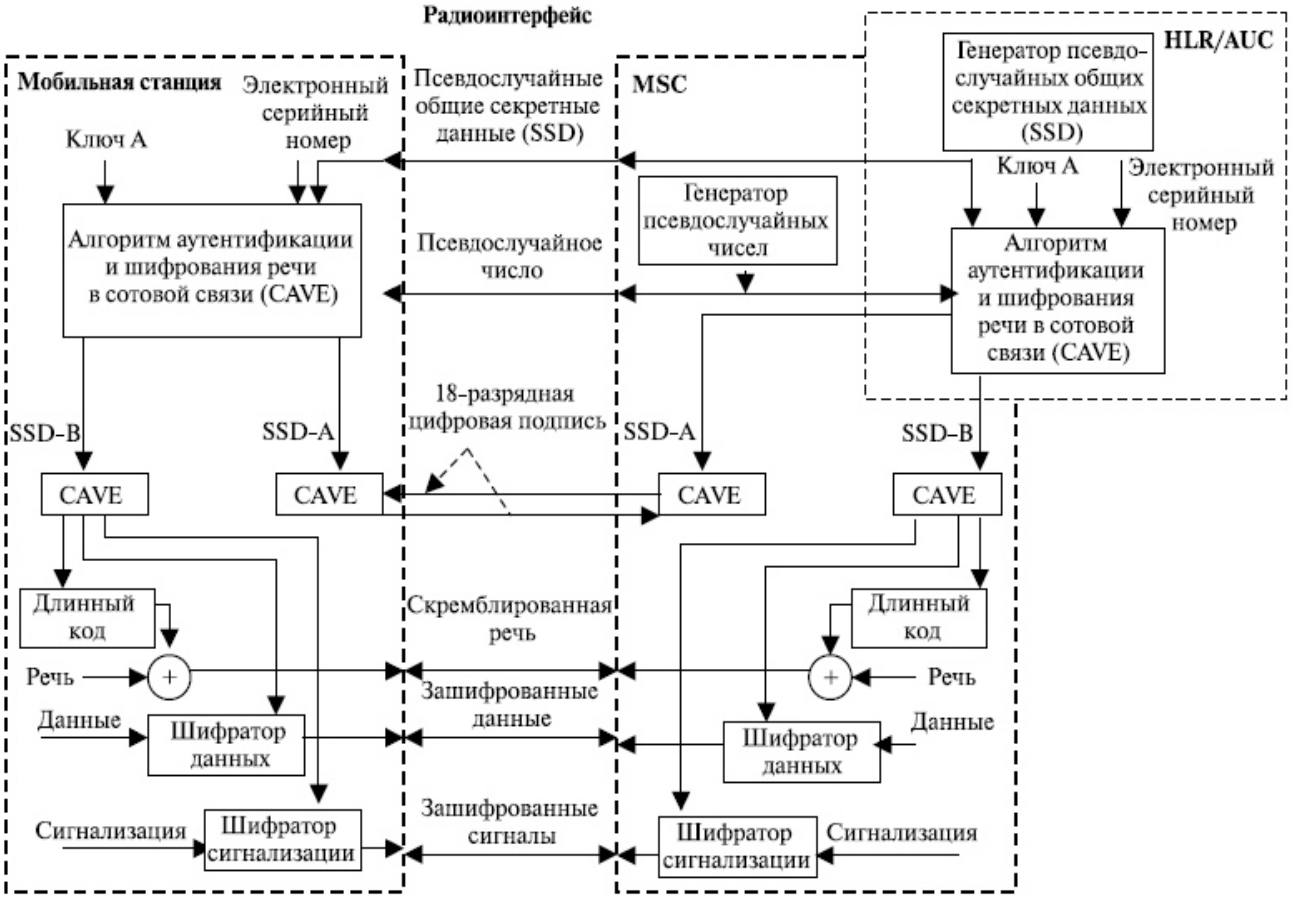

Рис. 2.4. Архитектура системы безопасности сети 3G (CDMA 2000)

В архитектуре безопасности сетей 3G выявляются следующие уровни безопасности:

- безопасность доступа к сети: защита радиоинтерфейса от злоумышленников как на начальной стадии установления соединения с сетью доступа, так и в процессе информационного обмена с обслуживающей сетью.

- безопасность на сетевом уровне: обеспечение безопасности сетевой инфраструктуры (узлы связи, проводные и радиорелейные линии) от атак, приводящих к нарушению режима сетевого обслуживания.

- безопасность на пользовательском уровне: использование вставляемого в трубку идентификационного модуля, для защиты терминала от клонирования.

- безопасность на прикладном уровне: обеспечение засекречивания информации в процессе обмена между приложениями пользователя и сервис-провайдера.

- контроль за трафиком и конфигурацией сети: проведение статистического анализа и отслеживание любых подозрительных изменений в трафике и конфигурации сети.

Таким образом переход к новым поколениям сетей сотовой связи влечёт за собой рост числа процедур механизмов аутентификации (рис. 2.5.) и усложнение архитектуры системы обеспечения безопасности.

