

**Маршаков Д.В., Фатхи Д.В.**



# **Программно-аппаратные средства защиты информации**



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Д.В. Маршаков, Д.В. Фатхи

# ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Ростов-на-Дону  
2020

*Рецензент*

профессор кафедры «Автоматика и телемеханика на железнодорожном транспорте»  
Ростовского государственного университета путей сообщения  
доктор технических наук, профессор *С.В. Соколов*

**Маршаков Д.В.**

Программно-аппаратные средства защиты информации: учебное пособие /  
Д.В. Маршаков, Д.В. Фатхи. – Ростов н/Д: издательский центр ДГТУ, 2020. – 190 с.

Рассмотрены современные методы и средства программно-аппаратной защиты информации, включая системы разграничения доступа, средства идентификации и аутентификации, криптографической и сетевой защиты информации, защиты от вредоносного программного обеспечения, а также приведены примеры специализированных программно-аппаратных средств защиты информации.

Предназначено для обучающихся бакалавриата, специалитета и магистратуры по направлениям информационной безопасности и информационной безопасности телекоммуникационных систем.

УДК 004.056

Печатается по решению редакционно-издательского совета  
Донского государственного технического университета

© Маршаков Д.В., Фатхи Д.В., 2020

© Издательский центр ДГТУ, 2020

## СОДЕРЖАНИЕ

Список условных сокращений	7
ВВЕДЕНИЕ	8
1 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА УПРАВЛЕНИЯ ДОСТУПОМ	12
1.1 Модели контроля и управления доступом	12
1.2 Показатели защищенности от несанкционированного доступа	18
1.3 Средства доверенной загрузки	27
1.4 Системы защиты информации от несанкционированного доступа	33
2 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ	37
2.1 Основные понятия идентификации и аутентификации	37
2.2 Парольная защита информации от несанкционированного доступа	38
2.2.1 Принцип парольной защиты	38
2.2.2 Возможности обхода парольной защиты	40
2.2.3 Повышение эффективности парольной защиты	44
2.2.4 Достоинства и недостатки парольной защиты	45
2.3 Программно-аппаратные системы идентификации и аутентификации	45
2.3.1 Классификация систем идентификации и аутентификации	45
2.3.2 Электронные идентификаторы	48
2.3.3 Биометрические идентификаторы	60
2.3.4 Комбинированные системы идентификации и аутентификации	68
2.4 Особенности применения внешних носителей ключевой информации для идентификации и аутентификации	73
3 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ	74
3.1 Классификация средств криптографической защиты информации	74
3.2 Симметричные криптографические системы	78
3.2.1 Принципы симметричного шифрования информации	78

3.2.2 Алгоритмы симметричного шифрования информации	79
3.2.3 Особенности практического применения симметричных криптографических систем	83
3.3 Асимметричные криптографические системы	85
3.3.1 Принципы асимметричного шифрования информации	85
3.3.2 Алгоритмы асимметричного шифрования информации	87
3.3.3 Особенности практического применения асимметричных криптографических систем	93
3.4 Применение криптографических систем защиты информации	94
3.5 Требованиям к средствам криптографической защиты информации	97
3.6 Программно-аппаратные средства криптографической защиты информации	99
3.7 Средства электронной подписи	103
3.8 Криптопровайдеры	112
4 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА СЕТЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ	114
4.1 Технологии межсетевых экранов	114
4.1.1 Понятие межсетевого экрана	114
4.1.2 Классификация межсетевых экранов	116
4.1.3 Структура и функции межсетевого экрана	117
4.1.4 Особенности функционирования межсетевых экранов на различных уровнях модели OSI	120
4.1.5 Политика межсетевого взаимодействия	123
4.1.6 Персональные и распределенные межсетевые экраны	124
4.1.7 Проблемы безопасности традиционных межсетевых экранов	126
4.1.8 Показатели защищенности межсетевых экранов	129
4.1.9 Программные и программно-аппаратные межсетевые экраны	133
4.2 Системы обнаружения вторжений	138
4.2.1 Понятие системы обнаружения вторжений	138
4.2.2 Структура системы обнаружения вторжений	139
4.2.3 Классификация систем обнаружения вторжений	140

4.2.4 Методы обнаружения сигнатур	144
4.2.5 Методы обнаружения аномалий	146
4.2.6 Проблемы безопасности систем обнаружения вторжений	147
4.2.7 Развертывание систем обнаружения вторжений	149
4.2.8 Требования к системам обнаружения вторжений	151
4.2.9 Программные и программно-аппаратные системы обнаружения вторжений	153
5 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ	157
5.1 Понятие вредоносного программного обеспечения	157
5.2 Классификация вредоносного программного обеспечения	158
5.2.1 Компьютерные вирусы	162
5.2.2 Троянские программы	164
5.2.3 Сетевые черви	167
5.3 Наименование вредоносного программного обеспечения	170
5.4 Методы и средства защиты от вредоносных программ	171
5.4.1 Признаки возможного заражения	171
5.4.2 Методы обнаружения вредоносных программ	172
5.4.3 Виды антивирусных программ	177
5.5 Классификация защищенности средств антивирусной защиты информации	179
5.6 Антивирусные программы и комплексы	181
ЗАКЛЮЧЕНИЕ	186
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	187

## Список условных сокращений

АРМ – автоматизированное рабочее место

АС – автоматизированная система

АСУ ТП – автоматизированная система управления технологическими процессами

ГИС – государственная информационная система

ИСПДн – информационная система персональных данных

ОЗУ (RAM) – оперативное запоминающее устройство

СВТ – средства вычислительной техники

СЗИ – средство защиты информации

СОВ – система обнаружения вторжений

НСД – несанкционированный доступ

ПЗУ (ROM) – постоянное запоминающее устройство

СИА – средства идентификации и аутентификации

СКЗИ – средство криптографической защиты информации

СППЗУ (EPROM) – стираемое программируемое постоянное запоминающее устройство

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ЦП – центральный процессор

ЦРК – центр распределения ключей

ЭСППЗУ (EEPROM) – электрически стираемое программируемое постоянное запоминающее устройство

NGFW – межсетевой экран нового поколения

## ВВЕДЕНИЕ

Уровень развития IT-технологий в настоящее время выдвигает ряд требований как к обеспечению информационной безопасности, вообще, так и к объектам защиты информации, в частности. В данном учебном пособии основное внимание уделяется методам и средствам программно-аппаратной защиты информации в современных условиях.

Под объектом защиты информации понимается компьютерная или автоматизированная система (АС). Предметом защиты в них является информация, материальной основой, для существования которой являются электронные и электромеханические устройства, а также машинные носители. Наряду с термином «информация» также применяют понятие «информационные ресурсы» – документы и массивы документов, существующие отдельно или в составе информационных систем.

Среди АС выделяют автоматизированные производственные системы и автоматизированные информационные системы. Автоматизированные информационные системы используются в управлении, исследованиях, проектировании и других областях, смысл которых заключается в обработке информации. Они также подразделяются на ряд классов в зависимости от выполняемых ими функций (автоматизированная система управления предприятием, автоматизированная система управления технологическими процессами, автоматизированная система технологической подготовки производства и т.д.).

**Автоматизированная система** – это система, обеспечивающая деятельность персонала, реализующего информационную технологию выполнения установленных функций посредством комплекса средств автоматизации. Она включает в себя:

- технические средства вычислительной техники и связи;
- методы и алгоритмы обработки информации, реализованные в виде программных средств;
- информацию (файлы, базы данных) на различных носителях;
- обслуживающий персонал и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам.

В отличие от автоматических систем, которые выполняют свои операции без участия человека, автоматизированные информационные системы выполняют операции как с помощью программных или технических средств, так и с помощью человека, при этом отводя основную роль компьютеру, как правилу, входящему в состав автоматизированного рабочего места (АРМ) сотрудника. В связи с этим далее в учебном пособии понятие компьютерная система отождествляется с понятием АС (автоматизированная

информационная система), которое по определению является более широким. С компьютерной системой соотносят: компьютеры всевозможных классов и назначений, вычислительные комплексы и системы, вычислительные сети (локальные, региональные и глобальные).

Одними из основных понятий теории защиты информации являются понятия «безопасность информации» и «безопасность автоматизированной системы».

**Безопасность автоматизированной системы** – состояние АС, определяющее защищенность обрабатываемой информации и ресурсов от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность АС выполнять предписанные функции без нанесения неприемлемого ущерба объектам и субъектам информационных отношений.

Под безопасностью информации (информационной безопасностью) в АС понимается такое состояние всех её компонент, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. Информационная безопасность является одной из основных составляющих обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы.

Задачей информационной безопасности является защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации.

Под угрозой безопасности информации в АС понимают потенциальное событие или действие, которое может вызвать изменение функционирования АС, нарушающее защищенность обрабатываемой в ней информации. Попытка реализации угрозы называется атакой, а источник угрозы, предпринимающий такую попытку – злоумышленником.

Результатом реализации угроз безопасности информации в АС может быть утечка (копирование) информации, ее утрата (уничтожение) или искажение (подделка), блокирование информации. Поскольку сложно заранее определить возможную совокупность угроз безопасности информации и результатов их реализации, модель потенциальных угроз безопасности информации в АС должна создаваться совместно заказчиком (собственником) АС и разработчиком с привлечением специалистов по защите информации на этапе её проектирования.

Обеспечение информационной безопасности АС является непрерывным процессом, целенаправленно проводимым на всех этапах ее жизненного цикла с комплексным применением всех имеющихся методов и средств.

Информационная безопасность достигается проведением руководством

соответствующего уровня *политики информационной безопасности*. Основным документом, на основе которого проводится политика информационной безопасности, является программа информационной безопасности. Программа разрабатывается и принимается как официальный руководящий документ высшими органами управления ведомством или организацией. В программе приводятся цели политики информационной безопасности, основные направления решения задач защиты информации в АС, а также содержатся общие требования и принципы построения систем защиты информации в АС.

В общем случае, политика информационной безопасности представляет собой некоторый набор требований, прошедших соответствующую проверку, реализуемых при помощи организационных мер и программно-технических средств, и определяющих архитектуру системы защиты. Она должна охватывать все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Реализация политики информационной безопасности для конкретной компьютерной системы осуществляется средствами управления механизмами защиты.

Существующие методы и средства защиты информации (СЗИ) можно подразделить на четыре основные группы:

- организационные методы и средства защиты информации;
- инженерно-технические методы и средства защиты информации;
- криптографические методы и средства защиты информации;
- программно-аппаратные методы и средства защиты информации.

К организационным методам и средствам защиты информации относятся организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации АС для обеспечения защиты информации. На этом уровне защиты информации рассматриваются международные договоры, подзаконные акты государства, государственные стандарты и локальные нормативные акты конкретной организации.

Под инженерно-техническими СЗИ понимают физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства, обеспечивающие комплекс мероприятий по обеспечению безопасности защищаемой АС главным образом от физического воздействия. Важнейшей составной частью инженерно-технических средств защиты информации являются технические средства охраны, которые образуют первый рубеж защиты АС и являются необходимым, но недостаточным условием сохранения конфиденциальности и целостности

информации ней.

Криптографические методы и средства защиты применяются для обеспечения конфиденциальности и целостности информации при её хранении на открытых носителях или передачи по открытым каналам связи, подтверждения подлинности (аутентификации) передаваемой информации, защиты программного обеспечения и других информационных ресурсов от несанкционированного использования и копирования и т.д.

Программно-аппаратные СЗИ сочетают в себе средства защиты данных, функционирующие в составе программного обеспечения, а также электронные и электронно-механические устройства, включаемые в состав технических средств компьютерной системы и выполняющие (самостоятельно или в комплексе с программным обеспечением) функции обеспечения информационной безопасности.

К программным средствам обеспечения защиты информации относятся: средства управления доступом, идентификации и аутентификации пользователей, архивации данных, криптографические средства, антивирусные программы, системы аудита и т.д. К аппаратным средствам – специальные регистры для хранения реквизитов защиты (паролей, идентифицирующих кодов, грифов или уровней секретности), устройства измерения индивидуальных характеристик человека (биометрических признаков) с целью его идентификации, схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных и пр.

Обеспечение защиты информации в автоматизированных информационных системах программными, аппаратными и программно-аппаратными методами и является предметом рассмотрения настоящего учебного пособия, которое представляет собой структурированную подборку материалов по наиболее актуальным средствам и методам защиты информации на момент его издания.

# 1 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА УПРАВЛЕНИЯ ДОСТУПОМ

## 1.1 Модели управления доступом

Основную роль в методе формальной разработки системы играет так называемая *модель безопасности*, также именуемая как *модель управления доступом* или модель политики безопасности. Целью этой модели является выражение сути требований по безопасности к данной системе, определение потоков информации, разрешенных в системе, и правил управления доступом к ней.

Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты. Так как она является формальной, возможно осуществить доказательство различных свойств безопасности системы.

Безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности.

Согласно руководящему документу «Защита от несанкционированного доступа к информации. Термины и определения» [22], приведем основные понятия, применяемые в моделях разграничения доступа.

*Доступ к информации* – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

*Правила разграничения доступа* – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

*Объект доступа* – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа. Далее под объектом доступа будем понимать различные контейнеры с информацией.

*Субъект доступа* – лицо или процесс, действия которого регламентируются правилами разграничения доступа. Далее под субъектом доступа будем понимать пользователя (или процесс, действующий от его имени), выполняющего различные операции над объектами доступа.

*Несанкционированный доступ к информации* (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или АС.

На практике выделяют три основные модели управления доступом к объектам:

мандатную, дискреционную и ролевую.

**Мандатная модель управления доступом.** *Мандатное управление доступом* (mandatory access control), называемое также полномочным разграничением доступа, основано на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

Согласно требованиям Федеральной службы по техническому и экспортному контролю<sup>1</sup> (ФСТЭК России) мандатное управление доступом является ключевым отличием систем защиты Государственной Тайны РФ старших классов 1В и 1Б от младших классов защитных систем на классическом разделении прав по матрице доступа (см. далее).

В соответствии с принципом мандатного управления доступом, каждому объекту можно присвоить метку конфиденциальности, для учетной записи пользователя (субъекта) также назначается уровень конфиденциальности, который определяет объекты, к которым он может иметь доступ.

Например, в системе защиты Dallas Lock 8.0 метки конфиденциальности имеют номера от 0 до 7 – чем больше номер, тем выше уровень конфиденциальности. Для удобства работы, на практике меткам конфиденциальности присваивают символические имена, например:

- 0 – Открытые данные;
- 1 – Конфиденциальные данные;
- 2 – Персональные данные;
- 3 – Секретные данные;
- 4 – Совершенно секретно и т.д.

Мандатная модель управления доступом является основой реализации разграничительной политики доступа к ресурсам при защите информации ограниченного доступа. Самое важное её достоинство заключается в том, что пользователь не может полностью управлять доступом к ресурсам, которые он создаёт. Политика безопасности системы, установленная администратором, полностью определяет доступ, и обычно пользователю не разрешается устанавливать более свободный доступ к его ресурсам, чем тот, который установлен администратором пользователю.

Классической моделью контроля и управления доступом, основанной на мандатной модели, является *модель Белла-Лападулы*, описанная в 1975 году сотрудниками компании

---

<sup>1</sup> До 2004 года – Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России).

MITRE Corporation (США) Дэвидом Беллом и Леонардом Лападулой. В данной модели анализируются условия, при которых невозможно создание информационных потоков от субъектов с более высоким уровнем доступа к субъектам с более низким уровнем доступа.

В модели Белла-Лападулы каждому объекту и субъекту системы назначается свой уровень доступа, все возможные уровни доступа системы четко определены и упорядочены по возрастанию секретности. При этом действуют два основных правила (рис. 1.1).

1. Пользователь может читать только объекты с уровнем допуска не выше его собственного.

2. Пользователь может изменять только те объекты, уровень допуска которых не ниже его собственного.

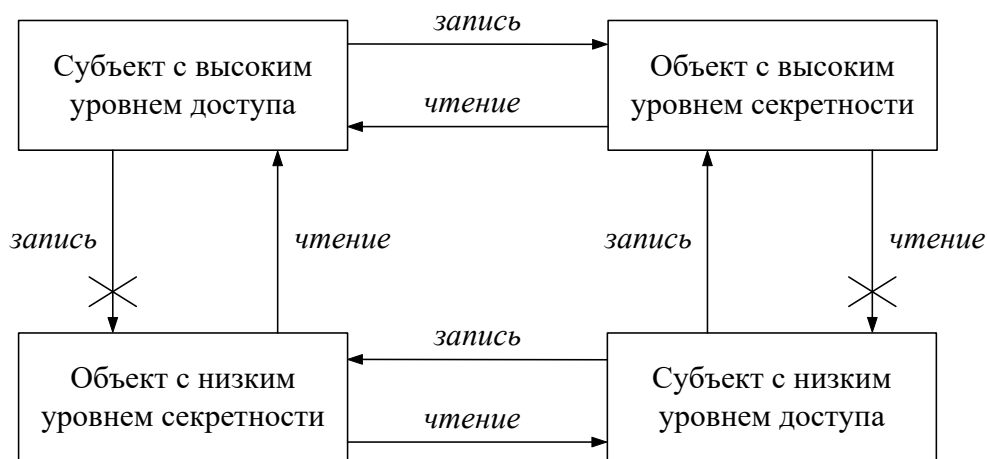


Рис. 1.1 – Отношения между объектами и субъектами с различным уровнем доступа в модели Белла-Лападулы.

Цель первого правила является очевидной. Смысл второго правила заключается в том, чтобы воспрепятствовать пользователю с высоким уровнем доступа, случайно или умышленно, раскрыть известную ему секретную информацию.

Модель Белла-Лападулы стала первой значительной моделью политики безопасности, применимой для компьютерных систем. Модель полностью формализована, но на практике практически не используется «в чистом виде», а дополняется элементами других моделей доступа, поскольку вызывает подчас ряд противоречий. Например, в модели игнорируется проблема изменения классификации: предполагается, что все сведения относятся к соответствующему уровню секретности, который остается неизменным, однако, бывают случаи, когда пользователи должны работать с данными, которые они не имеют права

увидеть.

**Дискреционная модель управления доступом.** *Дискреционное управление доступом* (discretionary access control), также именуемое избирательным или разграничительным управлением доступа, обеспечивает доступ к защищаемым объектам в соответствии со списками пользователей (субъектов), согласно содержимым которых вычисляются права на доступ к объекту для каждого пользователя.

В данной модели для каждого объекта существует субъект-владелец, который обладает на него полными правами и может делегировать часть прав другим субъектам, определив разрешенные операции доступа, к которым относятся: чтение, запись, выполнение (для программ) и пр. Таким образом, управление доступом осуществляется путем явной выдачи полномочий на проведение действий с каждым из объектов системы – для каждой пары субъект-объект устанавливается набор разрешенных операций доступа.

Одним из способов реализации такой модели является задание *матрицы доступа*, в которой определены права доступа субъектов системы к объектам. Строки матрицы соответствуют субъектам, а столбцы – объектам. Каждая ячейка матрицы содержит набор прав, которые соответствующий субъект имеет по отношению к соответствующему объекту. Пример матрицы доступа представлен на рис. 1.2.

	Объект №1	Объект №2	Объект №3	Объект №4	Объект №5	Объект №6
Субъект №1				П	П	П
Субъект №2				П	П	П
Субъект №3	Ч	Ч	Ч	П	Ч	П
Субъект №4	Ч	Ч	Ч	П	Ч	Ч
Субъект №5	П	П	П	П		П
Субъект №6		П	П	П		П
Субъект №7			П	П		П
Субъект №8	П	П	П	П		П
Субъект №9		П	П	П		П
Субъект №10			П	П		П

Рис. 1.2 – Пример матрицы доступа, где введены следующие обозначения:

П – полный доступ, Ч – только чтение, пробел – закрыть доступ.

Дискреционный подход, в сравнении с мандатным, позволяет создать гораздо более гибкую схему безопасности, но при этом он и гораздо более сложен в администрировании. С программной точки зрения его реализация проста, но при достаточно большом количестве объектов и субъектов система становится практически неуправляемой. Для решения этой проблемы применяется, например, объединение пользователей в группы, после чего права раздаются группам пользователей, а не каждому субъекту в отдельности.

Одной из уязвимостей дискреционной модели является то, что субъект, который имеет право на чтение информации, может, без уведомления владельца объекта, случайно или преднамеренно передать её неавторизованным пользователям. Кроме того, не во всех компьютерных системах каждому объекту можно назначить владельца (во многих случаях данные принадлежат не отдельным субъектам, а всей системе).

**Ролевая модель управления доступом.** *Управление доступом на основе ролей* (role based access control), так называемая ролевая модель, контролирует доступ субъектов к объектам на основе типов их активностей в системе – ролей. Под *ролью* понимается совокупность действий и обязанностей, связанных с определенным видом деятельности субъекта (администратор баз данных, секретарь, начальник отдела и т.д.).

В данной модели с каждым объектом сопоставлен набор разрешенных операций доступа для каждой роли (а не для каждого пользователя). В свою очередь, каждому пользователю сопоставлены роли, которые он может выполнять. В некоторых системах пользователю разрешается выполнять несколько ролей одновременно. К примеру, роль «секретарь» может включать в себя роль «регистратор» и, плюс к тому, еще несколько дополнительных операций. Для того чтобы множества операций, связанных с различными ролями, не пересекались, вводится иерархическая зависимость между ролями. Также есть ограничение на одну или несколько не противоречащих друг другу ролей в каждый момент времени.

Таким образом, ролевая модель контроля доступом является развитием политики дискреционного управления доступом, но не является её частным случаем. В данной модели, в отличие от дискреционной, у объектов отсутствуют определенные хозяева – вся информация расценивается как принадлежащая организации, владеющей системой, и, как следствие, пользователю невозможно делегировать права на какой-то определенный объект. Достоинством ролевой модели является упрощение процесса администрирования: отпадает необходимость прописывать разрешения для каждой пары объект-субъект, вместо чего задаются разрешения для пар объект-роль и определяются роли каждого пользователя. Роль

пользователя в системе обладает минимальными привилегиями, необходимыми для выполнения требуемых задач, и запрещает другие полномочия, что не позволяет обойти политику безопасности системы.

