Дисциплина: **Информационная безопасность**

специальность: **09.03.03 Прикладная информатика**

курс, группа: **2 к 2 г**

форма обучения: за**очная**

преподаватель: **Астахов В.К.**

электронная почта преподавателя: **vadast@mail.ru**

**Литература**

**Основная**

1. Горбенко, А. О. Основы информационной безопасности (введение в профессию): учебное пособие / А. О. Горбенко. — СПб.: Интермедия, 2017. — 335 c. — ISBN 978-5-4383-0136-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/66797.html (дата обращения: 20.11.2019). — Режим доступа: для авторизир. пользователей
2. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — М.: ЮНИТИ-ДАНА, 2017. — 287 c. — ISBN 978-5-238-02857-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/72444.html (дата обращения: 20.11.2019). — Режим доступа: для авторизир. пользователей (гриф)
3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — Саратов Профобразование, 2017. — 702 c. — ISBN 978-5-4488-0070-2. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/63594.html (дата обращения: 20.11.2019). — Режим доступа: для авторизир. пользователей

**Дополнительная**

1. Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — ISBN 978-5-94774-821-5. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/52209.html (дата обращения: 20.11.2019). — Режим доступа: для авторизир. пользователей
2. Коваленко Ю.И. Методика защиты информации в организациях [Электронный ресурс]: монография / Ю.И. Коваленко, Г.И. Москвитин, М.М. Тараскин.— Электрон. текстовые данные. — М.: Русайнс, 2016. — 162 c. — 978-5-4365-0887-0. —Режим доступа: http://www.iprbookshop.ru/61625.html
3. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю. Н. Сычев. — Саратов: Вузовское образование, 2018. — 195 c. — ISBN 978-5-4487-0128-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/72345.html (дата обращения: 20.11.2019). — Режим доступа: для авторизир. пользователей

**Задания по темам и датам**

| **дата, время** **занятия** | **вид** **занятия** | **кол-во часов** | **вопросы для изучения и обсуждения** | **контрольные** **вопросы** |
| --- | --- | --- | --- | --- |
| 08.06.20209.00-10.30 | Консультация | 2 | 1. Актуальность проблемы обеспечения безопасности информации 1.1 Предмет защиты 1.2 Типовые структуры автоматизированных систем и объекты защиты в них 1.3 Угрозы безопасности информации и их классификация 1.4 Физическая защита объектов 1.5 Концептуальные основы для построения защиты информации от несанкционированного доступа в вычислительной системе 1.6 Концептуальные основы для проектирования защиты информа-ции от несанкционированного доступа в вычислительной системе 1.7 Организационные меры защиты информации в вычислительной сети | 1. Информация как объект правового регулирования.2. Меры защиты информации: законодательного, административного, процедурного, программно-технического уровней.3. Законодательство РФ в области информационной безопасности.4. Информационная безопасность объекта при осуществлении международного сотрудничества.5. Виды угроз информационной безопасности.6. Угрозы конституционным правам и свободам гражданина в области информационной деятельности.7. Угрозы информационному обеспечению государственной политики Российской Федерации.8.Угрозы безопасности информационных и телекоммуникационных средств и систем.9. Внешние и внутренние источники угроз информационной безопасности.10. Основные виды угроз безопасности субъектов информационных отношений.11. Основные непреднамеренные и преднамеренные искусственные угрозы.12. Основные преднамеренные искусственные угрозы.13. Закон РФ от 21.09.93 "О государственной тайне". |
| 08.06.202010.35-12.05 | Консультация | 2 | 2. Идентификация и аутентификация 2.1 Программно-аппаратная защита информации 2.2 Модели управления доступом 2.3 Типы моделей управления доступом 3. Криптография 3.1 Алгоритмы и ключи 3.2 Криптоанализ | 1. Свойства защищенных автоматизированных систем обработки информации.
2. Специфика возникновения угроз и рисков в открытых сетях.
3. Что понимается под уязвимостью защищенных компьютерных систем?
4. Основные направления обеспечения информационной безопасности в компьютерных системах.
5. Основные понятия безопасности компьютерных систем.
6. Что понимается под лицензированием деятельности в области защиты информации?
7. Перечислить основные мероприятия, позволяющие решить задачу построения системы защиты рабочей станции.
8. Для чего используются системы многоуровневой защиты?
9. Какие вы знаете аспекты защиты информации в системе с разграничением полномочий?
10. Перечислите и дайте характеристику основным методам построения систем защиты с многоуровневым доступом.
 |

**Рекомендации и требования к выполнению указанных заданий**

Изучить материал лекций и подготовиться к ответам на контрольные вопросы, которые входят в перечень вопросов к экзамену по дисциплине. Для подготовки использовать рекомендованную литературу и краткий конспект лекций, представленный ниже. Полный перечень вопросов представлен на официальном сайте, на основе которого составлены билеты. Дополнительно отчитываться по контрольным вопросам и присылать материал преподавателю не надо.

Краткий конспект лекции по дисциплине для консультаций:

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Содержание

[1. Актуальность проблемы обеспечения безопасности информации](http://www.chemisk.narod.ru/html/ib01.html#A1)

[1.1 Предмет защиты](http://www.chemisk.narod.ru/html/ib01.html#A1.1)

[1.2 Типовые структуры автоматизированных систем и объекты защиты в них](http://www.chemisk.narod.ru/html/ib01.html#A1.2)

[1.3 Угрозы безопасности информации и их классификация](http://www.chemisk.narod.ru/html/ib01.html#A1.3)

[1.4 Физическая защита объектов](http://www.chemisk.narod.ru/html/ib02.html#A1.4)

[1.5 Концептуальные основы для построения защиты информации от несанкционированного доступа в вычислительной системе](http://www.chemisk.narod.ru/html/ib02.html#A1.5)

[1.6 Концептуальные основы для проектирования защиты информации от несанкционированного доступа в вычислительной системе](http://www.chemisk.narod.ru/html/ib02.html#A1.6)

[1.7 Организационные меры защиты информации в вычислительной сети](http://www.chemisk.narod.ru/html/ib03.html#A1.7)

[2. Идентификация и аутентификация](http://www.chemisk.narod.ru/html/ib03.html#A2)

[2.1 Программно-аппаратная защита информации](http://www.chemisk.narod.ru/html/ib04.html#A2.1)

[2.2 Модели управления доступом](http://www.chemisk.narod.ru/html/ib04.html#A2.2)

[2.3 Типы моделей управления доступом](http://www.chemisk.narod.ru/html/ib05.html#A2.3)

[3. Криптография](http://www.chemisk.narod.ru/html/ib06.html#A3)

[3.1 Алгоритмы и ключи](http://www.chemisk.narod.ru/html/ib06.html#A3.1)

[3.2 Криптоанализ](http://www.chemisk.narod.ru/html/ib06.html#A3.2)

**1. Актуальность проблемы обеспечения безопасности информации**

Проблемы защиты информации от постороннего доступа и нежелательного воздействия на нее возникло с той поры, когда человеку по каким-либо причинам не хотелось делиться ею ни с кем или не с каждым человеком.

Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцам получить какой-либо выигрыш.
С переходом на использование технических средств связи, информация подвергается воздействию случайных процессов (неисправностям и сбоям оборудования, ошибкам операторов и т.д.), которые могут привести к ее разрушению, изменению на ложную, а также создать предпосылки к доступу к ней посторонних лиц.

С появлением сложных автоматизированных систем управления, связанных с автоматизированным вводом, хранением, обработкой и выводом информации, проблемы ее защиты приобретают еще большее значение.
Этому способствует:

1. Увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств вычислительной техники.
2. Сосредоточение в единых базах данных информации различного назначения и принадлежности.
3. Расширение круга пользователей, имеющих доступ к ресурсам вычислительной системы, и находящимся в ней массивам данных.
4. Усложнение режима функционирования технических средств, вычислительной системы (широкое внедрение многопрограммного режима разделения времени и реального времени).
5. Автоматизация межмашинного обмена информацией, в т.ч. и на больших расстояниях.
6. Увеличение количества технических средств и связей в автоматизированных системах управления (АСУ) и обработки данных.
7. Появление ПЭВМ, расширяющих возможности не только пользователя, но и нарушителя.
8. Индустрия переработки информации достигла глобального уровня.
9. Появление электронных денег. Создало предпосылки для хищения крупных сумм.
10. Появилось удивительное порождение научно-технических работников. Хакеры - прекрасные знатоки информационной техники. Кракеры. Фракеры - приверженцы электронного журнала Phrack.

В последнее время широкое распространение получило новое компьютерное преступление - создание компьютерных вирусов.