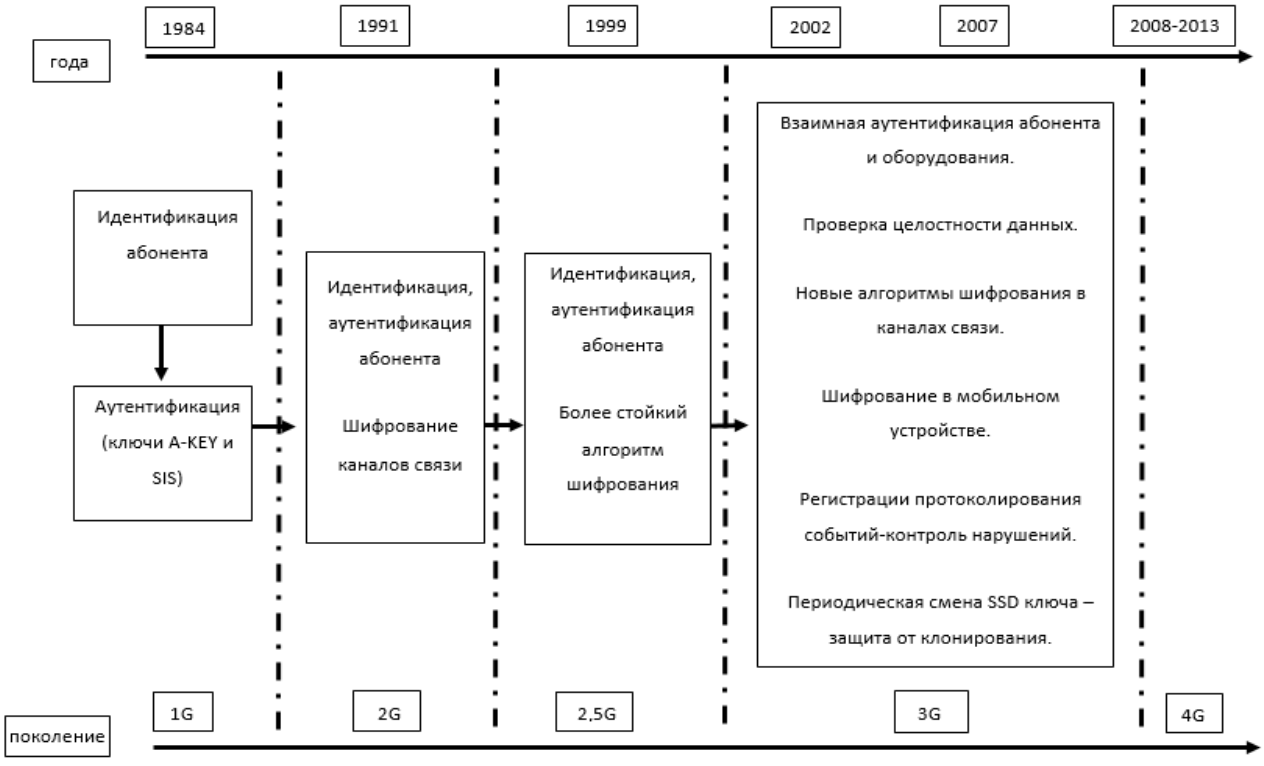

Рис. 2.5. Эволюция механизмов обеспечения безопасности в сетях сотовой связи.

В целом, как показывают представленные тенденции эволюции систем безопасности, переход к сетям следующих поколений (4G) ещё в большей степени обострит проблему выбора компромиссных решений между новыми потенциальными видами угроз и материальными ресурсами, которые необходимо затратить на борьбу с мошенничеством в сетях сотовой связи. При этом, в соответствии с прогнозами, существенно возрастёт относительная доля потерь операторов от человеческого фактора, связанного с инсайдерским мошенничеством.

2.3. Безопасность в сетях LTE

Безопасность в сетях LTE заключается в нескольких видах:

- Защита абонентов.
- Защита передаваемых сообщений.
- Шифрование сообщений.
- Аутентификация и абонента, и сети.

Защита абонента заключается в том, что в процессе обслуживания его скрывают временными идентификаторами.

Для закрытия данных в сетях LTE используется потоковое шифрование методом наложения на открытую информацию псевдослучайной последовательности (ПСП) с помощью оператора XOR (исключающее или). В этих сетях для обеспечения безопасности внутри сети применяется принцип туннелирования соединений. Шифрации можно подвергать пакеты S1 и X2 при помощи IPsec ESP, а также подвергаются шифрации сигнальные сообщения этих интерфейсов.

В момент подключения или активизации абонентского оборудования (UE) в сети, сеть запускает процедуру аутентификации и соглашения о ключах AKA (Authentication and Key Agreement). Целью этой процедуры является взаимная аутентификация абонента и сети и выработка промежуточного ключа K_{ASME}. Работа механизма AKA занимает доли секунды, которые необходимы для выработки ключа в приложении USIM и

для установления соединения с Центром регистрации (HSS). Вследствие этого, для достижения скорости передачи данных сетей LTE необходимо добавить функцию обновления ключевой информации без инициализации механизма AKA. Для решения этой проблемы в сетях LTE предлагается использовать иерархическую ключевую инфраструктуру. Здесь также, как и в сетях 3G, приложение USIM и Центр аутентификации (AuC) осуществляет предварительное распределение ключей. Когда механизм AKA инициализируется для осуществления двусторонней аутентификации пользователя и сети, генерируются ключ шифрования CK и ключ общей защиты, которые затем передаются из ПО USIM в Мобильное оборудование (ME) и из Центра аутентификации в Центр регистрации (HSS). ME и HSS, используя ключевую пару (CK;IK) и ID используемой сети, вырабатывает ключ K_{ASME}. Установив зависимость ключа от ID сети, Центр регистрации гарантирует возможность использования ключа только в рамках этой сети. Далее K_{ASME} передается из Центра регистрации в устройство мобильного управления (MME) текущей сети, где он используется в качестве мастер-ключа. На основании K_{ASME} вырабатывается ключ $K_{nas\text{-}enc}$, который необходим для шифрования данных протокола NAS между мобильным устройством (UE) и MME, и $K_{nas\text{-}int}$, необходимый для защиты целостности. Когда UE подключается к сети, MME генерирует ключ KeNB и передает его базовым станциям. В свою очередь, из ключа KeNB вырабатывается ключ Kup-enc, используемый для шифрования пользовательских данных протокола U-Plane, ключ Krrc-enc для протокола RRC (Radio Resource Control - протокол взаимодействия между Мобильными устройствами и базовыми станциями) и ключ Krrc-int, предназначенный для защиты целостности.

Алгоритм аутентификации и генерации ключа представлен на рис. 2.6:

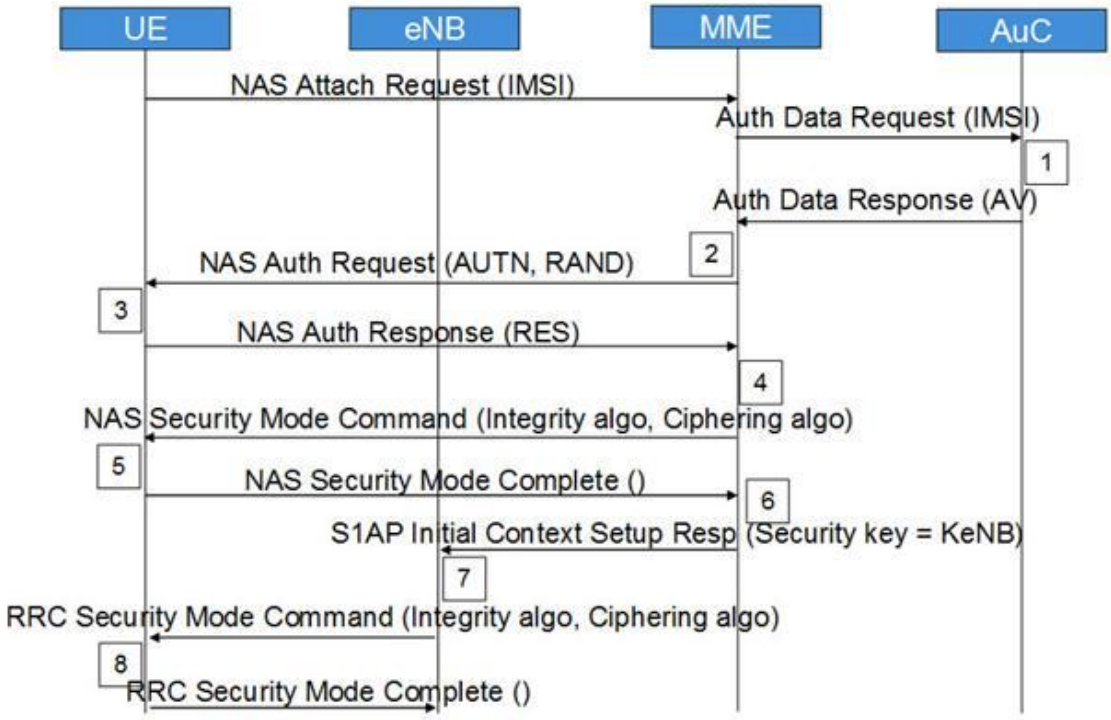

Рис. 2.6 Диаграмма аутентификации и генерации ключа

Здесь:

Шаг 1. Запрос о подключении к сети от мобильной станции (UE). MME запрашивает аутентификационные данные, относящиеся к конкретному IMSI, отправляя Authentication Data Request. AuC/HSS выбирает PSK, относящийся к конкретному IMSI и вычисляет аутентификационные данные по PSK. AuC/HSS отправляет обратно AV с Authentication Data Response.