С помощью ролевой модели управления доступом могут быть смоделированы как дискреционные и мандатные системы управления доступом. Модель широко используется для управления пользовательскими привилегиями в пределах единой системы или приложения. Список таких систем включает в себя: Microsoft Active Directory, SELinux, FreeBSD, Solaris, СУБД Oracle, PostgreSQL 8.1, SAP R/3, Lotus Notes и др.

**Системы разграничения доступа.** Конкретное воплощение модели разграничения доступа находят в системах разграничения доступа. *Система разграничения доступа* – это совокупность реализуемых правил разграничения доступа в СВТ или АС [22].

Система разграничения доступа к информации содержит четыре функциональных блока: блок идентификации и аутентификации субъектов доступа, диспетчер доступа, блок криптографического преобразования информации при ее хранении и передаче, блок очистки памяти.

Многие системы разграничения доступа базируются на концепции диспетчера доступа, необходимость использования которого возникает применительно к многопользовательским компьютерным системам. *Диспетчер доступа* реализуется в виде аппаратно-программных механизмов, выступает посредником при всех обращениях субъектов к объектам, и обеспечивает необходимую между ними дисциплину разграничения доступа, в том числе к аппаратным блокам, узлам, устройствам (рис. 1.3).

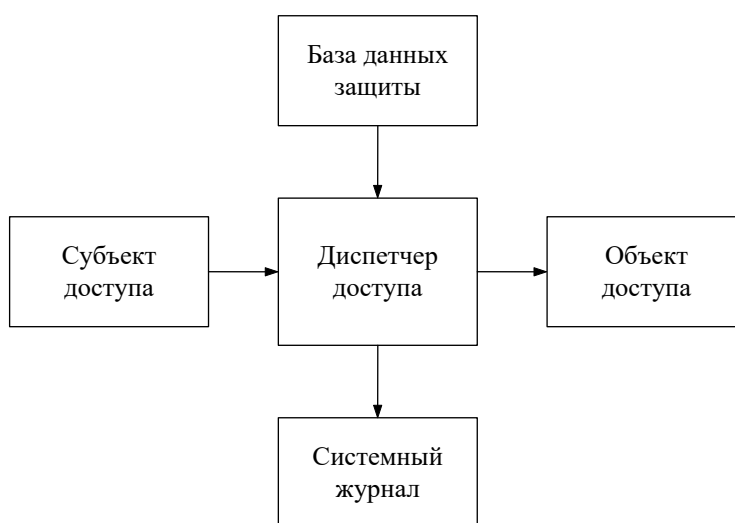


Рис. 1.3 – Сущность концепции диспетчера доступа.

Диспетчер доступа использует базу данных защиты, в которой хранятся правила разграничения доступа на основании которых он разрешает, либо запрещает субъекту доступ к объекту, а также фиксирует информацию о попытке доступа в системном журнале.

Основными требованиями к реализации диспетчера доступа являются:

- требование полноты контролируемых операций, согласно которому проверке должны подвергаться все операции всех субъектов над всеми объектами системы. Обход диспетчера предполагается невозможным;
- требование изолированности, т.е. защищенности диспетчера от возможных изменений субъектами доступа с целью влияния на процесс его функционирования;
- требование формальной проверки правильности функционирования;
- минимизация используемых диспетчером ресурсов.

Под *базой данных защиты* понимают базу данных, хранящую информацию о правах доступа субъектов системы к объектам и другим субъектам. База данных защиты строится на основе списка полномочий и характеристик доступа.

Кроме преднамеренных попыток НСД диспетчер фиксирует нарушения правил разграничения, явившихся следствием отказов, сбоев аппаратных и программных средств, а также вызванных ошибками персонала и пользователей.

В распределенных компьютерных системах криптографическая защита информации является единственным надежным способом защиты от НСД. В средствах разграничения доступа должна быть реализована функция очистки оперативной памяти и рабочих областей на внешних запоминающих устройствах после завершения выполнения программы, обрабатывающей конфиденциальные данные. Причем очистка должна производиться путем записи в освободившиеся участки памяти определенной последовательности двоичных кодов, а не удалением только учетной информации о файлах из таблиц операционной системы, как это делается при стандартном удалении её средствами.

## **1.2 Показатели защищенности от несанкционированного доступа**

Требования по безопасности информации, характеризующие применяемые средства защиты информации в проектируемых информационных системах, определяются различными актами, регулирующими деятельность по обеспечению защиты информации от утечки и несанкционированных действий, – так называемыми *регуляторами* в области обеспечения информационной безопасности.

В общем случае структурой, определяющей порядок и координирующей действия обеспечения некриптографическими методами информационной безопасности, является ФСТЭК России, криптографическими методами – Федеральная служба безопасности (ФСБ России).

Функциональность СЗИ от НСД должна предотвращать или существенно затруднять несанкционированное проникновение в обход правил разграничения доступа, реализованных штатными средствами. Под *штатными средствами* понимается совокупность программного и технического обеспечения средств вычислительной техники или автоматизированных систем.

В общей теории систем выделяют понятия система и элемент. Под системой понимается совокупность взаимосвязанных и взаимодействующих элементов. Элемент – простейшая, неделимая на данном уровне рассмотрения, часть системы. При этом регулятор полагает, что СВТ являются элементами, из которых строятся АС, поэтому, не решая прикладных задач, они не содержат пользовательской информации [5]. Совокупность требований по защите СВТ и АС, перечень показателей защищенности, образуют *класс защищенности*.

Деление АС на соответствующие классы с точки зрения защиты информации необходимо с целью разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Существует множество национальных и международных классификаций классов защищенности. В России роль национальных оценочных стандартов в области информационной безопасности выполняют руководящие документы, выпущенные Гостехкомиссией, и методические документы, утвержденные ФСТЭК, стратегически ориентированные на «Общие критерии оценки защищённости информационных технологий» (Common Criteria for Information Technology Security Evaluation) – международный стандарт по компьютерной безопасности.

**Классификация СЗИ по уровню контроля отсутствия недеklarированных возможностей.** Программное обеспечение СЗИ (как отечественного, так и импортного производства) должно соответствовать своим заявленным характеристикам, а значит не обладать функциональностью, способствующей организации успешных атак в отношении защищаемых объектов – недеklarированными возможностями.

*Недеklarированные возможности* (НДВ) – это функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности,

доступности или целостности обрабатываемой информации. Реализацией НДВ, в частности, являются программные закладки.

Согласно руководящему документу «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» [22] установлено 4 уровня контроля отсутствия НДВ, каждый из которых характеризуется определенной минимальной совокупностью требований (рис. 1.4).

1 уровень контроля	2 уровень контроля	3 уровень контроля	4 уровень контроля
<b>Особой важности</b>	<b>Совершенно секретно</b>	<b>Секретно</b>	Информация, не содержащая сведения, отнесенные к государственной тайне
Информация, содержащая сведения, отнесенные к государственной тайне			
<i>Информация ограниченного доступа</i>			

Рис. 1.4 – Классификация по уровню контроля на отсутствие НДВ

Первый уровень контроля (самый высокий) достаточен для программного обеспечения, используемого при защите информации с грифом «особой важности».

Второй уровень контроля достаточен для программного обеспечения, используемого при защите информации с грифом «совершенно секретно».

Третий уровень контроля достаточен для программного обеспечения, используемого при защите информации с грифом «секретно».

Четвертый уровень контроля (самый низкий) достаточен для программного обеспечения, используемого при защите конфиденциальной информации, не содержащей сведений, относящихся к государственной тайне.

Для программного обеспечения, используемого при защите информации, отнесенной к государственной тайне, должен быть обеспечен уровень контроля не ниже третьего.

**Классификация защищенности средств вычислительной техники.** Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем. Показатели защищенности СВТ применяются к общесистемным программным средствам и операционным системам.

Согласно руководящему документу «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [24] устанавливается 7 классов защищенности СВТ от НСД к информации: где первый считается самым высоким классом, а седьмой – самым низким.

Классы подразделяются на 4 группы, отличающиеся уровнем защиты (рис. 1.5).

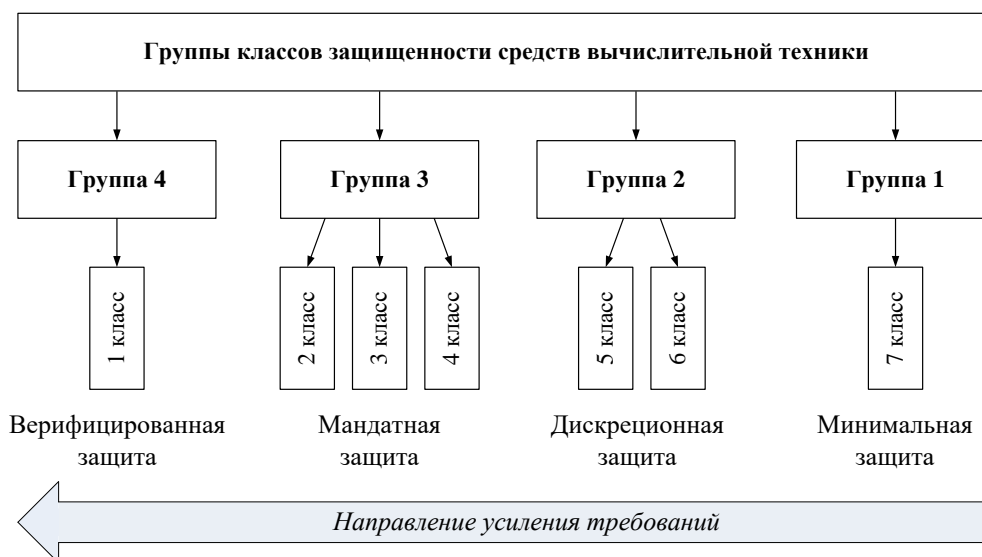


Рис. 1.5 – Группы классов защищенности СВТ.

Первая группа содержит только один 7 класс. Он устанавливается для СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований 6 класса.

Вторую группу образуют 6 и 5 классы защищенности, и она характеризуется наличием дискреционного управления доступом.

Третью группу составляют 4, 3 и 2 классы, отличающиеся реализацией мандатного управления доступом. При этом для СВТ данных классов присутствует механизм дискреционного управления доступом, где дискреционные правила служат дополнением мандатных.

Четвертая группа содержит только 1 класс и характеризуется верифицированной защитой, гарантированно обеспечивающим перехват диспетчером доступа всех обращений субъектов доступа к объектам.

Перечень показателей по классам защищенности СВТ приведен в таблице 1.1, в которой введены следующие обозначения: «–» – нет требований к данному классу, «+» –

новые или дополнительные требования, «=» – требования совпадают с требованиями к СВТ предыдущего класса.

Таблица 1.1 – Перечень показателей по классам защищенности СВТ

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	–	–	+	=	=	=
Очистка памяти	–	+	+	+	=	=
Изоляция модулей	–	–	+	=	+	=
Маркировка документов	–	–	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	–	–	+	=	=	=
Сопоставление пользователя с устройством	–	–	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	–	+	+	+	+	+
Регистрация	–	+	+	+	=	=
Взаимодействие пользователя с комплексом средств защиты	–	–	–	+	=	=
Надежное восстановление	–	–	–	+	=	=
Целостность комплекса средств защиты	–	+	+	+	=	=
Контроль модификации	–	–	–	–	+	=
Контроль дистрибуции	–	–	–	–	+	=
Гарантии архитектуры	–	–	–	–	–	+
Тестирование	+	+	+	+	+	=
Руководство для пользователя	+	=	=	=	=	=
Руководство по комплексу средств защиты	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Выбор класса защищенности СВТ для АС, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

**Классификация защищенности автоматизированных систем.** Нормативно-методическим материалом при формулировании и реализации требований по защите АС от НСД, описывающем порядок и правила проведения классификации АС, является руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [21]. В соответствии с этим документом установлено три группы классов

защищенности АС от НСД, отличающиеся особенностями обработки информации в АС (рис. 1.6).

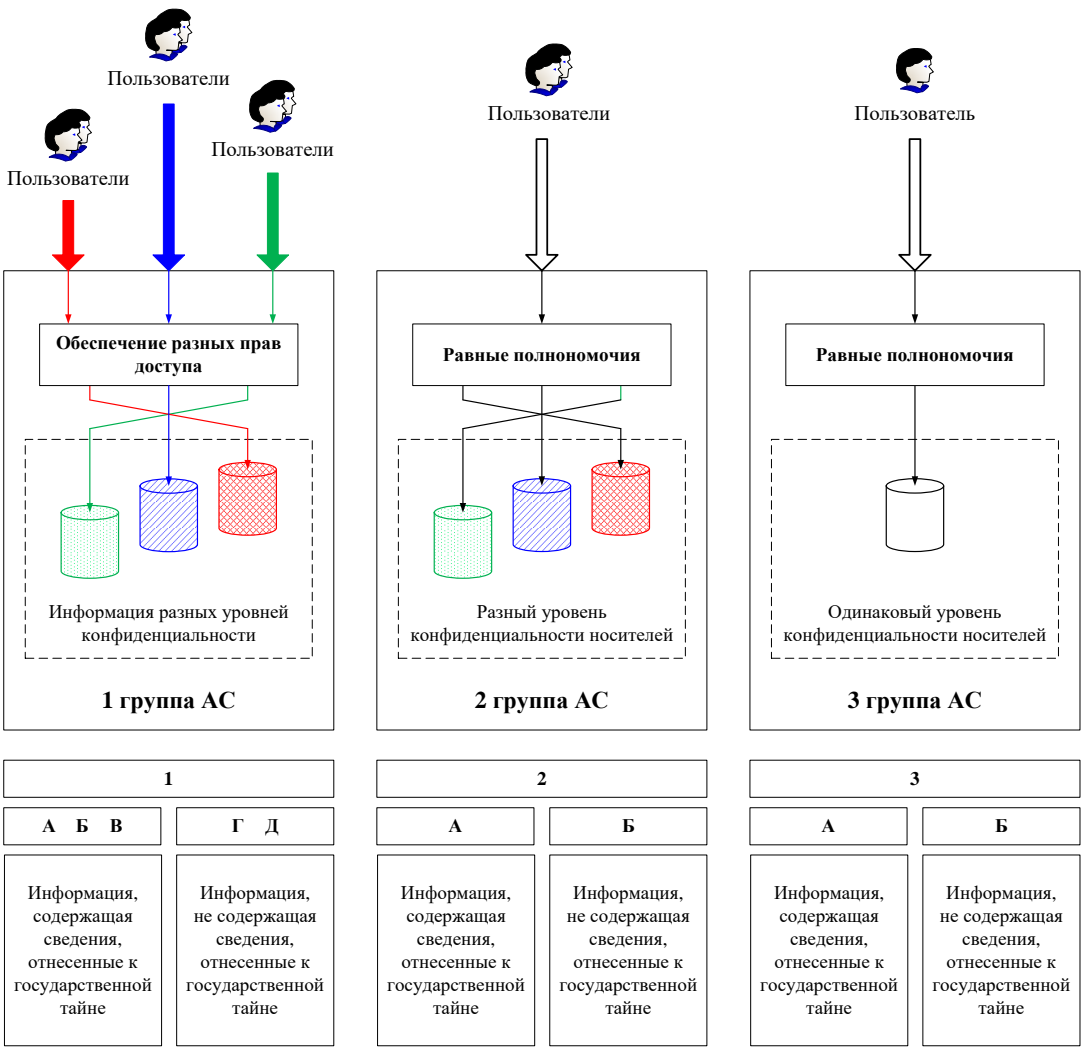


Рис. 1.6 – Классы защищенности АС [5].

Первая группа состоит из пяти классов – 1Д, 1Г, 1В, 1Б, 1А. Она охватывает многопользовательские АС, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности. Пользователи имеют разные права доступа к информации.

Вторая группа содержит классы 2Б и 2А. Она включает многопользовательские АС, в которых пользователи имеют равные полномочия доступа ко всем информационным ресурсам АС. При этом сама информация находится на носителях различного уровня конфиденциальности.

Третью группу образуют классы 3Б и 3А. Она подразумевает однопользовательские АС, в которых пользователь имеет доступ ко всем информационным ресурсам системы. Уровень конфиденциальности носителей одинаковый.

Следует отметить, что классы 3А, 2А, 1А, 1Б и 1В присваиваются АС, обрабатывающим информацию, содержащую сведения, составляющие государственную тайну (секретная, совершенно секретная, особой важности).

Перечень показателей по классам защищенности АС приведен в таблице 1.2, в которой введены следующие обозначения: «–» – нет требований к данному классу, «+» – есть требования к данному классу.

Таблица 1.2 — Требования к АС

Подсистемы и требования	Классы защищенности								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
<b>1. Подсистема управления доступом</b>									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	–	–	–	+	–	+	+	+	+
к программам	–	–	–	+	–	+	+	+	+
к томам, каталогам, файлам, записям, полям записей	–	–	–	+	–	+	+	+	+
Управление потоками информации			–	+	–	–	+	+	+
<b>2. Подсистема регистрации и учета</b>									
2.1. Регистрация и учет:									
входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов	–	+	–	+	–	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	–	–	–	+	–	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	–	–	–	+	–	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	–	–	–	+	–	+	+	+	+
изменения полномочий субъектов доступа	–	–	–	–	–	–	+	+	+
создаваемых защищаемых объектов доступа	–	–	–	+	–	–	+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+

2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	–	+	–	+	–	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	–	–	–	–	–	–	+	+	+
<b>3. Криптографическая подсистема</b>									
3.1. Шифрование конфиденциальной информации	–	–	–	+	–	–	–	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	–	–	–	–	–	–	–	–	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	–	–	–	+	–	–	–	+	+
<b>4. Подсистема обеспечения целостности</b>									
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	–	–	–	+	–	–	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	–	+	–	+	–	–	+	+	+

Согласно руководящему документу, необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС (коллективный или индивидуальный).

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации, для чего необходима схема анализа объекта защиты информации.

При разработке АС, предназначенной для обработки или хранения информации, отнесенной к государственной тайне, необходимо ориентироваться на классы защищенности не ниже 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

- не ниже 4 класса – для класса защищенности АС 1В;
- не ниже 3 класса – для класса защищенности АС 1Б;
- не ниже 2 класса – для класса защищенности АС 1А.

Автоматизированные системы, обрабатывающие коммерческую тайну, считается целесообразным относить к классам 3Б, 2Б или не ниже 1Д. Однако собственник информации может выдвинуть более жесткие требования к ее защите, в таком случае АС может быть присвоен более высокий класс.

Автоматизированным системам, обрабатывающим служебную тайну присваивается класс 3Б, 2Б или не ниже 1Г.

Автоматизированные системы, ведущие обработку персональных данных, относятся к классам 3Б, 2Б и не ниже 1Д.

Пересмотр класса защищенности АС производится в том случае, если произошло изменение хотя бы одного из критериев, на основании которых он был установлен [25].

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

**Классификация защищенности информационных систем.** Определение класса защищенности государственных информационных систем (ГИС) осуществляется в соответствии с приказом ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г. № 17 и в методическом документе «Меры защиты информации в государственных информационных системах», утвержденном ФСТЭК России 11.02.2014 г.

Устанавливаются три класса защищенности информационной системы, где первый считается самым высоким, третий – самым низким. Класс защищенности информационной системы (первый класс К1, второй класс К2, третий класс К3) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Классификация ГИС приведена в таблице 1.3.

Таблица 1.3 – Классификация ГИС

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ1	К1	К1	К1
УЗ2	К1	К2	К2
УЗ3	К2	К3	К3

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации и/или оператора от нарушения конфиденциальности, целостности или доступности информации.

Информация имеет высокий уровень значимости (УЗ1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба.

Информация имеет средний уровень значимости (УЗ2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

Информация имеет низкий уровень значимости (УЗ3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

При обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации определяются отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

Для определения степени возможного ущерба от нарушения конфиденциальности, целостности или доступности информации могут применяться национальные стандарты и/или методические документы, разработанные и утвержденные ФСТЭК России.

### 1.3 Средства доверенной загрузки

**Принцип доверенной загрузки.** Одним из способов реализации НСД является применение вредоносного программного обеспечения, функционирующего на уровне

BIOS/UEFI. Внедренное в микропрограмму, оно получает прямой доступ к аппаратному обеспечению и может использовать технологию виртуализации для компрометации системы без ведома пользователя и незаметно для операционной системы. Другим способом является, например, загрузка системы с внешнего носителя злоумышленника. В рамках реализации мер по управлению доступом предусмотрено обеспечение так называемой *доверенной загрузки*. Разрешать доступ только для авторизованных пользователей, контролировать целостность разделов и файлов, осуществлять доверенную загрузку – задача средств доверенной загрузки.

**Средство (модуль) доверенной загрузки** – программно-техническое средство, которое осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, контроль целостности своего программного обеспечения и среды функционирования (программной среды и аппаратных компонентов средств вычислительной техники), а также не препятствует доступу к информационным ресурсам в случае успешных контроля целостности своего программного обеспечения и среды функционирования, проверки подлинности пользователя и загружаемой операционной системы.

Блокирование средством доверенной загрузки подразумевает перезагрузку или выключение СВТ, если в течение определенного времени после включения питания управление загрузкой не будет передано на средство доверенной загрузки.

В соответствии с Приказом ФСТЭК России от 27 сентября 2013 г. №119 были утверждены требования к средствам доверенной загрузки, включающие общие требования к средствам доверенной загрузки и требования к функциям безопасности средств доверенной загрузки [27]. Согласно требованиям устанавливаются три типа средств доверенной загрузки:

- 1) средства доверенной загрузки уровня базовой системы ввода-вывода (УБ);
- 2) средства доверенной загрузки уровня платы расширения (ПР);
- 3) средства доверенной загрузки уровня загрузочной записи (ЗЗ).

Средства доверенной загрузки уровня базовой системы ввода-вывода (уровня BIOS) представляют собой многокомпонентные программные средства, один из модулей которых встраивается непосредственно в микропрограмму материнской платы. Для функционирования таких средств не требуется установка плат PCI/PCI-E, что существенно упрощает и ускоряет ввод СЗИ в эксплуатацию.