**1.1 Предмет защиты.**

**Свойства информации.**

Информация - это результат отражения и обработки в человеческом сознании многообразия окружающего мира. Это сведения об окружающих человека предметах, явлениях природы, деятельности других людей. Сведения, которыми обменивается человек через машину с другим человеком или машиной и являются предметом защиты. Однако, защите подлежит та информация, которая имеет цену. Для оценки требуется распределение информации на категории не только в соответствии с ее ценностью, но и важностью. Известно следующее распределение информации по уровню важности:

1. **Жизненно-важная**, незаменимая информация, наличие которой необходимо для функционирования организаций.
2. **Важная информация**, которая может быть заменена или восстановлена, но процесс восстановления очень труден и связан с большими затратами.
3. **Полезная информация** - это информация, которую трудно восстановить, однако организация может эффективно функционировать и без нее.
4. **Несущественная информация**.

Модель предмета защиты:


Рисунок 1.

В соответствии с описанными принципами деления, информацию, обрабатываемую в автоматизированных системах обработки данных (АСОД) для иллюстрации можно представить по категориям важности и секретности в виде пирамиды, состоящей из нескольких слоев по вертикали. Вершиной пирамиды является наиболее важная информация, а фундаментом - несущественная информация, но связанная с обработкой более важной информации. Каждый слой данной пирамиды, поделенный на части по горизонтали, отражает принцип деления информации по функциональному признаку и полномочиям ее пользователей.

Безопасность информации в АСО интерпретируется как опасность ее несанкционированного получения за все время нахождения в АСО, а также безопасность действий, для осуществления которых используется информация.
У информации в АСО есть свой жизненный цикл:


Рисунок 2.

Безопасные технологии - это технологии, которые не наносят материального ущерба субъектам, имеющим прямое или косвенное отношение к ним. Субъектом может быть государство, физические лица и др.
Технология - это совокупность методов переработки (преобразование исходного сырья, какими-либо средствами с целью получения конечной продукции). **Для правильного построения системы защиты необходимо определить:**

1. Виды воздействия на информацию.
2. Что из себя представляет автоматизированная система.
3. Какие существуют угрозы безопасности автоматизированных систем.
4. Меры противодействия угрозам безопасности.
5. Принцип построения систем защиты.

**Виды воздействия на информацию:**

1. *Блокирование информации.* Пользователь не может получить доступ к информации. При отсутствии доступа, сама информация не теряется.Причины:
	* отсутствие оборудования,
	* отсутствие специалиста,
	* отсутствие ПО.

1. *Нарушение целостности. Причины*:
	* утеря информации,
	* выход из строя носителя,
	* искажения:
		+ нарушение смысловой значимости,
		+ нарушение логической связанности,
		+ потеря достоверности.
2. *Нарушение конфиденциальности*. С информацией ознакомляются субъекты, которым это не положено. Уровень допуска к информации определяет ее владелец. Нарушение конфиденциальности может произойти из-за неправильной работы системы, ограничения доступа или наличия побочного канала доступа.
3. *Несанкционированное тиражирование*. Под защитой понимается защита авторских прав и прав собственности на информацию.

**1.2 Типовые структуры автоматизированных систем и объекты защиты в них.**

АСОИ - организационно-технические системы, представляющие собой совокупность компонентов:

1. Технические средства обработки и передачи данных
2. Системное и прикладное ПО
3. Информация на различных носителях
4. Персонал и пользователи системы

**Типовые структуры АС:**

1. *Автономные рабочие станции (АРС)*. Один или несколько ПК, не связанных между собой. На любом из них пользователи работают раздельно во времени. Обмен информацией осуществляется через сменные носители.
Объекты защиты в автономных рабочих станциях (АРС):
	* АРС,
	* сменные носители информации,
	* пользователи и обслуживающий персонал,
	* устройства визуального представления информации.
	* источники побочного электромагнитного излучения и наводок

ЛВС - создаются для коллективной обработки информации или совместного использования ресурса. Оборудование размещено в пределах одного помещения, здания или группы близкорасположенных зданий.

1. *Локальные системы коллективного пользования (ЛСКП).* Структура ЛСКП:
	* **без выделенного сервера или одноранговой сети** (не требует централизованного управления; любой пользователь делает доступными свои данные; используется однотипная ОС),
	* **с выделенным сервером** (требует централизованного административного управления. На РС и серверах могут быть установлены:
	* **многотерминальные системы на базе малых и больших компьютеров**. Основные ресурсы сосредоточены на сервере; РС - это терминалы; общее руководство осуществляет администратор; на центральном компьютере и РС используются различные ОС.
	* **многосегментные ЛС** - состоят из нескольких сегментов, любой из которых является сетью с выделенным сервером. Объединение осуществляется через мост, в качестве которого может использоваться либо выделенный сервер, либо специальной устройство. Любым сегментом управляет свой администратор. В любом сегменте может использоваться своя ОС.
	* **смешанные сети** - включают все вышерассмотренные системы.

 **Объекты защиты:**

* + все рабочие станции (РС),
	+ сервер и центральный компьютер,
	+ локальные каналы связи,
	+ реквизиты доступа.
1. *Глобальные системы коллективного пользования (ГСКП).* ГСКП - совместная обработка информации и совместное использование ресурсов. Отличия от ЛСКП:
	* Могут находиться на значительном удалении друг от друга.
	* Каналы связи не принадлежат собственнику системы.
	* Каналы связи являются коммутируемыми и взаимосвязанными.
	* Для использования каналов связи необходимо устройство сопряжения.
	* Подобные системы открыты и подключиться к ним могут все желающие.

**Объекты защиты:**

* + РС,
	+ глобальные каналы связи,
	+ информация, передаваемая по глобальным каналам связи,
	+ информация о реквизитах доступа в ГСКП.

**1.3 Угрозы безопасности информации и их классификация.**

***Угроза*** - это потенциально возможное событие, действие, процесс или явление, которое может привести к понятию ущерба чьим-либо интересам.
Нарушение безопасности - это реализация угрозы.

***Естественные угрозы*** - это угрозы, вызванные воздействием на АС объективных физических процессов, стихийных природных явлений, не зависящих от человека.

*Естественные* делятся на:

* природные (стихийные бедствия, магнитные бури, радиоактивное излучение, осадки);
* технические (связаны надежностью технических средств, обработки информации и систем обеспечения).

*Искусственные* делят на:

* непреднамеренные - совершенные по незнанию и без злого умысла, из любопытности или халатности
* преднамеренные

***Каналы проникновения в систему и их классификация***:

1. *По способу:*
	* прямые,
	* косвенные.
2. *По типу основного средства для реализации угрозы*:
	* человек,
	* аппаратура,
	* программа,
3. *По способу получения информации:*
	* физический,
	* электромагнитный,
	* информационный.

**Меры противодействия угрозам:**

1. *Правовые и законодательные*. Законы, указы, нормативные акты, регламентирующие правила обращения с информацией и определяющие ответственность за нарушение этих правил.
2. *Морально-этические*. Нормы поведения, которые традиционно сложились или складываются в обществе по мере распространения вычислительной техники. Невыполнение этих норм ведет к падению авторитета, престижа организации, страны, людей.
3. *Административные или организационные*. Меры организационного характера, регламентирующие процессы функционирования АС, деятельность персонала с целью максимального затруднения или исключения реализации угроз безопасности:
	* организация явного или скрытого контроля за работой пользователей
	* организация учета, хранения, использования, уничтожения документов и носителей информации.
	* организация охраны и надежного пропускного режима
	* мероприятия, осуществляемые при подборе и подготовке персонала
	* мероприятия по проектированию, разработке правил доступа к информации
	* мероприятия при разработке, модификации технических средств
4. *Физические.* Применение разного рода технических средств охраны и сооружений, предназначенных для создания физических препятствий на путях проникновения в систему.
5. *Технические*. Основаны на использовании технических устройств и программ, входящих в состав АС и выполняющих функции защиты:
	* средства аутентификации
	* аппаратное шифрование
	* другие

**Принципы построения систем защиты**:

1. **Принцип системности** - системный подход предполагает необходимость учета всех взаимосвязанных и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности.
2. **Принцип компетентности** - предполагает построение системы из разнородных средств, перекрывающих все существующие каналы реализации угрозы безопасности и не содержащих слабых мест на стыке отдельных компонентов.
3. **Принцип непрерывной защиты** - защита должна существовать без разрыва в пространстве и времени. Это непрерывный целенаправленный процесс, предполагающий не только защиту эксплуатации, но и проектирование защиты на стадии планирования системы.
4. **Принцип разумной достаточности**. Вложение средств в систему защиты должно быть построено таким образом, чтобы получить максимальную отдачу.
5. **Принцип гибкости управления и применения**. При проектировании системы защита может получиться либо избыточной, либо недостаточной. Система защиты должна быть легко настраиваема.
6. **Принцип открытости алгоритмов и механизмов защиты**. Знание алгоритма механизма защиты не позволяет осуществить взлом системы.
7. **Принцип простоты применения защитных мер и средств**. Все механизмы защиты должны быть интуитивно понятны и просты в использовании. Пользователь должен быть свободен от выполнения малопонятной многообъемной рутиной работы и не должен обладать специальными знаниями.