Шаг 2. MME получает IK, CK, XRES, RAND и AUTH из AV. MME отправляет AUTH и RAND при помощи Authentication Request к UE.

Шаг 3. UE аутентифицирует NW, проверяя полученный AUTH. После чего вычисляет IK, CK, RES, XMAC из своего ключа защиты, AMF, (OP), AUTH и RAND. Она отправляет RES с Authentication response.

Шаг 4. После получения RES, MME сравнивает его с XRES и если они совпадают, то аутентификация прошла успешно, в противном случае, MME отправляет сбой аутентификации (Authentication failure) к UE. MME сбрасывает счетчик DL NAS. Рассчитывает KASME, KeNB, Knas-int, Knas-enc. Отправляет NAS команду режима безопасности (алгоритм целостности,

алгоритм шифрования, NAS набор ключей ID, функцию безопасности UE) с целостностью охраняемых, но не зашифрованных, используя Knas-inc.

Шаг 5. После получения NAS команды режима безопасности, UE вычисляет KASME, KeNB, Knas-int, Knas-enc. UE отправляет NAS режима безопасности выполнен с целостностью, защищенных и зашифрованных.

Шаг 6. После получения NAS команды режима безопасности от UE, MME отправляет KeNB в eNB с S1AP первоначальная установка начального контекста (ключ защиты).

Шаг 7. После получения KeNB, eNB вычисляет Krrc-int, Krrc-enc, Kup-enc. Затем оно отправляет RRC ключ защиты команду с AS целостностью алгоритма и AS шифрующий алгоритм.

Шаг 8. После получения RRC команды ключа защиты UE вычисляет Krrc-int, Krrc-enc, Kup-enc. UE отправляет RRC выполненный ключ шифрования на eNB.

После всех описанных действий, все NAS и AS сообщения будут надежно защищены и зашифрованы, в отличие от пользовательских данных, которые будут только шифроваться. (рис.2.7)

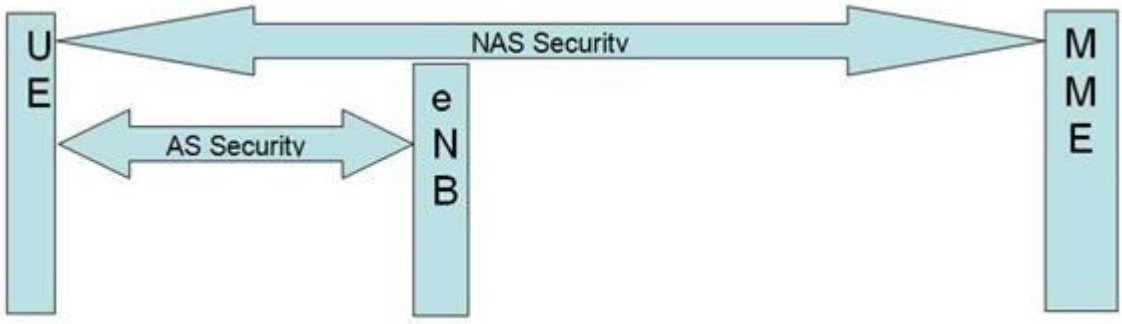

Рис.2.7. Слои безопасности

Архитектура безопасности LTE определяет механизм безопасности и для уровня NAS и для уровня AS.

Безопасность NAS (слоя без доступа):

Выполнена для NAS сообщений и принадлежит области UE и MME.

В этом случае необходима при передаче сообщений NAS между UE и MME – целостность, защищенная и зашифрованная с дополнительным заголовком безопасности NAS.

Безопасность AS (слоя с доступом):

Выполнена для RRC и плоскости пользовательских данных, принадлежащих области UE и eNB. Уровень PDCP на сторонах UE и eNB отвечает за шифрование и защиту целостности.

RRC сообщения защищены целостностью и зашифрованы, однако данные U-Plane только зашифрованы.

Для генерации векторов аутентификации используется криптографический алгоритм с помощью однонаправленных функций (f1, f2, f3, f4, f5) когда прямой результат получается путем простых вычислений, а обратный результат не может быть получен обратным путем, то есть не существует эффективного алгоритма получения обратного результата. Для этого алгоритма используется случайное 128 битное случайное число RAND, мастер-ключ K абонента, также 128 бит и порядковый номер процедуры SQN (Sequence Number). Счетчик SQN меняет свое значение при каждой генерации вектора аутентификации. Похожий счетчик SQN работает и в USIM. Такой метод позволяет генерировать каждый раз новый вектор аутентификации, не повторяя предыдущий уже использованный вектор аутентификации.

Помимо этих трех исходных величин: SQN, RAND и K в алгоритме f1 участвует поле управления аутентификацией Authentication Management Field (AMF), а в алгоритмах f2 – f5 исходные параметры – RAND и K, что и продемонстрировано на рис. 2.8, 2.9. На выходах соответствующих функций получают Message Authentication Code (MAC) - 64 бита; XRES – eXpected Response, результат работы алгоритма аутентификации <32 – 128 бит>; ключ шифрации CK, генерируемый с использованием входящих (K,RAND)->f3->CK; ключ целостности IK, сгенерированный с использованием входящего

(K,RAND)->f4->IK; и промежуточный ключ Anonymity Key (AK), генерируемый с помощью (K,RAND)->f5->AK - 64 бита.

При обслуживании абонента сетью E-UTRAN ключи CK и IK в открытом виде в ядро сети не передают. В этом случае HSS генерирует K_{ASME} с помощью алгоритма KDF (Key Derivation Function), для которого исходными параметрами являются CK и IK, а также идентификатор обслуживающей сети и SQNÅAK. Вектор аутентификации содержит RAND, XRES, AUTN и K_{ASME}, на основе которого происходит генерация ключей шифрации и целостности, используемых в соответствующих алгоритмах.

Когда мобильная станция получает из ядра сети три параметра (RAND, AUTN и KSI_{ASME}, где KSI – Key Set Identifier, индикатор установленного ключа, однозначно связанный с K_{ASME} в мобильной станции).

После чего используя RAND и AUTN, USIM на основе алгоритмов безопасности, тождественных хранящимся в HSS, производит вычисление XMAC, RES, CK и IK.