Средства доверенной загрузки уровня платы расширения всегда программно-аппаратные. Пример средства доверенной загрузки уровня платы расширения приведен на рис. 1.7.

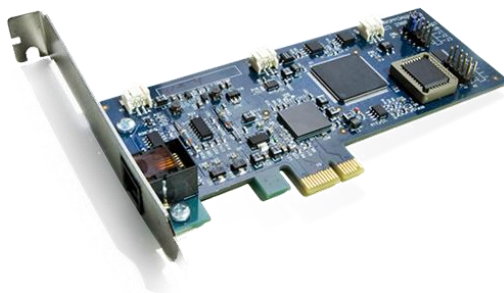


Рис. 1.7 – Средство доверенной загрузки уровня платы расширения («Соболь»).

Средства доверенной загрузки уровня загрузочной записи базируются на модификации загрузочных секторов логических разделов жестких дисков – их содержимое шифруется, что позволяет скрыть информацию о логических разделах при несанкционированной загрузке компьютера.

Доверенная загрузка относится не только к физическому оборудованию, но и к среде виртуализации (серверов виртуализации, виртуальных машин, серверов управления виртуализацией).

Для пояснения принципа доверенной загрузки рассмотрим загрузку физической среды на примере сценария загрузки компьютера с микропрограммой BIOS. В этом случае стандартная процедура начальной загрузки, вызываемая по определенному прерыванию, выбирает устройство начальной загрузки. Список устройств, которые могут являться загрузочными, хранится в энергонезависимой памяти компьютера, а порядок просмотра этого списка является одним из настраиваемых параметров BIOS Setup. При внедрении в процедуру загрузки вредоносного программного обеспечения (буткита) оно на начальном этапе своей работы заменяет оригинальный загрузчик и ожидает перезагрузки компьютера. К её основным задачам относится перехват прерывания, при помощи которого файловые компоненты операционной системы считываются с диска в память, чтобы подменить файлы операционной системы на свои компоненты [1]. В случае применения средств доверенной загрузки в момент завершения процедур самотестирования происходит сканирование области модулей расширений в поисках дополнительных модулей BIOS. В этот момент средство доверенной загрузки, переопределив на себя процедуру начальной загрузки, получает управление вне зависимости от приоритетности выбора загрузочных устройств в BIOS Setup. При этом отличие средства доверенной загрузки уровня платы расширения от средства доверенной загрузки уровня базовой системы ввода-вывода заключается в том, что

в первом случае загрузчик удостоверяется программой, записанной в энергонезависимой памяти контроллера, а во втором – модулем, встроенным в микропрограмму BIOS.

Большинство средств доверенной загрузки на сегодняшний день являются программно-аппаратными. Однако использование аппаратной платы не всегда возможно в силу, например, отсутствия необходимого слота на материнской плате или несовместимости платы с версией BIOS системной платы. Кроме того, установка аппаратной части на большое количество платформ требует значительных временных ресурсов.

**Классификация защищенности средств доверенной загрузки.** Для дифференциации требований к функциям безопасности средств доверенной загрузки выделяются 6 классов защиты средств доверенной загрузки. Самый низкий класс – шестой, самый высокий – первый.

Средства доверенной загрузки, соответствующие 6 классу защиты, применяются в информационных системах, не являющихся ГИС, информационными системами персональных данных (ИСПДн), информационными системами общего пользования и не предназначенных для обработки информации ограниченного доступа, содержащей сведения, составляющие государственную тайну.

Средства доверенной загрузки, соответствующие 5 классу защиты, применяются:

- в ГИС 3 класса защищенности в случае отсутствия взаимодействия этих систем с информационно-телекоммуникационными сетями международного информационного обмена, а также в ГИС 4 класса защищенности,
- в ИСПДн при необходимости обеспечения 3 уровня защищенности персональных данных, в случае актуальности угроз 3-го типа и отсутствия взаимодействия этих систем с информационно-телекоммуникационными сетями международного информационного обмена, а также при необходимости обеспечения 4 уровня защищенности персональных данных.

Средства доверенной загрузки, соответствующие 4 классу защиты, применяются:

- в ГИС 3 класса защищенности в случае их взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена, а также в ГИС 1 и 2 классов защищенности,
- в ИСПДн при необходимости обеспечения 3 уровня защищенности персональных данных в случае актуальности угроз 2-го типа или взаимодействия этих систем с информационно-телекоммуникационными

сетями международного информационного обмена, а также при необходимости обеспечения 1 и 2 уровня защищенности персональных данных;

- в информационных системах общего пользования II класса.

Средства доверенной загрузки, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Детализация требований к функциям безопасности средств доверенной загрузки, а также взаимосвязи этих требований приведены для каждого класса и типа средств доверенной загрузки в профилях защиты, утвержденных ФСТЭК России в качестве методических документов.

Идентификаторы профилей защиты представляются формате «ИТ.СДЗ.тип/класс.ПЗ», где ИТ – «информационная технология», СДЗ – «средство доверенной загрузки», ПЗ – «профиль защиты». Спецификация профилей защиты средств доверенной загрузки для каждого их типа и класса защиты приведена в таблице 1.4.

Таблица 1.4 – Идентификаторы профилей средств доверенной загрузки

Тип средства доверенной загрузки	Класс защиты					
	6	5	4	3	2	1
уровень базовой системы ввода-вывода	–	–	ИТ.СДЗ.УБ4.ПЗ	ИТ.СДЗ.УБ3.ПЗ	ИТ.СДЗ.УБ2.ПЗ	ИТ.СДЗ.УБ1.ПЗ
уровень платы расширения	–	–	ИТ.СДЗ.ПР4.ПЗ	ИТ.СДЗ.ПР3.ПЗ	ИТ.СДЗ.ПР2.ПЗ	ИТ.СДЗ.ПР1.ПЗ
уровень загрузочной записи	ИТ.СДЗ.336.ПЗ	ИТ.СДЗ.335.ПЗ	–	–	–	–

**Примеры средств доверенной загрузки.** Приведем примеры некоторых средств доверенной загрузки.

**Соболь**<sup>1</sup> – аппаратно-программный модуль доверенной загрузки от российской компании ООО «Код безопасности», соответствующий требованиям ФСТЭК к средствам доверенной загрузки уровня платы расширения 2 класса защиты (ИТ.СДЗ.ПР2.ПЗ).

**Dallas Lock**<sup>1</sup> – программно-аппаратное средство доверенной загрузки от российской компании ООО «Конфидент», соответствующее требованиям ФСТЭК к средствам доверенной загрузки уровня платы расширения 2 класса защиты (ИТ.СДЗ.ПР2.ПЗ).

<sup>1</sup> [www.securitycode.ru](http://www.securitycode.ru)

**Блокхост-АМДЗ 2.0**<sup>2</sup> – аппаратно-программный комплекс доверенной загрузки от российской компании ООО «Газинформсервис», соответствующий требованиям ФСТЭК к средствам доверенной загрузки уровня платы расширения 2 класса защиты (ИТ.СДЗ.ПР2.ПЗ).

**Максим-М1**<sup>3</sup> – аппаратно-программный модуль доверенной загрузки от российской компании АО «НПО РусБИТех», соответствующий требованиям ФСТЭК к средствам доверенной загрузки уровня платы расширения 2 класса защиты (ИТ.СДЗ.ПР2.ПЗ).

**Аккорд-АМДЗ**<sup>4</sup> – аппаратный модуль доверенной загрузки от российской компании ООО «Особое конструкторское бюро систем автоматизированного проектирования» (ОКБ САПР), соответствующее требованиям ФСТЭК к средствам доверенной загрузки уровня платы расширения 4 класса защиты (ИТ.СДЗ.ПР4.ПЗ).

**Горизонт-ВС**<sup>5</sup> – программно-аппаратный комплекс, предназначенный для построения доверенных виртуальных (облачных) инфраструктур различной конфигурации от российской компании ООО «ИЦ «Баррикады», соответствующий требованиям ФСТЭК к средствам доверенной загрузки уровня платы расширения 4 класса защиты (ИТ.СДЗ.ПР4.ПЗ).

**Витязь**<sup>6</sup> – программное средство доверенной загрузки от российской компании АО «Крафтвэй корпорэйшн ПЛС» (Kraftway), соответствующее требованиям ФСТЭК к средствам доверенной загрузки уровня базовой системы ввода-вывода 2 класса защиты (ИТ.СДЗ.УБ2.ПЗ).

**ALTELL TRUST**<sup>7</sup> – программное средство доверенной загрузки, встроенное в UEFI BIOS, от российской компании ООО «АльтЭль» (Altell), соответствующее требованиям ФСТЭК к средствам доверенной загрузки уровня базовой системы ввода-вывода 2 класса защиты (ИТ.СДЗ.УБ2.ПЗ).

Другими примерами средств доверенной загрузки являются: **Aladdin Trusted Security Module** (ЗАО «Аладдин Р.Д.»), **Криптон-замок** (ООО Фирма «Анкад»), **ViPNet SafeBoot** (ОАО «ИнфоТеКС»), **МДЗ-Эшелон** (АО «НПО «Эшелон») и др.

Для комплексной защиты системы от НСД помимо применения средства доверенной загрузки требуется системный подход, подразумевающий его совместное использование с

---

<sup>1</sup> [www.dallaslock.ru](http://www.dallaslock.ru)

<sup>2</sup> [www.gaz-is.ru](http://www.gaz-is.ru)

<sup>3</sup> [www.rusbitech.ru](http://www.rusbitech.ru)

<sup>4</sup> [www.okbsapr.ru](http://www.okbsapr.ru)

<sup>5</sup> [www.gorizont-vs.ru](http://www.gorizont-vs.ru)

<sup>6</sup> [www.kraftway.ru](http://www.kraftway.ru)

<sup>7</sup> [www.altell.ru](http://www.altell.ru)

СЗИ от НСД. В этом случае средство доверенной загрузки реализует свои основные функции до старта операционной системы, а с помощью средств администрирования СЗИ от НСД, наряду с его собственным функционалом, может осуществляться значительная часть функций управления средством доверенной загрузки.

#### **1.4 Системы защиты информации от несанкционированного доступа**

Как правило, все СЗИ от НСД имеют в своем составе следующие механизмы защиты:

- идентификация и аутентификация пользователей;
- дискреционный контроль доступа пользователей;
- мандатный контроль доступа пользователей и процессов;
- маркировка документов и контроль их вывода на печать;
- защита ввода и вывода информации на отчуждаемый физический носитель;
- регистрация событий безопасности в журнале событий;
- контроль целостности критичных файлов и данных;
- контроль доступа к периферийным устройствам и портам ввода-вывода;
- гарантированное удаление данных на дисках и выборочное затирание файлов и др.

По типу исполнения СЗИ от НСД подразделяются на программные и программно-аппаратные. Последние помимо средств разграничения доступа также содержат аппаратный модуль средства доверенной загрузки.

По архитектуре выделяют сетевые и автономные СЗИ от НСД. Сетевые включают в себя сервер безопасности, а также агенты защиты, устанавливаемые на конечные точки (рабочие станции и сервера). Они предусматривают централизованное управление защитными механизмами, а также централизованное получение информации от агентов об изменении состояния защищаемых компьютеров. Как правило, наиболее популярны комплексные решения для защиты рабочих станций и серверов. При этом комплексные решения помимо разграничения доступа к ресурсам обеспечивают контроль сетевых соединений, защиту от вторжений, а также антивирусную защиту.

Приведем примеры некоторых СЗИ от НСД.

*Secret Net Studio*<sup>1</sup> – сертифицированное комплексное решение для защиты от НСД рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования, разрабатываемое компанией ООО «Код Безопасности».

---

<sup>1</sup> [www.securitycode.ru](http://www.securitycode.ru)

Помимо защиты от НСД продукт включает: антивирус, персональный межсетевой экран и модуль авторизации сетевых соединений, систему обнаружения вторжений, а также расширенные средства централизованного управления и мониторинга. Интегрируется со средством доверенной загрузки «Соболь». Secret Net Studio представлено в двух редакциях: Secret Net Studio и Secret Net Studio-C.

*Secret Net Studio* соответствует требованиям ФСТЭК по 5 классу защищенности СВТ от НСД, по 4 уровню контроля отсутствия НВД. Может применяться для защиты: АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, автоматизированных систем управления технологическими процессами (АСУ ТП) до 1 класса включительно.

*Secret Net Studio-C* соответствует требованиям ФСТЭК к СВТ по 3 классу защищенности, к НВД – по 2 уровню контроля и может применяться для защиты: АС до класса 1Б включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно.

**Dallas Lock**<sup>1</sup> – сертифицированная комплексная система защиты информации накладного типа для автономных и сетевых АРМ, в том числе для сложных сетевых инфраструктур, разрабатываемое компанией ООО «Конфидент». Помимо защиты от НСД продукт также включает: персональный межсетевой экран, систему обнаружения вторжений, средство доверенной загрузки, средства централизованного управления и пр. Dallas Lock представлено двух редакциях: Dallas Lock 8.0-K и Dallas Lock 8.0-C

*Dallas Lock 8.0-K* предназначено для защиты конфиденциальной информации и соответствует требованиям ФСТЭК по 5 классу защищенности СВТ от НСД, по 4 уровню контроля отсутствия НДВ (НДВ4). Может применяться для защиты: АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно.

*Dallas Lock 8.0-C* предназначено для защиты конфиденциальной информации и информации, составляющей государственную тайну до уровня «совершенно секретно» включительно. Соответствует требованиям ФСТЭК по 3 классу защищенности СВТ от НСД, по 2 уровню контроля отсутствия НДВ (НВД2). Может применяться для защиты: АС до класса 1Б включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно.

---

<sup>1</sup> [www.dallaslock.ru](http://www.dallaslock.ru)

**Страж NT<sup>1</sup>** – сертифицированная комплексная система защиты информационных ресурсов от НСД на автономных рабочих станциях и серверах, рабочих станциях в составе рабочей группы или домена локальной вычислительной сети, разрабатываемая российской компанией ООО «Рубинтех». «Страж NT» может функционировать на одно- и многопроцессорных системах под управлением 32-х и 64-х разрядных операционных систем.

Соответствует требованиям ФСТЭК по 3 классу защищенности СВТ от НСД, по 2 уровню контроля отсутствия НДВ (НВД2). Может применяться: в АС до класса защищенности 1Б включительно, в ГИС до 1 класса защищенности включительно, в ИСПДн до 1 уровня защищенности включительно.

**Diamond ACS<sup>2</sup>** – программное решение для контроля и разграничения доступа, с возможностью подключения аппаратной платы от российской компании ООО «ТСС». Позволяет осуществлять доверенную загрузку и физическое разделение контуров различной степени конфиденциальности на АРМ. Может быть реализован в автономной или сетевой версиях в программном и программно-аппаратном видах (с подключением аппаратного модуля Diamond ACS HW), а также обеспечивает возможность совместной работы с Diamond VPN/FW по части обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

Соответствует требованиям ФСТЭК по 3 классу защищенности СВТ от НСД, по 2 уровню контроля отсутствия НДВ (НВД2). Может применяться в АС до классов 1Б, 2А, 3А и ИСПДн до 1 класса включительно.

**Блокхост-Сеть 2.0<sup>3</sup>** – комплексная система защиты информационных ресурсов рабочих станций и серверов, разрабатываемая российской компанией ООО «Газинформсервис». Помимо защиты от НСД продукт также включает персональный межсетевой экран для контроля доступа к сетевым ресурсам и фильтрация сетевого трафика.

Блокхост-Сеть 2.0 состоит из клиентской и серверной части. Клиентская часть обеспечивает защиту рабочей станции от НСД к информации и может работать как на автономной рабочей станции, так и на рабочей станции в составе сети. Серверная часть выполняет функции централизованного управления удаленными рабочими станциями.

Соответствует требованиям ФСТЭК по 3 классу защищенности СВТ от НСД, по 2 уровню контроля отсутствия НДВ (НВД2). Может использоваться в АС до класса 1Б включительно, в ГИС и АСУ ТП до класса К1 включительно, ИСПДн до УЗ1 включительно.

---

<sup>1</sup> [www.guardnt.ru](http://www.guardnt.ru)

<sup>2</sup> [www.tssltd.ru](http://www.tssltd.ru)

<sup>3</sup> [www.gaz-is.ru](http://www.gaz-is.ru)

**Панцирь**<sup>1</sup> – комплексная система защиты информации, разрабатываемая российской компанией ООО «НПП «Информационные технологии в бизнесе»». Представляет собой сетевую систему защиты информации, реализующую клиент-серверную архитектуру, в состав которой входят клиентские части (устанавливаются на объектах защиты), серверы безопасности, обеспечивающие удаленное администрирование клиентских частей «Панцирь+» и интерактивный режим обработки журналов аудита событий безопасности, и серверы аудита, осуществляющие удаленный аудит событий безопасности в реальном времени.

Соответствует требованиям ФСТЭК по 5 классу защищенности СВТ от НСД, по 4 уровню контроля отсутствия НДВ (НВД4). Может применяться для защиты корпоративных информационных систем, в ГИС до 1 класса защищенности включительно, а также вычислительных объектов в контуре управления АСУ ТП.

Другими примерами популярных российских СЗИ от НСД могут служить: **Аккорд** (ОКБ САПР), **Щит-РЖД**, **Аура** (СПИИРАН), **КРИПТОН-ЩИТ** (ООО Фирма «Анкад»), **Фантом** (АО «РНТ») и др.

Одной из главных причин востребованности сертифицированных СЗИ от НСД на российском рынке является необходимость выполнения требований действующего законодательства и нормативных актов в области защиты информации. Среди зарубежных СЗИ от НСД для защиты информации на конечных точках применяются комплексные решения классов Information-Centric Endpoint Protection и Endpoint Protection Platforms, подразумевающие наличие централизованного управления, функции защиты от вредоносных программ, персонального межсетевого экрана, а также управления доступом к портам ввода-вывода и периферийным устройствам [30]. Примерами таких систем являются: **Kaspersky Endpoint Security**, **McAfee Endpoint Security**, **Symantec Endpoint Protection**, **Check Point Endpoint Security** и др.

---

<sup>1</sup> [www.npp-itb.spb.ru](http://www.npp-itb.spb.ru)

## 2 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

### 2.1 Основные понятия идентификации и аутентификации

На каждого субъекта доступа зарегистрированного в компьютерной системе имеется некоторая информация, однозначно его идентифицирующая. Это может быть число, строка символов или алгоритм, составляющие уникальный признак субъекта доступа [32]. Эту информацию называют *идентификатором субъекта*. Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (санкционированным) пользователем; остальные пользователи относятся к нелегальным (несанкционированным). Прежде чем получить доступ к ресурсам защищаемой системы, пользователь должен пройти процесс первичного взаимодействия с ней, который включает процедуры идентификации и аутентификации.

*Идентификация* (identification) – действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов. Иными словами под идентификацией подразумевается процедура распознавание пользователя по его идентификатору.

*Аутентификация* (authentication) – действия по проверке подлинности субъекта доступа в автоматизированной информационной системе. Аутентификация позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет [18].

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов системы, от которых зависит последующее решение о предоставлении полномочий и прав доступа конкретному пользователю или процессу к информационным ресурсам системы. Такую процедуру называют предоставлением полномочий или авторизацией.

*Авторизация* (authorization) – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ [19].

С процедурами идентификации и авторизации тесно связана процедура администрирования действий пользователя.

*Администрирование* (administration) – регистрация действий пользователя в системе, включая его попытки доступа к ресурсам. Данная процедура важна для обнаружения, анализа инцидентов безопасности в защищаемой системе и соответствующего реагирования

на них. Записи в системном журнале, аудит и администрирование программного обеспечения – все это может быть использовано для обеспечения подотчетности пользователей, если что-либо случится при входе в сеть с их идентификатором.

Внедрение средств аутентификации, авторизации и администрирования является одним из основных механизмов защиты информации от НСД.

Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от предъявляемых субъектом сущностей процессы аутентификации могут быть по типу:

- 1) знания чего-либо (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- 2) обладания чем-либо (личная карточка или иное устройство аналогичного назначения);
- 3) наличия неотъемлемых характеристик (голос, отпечатки пальцев и другие биометрические характеристики).

Далее данные сущности будут рассмотрены более подробно.

## **2.2 Парольная защита информации от несанкционированного доступа**

### **2.2.1 Принцип парольной защиты**

Одним из способов аутентификации в защищенных АС является парольная аутентификация. Парольная система как неотъемлемая составляющая подсистемы управления доступом СЗИ является частью переднего рубежа защиты всей системы безопасности [14], вследствие чего становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему.

*Пароль* (password) представляет собой строку символов, служащую в качестве аутентификатора пользователя [7]. Это некоторое секретное количество информации, известное только пользователю и парольной системе, предъявляемое для проверки подлинности субъекта.

Совокупность идентификатора субъекта и его пароля составляет *учетную запись* пользователя. Одним из наиболее важных компонентов парольной системы является база данных учетных записей.

В системе возможны следующие варианты хранения паролей:

- 1) в открытом виде;
- 2) в виде хэш-значений;

3) в зашифрованном виде на некотором ключе.

Наибольший интерес представляют второй и третий способы, которые имеют ряд особенностей. Хранение пароля в виде хэш-значений подразумевает его преобразование из массива входных данных произвольной длины в (выходную) битовую строку установленной длины с помощью определенного алгоритма хэширования. Это позволяет вместо пароля в явном виде хранить в системе его хеш-значение, однозначно ему соответствующее. Хранение пароля на ключе подразумевает его запись в защищенную энергонезависимую память аппаратного носителя (например, Рутокен, JaCarta и пр.).

В плане надежности пароля условно выделяют слабый пароль и сильный пароль. Под слабым паролем понимают пароль, который может быть легко угадан или подобран методом полного перебора. Сильный пароль трудно угадать и долго подбирать методом полного перебора.

Одной из мер количественной оценки стойкости парольных систем является формула Андерсона:

$$4,32 \times 10^4 \times k \frac{M}{P} \leq A^l,$$

где  $k$  – количество попыток подбора пароля в минуту;  $M$  – время действия пароля в месяцах;  $P$  – вероятность подбора пароля в течение его срока действия;  $A^l$  – мощность пространства паролей, определяемая из мощности  $A$  алфавита паролей и длины  $l$  пароля.