**Модель элементарной защиты**



Рисунок 3.

Прочность защитной преграды является достаточной, если ожидаемое время преодоления ее нарушителем больше времени жизни предмета защиты, или больше времени обнаружения и блокировки его доступа при отсутствии путей скрытого обхода этой преграды.

**Модель многозвенной защиты**


Рисунок 4.

**Модель многоуровневой защиты**.



Рисунок 5.

**1.4 Физическая защита объектов.**

***Система охраны*** - этосовокупность технических средств, предназначенных для выполнения задач по охране объекта.
Технические средства охраны - вид техники, предназначенный для использования силами охраны с целью повышения надежности обнаружения нарушителя и обеспечения санкционированного доступа на объект.
Нарушитель - это лицо или группа лиц, несанкционированно проникающих или проникших на объект охраны.

Объект охраны - участок местности, с расположенными на нем зданиями, сооружениями, помещения здания, отдельные предметы, доступ к которым посторонних лиц запрещен.

**Технические средства охраны:**

1. *Периметровые средства обнаружения*:
	* стационарные,
	* мобильные.
2. *Объектовые средства обнаружения*:
	* оптические.
3. *Средства сбора и отображения информации*:
	* обнаружение проникновения,
	* определенный контроль за системой охраны,
	* регистрация факта срабатывания устройства обнаружения,
4. *Средства управления доступом*:
	* кодоблокировочные устройства,
	* домофоны,
	* магнитные карты,
	* вертушки на КПП,
	* ворота,
	* шлагбаум,
5. *Технические средства наблюдения*:
	* телесистемы наблюдения,
	* оптические устройства,
	* приборы ночного видения.
6. *Технические средства предупреждения*:
	* плакаты,
	* надписи.
7. *Технические средства воздействия*:
	* электрозаграждения,
	* применение боевых отравляющих веществ,
	* сигнальные мины,
8. *Проводные и кабельные линии*.
9. *Инженерные заграждения и ограждения.*

**К *созданию* на территории некоторой *замкнутой зоны* с установкой физической преграды по периметру предъявляют следующие *требования*:**

1. Максимальная полнота охвата контролируемой зоны.
2. Минимальная вероятность необнаруживаемого обхода преграды нарушителем.
3. Достаточные изобретательность и чувствительность к присутствию, перемещению и другим действиям нарушителя.
4. Возможность исключения мертвых зон и простота размещения датчиков обнаружения.
5. Высокая надежность работы в заданных климатических условиях.
6. Устойчивость к естественным случайным помехам.
7. Удовлетворительное время обнаружения нарушителя.
8. Достаточно быстрая и точная диагностика места нарушения.

**1.5 Концептуальные основы для построения защиты информации от несанкционированного доступа в вычислительной системе.**

Анализ модели вычислительной системы с безопасной обработкой информации позволяет рассматривать вычислительную систему как объект, в котором имеется некоторое множество возможных каналов несанкционированного доступа к предмету защиты информации. Для построения защиты информации в данной системе на каждом **возможном канале несанкционированного доступа (ВКНСД)**, а если возможно, сразу на нескольких установить соответствующую преграду. Чем большее количество ВКНСД перекрыто средствами защиты и выше вероятность их преодоления нарушителем, тем выше безопасность информации.

Структура защиты будет носить многозвенный и многоуровневый характер. Количество перекрываемых ВКНСД при этом будет зависеть от заданной квалификации нарушителя.

Поведение потенциального нарушителя может быть следующим:

1. Нарушитель может появиться в любое время и в любом месте периметра автоматизированной системы.
2. Квалификация и осведомленность нарушителя может быть на уровне разработчика данной системы.
3. Постоянно хранимая информация о принципах работы системы, включая секретную, нарушителю известна.
4. Для достижения своей цели нарушитель выверит наиболее слабое звено в защите.
5. Нарушителем может быть законный пользователь системы.
6. Нарушитель действует один.

Основные принципы построения защиты:

1. Необходимо построить вокруг предмета защиты постоянно действующий замкнутый контур защиты.
2. Свойства преграды составляющие защиту должны, по возможности, соответствовать ожидаемой квалификации и осведомленности нарушителя.
3. Для входа в систему законного пользователя необходима переменная секретная информация, известная только ему.
4. Итоговая прочность защитного контура определяется его слабейшим звеном.
5. При наличии нескольких законных пользователей полезно обеспечить разграничение их доступа к информации в соответствии с полномочиями и выполняемыми функциями, реализуя таким образом принцип наименьшей осведомленности каждого пользователя с целью сокращения ущерба в случае, если имеет место безответственность одного из них.

**Нарушители могут быть**:

1. Нарушитель-профессионал.
2. Нарушитель высокой квалификации.
3. Относительно квалифицированный нарушитель-непрофессионал.
4. Безответственный пользователь.

Можно установить следующее **распределение ВКНСД по классам**:

1. *Все возможные каналы* несанкционированного доступа, возможные в данной вычислительной системе и в данный момент времени.
2. *Все ВКНСД*, кроме машинных носителей с остатками информации, подлежащей защите специальными криптографическими методами.
3. *Только следующие ВКНСД*:
	* терминалы пользователей
	* аппаратура регистрации, документирования, отображения информации
	* машинные и бумажные носители информации
	* средства загрузки программного обеспечения
	* технологические пульты и органы управления
	* внутренний монтаж аппаратуры
	* линии связи между аппаратными средствами
4. *Только следующие ВКНСД*:
	* терминалы пользователей
	* машинные и бумажные носители информации
	* средства загрузки программного обеспечения

**Анализ возможных каналов НСД к информации показывает, что данные каналы необходимо разделить на 2 вида:**

1. *Контролируемые:*
	* терминалы пользователей,
	* аппаратура регистрации, документирования, отображения информации,
	* средства загрузки программного обеспечения,
	* технологические пульты и органы управления,
	* внутренний монтаж аппаратуры,
	* побочные наводки информации на сетях электропитания и заземления аппаратуры, вспомогательных и посторонних коммуникациях, размещенных вблизи аппаратуры вычислительной системы.
2. *Неконтролируемые:*
	* машинные носители ПО и информации, выносимые за пределы вычислительной системы,
	* долговременные запоминающие устройства с остатками информации, выносимыми за пределы вычислительной системы,
	* внешние каналы связи,
	* мусорная корзина.

**Основные тактики защиты информации от НСД в вычислительных системах заключаются в выполнении следующих задач:**

1. Предупреждении и контроле попыток НСД
2. Своевременном обнаружении места и блокировки несанкционированных действий
3. Регистрации и документировании событий
4. Установление и устранение причины НСД
5. Ведение статистики и прогнозирования НСД

**1.6 Концептуальные основы для проектирования защиты информации от несанкционированного доступа в вычислительной системе.**

Для сетей, кроме защиты самой АСОИ (автоматизированной системы обработки информации) необходимо защитить и каналы связи.
Принимая во внимание, что информация в сети постоянно обновляется, а также и то, что на каналах связи, в отличие от элементов сети нарушитель ничем не рискует, особенно при пассивном перехвате информации, прочность защиты здесь должна быть особенно высокой.

От активного вмешательства нарушителя в процесс обмена информацией между элементами сети должна быть применена система обнаружения и блокировки несанкционированного доступа, но и при этом риск нарушителя по-прежнему не высок, т.к. у него и в этом случае, по причине сложности определения его пребывания, остается достаточно времени на то, чтобы отключиться и уничтожить свои следы. Поэтому в качестве сходной модели потенциального нарушителя высокой квалификации такой подход поможет защититься также от нарушителей, являющихся законными пользователями данной сети. Кроме того это позволит защитить системные отношения между элементами сети.
Поскольку физически каналы связи в сети защитить не представляется возможным, целесообразно строить защиту информации и сопровождающих ее служебных признаков на основе специальных криптографических преобразований, т.е. на основе самой информации, а не на ресурсах сети.

Такой основой должна быть кодограмма сообщений, которой обмениваются между собой элементы сети. Целостность этой кодограммы и содержащаяся в ней информация должны быть защищены от несанкционированного доступа.