Затем в ответе RES UE передает в MME вычисленное RES, которое должно совпасть с XRES, полученным из HSS. Так сеть аутентифицирует абонента. Вычислив XMAC, UE сравнивает его с MAC, полученным ею в AUTN. При успешной аутентификации абонентом сети (MAC = XMAC) UE сообщает об этом в ответе RES. Если аутентификация сети не удалась (MAC ≠ XMAC), то UE направляет в MME ответ CAUSE, где указывает причину неудачи аутентификации.

При успешном завершении предыдущего этапа MME, eNB и UE производят генерацию ключей, используемых для шифрации и проверки целостности получаемых сообщений. В E-UTRAN имеется иерархия ключей, которая приведена на рис. 2.10.

Векторы аутентификации (рис.2.8, 2.9):

Ключи IK и CK генерируются и в центре аутентификации, и в USIM;

Ключ AK генерируется только в центре аутентификации;

Ответ XRES генерируется только в центре аутентификации, а RES генерируется в USIM;

Код MAC генерируется только в центре аутентификации, а соответствующий ему параметр XMAC генерируется в USIM;

Маркер AUTH генерируется только в центре аутентификации.

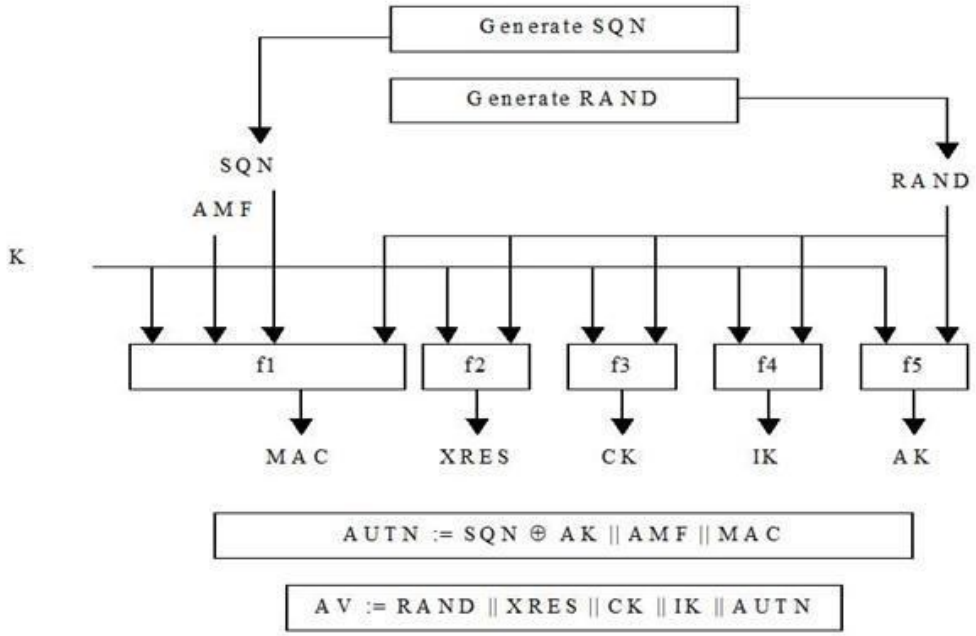

Рис.2.8. Создание векторов на передающей стороне

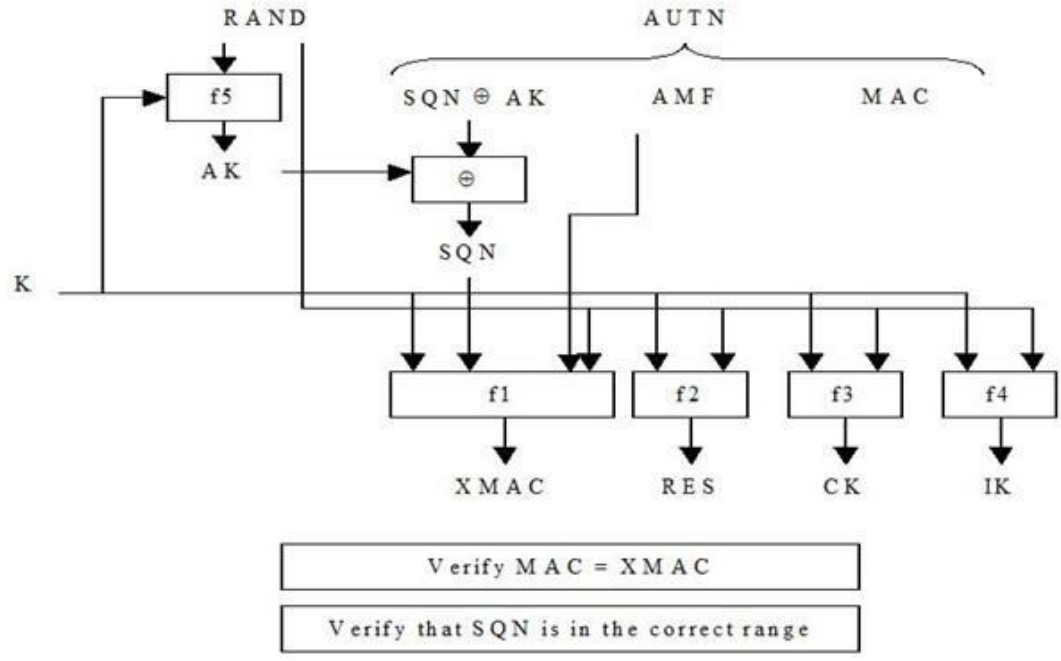

Рис.2.9. Преобразование векторов на приемной стороне (в USIM)

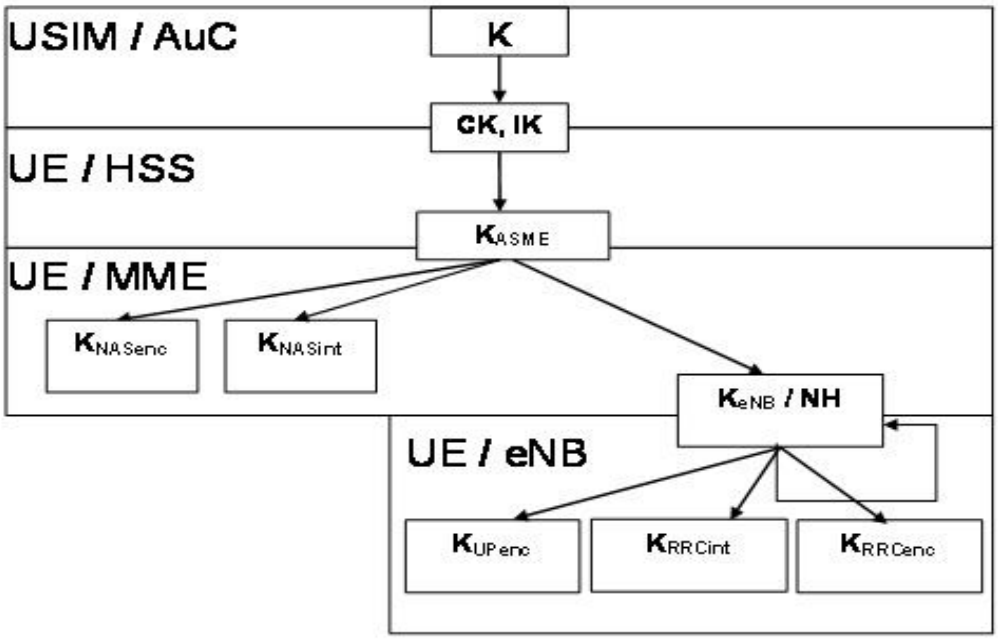

Рис. 2.10. Иерархия ключей в E-UTRAN

Исходным ключом для всей цепочки является K_{ASME} (256 бит). При передаче в радиоканале защиту обеспечивают для сигнального трафика (Control Plane) и для пользовательских пакетов (User Plane). При этом все сообщения сигнализации разделяют на сквозные сигнальные сообщения между UE и MME протоколов MM и SM (NAS – Non Access Stratum) и сигнальные сообщения между eNB протокола RRC (AS – Access Stratum).