Из данной формулы следует, что наибольшее влияние на вероятность раскрытия пароля оказывает величина длины пароля – увеличение длины пароля хотя бы на один символ значительно увеличивает требуемое злоумышленнику время для его раскрытия. Увеличение длины пароля на 2 символа даёт в 500 раз больше вариантов, чем увеличение алфавита на 18 символов.

Вероятность  $P$  подбора пароля в течение срока его действия при условии, что подбор осуществляется непрерывно в течение всего срока действия пароля, связана с мощностью  $A^l$  пространства паролей следующим соотношением:

$$P = \frac{V \times T}{A^l},$$

где  $V$  – скорость подбора паролей (скорость обработки одной попытки регистрации проверяющей стороной либо скорость вычисления хэш-значения одного пробного пароля);  $T$  – срок действия пароля (промежуток времени, по истечении которого пароль должен быть сменен).

В случае, когда неизвестна точная длина искомого пароля, максимальное время  $T_{\max}$  подбора пароля будет вычисляться в соответствии с выражением:

$$T_{\max} = \frac{1}{V} \sum_{i=1}^l A$$

Доскональное знание способов хранения учетных записей пользователей в базе данных системы защиты позволяет оптимизировать программы восстановления (вскрытия) паролей.

### 2.2.2 Возможности обхода парольной защиты

Существует ряд стандартных приемов и способов, применяемых злоумышленниками с целью обхода парольной защиты. Рассмотрим данные способы и приведем рекомендации противодействия им.

**Полный перебор (brute-force attack).** Данный способ применяется в случае полного отсутствия информации о пароле и состоит в переборе всех возможных вариантов пароля определенной длины для восстановления доступа. Он известен также под названием метод «грубой силы» или «лобовой атаки».

С технической точки зрения полный перебор является самым простым способом атаки на пароль – современные вычислительные мощности позволяют перебрать все пароли длиной до 5-6 символов за несколько секунд. Теоретически данный способ допускает бесконечный перебор всех комбинаций допустимых символов, начиная от односимвольных паролей, однако во многих системах предусмотрены механизмы реагирования на несколько попыток неправильно набранного пароля подряд, после чего происходит блокирование системы и что вызывает трудности его практической реализации.

Тем не менее, существует множество систем, позволяющих осуществить такой вид атаки, например, программы архивации, предусматривающие возможность установления пароля. Кроме того, в некоторых программах хэш-значение пароля хранится в общедоступном файле, в случае хищения которого подбор пароля может осуществляться удаленно с помощью специальных программ.

Атаки, основанные на методе полного перебора, являются наиболее универсальными, но все-таки достаточно медленными. Важной характеристикой пароля, затрудняющей полный перебор, является его длина, с увеличением которой сложность взлома этим методом возрастает экспоненциально. Современный безопасный пароль должен иметь длину в пределах 12-16 символов.

**Перебор в ограниченном диапазоне.** Способ предполагает сокращение диапазона подбираемых в пароле символов и применяется в случае априорно известной информации об его ограниченном диапазоне. Например, если известно, что пароль, состоит только из цифр или только из букв русского или латинского алфавита.

Ограничение диапазона может быть вызвано как особенностями защищаемой системы, так и легкостью запоминания с позиции пользователя. При этом в случае заранее известного или угаданного злоумышленником задействованного пользователем в пароле алфавита, количество комбинаций, которые необходимо проверить при подборе, существенно сокращается по сравнению с полным перебором. Как следствие, важным требованием к построению надежного пароля является использование в его составе букв разного алфавита, реестра (прописные и строчные), цифр и прочих символов (знаки препинания, подчеркивание и т.п.).

**Атака по словарю.** В качестве пароля пользователь часто назначает слово естественного языка или общеизвестную комбинацию. Совокупность слов или терминов какого-либо языка называется *словарем*. Существует множество доступных общих и частных как электронных, так и онлайн словарей, из которых программа автоматического перебора паролей проверяет слова. Современные вычислительные мощности позволяют проверить словарь из двухсот тысяч слов в течение нескольких секунд, а сам метод подбора паролей по словарю позволяет в десятки раз сократить время, требуемое для восстановления пароля.

При этом выполнение каких-либо несложных преобразований с паролем, по типу его написания задом наперед или русскими буквами в английской раскладке, намеренного допущения ошибки также не является средством для значительного повышения безопасности пароля в данном случае, поскольку также могут быть предусмотрены и в современных системах подбора пароля. В этом случае, по сравнению с подбором случайного пароля, подбор пароля по словарю с применением различных преобразований делает невыполнимую задачу вполне возможной, а значит, надежный пароль не должен строиться на основе слов естественного языка.

**Атака по персональному словарю.** Наряду со словарем общеизвестных слов для подбора пароля может применяться так называемый *персональный словарь* пользователя, составляемый на основе его личных данных. Для облегчения запоминания пароля многие пользователи часто прибегают к применению персональных сведений, к которым могут относиться: девичья фамилия матери, номер мобильного телефона, дата рождения, кличка домашнего питомца и пр. В этом случае для пользователя может быть составлен

индивидуальный словарь его личных данных, на основе которого сгенерированы пароли, включая самые разнообразные комбинации и преобразования.

В настоящее время, в силу широкого развития социальных сетей, различных мессенджеров и мобильных приложений многие данные пользователя могут оказаться в общем доступе, что значительно облегчает задачу злоумышленника. Вследствие этого обстоятельства надежный пароль должен быть полностью бессмысленным, без привязки к личности пользователя.

***Сбор паролей, хранящихся в общедоступных местах.*** Во многих организациях пароли создает и распределяет среди пользователей системный администратор, учитывающий описанные выше способы обхода парольной защиты. Пользователи обязаны пользоваться выданным им паролем, однако в силу сложности его запоминания зачастую имеет место его хранение в записанном виде, как правило, вблизи своего АРМ.

Несерьезное отношение к вопросам обеспечения безопасности своего служебного пароля может привести к его записи на бумажный стикер с последующим расположением на мониторе компьютера или под клавиатурой. Между тем проведение визуального осмотра рабочего места пользователя, в случае физического проникновения злоумышленника в помещение организации, является одним из его первичных действий.

Пароль не должен храниться в общедоступном месте и основным способом противодействия такой угрозе является проведение бесед или тренингов с персоналом, повышение его квалификации по части информационной безопасности.

***Применение вредоносного программного обеспечения.*** Под *вредоносным программным обеспечением* понимают широкий спектр программ, предназначенных для НСД к информации или воздействия на неё или ресурсы автоматизированной информационной системы. Среди них для хищения персональных и конфиденциальных данных пользователя, в частности паролей, широко применяются троянские или шпионские программы, предназначенные для скрытого наблюдения за использованием компьютера. Типичным представителем таких программ является клавиатурный шпион (кейлогер), регистрирующий каждое нажатие клавиш на клавиатуре компьютера и пересылающий собранные данные своему хозяину.

Способом защиты от такой угрозы является применение средств антивирусной защиты, функционирующих в непрерывном режиме для отслеживания всех обращений системы к файлам и проверки их на предмет заражения вредоносным программным обеспечением, а также периодически проверяющих все файлы в заданной области.

**Социальная инженерия (social engineering).** Социальная инженерия – общий термин, обозначающий совокупность приёмов манипулирования людьми с использованием социологии и психологии, направленных на создание таких условий и обстоятельств, которые максимально эффективно приводят к необходимому результату, а именно, проникновению в защищенные системы пользователя или организации.

В общем случае тактика социальной инженерии направлена на то, чтобы обманом заставить пользователя самостоятельно выдать пароль. Например, классическим приёмом является телефонный звонок злоумышленника жертве под убедительным предлогом сообщить необходимый пароль от имени того, кто имеет право на запрашиваемую информацию (системного администратора или руководителя). Также к методам социальной инженерии может относиться склонение пользователя к открытию по электронной почте вложения или переходу по ссылке, содержащим вредоносное программное обеспечение. Основным способом противодействия такой угрозе является проведение бесед с персоналом.

**Фишинг (phishing).** Фишинг<sup>1</sup> является одной из разновидностей социальной инженерии и представляет собой вид интернет-мошенничества, целью которого является получение доступа к авторизационным данным пользователей – логинам и паролям.

Основная тактика фишинга состоит в создании поддельных сайтов, которые обманом вынуждают пользователя ввести свой пароль. Это достигается путем рассылки электронных писем или личных сообщений внутри различных сервисов с прямой ссылкой на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом – автоматическим перенаправлением посетителей на другой интернет-ресурс. При попадании на поддельную веб-страницу, пользователь, не замечая подлога, вводит свои логин и пароль, которые сохраняются в базе данных злоумышленника, после чего перенаправляется на страницу настоящего сайта. При этом пользователь замечает, что вход не осуществлен, и, полагая, что ошибся при наборе пароля, пробует ввести его заново, после чего успешно проходит авторизацию в системе. Это рассеивает его подозрения, в то время как утечка пароля уже произошла.

Другая разновидность фишинга основана на том факте, что многие пользователи используют один и тот же пароль для разных ресурсов. В этом случае, произведя успешную атаку на менее защищенный ресурс, злоумышленник получает доступ к более защищенному.

---

<sup>1</sup> Слово «phishing» происходит от видоизмененного английского слова «fishing» – «рыбная ловля, выуживание».

Основными способами противодействия фишингу являются: совершенствование знаний в области сетевой безопасности, проверка адресов интернет-ресурсов, прежде чем вводить важный пароль.

### **2.2.3 Повышение эффективности парольной защиты**

Как следует из приведенных способов обхода парольной защиты, обеспечение безопасности пароля является сложной задачей, как в техническом, так и в организационном плане.

Повышение требований к паролю возникает из-за степени его важности. Примером может служить пароль, применяемый для работы в АС, обрабатывающих информацию ограниченного доступа (государственная тайна, конфиденциальная информация). Большинство СЗИ обладает следующими возможностями по увеличению эффективности парольной системы:

- установление минимальной длины пароля;
- установление максимального срока действия пароля;
- установление требования неповторяемости паролей (препятствует замене пароля по истечении его срока действия на один из используемых ранее);
- ограничение числа попыток ввода пароля (блокирует пользователя после превышения определенного количества попыток ввода, осуществляемых подряд; не действует на учетную запись администратора).

Многие СЗИ от НСД содержат встроенные механизмы генерации паролей и доведения их до пользователей. В случае же если пользователю самостоятельно необходимо сформировать пароль, в качестве рекомендаций можно выделить следующие:

- использование длины пароля в пределах 12-16 символов;
- совместное применение в пароле символов разного алфавита (цифр и спецсимволов совместно с буквами);
- использование смешанных регистров букв;
- пароль должен быть бессмысленным, не иметь привязки к личности;
- использование пароля, который просто запомнить, чтобы его не записывать на бумаге;
- формирование пароля, который возможно быстро набрать (желательно не глядя на клавиатуру), для исключения возможности его отследить в случае наблюдения сторонними лицами.

При организации парольной защиты следует также соблюдение следующих мер:

- наложение технических ограничений (длины пароля, алфавита и т.д.);
- управление сроком действия паролей, их периодическая смена;
- смена автоматически сформированного пароля после первого входа в систему;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему;
- обучение пользователей;
- использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

#### **2.2.4 Достоинства и недостатки парольной защиты**

Основным достоинством парольной защиты является простота и традиционность. Пароли интегрированы в операционные системы и иные сервисы и в совокупности с другими СЗИ от НСД при правильном использовании могут обеспечить приемлемый для многих организаций уровень безопасности.

Вместе с тем среди недостатков парольной защиты выделяют: возможность его подсмотреть в процессе ввода (в том числе с помощью технических средств), требования к квалификации персонала, его обучение. В ряде случаев имеет место человеческий фактор, в частности, не всегда после первого входа в систему производится смена пароля, имеет место распространение сведений о пароле среди коллег, например, на случай своего временного замещения на рабочем месте, не соблюдение рекомендаций к формированию сильного пароля. Хранение же пароля в зашифрованном виде на некотором ключе (внешнем аппаратном носителе) требует внимательного отношения к нему во избежание его утери или хищения.

### **2.3 Программно-аппаратные системы идентификации и аутентификации**

#### **2.3.1 Классификация систем идентификации и аутентификации**

Процедуры идентификации и аутентификации в защищенной АС осуществляются посредством специальных программных (программно-аппаратных) средств, встроенных в операционную систему или СЗИ, при использовании которых сотрудник получает к ней доступ. Такие средства называются *средства идентификации и аутентификации* (СИА).

В состав аппаратно-программных СИА входят:

- 1) идентификаторы, предназначенные для хранения уникальных идентификационных признаков;
- 2) считыватели – устройства ввода-вывода для идентификаторов (адаптеры, платы доверенной загрузки и др.), осуществляющие пересылку данных между идентификатором и защищаемой системой;
- 3) соответствующее программное обеспечение, включающее драйвера для аппаратных идентификаторов и присущих им считывателей.

По виду используемых идентификационных признаков СИА разделяются на электронные, биометрические и комбинированные (рис. 2.1).

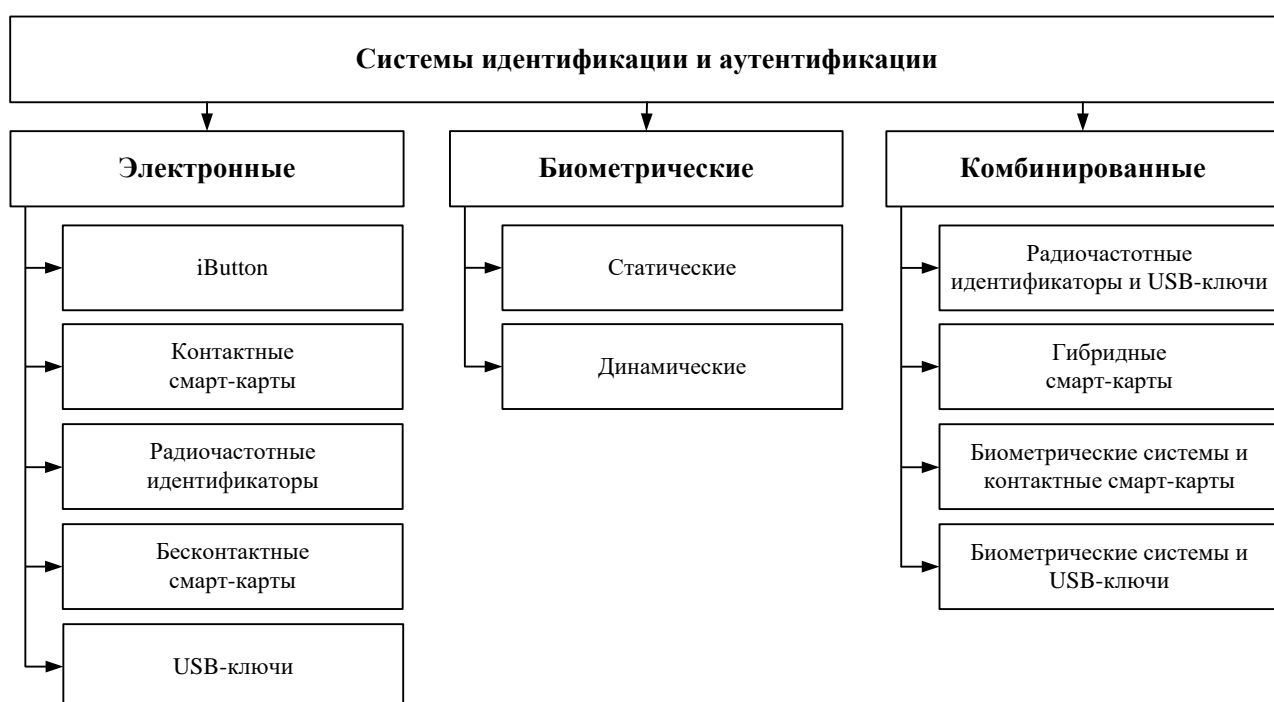


Рис. 2.1 – Классификация СИА по виду используемых идентификационных признаков.

В *электронных системах* идентификационные признаки представляются в виде цифрового кода, хранящегося в памяти идентификатора. Такие СИА разрабатываются на базе следующих идентификаторов:

- iButton (Touch Memory);
- контактные смарт-карты;
- радиочастотные идентификаторы;

- бесконтактные смарт-карты;
- USB-ключи.

В **биометрических системах** идентификационными признаками являются индивидуальные особенности человека, называемые биометрическими характеристиками. В основе идентификации и аутентификации этого типа лежит процедура считывания предъявляемого биометрического признака пользователя и его сравнение с предварительно полученным эталоном (шаблоном).

В зависимости от вида используемых характеристик биометрические системы делятся на статические и динамические.

*Статическая биометрия* (физиологическая) основывается на данных, получаемых из измерений анатомических особенностей человека, таких как отпечатки пальцев, форма кисти руки, узор радужной оболочки глаза, схема кровеносных сосудов лица, рисунок сетчатки глаза, черты лица и др.

*Динамическая биометрия* (поведенческая) основывается на анализе совершаемых человеком действий. Примерами являются: параметры голоса, динамика и формы подписи, клавиатурный почерк и пр.

В **комбинированных системах** для идентификации используется одновременно несколько идентификационных признаков. Такая интеграция создает дополнительные препятствия злоумышленнику, которые он не сможет преодолеть, а если и сможет, то со значительными трудностями и затратами времени. Разработка комбинированных систем осуществляется по двум направлениям:

- интеграция идентификаторов в рамках системы одного класса;
- интеграция систем разного класса.

В первом случае для защиты компьютеров от НСД используются системы, базирующиеся на бесконтактных смарт-картах и USB-ключях, а также на гибридных (контактных и бесконтактных) смарт-картах. Во втором случае, применяется сочетание биометрических и электронных СИА, называемое *биоэлектронные системы*.

По способу обмена данными между идентификатором и считывателем СИА подразделяются на контактные и бесконтактные.

**Контактный способ** (контактное считывание) подразумевает считывание идентификационных признаков через непосредственное соприкосновение идентификатора со считывателем.

**Бесконтактный способ** (дистанционное считывание) обмена данными не требует

четкого позиционирования идентификатора и считывателя – чтение или запись данных происходит при поднесении идентификатора на определенное расстояние от него.

Основным элементом электронных контактных и бесконтактных идентификаторов являются одна или более встроенных микросхем (чипов), которые могут представлять собой микросхемы памяти, микросхемы с жесткой логикой и микропроцессоры.

Выбор СИА целесообразно проводить путем сравнения таких характеристик как:

- структура идентификатора;
- структура и состав считывателя;
- интеграция с СЗИ;
- надежность изделия;
- стоимость изделия.

### 2.3.2 Электронные идентификаторы

**iButton (Touch Memory).** Идентификаторы *iButton* (information button) относятся к классу электронных контактных идентификаторов, имеющих однопроводный протокол обмена информацией (1-Wire) и помещённых в стандартный металлический корпус. Данные идентификаторы также называются *Touch Memory* (контактная память), что связано с первоначально запатентованным товарным знаком этого семейства микросхем американской компанией «Dallas Semiconductor» (в настоящее время «Maxim Integrated»).

В общем случае идентификатор iButton представляет собой микросхему, смонтированную в стандартный круглый герметичный стальной корпус (рис. 2.2). Питание микросхемы обеспечивает миниатюрная литиевая батарейка. Корпус имеет диаметр 17,35 мм и две стандартные толщины: 3,1 мм (корпус F3) и 5,89 мм (корпус F5). Корпус выполняет роль электрических контактов идентификатора, а также обеспечивает его высокую степень защищенности от воздействия агрессивных сред: пыли, влаги, внешних электромагнитных полей, механических ударов и пр. Кромка корпуса позволяет удобно его закреплять в держателях.



Рис. 2.2 – Идентификатор iButton.

На рис. 2.3 приведено общее внутреннее устройство iButton. Основу микросхемы составляют мультиплексор и память. При этом в структуре iButton можно выделить четыре основных блока: постоянное запоминающее устройство (ПЗУ/ROM), блокнотная память, оперативное запоминающее устройство (ОЗУ/RAM), часы реального времени, элемент питания (встроенная миниатюрная литиевая батарейка).

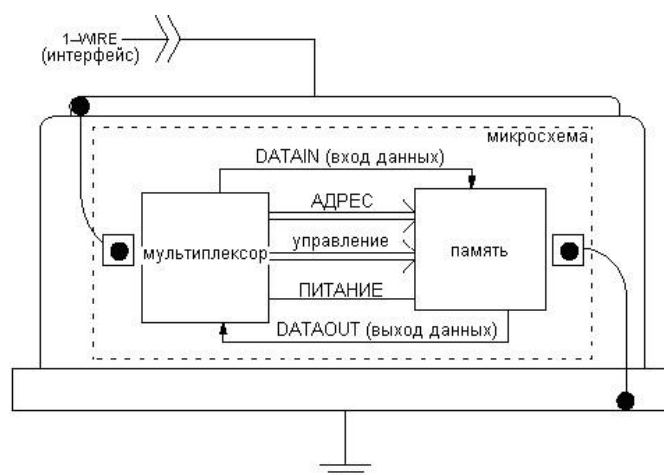


Рис. 2.3 – Структура iButton.

Существуют различные модификации идентификаторов iButton, которые различаются составом памяти, её ёмкостью и функциональными возможностями.

Простейшая модель из микросхем iButton (DS1990) содержит только ПЗУ, что достаточно для хранения адреса ключа. В ПЗУ хранится 64-разрядный код, состоящий из 48-разрядного уникального серийного номера (идентификационного признака), 8-разрядного кода типа идентификатора и 8-разрядной контрольной суммы. Размещаемые в ПЗУ данные представляют собой уникальную кодовую комбинацию, которая записывается в идентификатор во время его изготовления. Напряжение питания ПЗУ подается по сигнальной линии данных, что позволяет считывать память независимо от энергии встроенной в корпус литиевой батарейки, тем самым сэкономив её ресурс.