Данная кодограмма, как правило, содержит адрес получателя, заголовок, информацию отправителя, концевик, адрес отправителя, исходящий номер и время отправления. В пакетном режиме добавляется еще и номер пакета, поскольку сообщение разбивается на пакеты, которые на объекте-получателе должны быть собраны в одно сообщение, чтобы оно приобрело первоначальный вид. Для синхронизации, приема и обработки кодограммы, в нее включаются признаки кадра. Кадр содержит информационное поле, а также заголовок и концевик, присваиваемый протоколом. Заголовок содержит служебную информацию, используемую протоколом канального уровня принимающей станции и служащую для идентификации сообщения правильного приема кадров, восстановления и повторной передачи в случае ошибок. Концевик содержит проверочное поле, служащее для коррекции и исправления ошибок.
Для обеспечения передачи блоков данных от передающей станции приемной кодограмма содержит признаки маршрута. Все эти и другие составляющие кодограммы формулируются на основе известной семиуровневой модели протокола взаимодействия открытых систем.

Анализ проведенных исследований в области безопасности информации в вычислительных сетях, позволяет взять за основу следующие требования, которые должны быть конечной целью при создании средств ее защиты.

**После того, как соединение между абонентами вычислительной сети установлено, необходимо обеспечить четыре условия:**

1. Получатель сообщения должен быть уверен в истинности источника данных.
2. Получатель сообщения должен быть уверен в истинности полученных данных.
3. Отправитель должен быть уверен в доставке данных получателю
4. Отправитель должен быть уверен в истинности доставленных получателю данных

При этом предполагается, что выполнение этих условий включает защиту от следующих активных вторжений нарушителя:

1. Воздействие на поток сообщений (изменение, удаление, задержки, переупорядочивание, дублирование и посылка ложных сообщений),
2. Воспрепятствие передачи сообщений,
3. Осуществление ложных соединений.

Однако, приведенные выше 4 условия не включают защиту от пассивных вторжений:

1. Чтение содержания сообщения,
2. Анализ трафика и идентификаторов абонентов сети.

Отправитель и получатель должны в данной сети иметь полномочия на обмен друг с другом.

Для полноты постановки задачи к указанным 4-м условиям нужно добавить еще 4:

1. Отправитель и получатель должны быть уверены, что никому, кроме них и специального посредника факт передачи сообщения между ними не известен.
2. Отправитель и получатель должны быть уверены, что с доставленной информацией в сообщении никто кроме них не ознакомился.
3. Получатель должен быть уверен, что отправитель - это то лицо, за которое он себя выдает.
4. Отправитель должен быть уверен, что получатель - то лицо, которое ему необходимо для передачи сообщения.

Данные требования рассчитаны на защиту от квалифицированного нарушителя-профессионала. Защищать будем кодограмму. Нарушителю доступна вся кодограмма, включая служебные признаки. Единственный метод защиты - это криптографические преобразования. Один из методов должен быть таким, чтобы в кодограмме сохранились некоторые адреса и служебные признаки в открытом виде, поскольку всю кодограмму преобразовывать нецелесообразно по причине невозможности ее дальнейшей обработки. Таким методом может быть использование механизма формирования цифровой подписи на базе несимметричных алгоритмов шифрования.

Для того, чтобы обеспечить возможность контроля и разграничения доступа, необходимо для всех участников обмена информацией помимо условных номеров присвоить переменные идентификаторы в виде паролей, которые могут передаваться в открытом виде, и подлинность которых будет обеспечиваться механизмом цифровой подписи.

Тем абонентам, которым присвоены соответствующие полномочия, должны быть предоставлены соответствующие значения паролей и закрытых ключей шифрования. Стойкость защитного механизма определяется стойкостью к подбору примененного секретного ключа в количестве времени, затрачиваемого нарушителем на эту работу. Если оно составляет величину, превышающую время жизни защищаемой информации, то прочность этой преграды равна 1. При этом обратим внимание на существенную разницу во времени жизни самого сообщения и его служебных частей. Само сообщение в зависимости от назначения автоматизированных систем обработки данных может сохранять цену десятки лет, а его служебные части - не более 10 минут. Это позволяет существенно увеличить быстродействие шифрования и , может быть, даже упростить его для служебных частей. Такой большой набор процедур может вызвать сомнения у разработчиков по поводу реальности воплощения этой идеи из-за возможного увеличения времени обработки кодограммы. Однако, даже если это и случится, повышение безопасности информации стоит того. При реализации системы контроля и разграничении доступа в АСУ, потребуется также организовать систему сбора в сети сигналов, несовпадение кодов паролей, систему управления и распределения ключей шифрования информации и организационные мероприятия по безопасности информации.

**1.7 Организационные меры защиты информации в вычислительной сети.**

Для выполнения безопасности информации в вычислительной сети можно предложить следующую группу средств, ориентированных соответственно на выполнение приведенных выше 8 условий:

1. Средства формирования цифровой подписи сообщения.
2. Средства шифрования передаваемых данных.
3. Средства обеспечения цифровой подписи, служебных признаков передаваемой информации, включая адреса и маршруты сообщения, а также получение отправителем и посредником уведомления от получателя.
4. Все перечисленные в пунктах 1-3 средства.
5. Средства п.2.
6. Введение в сети маскирующих потоков сообщений при отсутствии активности в обмене информацией.
7. Присвоение всем участникам обмена сообщениями переменных идентификаторов и создание в АСУ и сети системы контроля и разграничения доступа с защитой цифровой подписи паролем от подмены их нарушителем.
8. Средства п.7.

Вычислительную сеть можно считать безопасной в смысле обработки информации, если в ней предусмотрена централизованная система управляемых и взаимосвязанных преград, перекрывающих с гарантированной прочностью заданное в соответствии с моделью потенциального нарушителя количество возможных каналов несанкционированного доступа и угроз, направленных на утрату или модификацию информации, а также несанкционированное ознакомление с нею посторонних лиц.

**Основные принципы проектирования защиты информации в АСОД.**

В процессе подготовки к началу работ по проектированию АСОД при согласовании технического задания уже известны предварительное распределение, места сосредоточения, характер, степень важности и секретности информации, подлежащей обработке. Таким образом определяется необходимость в разработке системы защиты информации и соответствующих требований к ним, которые обязательно должны быть приведены в техническом задании на систему. Отсюда следует основное требование к порядку проведения проектирования заключающееся в необходимости параллельного проектирования системы защиты информации с проектированием системы управления и обработки данных, начиная с момента выработки общего замысла построения АСОД.

**Созданию системы защиты информации, встроенную в АС, свойственны все этапы:**

* разработка технических предложений;
* разработка эскизного и технического проектов;
* выпуск рабочей документации;
* изготовление;
* испытание и сдача системы заказчику.

Невыполнение этого принципа, наложение или встраивание средств защиты в уже готовую систему может привести к низкой эффективности защиты, невозможности создания цельной системы защиты, снижению производительности и быстродействия вычислительных средств, а также большим затратам, чем если бы система защиты разрабатывалась и реализовывалась параллельно с основными задачами.

При параллельном проектировании, разработчиками системы защиты информации производится анализ циркуляции и мест сосредоточения информации в проекте АСОД, определяются наиболее уязвимые места для несанкционированного доступа и своевременно предлагаются взаимоприемлемые технические решения по сокращению их количества путем изменения принципиальной схемы АСОД, что позволит обеспечить простоту, надежность и экономическую реализацию защиты с достаточной эффективностью.
Кроме того параллельное проектирование необходимо в силу встроенного характера большей части технических средств защиты.

Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением процессов автоматизированной обработки информации, что важно для определения степени влияния средств защиты информации на основные вероятностно-временные характеристики АСОД, которые, как правило, изменяются в сторону ухудшения. Но это плата за приобретение нового и необходимого качества, которое иногда является причиной пренебрежительного отношения некоторых разработчиков и заказчиков к АСОД защите. Однако, за такую недальновидность им приходится расплачиваться более дорогой ценой. Не выполнив эту задачу они лишили владельца АСОД гарантии на собственность его информации, циркулирующей в ней. Техническое задание на проектируемую АСОД должно содержать перечень сведений и характеристик, подлежащих защите, возможные пути циркуляции и места их сосредоточения, а также специальные требования к системе защиты информации. Если это АСУ или вычислительная сеть, то должна соблюдаться иерархия требований средств защиты информации. Они должны входить:

* в общее техническое задание на АСУ или сеть в целом
* в частные технические задания на функциональные подсистемы управления, на отдельные автоматизированные звенья, объекты, комплексы, технические средства.
* в технические задания сопряжение внешних систем.
* в техническое задание на общее ПО отдельных ЭВМ и вычислительных комплексов на специальное программное обеспечение объектов элементов вычислительной сети и АСУ.

Решение вопросов создания систем защиты должно поручаться лицам одного уровня с лицами, занимающимися вопросами функционирования АСУ.
Разработка средств защиты информации требует привлечения специалистов широкого профиля, знающих кроме системных вопросов, вопросов программного обеспечения, разработки комплексов и отдельных технических средств, специальные вопросы защиты информации.