Для шифрации и защиты целостности можно использовать разные базовые алгоритмы:

- UEA2 (UMTS Encryption Algorithm 2) и UIA2 (UMTS Integrity Algorithm 2);
- разработанные для стандартов 3G,AES (Advanced Encryption Standard).

Сигнальные сообщения протокола RRC (AS) также шифруют и обеспечивают их целостность. Пакеты трафика только шифруют. Эти операции производят в обслуживающей eNB и UE. Схема получения ключей шифрации и целостности для AS и UP трафика отличается от предыдущего случая тем, что исходным параметром здесь служит вторичный промежуточный ключ KeNB (256 бит). Этот ключ генерируют, также

используя KDF, где входными параметрами являются: KASME, счетчик сигнальных сообщений NAS вверх, прежнее значение KeNB, идентификатор соты и номер частотного канала в направлении вверх. Следовательно, при каждой периодической локализации UE происходит изменение KeNB.

Также KeNB меняется и при хэндовере; при этом в алгоритме генерации нового KeNB можно использовать дополнительный параметр NH (Next Hop), фактически счетчик числа базовых станций, по цепочке обслуживающих абонента. Все реализуемые процедуры безопасности в сети E-UTRAN продемонстрированы на рис. 2.11.

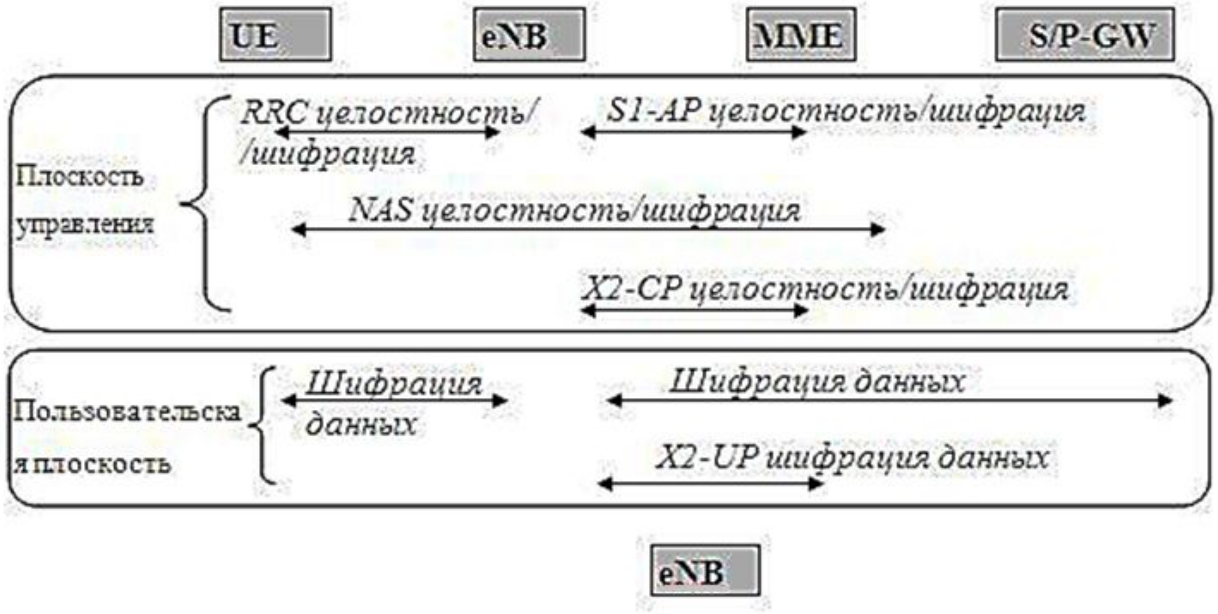

Рис. 2.11. Реализуемые процедуры безопасности в сети E-UTRAN

Алгоритм шифрации и дешифрации сообщений представлен на рис. 2.12.

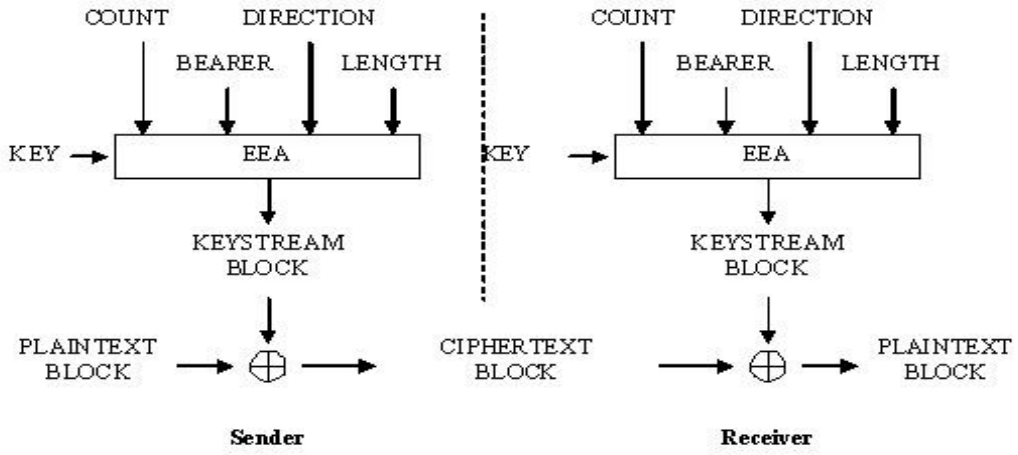

Рис. 2.12. Алгоритм шифрации в E-UTRAN

Исходными параметрами в этом алгоритме являются шифрующий ключ KEY (128 бит), счетчик пакетов (блоков) COUNT (32 бита), идентификатор сквозного канала BEARER (5 бит), указатель направления передачи DIRECTION (1 бит) и длина шифрующего ключа LENGTH. В соответствии с выбранным алгоритмом шифрации EEA (EPS Encryption Algorithm) вырабатывается шифрующее число KEYSTREAM BLOCK, которое при передаче складывают по модулю два с шифруемым исходным текстом блока PLAINTEXT BLOCK. При дешифрации на приемном конце повторно совершают эту же операцию.