Большинство всех остальных микросхем iButton помимо ПЗУ могут иметь в своем составе программируемую память (стираемое программируемое постоянное запоминающее устройство (СППЗУ/EPROM), электрически стираемое программируемое постоянное запоминающее устройство (ЭСПЗУ/EEPROM)) или энергонезависимую оперативную память (NVRAM) для хранения конфиденциальной информации (криптографических ключей, паролей доступа и других данных).

Программируемая память СППЗУ (семейство микросхем DS198х) обеспечивает возможность однократной записи и многократного считывания информации, что удобно в тех случаях, когда данные никогда не меняются (например, идентификатор сотрудника). Запись осуществляется блоками до полного заполнения ячейки. При этом система ограничивает количество доступов числом 100: после каждого доступа заполняется соответствующая ячейка памяти и после записи всех 100 ячеек ключ становится недействительным.

Программируемая память ЭСППЗУ (семейство микросхем DS197х) позволяет записывать условия пользовательского доступа и изменять их по мере необходимости.

Энергонезависимая оперативная память NVRAM (семейство микросхем DS199х) обеспечивает неограниченное количество циклов перезаписи и используется для приложений, требующих частое обновление данных ключа. Данные в такой памяти хранятся не менее 10 лет благодаря литиевой батарее.

Идентификатор iButton может иметь более сложную архитектуру оперативной памяти (DS1991), реализуя на аппаратном уровне защиту памяти от НСД. В этом случае для ограничения доступа к секретной информации доступ к памяти может быть защищен разными паролями на различные операции: для чтения один пароль и для полного доступа другой.

Также iButton (DS1994) может иметь встроенные часы реального времени, которые используются для учета времени действия доступа, по истечении которого доступ с помощью ключа iButton будет закрыт.

Некоторые типы идентификаторов iButton содержат дополнительные компоненты [32]. Например, в идентификаторе DS1963S имеется микроконтроллер, предназначенный для вычисления в соответствии со стандартом хэш-функции SHA-1 160-разрядного кода аутентификации сообщений и генерации ключей доступа для страниц памяти. Типичными применениями для такого интегрированного решения являются системы местного или удаленного аутентифицированного доступа, электронные кошельки для перевода денег, банкоматы, терминалы оплаты, счетчики парковки или доступ к компьютерной сети.

Обмен информацией между идентификатором и системой происходит в соответствии с протоколом 1-Wire с помощью разнообразных считывающих устройств (адаптеров последовательного, параллельного и USB-портов). Интерфейс 1-Wire обеспечивает обмен информацией на скоростях 16 или 142 Кбит/с (ускоренный режим). Для записи и считывания данных из идентификатора требуется контакт не более 5 мс корпуса iButton со считывающим устройством.

К достоинствам идентификаторов iButton относятся: надежность и долговечность, высокая степень механической и электромагнитной защищенности, малые габариты, относительно невысокая стоимость. Недостатками являются: зависимость его срабатывания от точности соприкосновения идентификатора и считывателя, осуществляемого вручную, а также отсутствие встроенных в идентификаторы криптографических средств, реализующих шифрование данных при их хранении и передаче в компьютер. Вследствие последнего недостатка iButton обычно используется совместно с другими системами, на которые возлагаются функции шифрования.

**Контактные смарт-карты.** *Контактные смарт-карты* (contact smart cards) относятся к классу электронных контактных идентификаторов и представляют собой пластиковую карту со встроенной микросхемой.

Первый шаг в создании карт-идентификаторов был сделан в Германии в 1968 году, когда Юргену Деслофу и Гельмуту Гротруппу удалось поместить интегральную схему в кусочек пластика. Независимо от них, в 1970 году Кунитака Аримура была запатентована аналогичная идея в Японии. В 1974 году французский изобретатель Ролан Морено запатентовал идею карты с защищенной памятью, а в 1977 году французский инженер Мишель Угон изобрел первую смарт-карту со встроенным микропроцессором.

Физический, электрический, механический и программный интерфейсы смарт-карт определяются стандартом ISO/IEC 7816. Пример контактных смарт-карт и их считывателя приведен на рис. 2.4.



Рис. 2.4 – Пример контактных смарт-карт со считывателем.

По функциональности смарт-карты разделяются на два типа: карты памяти и процессорные (интеллектуальные) карты.

Карты памяти предназначены для хранения информации – они содержат некоторое количество данных и механизм разграничения доступа к ним. Среди них существует три типа: карты с прямым типом памяти, карты с защищенным/сегментированным типом памяти и карты памяти с сохраненным значением.

Процессорные карты используются в задачах, требующих сложной обработки информации, содержат микропроцессор и возможность управлять данными на карте.

Контактные смарт-карты взаимодействуют со считывателем посредством соприкосновения своей контактной площадки с контактами считывателя. При этом смарт-карта получает от считывателя через контактные поверхности энергию питания и тактовые импульсы и, после проведения аутентификации пользователя и терминала, передает считывателю запрашиваемую информацию. Передача данных происходит через двунаправленный последовательный интерфейс.

Основу внутренней структуры процессорной смарт-карты составляет микросхема, в состав которой входят: центральный процессор (ЦП), ОЗУ, ПЗУ и ЭСППЗУ (рис. 2.5). Как правило, в ней также присутствует специализированный криптографический процессор [31].

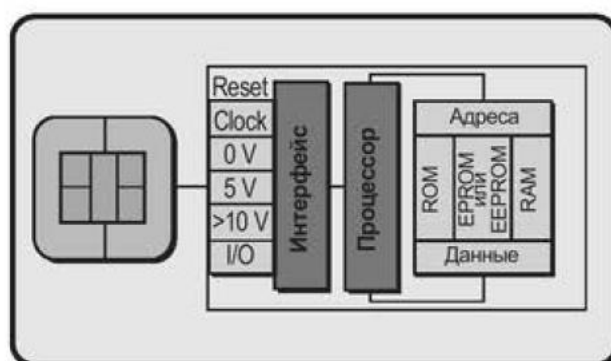


Рис. 2.5 – Структура контактной процессорной смарт-карты.

Центральный процессор (обычно это RISC-процессор<sup>1</sup>) используется для обработки и защиты информации, хранимой и обрабатываемой на смарт-карте, контроле доступа к памяти и управления ходом вычислительного процесса.

Оперативная память используется для временного хранения данных, например, результатов вычислений, произведенных процессором, информации при выполнении криптографических операций. Ёмкость ОЗУ составляет, как правило, составляет несколько килобайт.

<sup>1</sup> RISC (Reduced Instruction Set Computer) – микропроцессор с сокращенным набором команд.

Постоянная память хранит команды, исполняемые процессором, и другие неизменяемые данные, записываемые при производстве смарт-карты. Ёмкость ПЗУ может составлять десятки килобайт.

В ЭСППЗУ хранятся пользовательские данные, предназначенные для считывания, записи, модификации, а также конфиденциальные данные (например, криптографические ключи), недоступные для прикладных программ. Ёмкость памяти составляет десятки и сотни килобайт.

На специализированный криптографический процессор возлагается реализация различных процедур, необходимых для повышения защищенности СИА, в том числе: генерация криптографических ключей, реализация криптографических алгоритмов, выполнение операций с электронной подписью, PIN-кодом и др.

К достоинствам контактной смарт-карты относят её малые габариты и простоту реализации считывания. К недостаткам – уязвимость контактов к износу, коррозии и загрязнению, сравнительно высокая стоимость считывателей.

**Радиочастотные идентификаторы.** Радиочастотные идентификаторы, или *RFID-системы* (radio-frequency identification), относятся к классу электронных бесконтактных радиочастотных устройств. Также их называют идентификаторы *Proximity* (от англ. proximity – близость, соседство).

Основными компонентами данных идентификаторов являются осуществляющая связь со считывателем специализированная микросхема – транспондер (transmitter/responder – передатчик/приемник), и соединенная с ней встроенная антенна. В состав микросхемы входит элемент памяти (или микросхема с жесткой логикой) со вспомогательными блоками: модулем программирования, модулятором, блоком управления и другими модулями. В радиочастотном идентификаторе в основном используется СППЗУ, но встречается и ЭСППЗУ с ёмкостью от 8 до 256 байт. В памяти содержатся: уникальный номер идентификатора, код устройства и служебная информация (биты четности, биты начала и конца передачи кода и т.д.).

Конструктивно транспондеры могут быть вмонтированы в любой предмет. Для систем контроля доступа, широкое применение получили пластиковые карты, брелоки, браслеты и т.п. Для идентификации объектов применяются различные конструктивные исполнения идентификаторов, которые называются метками, тегами. Идентификаторы Proximity не предполагают реализации каких-либо алгоритмов шифрования и аутентификации.

По типу источника питания радиочастотные идентификаторы подразделяют на

активные и пассивные.

Активные идентификаторы обладают собственным источником питания (литиевая батарейка) и обеспечивают взаимодействие со считывателем на значительном расстоянии (в несколько метров). Однако широкого распространения они не получили, в связи с большей стоимостью, габаритами и ограниченным сроком службы.

Пассивные идентификаторы не имеют встроенного источника энергии. Питание микросхемы происходит посредством электромагнитного поля, излучаемого считывателем. Чтение данных осуществляется считывателем со скоростью 4 Кбит/с на расстоянии до 1 м. Принцип их работы приведен на рис. 2.6.

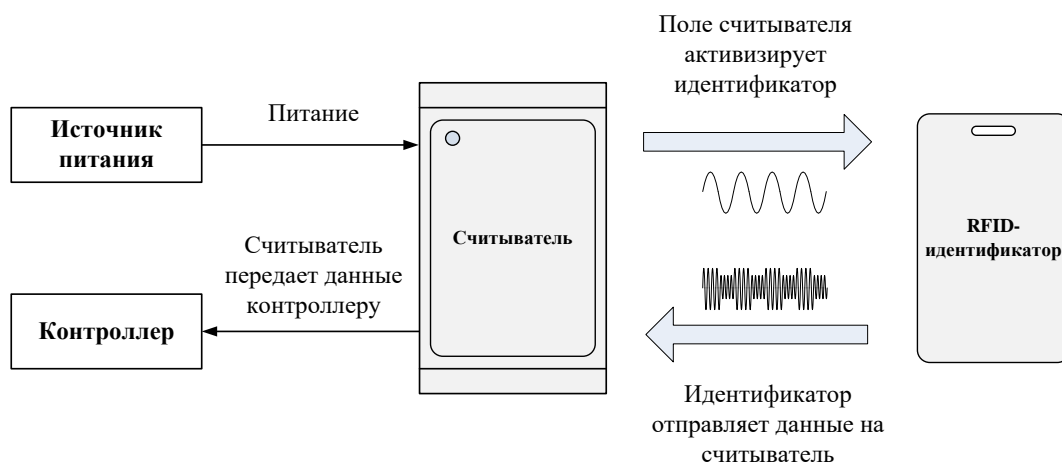


Рис. 2.6 – Принцип радиочастотной идентификации.

Считыватель содержит в своем составе передатчик и антенну, посредством которой постоянно излучает электромагнитное поле определенной частоты. Когда идентификатор оказывается в зоне действия считывателя, он активизируется – антенна поглощает сигнал и передает его на микросхему. Получив за счет индуктивной связи энергию для питания, идентификатор излучает записанные в памяти микросхемы идентификационные данные (цифровой код), принимаемые считывателем. Дистанция считывания в значительной степени зависит от характеристик антенного и приемо-передающего трактов считывателя. Весь процесс занимает несколько десятков микросекунд.

В соответствии с используемой несущей частотой RFID-системы классифицируются по частоте: низкочастотные, среднечастотные, высокочастотные.

*Низкочастотные* (100-500 кГц) характеризуются незначительным расстоянием считывания (5-30 см), которое ограничивается большими габаритами антенны, а также присутствием в этом диапазоне достаточно высокого уровня промышленных

электромагнитных помех. Широко применяются в бесконтактных картах (Proximity) для систем контроля доступа. Однако являются одними из самых незащищенных, и могут быть подделаны злоумышленниками.

*Среднечастотные* (10-15 МГц) при меньших габаритах антенны обеспечивают большую дальность считывания, более быстрый обмен данными, вследствие чего возможно построение на базе транспондеров с двухсторонним обменом данными, работающих на частоте 13,56 МГц, бесконтактных смарт-карт, о которых речь пойдет ниже. Являются более защищенными, чем низкочастотные. Позволяют реализовать множество функций, таких как одновременная идентификация в поле действия одного считывателя многих меток, криптозащищенный протокол обмена данными, хранение и модификация информации в памяти идентификатора и др.

*Высокочастотные* (850-950 МГц или 2,4-5 ГГц) характеризуются большой дистанцией считывания (в несколько метров). Они предназначены, в основном, для использования там, где требуются большое расстояние и высокая скорость считывания, например, контроль железнодорожных вагонов при движении состава, автомобилей и т.д. Такие системы значительно сложнее и дороже предыдущих и требуют специальной аппаратуры для считывания.

Основными достоинствами радиочастотных идентификаторов являются: бесконтактная технология считывания, долговечность пассивных идентификаторов, точность, надежность и удобство считывания идентификационных признаков. К их недостаткам относят слабую электромагнитную защищенность и относительно высокую стоимость, учитывая затраты на считыватели.

**Бесконтактные смарт-карты.** *Бесконтактные смарт-карты* относятся к классу электронных бесконтактных идентификаторов, реализующих технологию радиочастотной идентификации. Пример бесконтактных смарт-карт приведен на рис. 2.7.



Рис. 2.7 – Пример бесконтактных смарт-карт.

В отличие от контактных смарт-карт, бесконтактные смарт-карты дополнительно имеют радиочастотный модуль со встроенной в корпус индуктивной антенной, необходимой для связи со считывателем и питания микросхемы (рис. 2.8). Для лучшей механической защиты микросхема помещается в миниатюрный модуль, подключаемый к концам антенны [31].

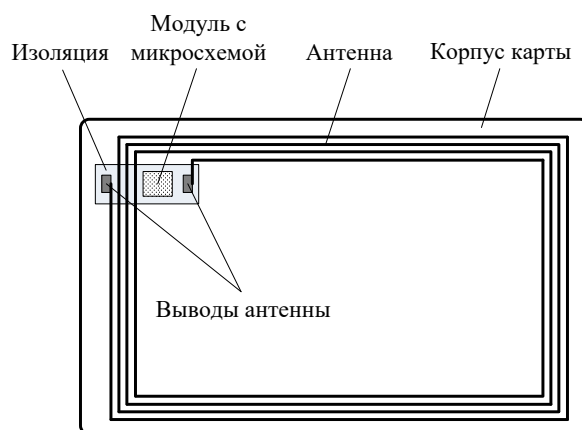


Рис. 2.8 – Конструктивные элементы бесконтактной смарт-карты.

Встроенная микросхема состоит из двух частей – микроконтроллера и бесконтактного радиочастотного интерфейса (рис. 2.9). Схема микроконтроллера является аналогичной контактной смарт-карте и рассмотрена выше. Схема радиочастотного интерфейса соединяется с выводами антенны смарт-карты и использует электромагнитное поле, излучаемое считывателем, для получения энергии питания и обмена данными.

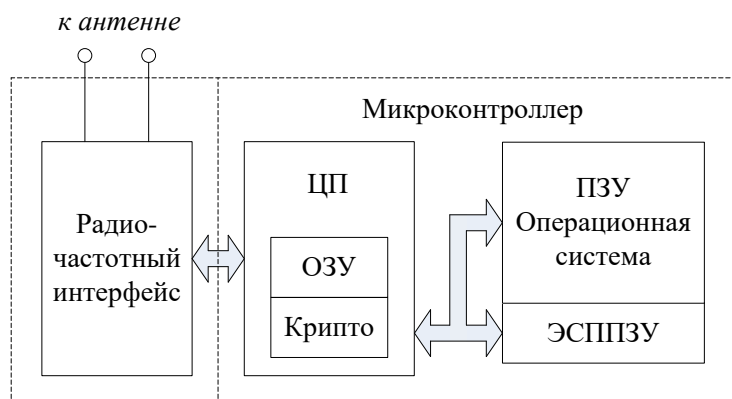


Рис. 2.9 – Архитектура микросхемы бесконтактной смарт-карты.

Бесконтактные смарт-карты относятся к среднечастотным RFID-системам, функционируют на частоте 13,56 МГц и разделяются на два класса, которые базируются на международных стандартах ISO/IEC 14443 и ISO/IEC 15693.

Стандарт ISO/IEC 14443 содержит несколько разных протоколов обмена, обозначаемых буквами (А, В и т.д.), различающиеся способами модуляции передаваемого радиосигнала. Стандарт поддерживает обмен (чтение/запись) данными со скоростью 106 Кбит/с (возможно увеличение скорости до 212,424 или 848 Кбит/с), дистанция чтения – до 10 см. Для реализации функций шифрования и аутентификации в идентификаторах данного стандарта могут применяться микросхемы трех видов: микросхема с жесткой логикой MIFARE, процессор или криптографический процессор. Технология MIFARE представляет собой расширение ISO/IEC 14443 (версии А).

Стандарт ISO/IEC 15693 увеличивает дистанцию применения бесконтактного идентификатора до 1 м. На этом расстоянии обмен данными осуществляется со скоростью до 26,6 Кбит/с.

В таблице 2.1 представлены основные характеристики бесконтактных смарт-карт и их сравнение с радиочастотными идентификаторами Proximity, рассмотренными выше [31].

Таблица 2.1 – Характеристики идентификаторов Proximity и бесконтактных смарт-карт

<b>Характеристики</b>	<b>Идентификаторы Proximity</b>	<b>Смарт-карта стандарт ISO/IEC 14443</b>	<b>Смарт-карта стандарт ISO/IEC 15693</b>
Частота радиоканала, МГц	125; 13,56	13,56	13,56
Дистанция чтения	до 1 м	до 10 см	до 1 м
Встроенные микросхемы	микросхема памяти, микросхема с жесткой логикой	микросхема памяти, микросхема с жесткой логикой, процессор	микросхема памяти, микросхема с жесткой логикой
Функции памяти	только чтение	чтение/запись	чтение/запись
Ёмкость памяти	8-256 байт	64 байт – 64 кб	256 байт – 2 кб
Алгоритмы шифрования и аутентификации	отсутствуют	технология MIFARE, DES, 3DES, AES, RSA, ECC	DES, 3DES
Механизм антиколлизии <sup>1</sup>	опционально	есть	есть

<sup>1</sup> Антиколлизия – разделения нескольких карт в поле считывателя по их уникальным идентификаторам.

К достоинствам идентификаторов на базе смарт-карт относятся малые габариты, удобство хранения и считывания идентификационных признаков. К недостаткам – ограниченный срок эксплуатации из-за неустойчивости смарт-карты к механическим повреждениям и относительно высокую стоимость считывателей смарт-карт.

**USB-ключи.** *USB-ключ* или *токен* (от англ. token – опознавательный знак, маркер) относится к контактными электронным идентификаторам и является преемником контактных смарт-карт. СИА на базе USB-ключей появились в конце 90-х годов прошлого века. Являясь преемником технологий смарт-карт и электронных ключей, используемых для защиты программного обеспечения, USB-ключи довольно быстро завоевали популярность.

Конструктивно USB-ключи выпускаются в виде брелоков в цветных корпусах, снабженных световыми индикаторами состояния, что делает их внешне похожими на флеш-накопители. Каждый идентификатор имеет прошиваемый при изготовлении собственный уникальный серийный номер. Пример USB-ключа приведен на рис. 2.10.



Рис. 2.10 –USB-ключ (Рутокен).

Структура и функциональность USB-ключей аналогична смарт-картам. В состав USB-ключей могут входить:

- процессор (обычно RISC) для управления и обработки данных;
- криптографический процессор для реализации различных криптографических преобразований (шифрование, хэширование, электронная подпись и пр.);
- USB-контроллер для обеспечения интерфейса с USB-портом компьютера;
- оперативная память для хранения изменяемых данных;
- перепрограммируемая память ЭСППЗУ для хранения ключей шифрования, паролей, сертификатов и т.д.;
- постоянная память для хранения команд и констант.

USB-ключ содержит некоторые секретные сведения, используемые для аутентификации субъектов доступа. Файловая система токена разделяется между

несколькими приложениями и службами. При этом множество паролей хранится в памяти USB-ключа, а его владельцу требуется ввести PIN-код, удостоверяющий его как владельца всех паролей, хранящихся в памяти токена. После нескольких неудачных попыток ввода PIN-кода процессор блокирует USB-ключ до привлечения администратора безопасности, поскольку предполагается, что ключ был украден или утерян.

USB-ключи обладают всеми преимуществами смарт-карт, связанными с безопасным хранением конфиденциальных сведений и осуществлением криптографических операций внутри токена, но лишены основного их недостатка – не требуют дорогостоящих аппаратных считывателей, поскольку подключаются непосредственно к USB-порту, являющемуся стандартным портом для подключения периферийных устройств.

Примерами наиболее популярных USB-ключей, служащих для обеспечения двухфакторной аутентификации являются семейства токенов:

- **Рутокен** (АО «Актив-софт»);
- **JaCarta** (ЗАО «Аладдин Р.Д.»);
- **eToken** (Gemalto).

В таблице 2.2 приведены некоторые характеристики данных USB-ключей.

Таблица 2.2 – Некоторые характеристики USB-ключей

Характеристики	Рутокен S	JaCarta PRO	SafeNet eToken 5110
Объем защищенной памяти	32, 64, 128 Кб	80 Кб	80 Кб
Сертификация	НДВЗ, НДВ4, ФСБ	НДВ4	НДВ4
Возможность встраивания радиометки (RFID)	есть	есть	есть
Поддерживаемые криптографические алгоритмы	ГОСТ 28147-89, 3DES, SHA-1, SHA-256, MD5, RC4, MD4, MD5, SHA-1	3DES, SHA-1, RSA, генератор последовательностей случайных чисел	3DES, AES, SHA-1, SHA-256, RSA, P-256, P-384, ECDH
Поддерживаемые операционные системы	Microsoft Windows 10/2016/8.1/8/2012/7/2008/Vista/2003/XP/2000, GNU/Linux, Apple macOS	Microsoft Windows 10/8.1/8/7/Vista/XP, Windows Server 2012/2008/2003/2000, GNU/Linux, Apple macOS	Microsoft Windows 10/8.1/8/7, Windows Server 2008/R2, Windows Server 2016/2012, Linux, Apple macOS,

Достоинствами USB-ключей являются малые габариты, высокая мобильность, отсутствие аппаратного считывателя, простота подсоединения идентификатора к USB-порту. К недостаткам относят: относительно высокую стоимость, слабую механическую защищенность брелока, а также ограниченный ресурс их USB-разъемов.