При проектировании защиты следует внимательно провести исследования разрабатываемой АСОД на предмет выявления всех возможных каналов несанкционированного доступа к информации, подлежащей защите, средствами ее ввода/вывода, хранения, и только после этого строить защиту.
Первое знакомство с разрабатываемой АСОД должно закончиться рекомендациями по сокращению обнаруженных каналов доступа путем ее принципиальных изменений без ущерба выполнения основных задач. Анализ важнейших задач организации и формирования функций, удовлетворяющих целям управления носит итеративный характер, обеспечивающий последовательное уточнение задач и функций, согласования их на всех уровнях и ступенях АСУ и сведения их в единую функциональную схему. Это означает, что проведенное на некотором этапе проектирование, технические решения, накладываемые системой защиты на основные задачи АСУ, должны проверяться по степени их влияния на решение основных процессов управления и наоборот, после принятия решения по изменению основных процессов управления и составу технических средств должно проверяться их соответствие решениям по защите информации, которые, при необходимости, должны корректироваться или сохраняться, если корректировка снижает прочность защиты. Важную роль играет простота системы защиты.

Она должна быть простой настолько, насколько позволяют требования по ее эффективности. Простота защиты повышает ее надежность, экономичность, уменьшает ее влияние на вероятностно-временные характеристики АСУ, создает удобство в обращении с ней. При неудобных средствах защиты, пользователь будет стараться найти пути ее обхода, отключить ее механизм, что сделает защиту бессмысленной и ненужной.

При проектировании защиты, как и в обычных разработках, вполне разумно применение унифицированных или стандартных средств защиты, однако желательно, чтобы указанные средства при применении проектируемой АСОД приобрело индивидуальные свойства защиты, которые бы потенциальному нарушителю не были известны.

Данные по защите информации в проектируемой АСОД должны содержаться в отдельных документах и засекречиваться, хотя некоторые зарубежные специалисты говорят о принципах несекретности проектирования защиты.
Ознакомление опытных и квалифицированных специалистов с уязвимыми точками проекта на предмет ее уязвимости можно осуществить путем организации контролируемого пропуска их к секретному проекту. В этом случае, по крайней мере будут известны лица, ознакомленные с проектом. Таким образом, сокращается число лиц потенциальных нарушителей, а лица, ознакомленные с проектом несут ответственность перед законом, что, как известно, является сдерживающим фактором для потенциального нарушителя.

В процессе проектирования и испытания рекомендуется по возможности использовать исходные данные, отличающиеся от действительных, но позволяющие при последующей загрузке системы действительными данными, не проводить доработки.

Загрузка действительных данных должна проводиться только после проверки функционирования системы защиты информации в данной АСУ.
Учитывая то, что система защиты в АСОД предусматривает кроме аппаратно-программных средств применение в качестве преграды и организационные мероприятия, выполняемые человеком (наиболее слабым звеном защиты), необходимо стремиться к максимальной автоматизации его функций и сокращению доли его участия в защите.

Для того, чтобы спроектированная система защиты приобрела жизнь, необходимо также, чтобы технические средства защиты по возможности не ухудшали вероятностно-временные характеристики АСОД (быстродействие, производительность и т.д.).

**2. Идентификация и аутентификация**

**Идентификация** - это присвоение субъектом или объектом доступа идентификатора или сравнения предъявленного идентификатора с перечнем присвоенных идентификаторов. ***Цель идентификации*** - отслеживание действий пользователя в системе.

**Аутентификация** - это проверка принадлежности субъекту доступа предъявленного им идентификатора.

***Принципы аутентификации:***

1. **Пользователь знает.**

Существует III (три) метода аутентификации:

* 1. **Метод пароля и его модификация**. Пароль выбирается пользователем. Ожидаемое безопасное время - это полупроизведение числа возможных паролей и времени, необходимого для того, чтобы попробовать все возможные пароли.

 *Модификация методов простых паролей*:

* + - *пароль с выборкой символов* (система просит ввести случайную цепочку символов, составляющую пароль),
		- *метод однократного пароля*.(пользователь вводит в систему, или система выдает пользователю значительное число паролей, которые тот должен запомнить или хранить. Каждый раз пользователь входит под новым именем. Проблемы: в случае аварийного завершения сеанса работы пользователь может не знать, какой пароль вводить.
		- *при завершении сеанса работы система просит ввести пароль на следующий сеанс*.

**Правила обращения с паролями:**

* + - пароли нельзя хранить в системе в явном виде,
		- пароли нельзя отображать в явном виде,
		- пароли необходимо менять как можно чаще,
		- система не должна вырабатывать новый пароль в конце сеанса работы.
	1. **Метод вопрос-ответ**. Пользователь при входе отвечает на m ориентированных и n стандартных вопросов. Стандартные вопросы не касаются пользователя и вводятся в систему заранее.
	2. **Метод секретного алгоритма**. Система выдает случайное число. Пользователь, зная секретный алгоритм, сообщает системе результаты вычислений по алгоритму.
1. Пользователь имеет.

Аутентификация производится по некоторому предмету, которым физически обладает пользователь.

* 1. **магнитные идентификационные карты**; носитель информации - магнитная полоса. В соответствии с международным стандартом ISO 1811-1/9 1989 полоса содержит три дорожки: две для идентификации и одна - для перезаписи информации. Проблемы: невысокая механическая стойкость.
	2. **полупроводниковые id-карты**. Имеется встроенная информационная система с металлическими контактами. По стандарту ISO 1816-1 1988, таких контактов должно быть 8 и они должны быть позолочены. В настоящее время используется 4-6 контактов. В данные карты встраиваются системы шифрования.
	3. **электрический идентификатор** - это таблетка диаметром 17 мм, толщиной 5.8 или 3.2 мм, внутри находится литиевая батарейка, срок службы - 10 лет.
	4. **оптические идентификационные карты**. Емкость от 40 до 200 Мбайт. Выполнены по технологии WORM.
1. Пользователь есть.

Аутентификация производится с помощью основных биометрических показателей человека:

* 1. **узор сетчатки глаза**. Осуществляется сканирование сетчатки; измеряется угловое распределение кровеносных сосудов относительно слепого пятна. Стоимость устройств 5-7 тыс. долларов. Контрольный образ - 40 байт.
	Существует несколько процентов вероятности не признания законного пользователя, но зато 100%-я вероятность обнаружения чужака.
	2. **отпечатки пальцев**. Основан на выделении основных дактилоскопических признаков, измерения расстояния между ними, вычисления их относительных координат. Контрольный образ 400-1000 байт. Цена - 2-4 тыс. долл. Надежность - 95%. Руки человека должны быть теплыми. Термохромные материалы значительно изменяют отражающую способность при незначительном изменении температуры. Прибор представляет собой матрицу 250х250 ячеек. Каждая ячейка имеет 16 градаций оттенков.
	3. **геометрия руки**.Образ занимает от 9 до 1000 байт, в зависимости от фирмы производителя. Цена - 3-5 тыс. долл. Рука облучается мощным световым потоком. Фотоячейки фиксируют контур руки. Система обнаруживает возрастные изменения, производственные изменения и муляжи.

Параметры, уникальные для человека:

* + - положение краев контура каждого пальца,
		- положение центральных осей для каждого контура пальца,
		- смещение осей контуров всех пальцев до положения, перпендикулярного опорной линии,
		- ширина контура каждого пальца в определяющих местах опорной линии.
	1. **динамика подписи**.
		+ динамическая аутентификация (специальный планшет и ручка). В ручке установлен преобразователь ускорения по осям x и y; планшет измеряет силу нажатия.
		+ статическая аутентификация. Подпись сверяется с контрольным образом. Расписываются 4-5 раз. Контрольный образ от 40 байт до 4 Кбайт. Стоимость оборудования - 100-1200 долл.
	2. **особенности речи**. Характеристики голоса:
		+ высота тона (диапазон частот вибрации голосовых связок),
		+ резонансные частоты глотки носовой и ротовой полости,
		+ мелодичность (высота тона как функция времени),
		+ интонация (громкость как функция времени),

*Методы аутентификации:*

* + - фразонезависимые,
		- текстозависимые,

Контрольный образ от 2 до 20 Кбайт. Стоимость оборудования - от 300 долл.

* 1. **ритм работы на клавиатуре**. Существуют определенные временные интервалы при последовательном нажатии клавиш на клавиатуре. Позволяет производить аутентификацию постоянно и скрытно. Способы:
		+ по свободному тексту,
		+ по набору ключевых фраз.