Процедура защиты целостности сообщения состоит в генерации “хвоста“ MAC (Message Authentication Code) (32 бита), присоединяемого к передаваемому пакету. Алгоритм генерации MAC и проверки целостности полученного пакета путем сравнения XMAC с MAC (они должны совпасть) отображен на рис. 2.13.

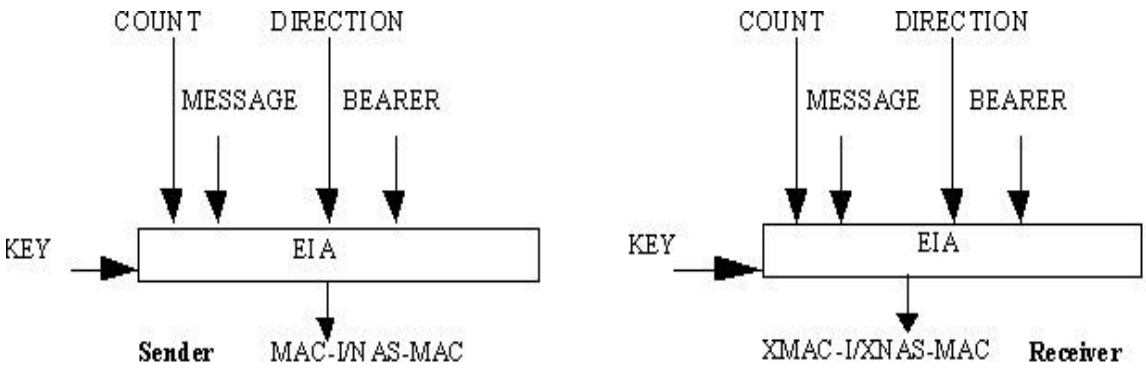

Рис. 2.13. Алгоритм проверки целостности в E-UTRAN

В алгоритме EIA (EPS Integrity Algorithm) использован ключ целостности KEY (128 бит), счетчик сообщений COUNT (32 бита), идентификатор сквозного канала BEARER (5 бит), указатель направления передачи DIRECTION (1 бит) и само сообщение MESSAGE.

3. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ. ЭКОЛОГИЯ

3.1. Анализ производственной среды

Под производственной средой понимается все то, что окружает человека.

Сюда входят организация производственного процесса, использование материалов, инструментов, оборудования, организация производственных помещений и комфортных условий труда.

В любом случае для изучения охраны труда важна связь между человеком и производственной средой.

Производственную среду принято характеризовать двумя параметрами:

1. Физическими параметрами – к ним относятся:

- Характер микроклимата
- Уровень освещенности, шумов, вибрации, радиации, электромагнитных излучений
- Атмосферное давление
- Цветоритм
- Характер оборудования

2. Химические параметры – сюда относятся:

- Естественный состав атмосферного воздуха
- Наличие в атмосферном воздухе вредных выделений

По особенности восприятия человеком этих параметров можно выделить две группы факторов:

1. факторы мобилизирующие организм
2. факторы, приводящие к динамическому рассогласованию.

На человека воздействуют:

1. производственные опасности – это неправильно организованное рабочее место, наличие не огражденных деталей механизмов, которые могут ударить при прикосновении, возможность электропоражения, необходимость совершать много лишних непроизводственных движений.

По всем этим причинам повышается утомляемость человека. В результате производственных опасностей человек может получить травму.

Производственной травмой называется физическое нарушение тканей или органов человека под воздействием производственной среды.

2. Производственные вредности – это нарушение санитарно-гигиенических условий в условиях производственного помещения, неудовлетворительный микроклимат, наличие в воздухе вредных выделений, химически активных веществ, повышенный уровень шума, плохое освещение, т.е. любые причины приводящие к возникновению профессиональных заболеваний.

Профессиональным заболеванием называется резкое или постепенное ухудшение здоровья человека под воздействием вредных факторов производственной среды.

Причины профессиональных заболеваний могут быть:

1. Объективными причинами – относятся физические особенности каждого конкретного человека и его склонность к появлению определенных заболеваний.

2. Субъективными причинами – относятся все причины, связанные с неправильной организацией трудового процесса и рабочего места.

3.2. Обеспечение безопасности жизнедеятельности в чрезвычайных ситуациях

Обеспечение безопасности жизнедеятельности в ЧС представляет собой комплекс организационных, инженерно-технических мероприятий и средств, направленных на сохранение жизни и здоровья человека во всех сферах его деятельности.

В качестве основных направлений в решении задач обеспечения безопасности жизнедеятельности могут рассматриваться следующие:

—прогнозирование и оценка возможных последствий ЧС;

—планирование мероприятий по предотвращению или уменьшению вероятности возникновения ЧС, а также сокращению масштабов их последствий;

—обеспечение устойчивой работы объектов народного хозяйства в ЧС;

—обучение населения действиям в ЧС;

— ликвидация последствий чрезвычайных ситуаций. Рассмотрим коротко содержание каждого из этих направлений.

Прогнозирование и оценка возможных последствий ЧС Прогнозирование чрезвычайных ситуаций — метод ориентировочного выявления и оценки обстановки, складывающейся в результате стихийных бедствий, аварий и катастроф. В отличие от прогнозирования во многих естественных науках, где оно имеет целью приспособить действия к ожидаемому состоянию, в безопасности жизнедеятельности его значение определяется степенью использования полученных данных для изменения обстановки. При этом сложность заключается в том, что требуется оценить район, характер и. масштабы ЧС в условиях неполной и ненадежной информации, а на их основе ориентировочно определить характер и. объем работ по ликвидации последствий ЧС.

В настоящее время хорошо изучены и определены сейсмические районы, районы и места возможных обвалов и селевых потоков, установлены границы зон возможного затопления при разрушении плотин, при наводнениях, а также выявлены промышленные объекты, аварии на которых могут привести к большим разрушениям, поражениям людей, заражению территории. Это долгосрочный прогноз.

В задачу прогнозирования в области безопасности жизнедеятельности входит также ориентировочное определение времени возникновения ЧС (краткосрочный прогноз), по которому принимаются оперативные решения по обеспечению безопасности населения во всех сферах его деятельности. В настоящее время усилия многих ученых и специалистов направлены на

поиски надежных способов прогнозирования процесса формирования и начала ЧС. Наметились реальные, возможности прогнозирования начала некоторых стихийных бедствий. При этом используются расчетные статистические данные цикличности солнечной активности, данные, полученные с искусственных спутников Земли, а также данные метеорологических, сейсмических, вулканических, противоселевых, противолавинных и других станций. Например, ураганы, тайфуны, извержение вулканов, селевые потоки прогнозируются с помощью метеорологических спутников Земли. Прогнозирование землетрясений возможно путем систематических анализов химического состава воды в сейсмических районах, измерением упругих, электрических и магнитных характеристик грунта, наблюдение за изменением уровня поды в колодцах, поведением животных, пресмыкающихся, рыб, птиц. Широко практикуется прогнозирование лесных, торфяных и других ландшафтных пожаров по комплексному показателю на основе суммирования коэффициентов, учитывающих температурные, географические, погодные, статистические и другие условия. Для поиска скрытых очагов пожара (торфяные, подземные) и тем самым прогнозирования угрозы возникновения лесных пожаров применяется инфракрасная аппаратура для съемки с самолетов и спутников Земли,

Прогнозирование обстановки, связанной с возникновением ЧС осуществляется математическими методами.