Помимо аппаратной идентификации и аутентификации (подразумевающей защищенное хранение секретных ключей, паролей маркеров доступа) USB-ключи в зависимости от своих функциональных особенностей могут также реализовывать функции:

- электронной подписи (хранить секретные ключи и выполняться операции создания и проверки подписи);
- шифрования данных (генерировать ключи шифрования, выполняться операции симметричного и асимметричного шифрования, производиться процедуры экспорта ключа в открытом или зашифрованном виде);
- хеширования (вычислять значения хеш-функции для блоков данных).

USB-ключи, в которых реализованы криптографические алгоритмы преобразования информации, относятся к числу средств криптографической защиты информации, основным применением которых является реализация функции электронной подписи. Среди таких токенов известны ключевые носители: *vdToken*, *MS\_KEY K «АНГАРА»*, *Рутокен ЭЦП 2.0*, *JaCarta ГОСТ*, *VPN-Key-TLS* и др.

Многофункциональность USB-ключей обеспечивает широкие возможности их применения – от строгой аутентификации и организации безопасного локального или удаленного входа в вычислительную сеть до построения на основе токенов систем юридически важного документооборота, шифрования файлов, электронной подписи, организации защищенных каналов передачи данных, управления правами пользователя и др.

### 2.3.3 Биометрические идентификаторы

В основе биометрической идентификации и аутентификации лежит считывание и сравнение предъявляемого биометрического признака пользователя с имеющимся эталоном (шаблоном). Высокий уровень защиты определяется тем, что биометрия позволяет идентифицировать человека, а не устройство. Биометрические идентификаторы могут быть контактными и бесконтактными (дистанционными).

Основными достоинствами биометрических методов идентификации и аутентификации пользователя по сравнению с электронными являются: высокая степень достоверности идентификации по биометрическим признакам из-за их уникальности,

неотделимость биометрических признаков от дееспособной личности и трудность фальсификации биометрических признаков.

Общая схема системы управления доступом на основе биометрической аутентификации имеет вид, представленный на рис. 2.11.

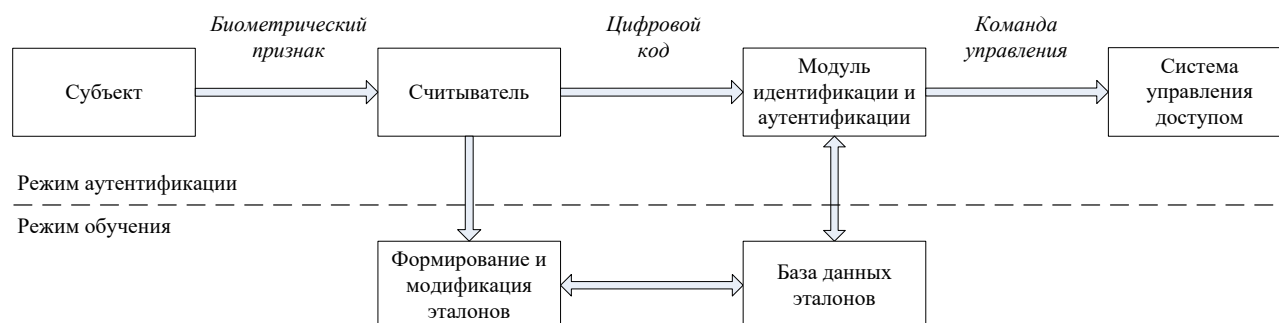


Рис. 2.11 – Схема системы управления доступом на основе биометрической аутентификации

Предъявленный пользователем (субъектом доступа) при физической регистрации биометрический параметр посредством считывателя (сканера) преобразуется в цифровой код заданной длины (как правило, до 1000 бит), который анализируется на этапе обработки информации с целью выявления характерных признаков данного параметра, после чего осуществляется распознавание пользователя путем их сравнения с ранее введенными и хранящимися в базе параметрами-эталонами санкционированных пользователей. В случае успешной процедуры аутентификации происходит авторизация пользователя и предоставление ему доступа к запрашиваемой информации.

В приведенной на рис. 2.11 схеме выделено два режима работы: режим обучения, на котором происходит формирование новых эталонов и модификация существующих, и режим непосредственно аутентификации. При регистрации пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки.

Как отмечалось ранее, в качестве биометрических признаков, которые могут быть использованы при идентификации и аутентификации потенциального пользователя, применяются его статические (физиологические) и динамические (поведенческие) характеристики.

**Статические биометрические признаки.** К статическим биометрическим признакам пользователя относятся:

- отпечатки пальцев;
- узор радужной оболочки или сетчатки глаз;

- геометрическая форма руки;
- геометрия, термограмма лица и др.

*Системы аутентификации по отпечаткам пальцев* являются самыми распространенными. Метод основан на использовании уникальности рисунка папиллярных узоров на пальцах людей. Отпечаток, полученный с помощью дактилоскопического сканера, преобразовывается в цифровой код, а затем сравнивается с ранее введенными наборами эталонов. Преимуществами использования аутентификации по отпечаткам пальцев – его простота и надежность. Пример дактилоскопического сканера приведен на рис. 2.12.



Рис. 2.12 – Сканер отпечатков пальцев (BioLink U-Match 3.5)

В зависимости от используемых физических принципов, дактилоскопические сканеры подразделяются на следующие виды: оптические, емкостные, радиочастотные, давления, ультразвуковые, температурные.

Оптические сканеры основаны на использовании оптических методов получения изображения отпечатка пальцев. Среди них в свою очередь выделяют: FTIR-сканеры (frustrated total internal reflection), протяженные, оптоволоконные, электрооптические и роликовые сканеры. Их основным недостатком является неустойчивость к муляжам и мертвым пальцам.

Емкостные сканеры основаны на изменении электрической емкости с последующей покадровой сборкой изображения отпечатка пальца с целью построения изображения папиллярных узоров. Изменение электрической емкости возможно: либо между неровностями кожи и чувствительными элементами полупроводниковой матрицы, выполняющими роль пластин микроконденсаторов; либо вследствие изменения  $p$ - $n$ -перехода в элементах полупроводниковой матрицы при их соприкосновении с неровностями поверхности пальца; либо в элементах полупроводникового датчика емкости. Недостатком емкостных сканеров, как и оптических также является их неустойчивость к муляжам.

Радиочастотные сканеры используют отраженные от точечных участков поверхности пальца слабые радиочастотные волны. Данные сканеры являются более устойчивыми к муляжам, однако требуют качественного контакта пальца с передатчиком.

Чувствительные к давлению сканеры основаны на использовании матриц, состоящих из чувствительных к давлению пьезоэлементов. Они обладают достаточно низкой чувствительностью и неустойчивостью к муляжам.

Ультразвуковые сканеры сканируют поверхность пальца ультразвуковыми волнами, измеряя расстояния между источником волн и выступами и впадинами папиллярного узора по отраженному от них эхо-сигналу. Данные сканеры имеют наилучшую защиту от муляжей и мертвых пальцев.

Температурные сканеры (термосканеры) используют матрицы пироэлектрических элементов, преобразующих разницу температур в выступах и впадинах папиллярного узора в напряжение, на основе чего строится цифровое изображение отпечатков пальцев. Они также эффективны против муляжей и обладают высокой устойчивостью к электростатическому заряду.

*Системы аутентификации по узору радужной оболочки глаза* основаны на уникальности признаков и особенностей радужной оболочки человеческого глаза – тонкой подвижной диафрагмы глаза с отверстием (зрачком) в центре, расположенной за роговицей перед хрусталиком между передней и задней камерами глаза (рис. 2.13).



Рис. 2.13 – Пример радужной оболочки глаза.

Радужная оболочка глаза образовывается ещё до рождения человека, и не меняется на протяжении всей его жизни. По текстуре она напоминает сеть с большим количеством окружающих кругов и рисунков, которые могут быть измерены компьютером. Обычно делается серия из нескольких фотографий, т.к. зрачок чувствителен к свету и постоянно меняет свой размер. Затем из полученных фотографий выбирается одна наиболее удачная, определяются границы радужки и контрольная область. К каждой точке выбранной области

применяют специальные фильтры, чтобы извлечь фазовую информацию и преобразовать рисунок оболочки в цифровой формат. Очки и контактные линзы, даже цветные, не влияют на качество аутентификации.

Достоинствами такого подхода является высокая надежность и скорость идентификации, невозможность фальсификации, средняя чувствительность к влиянию внешних факторов. Недостатком является высокая стоимость считывателя.

*Системы аутентификации по сетчатке глаза* базируются на уникальности рисунка кровеносных сосудов глазного дна. Даже у близнецов данные рисунки не совпадают. Для сканирования сетчатки используется инфракрасное излучение низкой интенсивности, направленное через зрачок к кровеносным сосудам на задней стенке глаза. Из полученного сигнала выделяется несколько сотен особых точек, информация о которых сохраняется в эталоне.

Достоинствами таких систем являются: невозможность фальсификации и возможность однофакторной идентификации. К недостаткам относят психологический фактор, чувствительность к неправильной ориентации сетчатки, а также высокую стоимость оборудования.

*Системы аутентификации по геометрической форме руки* используют несколько характеристик кисти руки, таких как: изгибы пальцев, их длина и толщина, ширина и толщина тыльной стороны руки, расстояние между суставами и структура кости. Пример биометрического считывателя, идентифицирующего пользователей по характеристикам геометрии ладони приведен на рис. 2.14.



Рис. 2.14 – Биометрический считыватель, идентифицирующий пользователей по характеристикам геометрии ладони (HandKey II).

С помощью сканера, который состоит из камеры и подсвечивающих диодов (при сканировании кисти руки, диоды включаются по очереди, что позволяет получить различные проекции руки), строится трехмерная модель кисти руки. Надежность такой аутентификации сравнима с аутентификацией по отпечатку пальца.

Хотя структура суставов и костей являются относительно постоянными признаками, но распухание тканей, ушибы руки или заболевания суставов (например, вследствие артрита) могут исказить исходную структуру кисти, что в свою очередь сильно повлияет на работу считывателя.

*Системы аутентификации по геометрии лица* основаны на уникальных характеристиках лиц. Они разделяются на двумерное и трехмерное распознавание лица.

Двумерный метод базируется на плоских изображениях, в качестве характеристик выступает расположение частей лица, расстояние между определенными точками или набор математических признаков. Он не требует дополнительного оборудования, однако менее точен, чем трехмерный, и чувствителен к изменениям положения головы и света.

Трехмерный метод реализует сложную математическую задачу и требует использования различных устройств для получения информации о форме лица. Для построения трехмерной модели лица выделяются контуры глаз, бровей, губ, носа и других различных элементов лица, после чего вычисляются расстояния между ними, на основании которых выполняется построение модели. Для определения уникального шаблона, соответствующего определенному человеку, требуется от 12 до 40 характерных элементов. Шаблон должен учитывать множество вариаций изображения на случаи поворота лица, наклона, изменения освещённости, изменения выражения. Диапазон таких вариантов варьируется в зависимости от целей применения данного способа (для идентификации, аутентификации, удаленного поиска на больших территориях и т. д.). Некоторые алгоритмы позволяют компенсировать наличие у человека очков, шляпы, усов и бороды. Такой метод имеет более высокую точность и меньше ошибок, но требует больших затрат на оборудование и сложен для внедрения в уже имеющиеся системы.

*Системы аутентификации по термограмме лица* основаны на использовании уникальных тепловых характеристик лица человека – расположения на нем горячих кровеносных сосудов.

Термограмма получается с помощью камер инфракрасного диапазона, что позволяет получать биометрическую информацию даже в темноте. На функционирование этой системы не влияют возрастные или пластические изменения, изменения температуры лица,

т.к. они не изменяют положение вен и артерий на лице. Однако из-за достаточно низкого качества аутентификации данный метод на сегодняшний день не находит широкого распространения.

**Динамические биометрические признаки.** К динамическим биометрическим признакам пользователя относятся:

- особенности голоса;
- биомеханические характеристики рукописной подписи;
- биомеханические характеристики «клавиатурного почерка» и др.

*Системы аутентификации по голосу* используют сочетания частотных и статистических голосовых характеристик, могут рассматриваться такие параметры как интонация, модуляция, высота тона, тембр голоса и др.

К их преимуществу относится простота реализации, поскольку не требуется применение дорогостоящего оборудования, а достаточно микрофона, звуковой платы и специализированного программного обеспечения. Также его достоинством является неявная аутентификация и отсутствие прямого контакта с пользователем. Основным недостатком метода является его низкая точность, вызванная различными факторами влияния на звук: болезнь, настроение или эмоциональный стресс, наличие фонового шума. В силу этого однофакторная аутентификация по голосу применяется для управления доступом в помещениях среднего уровня безопасности, но может являться дополнительным способом при осуществлении мультифакторной аутентификации.

*Системы аутентификации по динамике рукописной подписи* основываются на уникальности написания человеком своей подписи. Процесс обработки заключается в сравнении двух образцов подписи или сравнении метода написания подписи. При этом, в зависимости от необходимого уровня защиты, выделяют два способа обработки данных о подписи:

- анализ самой подписи по степени совпадения двух картинок;
- анализ динамических характеристик написания с помощью построения свертки, в которую входят дополнительные биомеханические характеристики.

Во втором случае метод учитывает интенсивность усилия подписывающего (давление и скорость), частотные характеристики написания каждого элемента подписи и начертание подписи в целом. Для получения данных используются специализированные ручки и поверхности для записи движения различных элементов подписи. Пример графического планшета, реализующего данный метод, приведен на рис. 2.15.



Рис. 2.15 – Аутентификация по динамике рукописной подписи (WACOM STU-300B).

*Системы аутентификации по «клавиатурному почерку»* используют индивидуальные параметры скорости и последовательности нажатия клавиш на клавиатуре при наборе текста (в частности пароля). При работе на компьютере, пользователи вырабатывают собственные особенности использования клавиатуры, которые зависят от таких факторов как: строение пальцев рук и манера набора текста, время нажатия и ввода текста, часто используемые комбинации клавиш, использование конкретных частей клавиатуры. Данный динамический ритм набора носит название «клавиатурный почерк».

Достоинством аутентификации по «клавиатурному почерку» является его простота реализации. Вместе с тем он обладает достаточно низкой надёжностью, вызванной высокой чувствительностью к изменению параметров набора текста, которые могут быть связаны, например, с изменением психофизического состояния пользователя.

**Особенности биометрической аутентификации.** Эффективность системы биометрической аутентификации оценивается двумя параметрами:

- коэффициентом ложного пропуска – FAR (False Acceptance Rate);
- коэффициентом ложного отказа в доступе – FRR (False Rejection Rate).

*Ложный пропуск* (ошибка первого рода) характеризуется тем, что система предоставляет доступ незарегистрированному пользователю. *Ложный отказ в доступе* (ошибка второго рода) возникает в случае не подтверждения зарегистрированного в системе пользователя. Коэффициенты FAR/FRR тесно связаны друг с другом – каждому коэффициенту ложных отказов соответствует определенный коэффициент ложных пропусков. На сегодняшний день все биометрические технологии являются вероятностными, ни одна из них не способна гарантировать полное отсутствие ошибок FAR/FRR.

В целях повышения достоверности решения задачи биометрической идентификации и аутентификации пользователей особое внимание уделяется развитию систем так называемой *мультифакторной аутентификации*. Реализация такого рода систем подразумевает необходимость предоставления пользователем двух или более биометрических признаков для получения доступа к защищенному объекту или запрашиваемой информации.

Применение различных дополнений для использования нескольких типов биометрических характеристик в комбинированной биометрической системе аутентификации позволяет удовлетворить самые строгие требования к эффективности системы аутентификации. Например, аутентификация по отпечаткам пальцев может сочетаться с аутентификацией по геометрической форме руки, а аутентификации по сетчатке глаза с аутентификацией по геометрии лица и т.д. Такая структура может использовать все виды биометрических данных человека и может применяться там, где приходится форсировать ограничения одной биометрической характеристики.

Комбинированные (мультимодальные) биометрические системы являются более надежными с точки зрения возможности имитации биометрических данных человека, поскольку целый ряд характеристик подделать труднее, чем фальсифицировать один биометрический признак. Практика показывает, что уже при использовании двух биометрических параметров вероятность ошибок снижается до 1,5%.

К известным средствам биометрической аутентификации относятся:

- программный комплекс мультимодальной биометрической аутентификации **«VoiceKey.PLATFORM»** (ООО «ЦРТ-инновации»);
- специальное программное обеспечение автоматизированной системы биоидентификации **«ACCaD-ID»** (ЗАО «АЛГОНТ»);
- программный комплекс **«Система биометрии»** (АО «Ай-Теко»);
- программный комплекс **«Программное обеспечение системы Biolink IDenium»** (ООО «Биолинк Солюшенс») и др.

#### **2.3.4 Комбинированные системы идентификации и аутентификации**

В комбинированных СИА применяется одновременно несколько идентификационных признаков. Внедрение комбинированных идентификаторов различных типов в корпоративную систему информационной безопасности позволяет повысить эффективность защиты компьютеров от НСД. Кроме того, некоторые типы таких систем способны управлять физическим доступом в здания и помещения и контролировать его.

В настоящее время применяются комбинированные СИА следующих типов:

- системы на базе радиочастотных идентификаторов и USB-ключей;
- системы на базе гибридных смарт-карт;
- биоэлектронные системы.

Основные функции комбинированных СИА приведены в таблице 2.3 [32].

Таблица 2.3 – Основные функции комбинированных СИА

<b>Функции</b>	<b>Системы на базе радиочастотных идентификаторов и USB-ключей</b>	<b>Системы на базе гибридных смарт-карт</b>	<b>Биоэлектронные системы</b>
Идентификация и аутентификация пользователей компьютеров	есть	есть	есть
Блокировка работы компьютера и разблокирование при предъявлении персонального идентификатора	есть	нет	есть
Идентификация и аутентификация сотрудников при их доступе (или выходе) в здание, помещение	есть	есть	нет
Хранение конфиденциальной информации (ключей шифрования, паролей, сертификатов и пр.)	есть	есть	есть
Визуальная идентификация	нет	есть	есть

**Системы на базе радиочастотных идентификаторов и USB-ключей.** Аппаратная интеграция USB-ключей и радиочастотных идентификаторов предполагает, что в корпус брелока встраивается радиометка (RFID) – антенна и микросхема Proximity, поддерживающая бесконтактный интерфейс (рис. 2.16). Это позволяет с помощью одного идентификатора организовать управление доступом и к компьютеру, и в помещения офиса.



Рис. 2.16 – Пример системы на базе радиочастотного идентификатора и USB-ключа.

Для входа в служебное помещение сотрудник использует свой идентификатор в качестве радиочастотного идентификатора, а при допуске к защищенным компьютерным данным – в качестве USB-ключа. Кроме того, при выходе из помещения он извлекает идентификатор из USB-разъема (чтобы потом войти обратно) и тем самым автоматически блокирует работу компьютера.

Возможность встраивания радиометки поддерживают USB-ключи: *Рутокен*, *JaCarta*, *ESMART*, *eToken* и др.

Разница между стоимостью комбинированных и обычных USB-ключей приблизительно соответствует цене радиочастотного идентификатора Proximity. Отсюда следует, что интеграция бесконтактных радиочастотных идентификаторов и USB-ключей почти не ведет к росту затрат на аппаратную часть при переходе на комбинированную систему идентификации и аутентификации.

**Системы на базе гибридных смарт-карт.** Гибридные смарт-карты содержат не связанные между собой разнородные чипы (рис. 2.17). Один чип поддерживает контактный интерфейс, другие – бесконтактный (Proximity, ISO 14443/15693).



Рис. 2.17 – Пример гибридной смарт-карты.

Как и в случае интеграции USB-ключей и радиочастотных идентификаторов, СИА на базе гибридных смарт-карт позволяют решить двойную задачу: защиту от НСД к компьютерам и в помещения компании, где они содержатся. При этом гибридная смарт-карта исполняет роль пропуска, на который может быть помещена фотография сотрудника, позволяющая его идентифицировать визуально. Цена на такие карты различается в зависимости от объема микросхем памяти.

**Биоэлектронные системы.** *Биоэлектронные системы* представляют собой сочетание биометрических и электронных СИА. Для защиты компьютеров от НСД биометрические системы обычно объединяются с двумя классами электронных СИА – на базе контактных смарт-карт и на базе USB-ключей.

При этом в большинстве случаев применяется наиболее распространенный биометрический признак – отпечаток пальца, в силу его простоты, удобства процедуры сканирования, а также малого размера сканирующего устройства.

Примером такого рода интеграции могут служить биометрический считыватель смарт-карт *ASEDrive IIIe Bio Combo Swipe* и *JaCarta-2 PKI/BIO/ГОСТ* (рис. 2.18), реализующая поддержку биометрической идентификации пользователя по отпечаткам пальцев с вычислением «на карте», которая используется для замены PIN-кода вводом отпечатка пальца или для строгой трёхфакторной аутентификации при доступе к защищённым корпоративным ресурсам предприятий.



Рис. 2.18 – Смарт-карта JaCarta-2 PKI/BIO/ГОСТ и биометрический считыватель смарт-карт ASEDrive IIIe Bio Combo Swipe.

Другим решением может служить биометрическая платежная смарт-карта *Zwipe*, сочетающая в себе сканер отпечатка пальцев и биометрический процессор (*biometric engine*),

выполняющий обработку и сопоставление полученных биометрических признаков (рис. 2.19).



Рис. 2.19 – Биометрическая платежная смарт-карта Zwipe.

Объединение USB-ключа со сканером отпечатка пальцев также называют *USB-биоключом*. Принцип его действия аналогичен биометрической смарт-карте. Кроме того на сегодняшний день также существует больше число USB-накопителей с дактилоскопическим, как правило емкостным, сканером (рис. 2.20).