Средства биометрической аутентификации используются в системах, работающих в двух вариантах:

* открытые системы. Средства аутентификации используются неподготовленным пользователем и количество средств аутентификации - 1-2,
* системы управления оружием или серьезная закрытая информация. Пользователи заранее подготовлены и четко знают последовательность действий.

За невыполнение последовательности действий могут быть применены технические средства охраны.

**2.1 Программно-аппаратная защита информации.**

При создании программно-аппаратных средств защиты, руководствуются следующими принципами:

1. **Принцип обоснованности доступа**. Для предоставления доступа пользователя к системе необходимо выполнить два условия:
	* исполнитель должен иметь достаточную форму допуска к закрытой информации соответствующего уровня
	* исполнителю данные сведения должны быть нужны для выполнения его профессиональных обязанностей.

Исполнитель должен работать в своей исполнительной среде. Пользователь видит только доступную ему информацию. Правила создания данной среды представляются в виде математической модели (модели управления доступом). В этой модели необходимо учитывать динамику изменения взаимодействия ресурсов в системе.

1. **Принцип достаточной глубины контроля доступа**. Средства защиты информации должны включать механизмы контроля доступа ко всем видам информационных и программных ресурсов.
2. **Принцип разграничения потоков информации**. Не позволяет переписывать закрытую информацию на незакрытые носители. Осуществляется нанесением меток на носители информации и идентификация таких носителей.
3. **Принцип чистоты повторно используемых ресурсов**. Заключается в освобождении от закрытой информации ресурсов при их удалении или освобождении исполнителя до занятия другим исполнителем.
4. **Принцип персональной ответственности**. Исполнитель должен нести персональную ответственность за свою деятельность в системе, включая все действия с закрытой информацией. Необходимо выполнение трех требований:
	* идентификация всех пользователей и процессов, запущенных от их имени
	* аутентификация пользователя
	* регистрация или протоколирование механизмами контроля доступа всех попыток доступа к закрытой информации, в т.ч. и неудачных.
5. **Принцип целостности средств защиты**. Средства защиты должны точно выполнять свои функции и быть изолированы от пользователя. Все средства защиты должны выполняться в виде отдельного модуля, и называется он "монитор обращения".



Рисунок 1.

Для построения монитора обращений необходимо выполнить следующие требования:

* + *Монитор обращений должен быть защищен* от постороннего вмешательства в его работу, включая несанкционированную подмену и модификацию.
	+ *Монитор обращений должен всегда присутствовать* и работать надлежащим образом .
	+ *Монитор обращений должен быть компактен* и удобен для проведения анализа и тестирования.

**2.2 Модели управления доступом.**

Модели управления доступом определяют правила управления доступом к информации, разрешениями в системе таким образом, чтобы система всегда была безопасна. При создании механизмов контроля доступа необходимо определить множество субъектов и объектов доступа.

**Субъектами** могут быть пользователи, процессы и процедуры.

**Объекты**: файлы, программы, директории, терминалы, каналы связи, устройства и т.д.

*Субъекты* могут одновременно рассматриваться и как объекты, поэтому у субъекта могут быть права на доступ к другому субъекту.
В конкретном процессе в данный момент времени субъекты являются активными элементами, а объекты пассивными. Для осуществления доступа к объекту, субъект должен владеть соответствующими полномочиями.
Полномочия можно отобразить определенным символом, владение которым дает субъекту определенные права доступа по отношению к объекту. Область защиты определяет права доступа некоторого субъекта к множеству объектов, что защищаются и являются совокупностью всех полномочий данного субъекта.

При функционировании системы необходимо иметь возможность создавать новые субъекты и объекты. При создании объекта одновременно создается и полномочие субъектов по использованию этого объекта. Субъект, что создал такое полномочие может воспользоваться им для осуществления доступа к объекту, или же может создать несколько копий привилегий, для передачи их другим субъектам.

Успех достижения высокой степени безопасности АС зависит от тщательности разработки и реализации управления имеющимися в системе механизмами безопасности. Как показывает практика, наилучшие результаты создания безопасных систем достигаются в том случае, когда разработчики системы учитывают требования безопасности уже на этапе формулирования целей разработки и самых общих принципов построения системы. При этом разработчики должны четко понимать суть требований безопасности.

В таком случае разрабатываемая система может быть небезопасной в силу одной из двух причин:

1. Есть ошибки в реализации механизмов защиты или механизмов управления ими.
2. Ошибочно, не достаточно полно или не верно понято само определение того, что значит в отношении системы выражение "быть безопасным".

Для устранения первой причины необходимо применение современных технологий создания ПО в сочетании с принципами разработки, специфичными для выполнения требований безопасности.

Для устранения второй причины необходимо как можно точнее сформулировать понятие "быть безопасной" в отношении разрабатываемой системы.

Известно, что при разработке современных АС используется один из двух методов:

1. **Нисходящий метод** (сверху вниз). Сначала составляется общее описание системы, выделяются компоненты системы, поэтапно увеличивается степень детализации компонентов системы (выделение компонентов в компонентах) до момента окончания разработки.
2. **Восходящий метод** (снизу вверх). Сначала формируется задача системы, затем разрабатывается некоторый набор элементарных функций. На базе элементарных функций разрабатываются более крупные компоненты системы, и так, поэтапно разработка ведется до момента объединения отдельных компонентов в единую систему.

Наибольшее распространение получил компромиссный вариант, при котором разработка системы в целом ведется нисходящим методом, а разработка отдельных компонентов системы, в основном элементарных - восходящим.
Для нас большой интерес представляет нисходящий метод создания систем, т.к. этот метод позволяет задавать требования безопасности ко всей системе в целом, и затем их детализировать, применительно к каждой подсистеме.
Нисходящий метод разработки системы обеспечения безопасности может быть неформальным и формальным.



Рисунок 2.

Метод неформальной разработки применяется при создании относительно простых систем с небольшим числом компонентов и очевидными алгоритмами их взаимодействия.

По мере увеличения сложности системы, взаимосвязи ее компонентов становятся все менее очевидными. Становится сложно описать эти взаимосвязи с достаточной степенью точности некоторым неформальным образом.
При разработке систем обеспечения безопасности, точность в описании компонентов и их взаимосвязи являются едва ли не решающим условием достижения успеха, поэтому для обеспечения надлежащей степени точности, применяется строгий аппарат формальной математики, что и составляет суть формального метода разработки. Основную роль в методе формальной разработки системы играет т.н. модель управления доступом. Эта модель определяет правила управления доступом к информации, потоки информации, разрешенные в системе таким образом, чтобы система всегда была безопасной.
Целью модели управления доступом является выражение сути требований по безопасности к данной системе.

**Для этого модель должна обладать несколькими свойствами:**

* быть адекватной моделируемой системе и неизбыточной
* быть простой и абстрактной и поэтому несложной для понимания

***Модель*** позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты.
Т.к. модель является формальной, возможно осуществить доказательство различных свойств безопасности всей системы.

Моделирование требует значительных усилий и дает хорошие результаты только при наличии времени и ресурсов. Если система уже создана и имеется возможность сделать лишь отдельные изменения в отдельных местах существующей системы, в любом случае маловероятно значительное улучшение состояния безопасности системы и моделирование будет непродуктивным занятием.

**2.3 Типы моделей управления доступом.**

1. ***Модель конечного автомата описывает систему как абстрактную математическую машину***. В этой модели переменные состояния представляют состояния машины, а функции перехода описывают способ изменения переменных. Модель управления доступом имеет дело только с наиболее существенными переменными состояниями, влияющими на безопасность и потому намного проще, чем полная модель конечного автомата для данной системы.
2. ***Модель матрицы доступа*** (частный случай реализации модели машины состояний). Состояния безопасности системы представлены в виде таблицы, содержащей по одной строке для каждого субъекта системы и по одной колонке для каждого субъекта и объекта. Каждое пересечение в массиве определяет режим доступа данного субъекта к каждому объекту или другому субъекту системы.

Таблица 1.

|  |  |  |
| --- | --- | --- |
| Субъекты | Объекты | Субъекты |
| 1 | 2 | 3 | 1 | 2 | 3 |
| 1 | чтение, запись | чтение | - | - | запись | запись |
| 2 | чтение | чтение, исполнение | чтение, запись | пересылка | - | - |
| 3 | - | чтение, запись | исполнение | пересылка | запись | - |

1. ***Второй составляющей модели матрицы доступа является набор функций перехода, описывающих способ изменения матрицы доступа.*** Более часто матрица доступа используется не как самостоятельная модель управления доступом, а в качестве одной из нескольких переменных состояния в более общей модели конечного автомата.
2. Другим способом описания управления доступом является ***модель, выраженная в терминах меток безопасности, приписываемых субъектом и объектом системы.*** Режим доступа, которым обладает субъект по отношению к объекту, определяется при сравнении их меток безопасности вместо того, чтобы искать соответствующие пересечения строки и столбца в матрице доступа. Модель может использовать как матрицу доступа, так и атрибуты безопасности.
3. Вариантом модели управления доступом является ***модель информационных потоков, которая предназначена для анализа потоков информации из одного объекта в другой на основании их меток безопасности.***
4. ***Модель интерференции***, в которой субъекты, работающие в различных доменах, защищены от взаимовлияния друг на друга, любым способом, нарушающим свойства безопасности системы.