Исходными данными для. прогнозирования обстановки являются; места (координаты) потенциально опасных объектов и запасы веществ или энергии; численность и плотность населения; характер построек, количество и тип защитных сооружений, их вместимость и другие сведения. При прогнозировании учитываются метеорологические условия, характер местности.

При прогнозировании обстановки в зависимости от вида ЧС определяются границы зон разрушения, катастрофического затопления,

пожаров и заражения (радиационного, химического и бактериологического), а также возможные потери населения и ущерб, наносимый объектам народного хозяйства.

Данные прогнозирования обстановки в очагах поражения обобщаются, анализируются и делаются выводы для принятия решения, связанного с организацией и ведением спасательных и других неотложных работ.

Как использовать прогнозы, которые можно сделать сегодня — неточные и недостаточно - надежные? Обеспечение безопасности жизнедеятельности в ЧС — далеко не единственная область, где приходится принимать решения на основе неполной и ненадежной информации.

Для решения рассматриваемой проблемы в этих условиях изначально нужен иной, системный подход, «новая философия» обеспечения безопасности человека в ЧС, включая как предотвращение и уменьшение вероятности их возникновения, так и сокращение масштабов их последствий.

На данной методологической основе с учетом отечественного и зарубежного практического опыта можно заранее подготовить комплекс мероприятий нарастающей эффективности и в зависимости от текущих прогнозов ЧС выбирать ту или иную их совокупность, т. е. ввести в действие многостадийную систему обеспечения безопасности жизнедеятельности человека в современной техносоциальной среде.

Мероприятия, необходимые для предотвращения ущерба от ЧС, можно сгруппировать следующим образом.

Фоновые (постоянно проводимые) мероприятия, основанные на долгосрочном прогнозе: выполнение строительно-монтажных работ с учетом требований СНиП, создание надежной системы оповещения населения об опасностях; накопление фонда защитных сооружений и обеспечение населения СИЗ; организация радиационного, химического и

бактериологического наблюдения, разведки и лабораторного контроля; всеобщее обязательное обучение населения правилам поведения и действиям в ЧС; проведение режимных, санитарно-гигиенических и противоэпидемических мероприятий; отказ от строительства АЭС, химических и целлюлозно-бумажных и других потенциально опасных объектов в экономически уязвимых зонах; перепрофилирование объектов — источников повышенной опасности для здоровья и жизни людей; разработка, материальное, финансовое обеспечение и практическая отработка планов ликвидации последствий ЧС и т. и.

Защитные мероприятия, которые необходимы, когда предсказан момент ЧС: развертывание системы наблюдения и разведки, необходимых для уточнения прогноза; приведение в готовность системы оповещения населения о ЧС; ввод в действие специальных правил функционирования экономики и общественной жизни, вплоть до чрезвычайного положения; нейтрализация источников повышенной опасности при ЧС (АЭС, токсичных и взрывоопасных производств и т. п.), прекращение операций с ними, дополнительного укрепления или демонтажа; приведение в готовность аварийно-спасательных служб; частичная эвакуация населения.

Как следует из этого перечня, для осуществления ряда важнейших мероприятий нужны многие годы и следовательно, долгосрочный прогноз. Другие, но менее важные мероприятия можно осуществить быстро, но на короткое время. Для таких мероприятий необходим краткосрочный прогноз. Для осуществления многих защитных мероприятий необязательно точно знать время возникновения ЧС, и их характера; разные мероприятия можно начинать при разной определенности предсказаний.

Эти соображения и определяют выбор конкретного набора защитных мероприятий. Исходными материалами должны служить каталог возможных мероприятии и оценкой их стоимости и предотвращенного ими ущерба а также набор типовых сценариев (вариантов) действий.

В настоящее время ученые и специалисты не в состоянии заранее с высоким уровнем достоверности точно указать место, время и последствия той или иной ЧС.

3.3. Затраты на охрану окружающей среды и природных экосистем

До определения затрат на экологизацию экономики и производства следует остановиться на том, к каким издержкам готово современное общество ради поддержания качества среды. В сложившейся системе взглядов выделяют три подхода, условно названные экстенсивным, экономическим и глобальным. Крайние сторонники *экстенсивного направления* считают существующую практику техногенной экспансии неизбежной, а природоохранные усилия и затраты - неэффективными или даже бесполезными, лишь замедляющими экономический рост. Угроза исчерпания ресурсов и экологического кризиса воспринимается ими лишь как стимул научно-технического прогресса, человеческой изобретательности и предприимчивости. Неудивительно, что такой технократический цинизм минимизирует и оценки экологического ущерба, и компенсационные затраты.

Представители *экономического подхода* ограничивают природоохранные затраты сопоставлением с текущими экономическими результатами на основе временно согласованных нормативов. При этом избираются самые дешевые природоохранные и средозащитные меры, затраты на которые перекрываются достигнутым с их помощью предотвращением ущерба. Такой результат почему-то называют экономическим оптимумом качества природной среды, хотя мыслимы и бывают ситуации, когда этот «оптимум» соответствует ПДК загрязнителя или даже временно согласованным нормативам. Экономический подход, опирающийся на несовершенные нормативы и принимающий долговременные эффекты и последствия лишь в виде оговорок, явно недооценивает экономические убытки, вызванные экологическим неблагополучием. Правда, как раз в рамках этого подхода разработаны

методы определения экономического ущерба и экономической эффективности природоохранных мероприятий.

Глобальное направление опирается на идею эколого-экономической сбалансированности и строится на самом полном учете экологических и социальных составляющих в долговременных целях общества. Естественно, что при этом оценки необходимых затрат достигают самых больших значений. Но и в этом направлении существуют расхождения, определяемые мерой оптимизма по отношению к реальным перспективам экоразвития.

По оценкам западных экономистов, совокупные национальные затраты, гарантирующие сохранение качества среды обитания и благополучие природных объектов, могут составлять до 8-10% ВНП. Часто ставят вопрос о разумной величине вложений в охрану природной среды, имея в виду, что «такие вложения тормозят темпы экономического и социального развития, поскольку вкладываемый в защиту природы капитал практически не дает отдачи с точки зрения производства и в явном виде не ведет к повышению материального уровня жизни населения» (Тихомиров, 1992). К несчастью, это суждение широко распространено. Оно уходит корнями в затратную концепцию прежней экономической практики и основано на глубокой недооценке экологической обусловленности экономики. Но если общество признает своей главной целью здоровье человеческой популяции, то явно следует отказаться от остаточного принципа в деле сохранения среды обитания и охраны природы. С позиций экоразвития, *граница разумных затрат проходит как раз там, где объем вложений гарантирует стабилизацию качества среды обитания и основных процессов биосферы.* Если общество не посчитает эти расходы разумными, то в скором будущем, по прогнозам ученых, они составят 40-50% ВНП.