Рис. 2.20 – Пример USB-накопителя с дактилоскопическим сканером (Apacer AH651).

Достоинствами USB-биоключей являются:

- высокий уровень защищенности (наличие дактилоскопического сканера, хранение секретных данных, в частности эталонов отпечатков пальцев, в защищенной энергонезависимой памяти идентификатора, шифрование обмена данными с компьютером);
- аппаратная реализация криптографических преобразований;
- отсутствие аппаратного считывателя;
- уникальность признака, малые размеры и удобство хранения идентификаторов.

## **2.4 Особенности применения внешних носителей ключевой информации для идентификации и аутентификации**

Применение внешних носителей ключевой информации подразумевает хранение авторизационных данных пользователя на внешнем ключе – при входе в систему пользователь предъявляет компьютеру носитель ключевой информации, и операционная система считывает с него идентификатор пользователя и соответствующий ему ключ. При этом идентификатор пользователя выступает в качестве имени пользователя, а ключ – в качестве пароля. Ключ, хранящийся на внешнем носителе, может быть гораздо длиннее и безопаснее, чем пароль, и подобрать его становится практически невозможно.

Однако в случае применения внешних носителей ключевой информации актуальна угроза их утери или кражи. Если процедура аутентификации не предусматривает дополнительных мер защиты, то любой обладатель носителя ключевой информации, в том числе и злоумышленник, укравший этот носитель у легального пользователя системы, может беспрепятственно войти в систему с правами пользователя, которому принадлежит данный носитель.

Именно поэтому данный механизм аутентификации, подразумевающий обладание ключевым носителем, используется в совокупности с паролем, обеспечивающим знание дополнительной ключевой информации. В этом случае пользователь должен не только предъявить носитель ключевой информации, но и ввести соответствующий этому носителю пароль (PIN-код). Ключевая информация на носителе хранится зашифрованной на этом пароле, что не позволяет случайному обладателю ключа им воспользоваться.

Основной угрозой при использовании описанного механизма аутентификации является угроза кражи носителя ключевой информации с последующим его копированием и подбором пароля на доступ к ключу. Для затруднения подбора этого пароля используют защиту ключевого носителя от копирования и блокировку или уничтожение ключевой информации после определенного количества неудачных попыток его ввода. Однако важно помнить, что эти меры защиты неприменимы для электронных ключей iButton и бесконтактных смарт-карт Proximity.

В целом использование для аутентификации пользователей не только паролей, но еще и внешних носителей информации позволяет заметно повысить защищенность операционной системы. В наибольшей мере защищенность системы повышается при использовании процессорных смарт-карт.

## **3 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

### **3.1 Классификация средств криптографической защиты информации**

К *средствам криптографической защиты информации (СКЗИ)*, относятся аппаратные, программные и программно-аппаратные средства, реализующие криптографические алгоритмы преобразования информации. СКЗИ используются в некоторой АС (информационно-телекоммуникационной системе, сети связи), совместно с механизмами реализации и гарантирования политики безопасности.

Преобразование информации с применением методов криптографии называют криптографическим преобразованием информации. Принято считать, что криптография – это наука о шифрах. Однако возможности современной криптографии значительно шире и помимо шифрования данных и сообщений с целью обеспечения их конфиденциальности, включают в себя также их контроль целостности (защиту от модификации информации), аутентификацию данных, защиту программ от несанкционированного копирования и распространения, организацию парольных систем и пр. Исходя из этого, рассмотрим классификацию СКЗИ по различным их характеристикам.

По назначению [20] СКЗИ можно разделить на следующие группы:

- системы аутентификации электронных данных;
- системы идентификации и аутентификации пользователей;
- системы шифрования дисковых данных;
- системы шифрования данных, передаваемых по сети;
- средства управления ключевой информацией.

*Системы аутентификации электронных данных* направлены на установление подлинности авторства и контроля целостности электронного документа для чего применяются код аутентификации сообщения (имитовставка) или электронная подпись.

*Системы идентификации и аутентификации пользователей* включают в себя ранее рассмотренные механизмы защищенного хранения авторизационных данных.

*Системы шифрования дисковых данных* напрямую направлены на криптографические преобразования данных на уровне файлов или дисков, в том числе в режиме реального времени («на лету»).

*Системы шифрования данных, передаваемых по сети*, осуществляют канальное и сквозное (оконечное) шифрование информации, передаваемой по каналу связи. В случае

канального шифрования защищается вся передаваемая по сети информация, включая служебную. В случае сквозного шифрования защищается только содержание сообщений, а служебная информация остается открытой.

*Средства управления криптографическими ключами* включают в себя функции генерации, хранения и безопасного распределения ключей между участниками информационного обмена.

По применяемым криптографическим алгоритмам выделяют два основных подкласса СКЗИ:

- симметричные криптосистемы;
- асимметричные криптосистемы.

Под *криптосистемой* понимают совокупность пространства ключей, пространства открытых текстов, пространства шифротекстов, алгоритмов шифрования и расшифровывания. Алгоритм шифрования представляет собой набор преимущественно обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования или криптоалгоритмом. Сменный элемент шифра, применяемый для защиты отдельного сообщения, называется *ключом* шифрования.

В зависимости от числа используемых в криптографических алгоритмах ключей (рис. 3.1) можно выделить:

- *бесключевые*, которые для осуществления криптографических преобразований не требуется вычисление ключей, например, некоторые алгоритмы хэширования;
- *одноключевые*, в которых для выполнения криптографических преобразований требуется один ключевой параметр (секретный ключ), классическим представителем которых являются алгоритмы симметричного шифрования;
- *двухключевые*, где на различных стадиях работы применяются два ключевых параметра (открытый и секретный ключи), – алгоритмы асимметричного шифрования и электронной подписи.

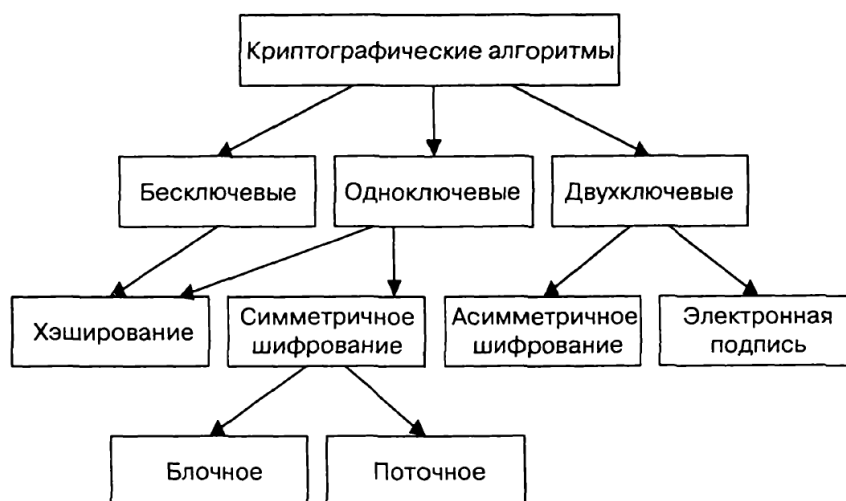


Рис. 3.1 – Классификация криптографических алгоритмов по количеству ключей.

Поясним определения криптографических преобразований, приведенные на рис. 2.

**Хэширование** – это метод криптозащиты, представляющий собой контрольное преобразование информации: из данных неограниченного размера путем выполнения криптографических преобразований вычисляется хэш-значение фиксированной длины, однозначно соответствующее исходным данным.

Процедура хэширования является открытым односторонним (необратимым) преобразованием. В случае, когда она зависит от ключа, результат её вычисления носит название *имитовставки* или кода аутентификации сообщения (message authentication code).

**Симметричное шифрование** использует один и тот же ключ, как для шифрования, так и для расшифровывания информации. Фактически оба ключа могут и различаться, но если в криптоалгоритме их возможно вычислить один из другого в обе стороны, то такой алгоритм однозначно относится к симметричному шифрованию.

Симметричное шифрование подразделяется на два вида: блочное и поточное, хотя стоит сразу отметить, что в некоторых классификациях они не разделяются, считая, что поточное шифрование – это шифрование блоков единичной длины.

**Блочное шифрование** характеризуется тем, что информация предварительно разбивается на блоки открытого текста фиксированной длины (64, 128, 256 бит), после криптографических преобразований которых, получаются блоки шифрованного текста такой же длины. При этом в различных криптоалгоритмах (или даже в разных режимах работы одного и того же алгоритма) блоки могут шифроваться как независимо друг от друга, так и «со сцеплением» – когда результат шифрования текущего блока данных зависит от значения предыдущего блока или от результата шифрования предыдущего блока.

*Поточное шифрование* подразумевает преобразование каждого символа открытого текста в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста. Данный вид шифрования устраняет необходимость разбиения сообщения на целое число блоков большой длины, а значит, может работать в режиме реального времени. Алгоритмы поточного шифрования шифруют данные побитно или посимвольно, что достигается применением операции гаммирования – процедуры наложения на входную информационную последовательность гаммы шифра, т.е. последовательности с выходов генератора псевдослучайных кодов.

*Асимметричное шифрование* характеризуется применением двух типов ключей: открытого (публичного), применяемого для зашифровывания информации, и секретного (личного), используемого для ее расшифровывания. Открытый и секретный ключи математически связаны между собой достаточно сложным соотношением, особенность которого – возможность вычисления открытого ключа из секретного и невозможность (за ограниченное время при реальных ресурсах) вычисления секретного ключа из открытого.

*Электронная подпись* представляет собой реквизит электронного документа, полученный в результате криптографического преобразования информации, для подтверждения целостности и авторства данных. Как и в случае асимметричного шифрования, в данном методе применяются двухключевые алгоритмы с вычислением открытого ключа из секретного, однако их назначение носит иной характер: секретный ключ применяется для вычисления электронной подписи, а открытый ключ – для ее проверки. При соблюдении правил безопасного хранения секретного ключа никто, кроме его владельца, не может вычислить верную электронную подпись какого-либо электронного документа.

Перед тем как перейти к дальнейшему рассмотрению СКЗИ, уточним некоторые особенности последующей терминологии. На практике, наряду с термином «средство криптографической защиты информации», в ряде источников можно встретить эквивалентный ему термин «шифратор» и «дешифратор», и соответствующее обозначение реализуемых ими процессов как «шифрации» и «дешифрации». На взгляд авторов это может вызвать путаницу с обозначениями одноименных комбинационных схем цифровой техники, выполняющих операции преобразования позиционного  $n$ -разрядного кода в  $m$ -разрядный двоичный код и наоборот выполняемых, соответственно, шифратором (encoder) и дешифратором (decoder). В силу этого обстоятельства далее процесс шифрации информации будет обозначаться как «шифрование» (encryption), а обратный ему – «расшифровывание» (decryption).

## 3.2 Симметричные криптографические системы

### 3.2.1 Принципы симметричного шифрования информации

В основе данного рода криптосистем лежит симметричное шифрование информации, которое также называется *шифрованием с закрытым ключом*. Общая схема симметричной криптосистемы представлена на рис. 3.2.

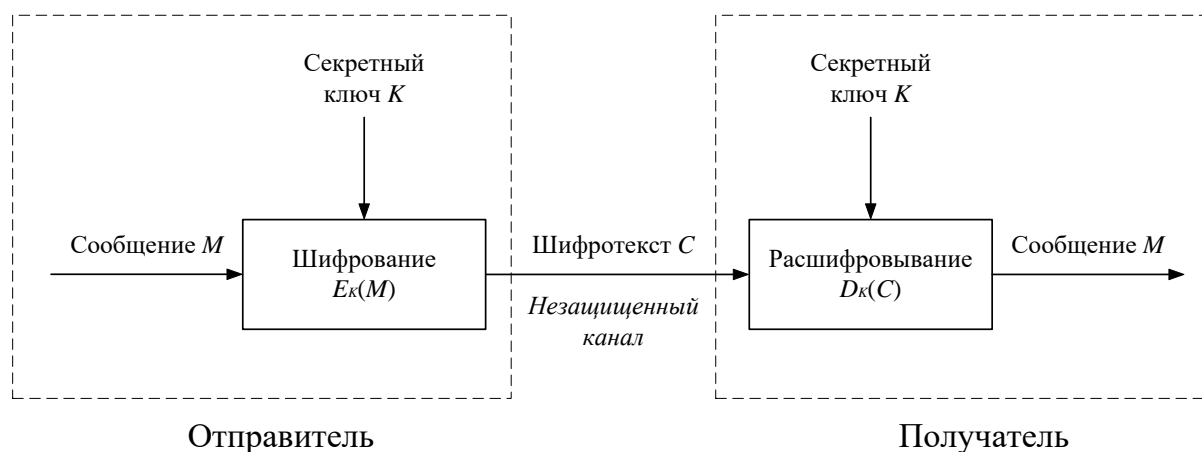


Рис. 3.2 – Схема симметричной криптосистемы.

На схеме сообщение, или открытый текст,  $M$  (message) шифруется с помощью обратимого преобразования  $E_K(M)$ , формирующего шифротекст  $C$  (ciphertext). Процесс такого преобразования задается с помощью алгоритма шифрования  $E$  (encryption) и ключа  $K$  (key). Шифрованный текст пропускается через общедоступный (открытый, незащищенный) канал связи, после чего его подвергают восстановлению с помощью операции расшифровывания  $D$  (decryption), представляющей собой обратное преобразование, соответствующее выражению:  $D_K(C) = E_K^{-1}[E_K(M)] = M$ .

Примером самых примитивных симметричных алгоритмов являются шифры Цезаря, Вижинера, представляющие собой простейшие алгоритмы подстановки. Шифрование данными алгоритмами представляет собой тривиальную задачу. Современные симметричные алгоритмы закрепляются государственными стандартами. Например, в США в течение нескольких десятилетий применялся широко распространенный во всем мире алгоритм DES (Data Encryption Standard).

Перечислим некоторые известные алгоритмы симметричного блочного шифрования с указанием стран их разработки:

- AES, Blowfish, Twofish, RC5, RC6, Mars (США);

- CAST (Канада);
- LOKI (Австралия);
- IDEA (Швейцария);
- Camellia (Япония);
- ГОСТ 28147-89 (СССР);
- ГОСТ 34.12-2018 (Россия).

Блочные шифры являются той основой, на которой реализованы почти все симметричные криптосистемы. Практически все алгоритмы используют для преобразований определенный набор обратимых математических процедур, задачами которых является рассеяние статистических особенностей открытого текста по широкому диапазону характеристик шифрованного текста, что достигается применением нескольких последовательных перестановок данных, шифров перестановки (substitution), и усложнении статистической взаимосвязи между шифротекстом и ключом, что реализуется использованием сложных подстановок, шифров подстановки (permutation). На практике схемами, реализующими такие преобразования, являются *сеть Фейстеля* (Feistel cipher) и *подстановочно-перестановочная сеть* (substitution-permutation network), называемая также *SP-сеть*. Основное отличие их заключается в том, что при использовании *SP-сети* преобразуется весь входной блок данных, а при сети Фейстеля его половина.

### 3.2.2 Алгоритмы симметричного шифрования информации

Рассмотрим более подробно некоторые из приведенных выше алгоритмов симметричного шифрования.

**Алгоритм DES.** Алгоритм блочного шифрования данных DES (Data Encryption Standard) был опубликован в 1977 году и построен в соответствии с методологией сети Фейстеля. Он осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (остальные 8 бит – проверочные биты для контроля на четность).

Процесс шифрования заключается в начальной перестановке битов 64-битового блока, 16 раундах шифрования и в конечной перестановке битов. Расшифровывание в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности.

Развитие вычислительной техники привело к тому, что полный перебор всех 56-битных ключей представляется возможным, поэтому DES не может больше использоваться в

качестве надёжного средства защиты электронной информации, его можно рекомендовать лишь для целей тестирования.

Альтернативой классическому алгоритму DES является **Triple DES** (3DES), представляющий собой троекратное преобразование данных по алгоритму DES с тремя различными 56-битными ключами. При этом длина ключа 3DES составляет 168 бит, что приводит к его существенной надёжности по сравнению с DES, однако увеличивает время преобразование данных в три раза, что на практике приводит к заметному замедлению процессов обращения к данным на зашифрованных дисках.

**Алгоритм AES.** Алгоритм блочного шифрования AES (Advanced Encryption Standard), также известный под своим первоначальным названием Rijndael («Рейндал») был опубликован в 2001 году и принят в качестве стандарта шифрования правительством США. Шифр Rijndael был объявлен победителем конкурса, организованного Национальным институтом стандартов и технологий США в 1997 году по выбору нового криптографического стандарта, который должен был стать преемником DES.

Алгоритм AES шифрует блоки длиной 128 бит и имеет поддержку размеров ключей шифрования в 128, 192, 256 бит. В зависимости от размера ключа конкретный вариант алгоритма AES может обозначаться, соответственно, как AES-128, AES-192, AES-256.

Алгоритм хорошо изучен, обладает ясной, простой структурой алгоритма, высокой скоростью шифрования данных и возможностью параллельного выполнения операций в многопроцессорных системах. Алгоритм построен в соответствии с методологией *SP*-сети, при этом каждый блок обрабатываемых данных представляется в виде двухмерного байтового массива размером  $4 \times 4$ . Количество раундов шифрования составляет 10, 12 или 14 в зависимости от длины ключа.

**Алгоритм ГОСТ 28147-89.** Стандарт «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» был принят в 1989 году в качестве алгоритма шифрования данных, составляющих Государственную тайну.

Работы над алгоритмом, положенным впоследствии в основу стандарта, начались в рамках темы «Магма» практически сразу после публикации алгоритма DES, и сам он был разработан в 70-е годы прошлого века по поручению Научно-технического совета восьмого Главного управления КГБ СССР (структурного подразделения КГБ, ответственного за защиту технических средств связи и создание шифров). Тогда он имел гриф «Совершенно секретно». Затем гриф был понижен до «Секретно», после чего был переведен в «Для служебного пользования», с которым и был подготовлен к публикации в 1989 году.

Алгоритм ГОСТ 28147-89 считается одним из наиболее криптостойких симметричных алгоритмов шифрования. Аналогично алгоритму DES, в его основе лежит сеть Фейстеля, размер блока шифрования данных составляет 64 бита, размер ключа – 256 бит. Алгоритм использует 32 раунда шифрования и имеет 4 режима работы: простая замена, гаммирование, гаммирование с обратной связью, выработка имитовставки. Отличительной чертой алгоритма ГОСТ 28147-89 являются не фиксированные узлы подстановки (*S*-блоки) – поставка заполнения *S*-блоков производится в установленном порядке, т.е. разработчиком алгоритма.

В 2015 году вместе с вновь разработанным в России алгоритмом симметричного шифрования «Кузнечик» один из вариантов алгоритма ГОСТ 28147-89 (с фиксированным набором подстановок) был опубликован под названием «Магма» как часть стандарта ГОСТ Р 34.12-2015, а позже как часть стандарта ГОСТ 34.12-2018.

**Алгоритм ГОСТ 34.12-2018.** Стандарт ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры» был подготовлен на основе применения ГОСТ Р 34.12-2015 и приводит описание двух базовых блочных шифров с длинами блоков 128 бит (шифр «Кузнечик») и 64 бит (шифр «Магма») и длинами ключей 256 бит.

Шифр «Кузнечик» (Kuznechik) был разработан Центром защиты информации и специальной связи ФСБ России с участием ОАО «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

В основе шифра лежит *SP*-сеть, длина блока шифрования данных составляет 128 бит, длина ключа – 256 бит. Шифр имеет в общей сумме 10 раундов шифрования, каждый раунд включает в себя линейное и нелинейное преобразование и операцию наложения итерационного ключа. Итерационные (или раундовые) генерируются на основе сети Фейстеля.

В России при обработке информации, составляющей государственную тайну, регламентировано использовать только отечественный стандарт шифрования.

**Алгоритм IDEA.** Блочный алгоритм IDEA (International Data Encryption Algorithm) был создан и запатентован швейцарской фирмой Ascom в 1991 году и известен своим изначальным применением в пакете программ шифрования PGP.

В основе шифра лежит сеть Фейстеля. Размер блока шифрования данных составляет 64 бита, длина ключа – 128 бит. Процесс шифрования состоит из 8 одинаковых раундов шифрования и одного выходного преобразования. Все алгебраические операции, применяемые в процессе шифрования, совершаются над 16-битными числами.

Особенностью алгоритма является использование операций из разных алгебраических групп, а именно сложение по модулю  $2^{16}$ , умножение по модулю  $(2^{16}+1)$ , побитовое исключающее ИЛИ. Применение этих трех операций затрудняет криптоанализ IDEA по сравнению с DES, а также позволяет отказаться от использования S-блоков и таблиц замен.

**Алгоритм Blowfish.** Данный блочный алгоритм шифрования был разработан американским криптографом Брюсом Шнайером в 1993 году в качестве быстрой и свободной альтернативы устаревшему DES и запатентованному IDEA. В его основе лежит сеть Фейстеля с 16 раундами шифрования. Размер блока шифрования составляет 64 бит, длина ключа изменяемая – 32-448 бит. Алгоритм шифрования выполнен на простых и быстрых операциях: исключающее ИЛИ, подстановка и сложение по модулю  $2^{32}$ . Blowfish зарекомендовал себя как надёжный алгоритм, поэтому реализован во многих приложениях, где не требуется частая смена ключа и необходима высокая скорость шифрования/расшифровывания информации.

**Алгоритм Twofish.** Был разработан в 1998 году группой специалистов во главе с Брюсом Шнайером на основе алгоритмов Blowfish, SAFER и Square. Данный алгоритм готовился специально для конкурса AES и стал одним из пяти финалистов его второго этапа.

Алгоритм Twofish построен согласно методологии сети Фейстеля с 16 раундами преобразований, шифрует блоки длиной 128 бит и имеет поддержку размеров ключей шифрования в 128, 192, 256 бит.

По сложности своей реализации и анализа на предмет слабых ключей или скрытых связей данный алгоритм превосходит Rijndael, но при этом в сравнении с ним имеет достаточно медленное время выполнения. Тем не менее, его изучение показало, что он обладает большим запасом прочности, и, по сравнению с остальными финалистами конкурса AES, он оказался наиболее стойким.