**Характеристики модели безопасности.**

Модель является лишь формулировкой математических терминов, свойств безопасности, которым должна удовлетворять система. Не существует формального способа, с помощью которого можно доказать, что формальная модель управления доступом соответствует правилам управления доступом, принятым в данной системе.

С другой стороны, модель может иметь ряд характеристик, назначение которых не столь очевидно. Поскольку модель должна стремиться к математическому совершенству в определении свойств, составляющих политику безопасности, это часто влечет за собой включение ограничений или дополнительных свойств, присутствие которых ранее не предусматривалось.

**Описание модели управления доступом (МУД) к системе**

**как конечного автомата**

Представление МУД как конечного автомата получило предпочтение из-за того, что они представляют компьютерную систему способом, имитирующим работу ОС и аппаратуры. Переменное состояние является абстракцией для каждого бита и байта в системе, изменяющихся по мере работы в системе. Функция перехода из состояния в состояние - это абстракция обращений к ОС, явно описывающая то, как состояние может (или не может) измениться.
МУД работает не со всеми переменными состояния и функциями системы.
Выбор для моделирования переменных и функций, имеющих отношение к безопасности, остается за разработчиком модели.

Разработка моделей управления доступом включает в себя определение элементов моделей (переменных, функций, правил и т.д.), а также безопасного начального состояния.

Математически доказывается, что начальное состояние безопасно, и что все функции безопасны, после чего, путем математической индукции делается вывод о том, что если система первоначально находилась в безопасном состоянии, система остается в безопасном состоянии независимо от того, какие функции, и в каком порядке будут выполнены.

**Таким образом, в разработке МУД можно выделить следующие шаги:**

* 1. *Определение переменных состояний, имеющих отношение к безопасности.* Обычно переменные состояния представляют объекты и субъекты системы, их атрибуты безопасности и права доступа между субъектами и объектами.
	2. *Определение условий для безопасного состояния.* Это определение является выражением отношений между значениями переменных состояния, истинность которого должна обеспечиваться при переходах состояния.
	3. *Определение функций переходов из состояния в состояние.* Эти функции описывают допустимые способы изменения переменных состояния. Они также называются правилами изменения доступа, поскольку их цель состоит в указании изменений, которые может производить система, а вовсе не в определении всех возможных изменений. Правила могут быть очень общими и могут допускать наличие функций, которых нет в реальной системе, однако система не может менять переменные состояния каким-либо способом, который не допускается функциями.

Можно выделить несколько характерных черт функций перехода:

* + - назначение функции.
		- определение взаимосвязи между переменными, предыдущим и новым состояниями.
		- функция не задает какого-либо конкретного порядка в выполнении алгоритма операции.
		- функция элементарна.
	1. *Доказывается, что функции обеспечивают сохранение безопасного состояния.* Чтобы удостовериться в том, что модель является безопасной, необходимо для каждой функции перехода доказать, что если система находится в безопасном состоянии до начала выполнения функции перехода, то система останется в этом состоянии по ее завершении.
	2. *Определение начального состояния.* Математически, начальное состояние выражается как множество начальных значений всех переменных состояний системы. Простейшим начальным состоянием является состояние вообще без каких-либо субъектов и объектов. При этом нет необходимости определять начальные значения каких-либо других переменных состояний, поскольку состояние будет безопасным независимо от их значения. Более реалистичное безопасное начальное состояние предполагает наличие некоторого начального множества субъектов и объектов.
	3. *Доказывается, что начальное состояние безопасно в соответствии с определением.*
1. *Списки управления доступом к объектам*. В данной модели полномочия доступа определяются в виде списка картежей для всех субъектов, имеющих доступ к данному объекту.

Таблица 2.

|  |  |  |
| --- | --- | --- |
| Объекты | Списки картежей | Методы доступа |
| O1 | S1 | r (чтение) | w (запись) | c (копирование) |
| O2 | S2 | w | r | x (удаление) |

Достоинства данной модели:

* 1. экономия памяти
	2. удобство получения сведений о субъектах, имеющих доступ к данному объекту

Недостатки:

* 1. неудобство получения сведений об объектах, к которым имеет доступ данный субъект
	2. неудобство отслеживания ограничений и зависимостей по наследованию полномочий субъекта
1. *Списки полномочий субъектов*.

Таблица 3.

|  |  |  |
| --- | --- | --- |
| Списки картежей | Объекты | Методы доступа |
| S1 | O1 | r (чтение) | w (запись) | c (копирование) |
| S2 | O2 | w | r | x (удаление) |

В данной модели полномочия доступа субъекта представляются в виде списка картежей для всех объектов, в которых он имеет доступ.
Профиль субъекта используется для отслеживания событий аудита в ОС Microsoft и MSNT.

Достоинства модели:

* 1. экономия памяти,
	2. удобство получения сведений об объектах, к которым имеет доступ данный субъект,

Недостатки:

* 1. неудобство получения сведений о субъектах, которые имеют доступ данному объекту
1. *Атрибутная схема.* Атрибутные способы задания матрицы доступа основаны на присвоении субъектом и объектом определенных меток (содержащих значения атрибутов). Такая схема используется в ОС семейства Unix.
Матрица задана в неявном виде. Вычисление уровня доступа субъекта к объекту происходит динамически. Существуют также многоуровневые модели управления доступом.

**3. Криптография**

Открытым текстом называется исходное сообщение. ***Изменение вида сообщения так, чтобы спрятать его суть называется шифрованием.*** *Шифрованное сообщение называется* ***шифротекстом****. Процесс преобразования шифротекста в открытый текст называется* ***дешифрованием****.* Искусство и наука безопасных сообщений называется **криптографией.** *Криптоаналитиками* называются те, кто постоянно использует *криптоанализ (искусство и наука взламывать шифротекст)*.

Криптография часто используется и для других целей:

1. **Проверка подлинности**. Получатель сообщения может проверить его источник. Злоумышленник не сможет замаскироваться под кого-либо.
2. **Целостность**. Получатель сообщения может проверить не было ли сообщение изменено в процессе доставки.
3. **Неотрицание авторства**. Отправитель не сможет ложно отрицать отправку сообщения.

**3.1 Алгоритмы и ключи.**

Криптографический алгоритм, также называемый шифром, представляет собой математическую функцию, используемую для шифрования и дешифрования. Обычно это две связанные функции: одна для шифрования, другая - для дешифрования.

**Основные требования, предъявляемые к методам защитного преобразования:**

1. Применяемый метод должен быть достаточно устойчив к попыткам раскрыть исходный текст имея только зашифрованный текст.
2. Объем ключа не должен затруднять его запоминание и пересылку.
3. Алгоритм преобразования информации и ключ, используемый для шифрования и дешифрования не должны быть очень сложными. Затраты на защитные преобразования должны быть приемлемы при заданном уровне сохранности информации.
4. Ошибки в шифровании не должны вызывать потерю информации. Из-за появления ошибок передачи шифрованного сообщения по каналам связи не должна исключаться возможность надежной расшифровки текста на приемном конце.
5. Длина зашифрованного текста не должна превышать длину исходного текста.
6. Необходимые временные и стоимостные ресурсы на шифрование и дешифрование информации определяются требуемой степенью защиты информации.

**Множество современных методов защитных преобразований можно классифицировать на 4 большие группы:**

1. Перестановки.
2. Замены.
3. Аддитивные.
4. Комбинированные.

*Методы перестановки и подстановки* обычно характеризуются короткой длиной ключа, а надежность их защиты определяется сложностью алгоритмов преобразования.

Для *аддитивных методов* характерны простые алгоритмы преобразования, а их надежность основана на увеличении длины ключа.
Все перечисленные методы относятся к симметричному шифрованию (для шифрования и дешифрования используется один и тот же ключ).
Асимметричное - один ключ для шифрования (открытый), другой - для дешифрования (закрытый).

1. **Метод перестановки**.

Суть состоит в том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов.
Простейшим примером перестановки является запись исходного текста по строкам некоторой матрицы и чтение его по столбцам этой матрицы. Последовательность заполнения строк и чтение столбцов может быть любой и задается ключом.