Все общественные издержки, связанные с необходимостью сохранить надлежащее качество окружающей природной среды, можно подразделить на предупреждающие затраты - *предзатраты, экономический ущерб* и затраты

на ликвидацию, нейтрализацию и компенсацию уже допущенных экологических нарушений - *постзатраты*.

Сумма упреждающих затрат стремится к некой идеальной стоимости полного экологического благополучия, но практически никогда не достигает ее, так как какая-то часть экологического ущерба, обусловленного деятельностью человека, принципиально неустранима. Если все предзатраты сделаны сполна и эффективно реализованы, то обеспечивается экологически сбалансированное развитие, причем без обязательного сокращения экономического роста. Если же предзатраты не произведены или неполны, что фактически и происходит, то хозяйственная и иная человеческая деятельность приводит к негативным экологическим эффектам, наносящим значительный экономический ущерб. Величина этого ущерба всегда намного больше, чем недостаток предзатрат, так как постоянно растет со временем. Поэтому и постзатраты, даже если они сделаны полно и своевременно, всегда намного больше предзатрат («скупой платит дважды»). Если ущерб не нейтрализован постзатратами, то потери общества продолжают расти, так как экологический ущерб, причиненный людьми, никогда сам по себе не сходит на нет, а только увеличивается со временем, увеличивая долг людей перед потомками и природой.

Основными источниками капитальных затрат в природоохранной сфере остаются средства предприятий и организаций всех форм собственности. Из федерального бюджета финансировалось незначительное число мероприятий, включенных в федеральные программы и деятельность природоохранных ведомств.

Плана действий по реализации решений Конференции ООН по окружающей среде и развитию» содержатся следующие рекомендации:

- разработать и внедрить систему территориальных кадастров природных ресурсов, включающих их стоимостные оценки;
- сформировать систему экологических ограничений и регламентации режимов природопользования;

- осуществить мероприятия по развитию и поддержке экологического предпринимательства и совершенствованию законодательства в интересах развития рынка экологических услуг.

Плата за природные ресурсы включает и платежи на восстановительное природопользование, поддержание возобновимых ресурсов территорий в устойчивом продуктивном состоянии (рыборазведение, агролесомелиорация, противоэрозионные меры, рекультивация и др.). Соответствующие нормативы платы определяются на основании объема затрат на восстановление природных объектов и проведение мероприятий по их охране, на создание и ведение системы государственного контроля за состоянием природных ресурсов и иные мероприятия.

ЗАКЛЮЧЕНИЕ

В связи с тем, что вся передаваемая информация в сотовой телефонии посылается через радиоканал, любой, обладающий соответствующим оборудованием, может прослушивать все телефонные разговоры, ведущиеся в зоне приема без опасения быть обнаруженным. При проектировке ранних систем сотовой телефонии обеспечению безопасности уделялось не так много внимания в связи с тем, что высокая цена необходимого для прослушивания оборудования делала его экономически нецелесообразным. Когда же подобные устройства стали широко распространенными и доступными по цене, проблему попытались решить с помощью создания соответствующей законодательной базы. Но введение правовых норм ситуации не изменило, и проектировщики систем для решения проблемы были вынуждены все в большей и большей степени обращаться за помощью к криптографии и, как оказалось, не зря. Криптографические методы являются одним из самых очевидных и эффективных способов предотвращения несанкционированного доступа к каналам связи и дублирования аппаратов, и вскоре они заслуженно нашли применение во всех последующих стандартах.

Основными целями защиты информации в МСС являются:

– достижение состояния информационной безопасности во всех звеньях МСС от внешних угроз, как в мирное время, так и в особый период, а также при возникновении чрезвычайных ситуаций;

– предотвращение нарушений прав личности, общества и государства на сохранение секретности и конфиденциальности информации, циркулирующей в МСС.

На основании целей формируются и задачи защиты информации в МСС:

– выявление и прогнозирование внутренних и внешних угроз информационной безопасности, разработка и осуществление комплекса

адекватных и экономически обоснованных мер по их предупреждению и нейтрализации;

– формирование единой политики государственной власти по защите информации в МСС;

– совершенствование и стандартизация применяемых методов и средств защиты информации в МСС;

– создание и реализация механизма государственного регулирования (лицензирования) деятельности в области защиты информации, а также обеспечение функционирования системы сертификации МСС и входящих в их состав защищенных технических средств, средств защиты информации и средств контроля эффективности применяемых мер защиты.

Система обеспечения защиты информации в каждой конкретной МСС, а также подход к ее построению и реализации индивидуальны. Однако во всех случаях для создания эффективной комплексной защиты информации В МСС необходимо:

– выявить все возможные факторы, влияющие на уязвимость информации, подлежащей защите, т.е. построить модель угроз информационной безопасности МСС и выявить каналы утечки.

– обосновать возможные методы защиты информации, направленные на устранение выявленных угроз.

– создать комплексную систему, обеспечивающую качественное решение задач защиты информации в МСС, основанную на минимизации ущерба от возможной утечки информации.

В данной выпускной работе выполнен анализ эволюции аспектов безопасности в сотовых системах связи. Также рассмотрены вопросы безопасности жизнедеятельности и экологии.

ЛИТЕРАТУРА

1. Доклад Президента Республики Узбекистан И.А. Каримова на заседании Кабинета Министров, посвященном итогам социально-экономического развития в 2015 году и важнейшим приоритетным направлениям экономической программы на 2016 год. (http://uza.uz/)

2. А.Л. Гельгор, Е.А. Попов «Технология LTE мобильной передачи данных” 2011 г. 205 с.

3. А.Абдукадиров, Д.Давронбеков. Мобильные системы связи поколения 4G. Учебное пособие. “O`quv-ta`lim metodika” DUK bosmaxonasi, - 2015 г. 328 с.

4. Максименко В.Н., Афанасьев В.В., Волков Н.В. «Защита информации в сетях сотовой подвижной связи» 2007 г. 360 с.

5. Чекалин А.А., Заряев А.В., Скрыль С.В., Вохминцев В.А.,Обухов А.Н., Хохлов Н.С., Немцов А.Д., Щербаков В.Б.,Потанин В.Е. «Защита информации в системах мобильной связи» 2005 г. 171 с.

6. Максименко В.Н., Кудин А.В., Ледовской А.И. «Безопасность и качество услуг сотовой подвижной связи. Терминологический справочник» 2014 г. 244 с.

7. А.Абдуазизов. Электралоқа назарияси. (Дарслик). – Т.: «Фан ва технология», 2011, 416 с.

8. В.В. Ломовицкий, А.И. Михайлов, К.В. Шестак, В.М. Щекотихин. Основы построения систем и сетей передачи информации. М.: Горячая линия - Телеком, 2005. 382 с.

9. Wolfgang Eberle. Wireless Transceiver Systems Design. Katholieke Universiteit Leuven. Interuniversity Microelectronics Center (IMEC). Leuven. Belgium. 2008 y. 289 p.

10. https://tuit.uz/

11. http://cyberleninka.ru/

12. http://www.infolib.uz/

ПРИЛОЖЕНИЕ