Для матрицы размером 8х8 возможно 1,6\*109 ключей.
Для методов перестановки характерны простота алгоритма, возможность программной реализации и низкий уровень защиты. Т.к. при большой длине исходного текста в шифрованном тексте проявляются статистические закономерности ключа, - это позволяет его быстро раскрыть. Другой недостаток этого метода - легкое раскрытие, если удается направить в систему для шифрования несколько специально подобранных сообщений. Если длина блока в исходном тексте равна k символам, то для раскрытия ключа достаточно пропустить через шифрованную систему (k-1) блоков исходного текста, в которых все символы кроме одного одинаковы.

1. **Метод замены (подстановки)**.

Заключается в том, что символы исходного текста, записанные в одном алфавите, заменяются символами другого алфавита в соответствии с принятым ключом преобразования. Одним из простейших методов является прямая замена исходных символов их эквивалентом из вектора замен. Для очередного символа исходного текста отыскивается его местоположение в исходном алфавите. Эквивалент из вектора замены выбирается как отстоящий на полученное смещение от начала алфавита.При дешифровании поиск производится в векторе замен, а эквивалент выбирается из алфавита. Полученный таким образом текст имеет низкий уровень защиты.

Более стойкой отношении раскрытия является схема шифрования, основанная на использовании **таблицы Вижинера**: таблица представляет собой квадратную матрицу с числом элементов k, где k - количество символов в алфавите. В первой строке матрицы записываются буквы в порядке очередности их в алфавите, во второй - та же последовательность букв, но со сдвигом влево на одну позицию, в третьей - со сдвигом на 2 позиции и т.д. Освободившиеся места справа заполняются вытесненными влево буквами, записанными в естественной последовательности.

Для шифрования текста устанавливается ключ, представляющий собой некоторое слово или набор букв. Далее, из полной матрицы выбирается подматрица шифрования, включающая, например, первую строку и строку матрицы, начальные буквы которой являются последовательной буквой ключа.

Пример:
Ключ – МОРЕ

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

МНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛ
ОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМН
РСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОП
ЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГД

Исходный текст:
ЗАЩИТА ИНФОРМАЦИИ
МОРЕМО РЕМОРЕМОРЕ
Зашифрованный текст:
УОИОЭО ШТЯЫЯСМГШО

**Процесс шифрования включает следующую последовательность действий:**

1. Под каждой буквой шифруемого текста записываются буквы ключа, повторяющие ключ требуемой число раз.
2. Шифруемый текст по подматрице заменяется буквами, расположенными на пересечении линий, соединяющих буквы текста первой строки подматрицы и буквы ключа, находящиеся под ней.

Пример:
Ключ - ОКНО
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

ОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМН
КЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙ
НОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМ
ОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМН

ЗАЩИТА ИНФОРМАЦИИ
ОКНООК НООКНООКНО
ЦКЁЧАК ЦЫВШЭЪОАЦЧ

**Расшифровка текста выполняется в следующей последовательности:**

1. Над буквами шифрованного текста последовательно записываются буквы ключа.
2. В строке подматрицы таблицы Вижинера для каждой буквы ключа отыскивается буква, соответствующая знаку шифрованного текста. Находящаяся над ней буква первой строки и будет знаком расшифрованного текста.
3. Полученный текст группируется в слова по смыслу.

Один из недостатков шифрования по таблице Вижинера - ненадежность шифрования при небольшой длине ключа и сложность формирования длинных ключей.

Т.к. в ключе не допускается повторение букв (в противном случае шифрование будет неоднозначным), а сам ключ должен легко запоминаться, последовательность букв, не имеющих определенного смысла, запомнить трудно.
С целью повышения надежности шифрования текста, предлагается ***усовершенствованный вариант таблицы Вижинера,*** который заключается в следующем:

1. Во всех строках, кроме первой, буквы алфавита располагаются в произвольном порядке.
2. Выбирается 10, не считая первой, строк, пронумерованных натуральными числами от 0 до 9.
3. В качестве ключа используются величины, выраженные бесконечным рядом чисел (например, число Пи).

Шифрование и расшифрование осуществляется в той же последовательности, что и в случае простой таблицы Вижинера.

***Частным случаем метода замены***, обеспечивающим надежное шифрование информации является использование алгебры матриц. Например, правило умножения матрицы на вектор. Это правило заключается в следующем:



 В соответствии с этим правилом, матрицу можно использовать в качестве основы для шифрования. Знаками вектора b1 могут быть символы шифруемого текста, а знаками вектора результата c1 - символы зашифрованного текста.
Для шифрования буквенных сообщений необходимо прежде всего заменить знаки алфавита их цифровым эквивалентом, которым может быть порядковый номер буквы в алфавите.

Для дешифрования используются те же самые правила умножения матрицы на вектор, только в качестве основы берется обратная матрица, а в качестве умножаемого вектора - соответствующее количество чисел шифрованного текста.

Цифрами вектора результата будут цифровые эквиваленты знаков исходного текста.

Существуют и другие методы подстановки. Приведенные выше методы относятся к моноалфавитным подстановкам, которые можно представить как числовые преобразования букв исходного текста, рассматриваемых как числа.
Каждая буква в тексте умножается на некоторое число, называемое десятичным коэффициентом и прибавляется к некоторому другому числу (коэффициенту сдвига).



Получающееся число уменьшается по правилу вычитания модуля A, где A - размер алфавита и зашифрованный текст формируется из соответствующих ему алфавитных эквивалентов.

**Аддитивные методы**.

В качестве ключа в этих методах используется некоторая последовательность букв того же алфавита и такой же длины, что и в исходном тексте.
Шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Примером такого же метода является гаммирование, т.е. наложение на исходный текст некоторой последовательности кодов, называемой гаммой. Процесс наложения осуществляется следующим образом:

1. Символы исходного текста и гамма представляются в двоичном коде и располагаются один под другим.
2. Каждая пара двоичных знаков заменяется одним двоичным знаком шифрованного текста в соответствии с принятым алгоритмом.
3. Полученная последовательность двоичных знаков шифрованного текста заменяется символами алфавита в соответствии с выбранным кодом.

Если ключ шифрования выбирается случайным образом, например, формируется с помощью датчика псевдослучайных чисел, то раскрыть информацию, не зная ключа практически невозможно.

**3.2 Криптоанализ.**

***Криптоанализ*** - это наука получения открытого текста не имея ключа.
Успешно проведенный криптоанализ может раскрыть открытый текст или ключ.

Раскрытие ключа не криптологическим способом называют ***компрометацией.*** ***Попытка криптоанализа называется вскрытием***.

 Существует 4 основных типа криптоаналитического вскрытия.
Для каждого из них предполагается, что криптоналитик обладает полнотой знаний об использовании алгоритма шифрования:

1. **Вскрытие с использованием только шифротекста**. У криптоаналитика есть шифротексты нескольких сообщений, зашифрованных одним и тем же алгоритмом шифрования. Задача криптоаналитика состоит в раскрытии открытого текста как можно большего числа сообщений или получения ключа, использованного для шифрования других сообщений, зашифрованных тем же ключом.
2. **Вскрытие с использованием открытого текста**.У криптоаналитика есть доступ не только к шифротекстам нескольких сообщений, но и к открытому тексту этих сообщений. Его задача состоит в получении ключа, использованного для шифрования сообщения, для дешифрования других сообщений, зашифрованных тем же ключом.
3. **Вскрытие с использованием выбранного открытого текста**. У криптоаналитика не только есть доступ к шифротекстам и открытым текстам нескольких сообщений, но и возможность выбирать открытый текст для шифрования.
4. **Адаптивное вскрытие с использованием открытого текста**. Это частный случай вскрытия с использованием выбранного открытого текста.
Криптоаналитик не только может выбирать шифруемый текст, но также может строить свой последующий выбор на базе полученных результатов.
5. **Вскрытие с использованием выбранного шифротекста**. Криптоаналитик может выбрать различные шифротексты для шифрования и имеет доступ к дешифрованным открытым текстам.

Криптоаналитики часто используют индекс соответствия для определения того, находятся ли они на правильном пути.
Теоретически ожидаемое значение индекса соответствия определяется следующим выражением:



где N - длина сообщения в буквах, m - число алфавитов.

Шифровки, которые дают значение индекса соответствия больше чем 0,066 - сами сообщают о том, что вероятно использовалась одноалфавитная подстановка. Если индекс соответствия находится между 0,052 и 0,066, то вероятно был использован двухалфавитный шифр подстановки.

0,047 < И.С. < 0,052 - трехалфавитный шифр.

Криптоаналитик берет наиболее часто встречающийся символ и предполагает, что это пробел, затем берет следующий наиболее частый символ и предполагает, что это буква "e" (для английских текстов) и т.д.
Принципиальное значение для надежности шифрования имеет длина кода ключа, т.е. отношение его длины к длине закрываемого им текста. Чем больше оно приближается к 1, тем надежнее шифрование.