**Алгоритм CAST.** Под CAST понимают методологию построения симметричных алгоритмов шифрования, разработанную канадскими криптографами Карлайлом Адамсом и Стаффордом Таваресом, первые две буквы имени которых и формируют её название. В рамках данной методологии выделяют CAST-128 и CAST-256, где числа в названии указывают на максимальный размер ключа.

CAST-128 разработан в 1996 году и состоит из 12 или 16 раундов сети Фейстеля (количество раундов зависит от длины ключа). Размер блока составляет 64 бита при переменной длине ключа от 40 до 128 бит. 16 раундов шифрования применяется в случае, когда размеры ключа превышают 80 бит.

CAST-256 разработан в 1998 году в качестве кандидата на участие в конкурсе AES и

основан на CAST-128. Основу алгоритма составляет сеть Фейстеля из 48 раундов. Длина блока соответствует 128 битам, размер ключа может составлять 128, 160, 192, 224 или 256 бит с возможностью его быстрого расширения.

**Алгоритм Camellia.** Был представлен в 2000 году японскими компаниями «Nippon Telegraph and Telephone Corporation» и «Mitsubishi Electric Corporation» в рамках европейского конкурса криптоалгоритмов NESSIE (New European Schemes for Signatures, Integrity, and Encryption – «Новые европейские алгоритмы для электронной подписи, целостности и шифрования»).

Алгоритм основан на сети Фейстеля. Размер блока шифрования данных составляет 128 бит, длина ключа поддерживается 128, 192 и 256 бит. В зависимости от размера ключа имеет 18 или 24 раунда шифрования, соответственно, для длин ключа 128 и 192/256 бит. По результатам конкурса NESSIE данный алгоритм был признан надежным и быстрым алгоритмом, не требовательным к ресурсам. Алгоритм патентован, однако распространяется под рядом свободных лицензий, в частности, является частью проекта OpenSSL.

### **3.2.3 Особенности практического применения симметричных криптографических систем**

Симметричные криптосистемы характеризуются наиболее высокой скоростью шифрования, и с их помощью обеспечивается как конфиденциальность и подлинность, так и целостность передаваемой информации. При этом конфиденциальность передачи информации в данном случае зависит от стойкости шифра и обеспечения безопасности ключа шифрования. Обычно ключ шифрования представляет собой файл или массив данных и хранится на персональном ключевом носителе, например USB-ключе или смарт-карте.

Симметричное шифрование подходит в случаях шифрования информации «для себя», например, с целью предотвращения НСД к хранимой информации в отсутствие владельца, архивного шифрования выбранных файлов и прозрачного шифрования целых логических или физических дисков.

Помимо этого, данные криптосистемы широко применяются для абонентского шифрования данных, т.е. для шифрования информации, предназначенной для отправки по сети, однако автономное использование симметричных криптосистем в компьютерных сетях порождает проблему безопасного распределения ключей шифрования между пользователями. Использование только одного секретного ключа для всех абонентов сети недопустимо по соображениям безопасности, поскольку в случае его компрометации (хищения, утери) под угрозой будет находиться документооборот всех абонентов сети. В

связи с этим, на практике требуется частое изменение ключей, вследствие чего надежность симметричной криптосистемы во многом зависит от используемой *системы распределения ключей*, представляющей собой средства конфиденциальной доставки ключей сторонам информационного обмена.

Распределение ключей между двумя условными сторонами информационного обмена (пользователями, ведущими узлами, процессами, приложениями) можно организовать различными способами [12]:

- 1) ключ может быть выбран одной из сторон и физически доставлен другой;
- 2) ключ может быть выбран третьей стороной и физически доставлен участникам информационного обмена;
- 3) если участники информационного обмена уже используют некоторый общий ключ, то одна из сторон может передать новый ключ другой стороне в зашифрованном виде, используя старый ключ;
- 4) если обе из сторон информационного обмена имеют криптографически защищенные каналы связи с некоторой третьей стороной, то последняя может доставить им ключ по этим защищенным каналам.

Физическая доставка ключей в ряде случаев оказывается неприемлема, поэтому на практике широко применяется схема централизованного распределения ключей, являющаяся вариацией способа 4, где за доставку ключей сторонам информационного обмена отвечают некоторые *центры распределения ключей* (ЦРК). При централизованном управлении ключей определяется некоторая иерархия ЦРК. Например, выделяются локальные ЦРК, ответственные за малые домены всей сети (отдельные локальные сети), которые для связи объектов из разных доменов могут использовать ЦРК глобального уровня. Такая иерархия может состоять из трех и большего числа уровней, в зависимости от количества пользователей и географического распространения сети. Применение ЦРК предполагает, что он должен внушать доверие и быть надежно защищенным от посягательств.

Возможна также схема децентрализованного управления ключами. При децентрализации требуется, чтобы каждая конечная система имела возможность обмениваться данными некоторым защищенным образом со всеми другими потенциально достижимыми конечными системами с целью распределения сеансовых ключей. При таком способе распределения ключей в сети из  $n$  конечных системам потребуется  $\frac{n(n-1)}{2}$  обменов, что на практике резко ограничивает возможность использования такой схемы. И хотя полная

децентрализация в больших сетях практически не применяется, децентрализация может быть полезной в контексте локальных сетей.

Проблема распределения ключей в симметричных криптосистемах привела к разработке асимметричных методов шифрования, с помощью которых возможно обеспечить как защищенный информационный обмен, так и обеспечить распределение ключей симметричного шифрования между его участниками, без привлечения дополнительной стороны.

### **3.3 Асимметричные криптографические системы**

#### **3.3.1 Принципы асимметричного шифрования информации**

В основе данного рода криптосистем лежит асимметричное шифрование информации, которое также называется *шифрованием с открытым ключом*. Идея применения методов криптографии с открытым ключом возникла с целью разрешения двух наиболее сложных проблем, возникающих при использовании симметричного шифрования – проблемы распределение ключей и электронной подписи.

Американский криптограф, один из основателей метода асимметричного шифрования Уитфилд Диффи, считал, что использование услуг ЦРК противоречит сути криптографии, а именно возможности обеспечения секретности передачи информации, в виду наличия дополнительной стороны, также обладающей ключом шифрования/расшифровывания. Кроме того развитие электронного документооборота породило необходимость, помимо обеспечения конфиденциальности информации, также разработки криптографических механизмов контроля её целостности, т.е. подписей, эквивалентных применяемым в бумажных документах (что будет рассмотрено в разделе 3.7).

Исходя из этих предпосылок, Уитфилд Диффи совместно Мартином Хеллманом в 1976 году предложили метод, радикально отличающийся от всех известных ранее подходов в криптографии и снимающий основную проблему классической криптографии – проблему распределения ключей.

Общая схема асимметричной криптосистемы представлена на рис. 3.3.

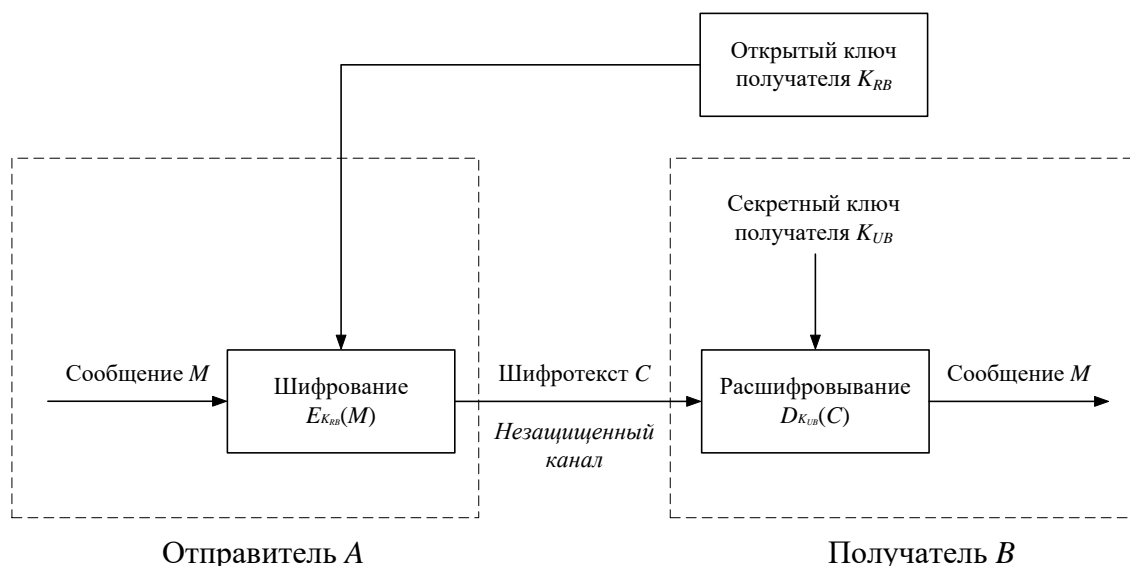


Рис. 3.3 – Схема асимметричной криптосистемы.

Принцип данной криптосистемы заключается в следующем. Каждая сторона информационного обмена генерирует пару ключей  $\{K_R, K_U\}$ , предназначенных, соответственно, для шифрования и расшифровывания сообщений. Ключ шифрования  $K_R$  (открытый ключ) стороны получателя размещается в открытом реестре или файле, ключ расшифровывания  $K_U$  (секретный ключ) остается в его личном владении. Сторона А отправителя зашифровывает передаваемое сообщение с помощью открытого ключа получателя  $C = E_{K_{RB}}(M)$ , после чего получатель В расшифровывает принятое сообщение с помощью хранимого у него секретного ключа  $M = D_{K_{UB}}(C)$ . Аналогичным образом происходит и ответная передача шифруемых сообщений, в чем и состоит асимметрия криптографических процессов данного метода.

Открытый и секретный ключи связаны между собой математически и имеют важную особенность: с вычислительной точки зрения невозможно определить ключ расшифровывания, обладая только ключом шифрования и зная используемый криптографический алгоритм. Данная особенность позволяет использовать асимметричные криптографические системы как в качестве непосредственно средства шифрования передаваемой и хранимой информации, так и средства аутентификации пользователей (создания электронной подписи) и распределения ключей.

Основным преимуществом асимметричных алгоритмов перед симметричными является отсутствие необходимости предварительной передачи секретного ключа,

недостатком – их вычислительная сложность, а следовательно, бóльшая ресурсоёмкость по сравнению с симметричными алгоритмами.

В настоящее время существует множество различных алгоритмов асимметричного шифрования. Среди наиболее известных выделяют следующие алгоритмы шифрования и создания электронной подписи:

- RSA;
- алгоритм Диффи-Хеллмана (Diffie-Hellman (DH));
- алгоритм Эль-Гамала (Elgamal);
- ГОСТ 34.10-2018;
- Rabin;
- McEliece и др.

Большинство асимметричных криптосистем основаны на факторизации больших чисел или теории эллиптических кривых.

### 3.3.2 Алгоритмы асимметричного шифрования информации

Рассмотрим более подробно некоторые из приведенных алгоритмов асимметричного шифрования.

**Алгоритм RSA.** Алгоритм RSA был предложен в 1977 году и получил название по первым буквам фамилий его авторов, а именно Р. Ривеста (Rivest), А. Шамира (Shamir) и А. Адлемана (Adleman). Данный алгоритм стал первым алгоритмом с открытым ключом, который может работать в режиме шифрования данных и электронной подписи.

В основу алгоритма RSA положена сложность задачи факторизации произведения двух больших простых чисел. Для шифрования используется операция возведения в степень по модулю большого числа. Для расшифровывания за разумное время (обратной операции) необходимо вычислить функцию Эйлера от данного большого числа, для чего необходимо разложение числа на простые множители.

Схема RSA представляет собой блочный шифр, в котором и открытый текст, и шифрованный текст представляются целыми числами из диапазона от 0 до  $(n-1)$  для некоторого  $n$ . Процесс шифрования одинаков для каждого блока, содержащего двоичное значение, меньшее некоторого заданного числа  $n$ . Длина блока должна быть меньше или равна  $\log_2 n$  и на практике выбирается равной  $2^k$  битам, где  $2^k < n < 2^{k+1}$ .

Первоначально вырабатывается пара ключей. Для этого генерируются два больших простых числа  $p$  и  $q$ , после чего вычисляется их произведение  $n = pq$ . Затем выбирается

случайное число  $e$ , взаимно простое<sup>1</sup> со значением функции Эйлера от числа  $n$ , определяемой выражением  $\varphi(n) = (p-1)(q-1)$ . Далее вычисляется единственное число  $d$  из условия  $de \equiv 1 \pmod{\varphi(n)}$ . Пара чисел  $(e, n)$  объявляется открытым ключом, а пара  $(d, n)$  – секретным ключом.

**В режиме шифрования данных** процедуру шифрования для блока открытого текста  $M$  и расшифровывания для блока шифротекста  $C$  можно представить в виде следующих выражений:

$$C = M^e \pmod{n},$$

$$M = C^d \pmod{n}.$$

Все приведенные процессы реализуются в СКЗИ преимущественно автоматически. Большинство общепринятых алгоритмов вычисления простых чисел  $p$  и  $q$  носят вероятностный характер.

**В режиме электронной подписи** секретным ключом вычисляется сообщение

$$C = M^d \pmod{n},$$

которое рассматривается как подпись передающей стороны, поскольку секретный ключ известен только ей. Сторона получателя, используя открытый ключ  $(e, n)$  выполняет проверку подписанного документа, согласно выражению:

$$C^e = (M^d)^e \pmod{n} \equiv M.$$

При этом в качестве  $M$  выступает не передаваемый электронный документ, а его хэш-значение (дайджест). Изначально дайджест не является зашифрованным и может пересылаться в исходном виде, однако путём совместного применения схем шифрования и электронной подписи в системе RSA можно создавать сообщения, которые будут и зашифрованы, и содержать электронную подпись. Для этого сторона отправителя сначала добавляет к передаваемому электронному документу свою электронную подпись, а затем выполняет шифрование полученной пары с помощью открытого ключа получателя. Получатель расшифровывает полученное сообщение с помощью своего секретного ключа.

**Алгоритм Диффи-Хеллмана.** Алгоритм Диффи-Хеллмана (известный также как схема или *протокол Диффи-Хеллмана*) не применяется для шифрования сообщений или формирования электронной подписи, а предназначен для распределении ключей – обмену без посредников между сторонами информационного обмена ключом, который может быть

---

<sup>1</sup> **Взаимно простые числа** – целые числа, не имеющие общих делителей, кроме единицы. В этом случае их наибольший общий делитель (НОД) равен 1.

использован для симметричного шифрования. Данная технология обмена ключами реализована в целом ряде коммерческих продуктов. Эффективность алгоритма опирается на трудность вычисления дискретных логарифмов.

Суть алгоритма состоит в следующем. Вначале специальным образом подбирается некоторое натуральное число  $A$ , которое является первообразным корнем простого числа  $p < A$ , как число, степени которого порождают все целые положительные числа от 1 до  $(p-1)$ . Число  $A$  должно обладать свойством: все числа вида

$$A \bmod p, A^2 \bmod p, A^3 \bmod p, \dots, A^{p-1} \bmod p,$$

должны быть различными и состоять из целых положительных значений в диапазоне от 1 до  $(p-1)$  с некоторыми перестановками.

В этом случае для любого целого числа  $Y < p$  и любого первообразного корня  $A$  простого числа  $p$  однозначно определяется показатель степени  $x$  (дискретный логарифм), при котором

$$Y = A^x \bmod p, \text{ где } 0 \leq x \leq (p-1).$$

Задача выбора параметра  $A$  при произвольно заданном  $p$  является достаточно трудной в связи с разложением на простые множители числа  $(p-1)$ . На практике простое число  $p$  выбирается так, чтобы выполнялось равенство  $p = 2q + 1$ , где  $q$  – также простое число. В этом случае в качестве  $A$  можно взять любое число, для которого справедливы неравенства  $1 < A < (p-1)$  и  $A^q \bmod p \neq 1$ . На подбор параметров  $A$  и  $p$  необходимо некоторое время, которое не критично для системы связи и не замедляет ее работу.

Процедура формирования общего ключа  $K$  для двух абонентов состоит в следующем. Изначально имеется два общих открытых параметра: простое число  $p$  и целое число  $A$ , являющееся первообразным корнем  $p$ .

Первый абонент вырабатывает случайным образом число  $x_1$  ( $x_1 < p$ ), которое является его секретным ключом. На основе этого ключа вычисляется число  $Y_1 = A^{x_1} \bmod p$ , которое служит его открытым ключом, и отправляется второму абоненту.

Второй абонент аналогичным образом независимо генерирует случайное число  $x_2$  ( $x_2 < p$ ), принимаемое в качестве секретного ключа данного абонента, и вычисляет  $Y_2 = A^{x_2} \bmod p$ , которое является его открытым ключом и отправляется первому абоненту.

После этого каждая сторона из чисел  $Y_1$  и  $Y_2$ , а также своих секретных ключей  $x_1$  и  $x_2$  формирует общий секретный ключ  $K$  для сеанса симметричного шифрования:

– первый абонент:  $K = (Y_2)^{x_1} \bmod p$ ;

– второй абонент:  $K = (Y_1)^{x_2} \bmod p$ .

Если весь протокол формирования общего секретного ключа выполнен верно, значения  $K$  у обоих абонентов являются одинаковыми.

Данный алгоритм, как и все алгоритмы асимметричного шифрования, уязвим для атак типа «человек посередине» (man in the middle), однако на практике существует ряд его модификаций по предотвращению такой атаки.

**Алгоритм Эль-Гамала.** Алгоритм был предложен криптографом египетского происхождения Тахером Эль-Гамалем в 1985 году в качестве усовершенствованной системы Диффи-Хеллмана и включает в себя алгоритм непосредственно шифрования, алгоритм формирования электронной подписи и обмена ключей. В отличие от RSA алгоритм Эль-Гамала не был запатентован и, поэтому, стал его более дешевой альтернативой.

Фактически алгоритм Эль-Гамала использует схему Диффи-Хеллмана, чтобы сформировать общий секретный ключ для абонентов информационного обмена, после чего передаваемое сообщение шифруется путем умножения на этот ключ.

Первоначально вырабатывается пара ключей. Для этого аналогично схеме Диффи-Хеллмана, выбирается некоторое большое простое число  $p$  и число  $A$  такие, что различные степени  $A$  представляют собой различные числа по модулю  $p$ . Данные числа являются общими для всех абонентов информационного обмена. Далее каждый абонент генерирует ключевую пару: случайным образом выбирает секретный ключ  $x$  ( $0 < x < p$ ) и вычисляет открытый ключ  $Y = A^x \bmod p$ .

**В режиме шифрования** сообщение  $M$  представляется в виде одного числа или набора чисел, каждое из которых меньше  $p$ , т.е.  $0 \leq M < p$ . Процедура шифрования для двух абонентов состоит в следующем.

Первый абонент (отправитель) выбирает случайное число  $k$ , взаимно простое с  $(p-1)$ , и вычисляет числа  $r = A^k \bmod p$  и  $e = (M \cdot Y_2^k) \bmod p$ , где  $Y_2$  – открытый ключ второго абонента. Число  $k$  держится в секрете. Пара чисел  $(r, e)$  является шифротекстом и отправляется второму абоненту (получателю).

Для расшифровывания полученного шифротекста второй абонент вычисляет  $M = (e \cdot r^{p-1-x_2}) \bmod p$ , где  $x_2$  – его секретный ключ.

При использовании алгоритма Эль-Гамала требуется, чтобы выбираемое в процессе шифрования число  $k$  каждый раз менялось и неизменно хранилось в секрете. Вычислительно

определить значение  $k$  практически невозможно, т.к. это задача дискретного логарифмирования. Таким образом, вычислить сообщение  $M$  третьей стороной без знания умноженного на него числа  $k$  не получится, как и воспроизвести действия получателя (второго абонента), поскольку его секретный ключ  $x_2$  также неизвестен (вычисление  $x_2$  на основании  $Y_2$  также является задачей дискретного логарифмирования).

**В режиме обмена ключей** симметричного шифрования их распределение производится аналогичным образом. На практике наиболее целесообразно использовать алгоритм Эль-Гамала именно для согласования общего ключа сессии, а не прямого шифрования больших сообщений, вследствие применения операции возведения в степень и умножения по большому модулю, что приводит к крайне медленному шифрованию больших сообщений.

**В режиме электронной подписи**, как и при шифровании, стороны информационного обмена согласуют параметры  $A$  и  $p$ , после чего отправитель выбирает секретный ключ  $x$  и рассчитывает открытый ключ  $Y = A^x \bmod p$ .

Подписываемое сообщение  $M$  должно удовлетворять условию  $0 \leq M < p$ . Подписью абонента служит пара чисел  $r$  и  $s$  ( $0 \leq r < p$ ,  $0 \leq s < p$ ), которые удовлетворяют соотношению  $A^M \equiv (Y^r r^s) \bmod p$ . Получатель, имея сообщение  $M$  и открытый ключ  $Y$  отправителя, может проверить выполнение этого равенства, но только владелец секретного ключа  $x$  может правильно рассчитать значения  $r$  и  $s$ .

Вычисление пары чисел  $(r, s)$ , т.е. процедура формирования электронной подписи, заключается в следующем. Отправитель выбирает случайное число  $k < (p-1)$ , взаимно простое с  $(p-1)$ , и вычисляет число  $r = A^k \bmod p$ . Затем из уравнения  $M \equiv (xr + ks) \bmod (p-1)$  определяется  $s \equiv (M - xr)k^{-1} \bmod (p-1)$ . При этом для подписи двух разных сообщений недопустимо использование одного и того же значения  $k$ .

Главным преимуществом схемы электронной подписи Эль-Гамала является возможность вырабатывать электронные подписи для большого числа сообщений с использованием только одного секретного ключа.

Существует большое количество алгоритмов формирования электронной подписи, основанных на схеме Эль-Гамала: DSA, ECDSA, KCDSA, схема Шнорра. Также данная схема лежала в основе российского стандарта электронной подписи ГОСТ Р 34.10-1994, но в последующих за ним ГОСТ Р 34.10-2001, утвержденном взамен его ГОСТ Р 34.10-2012 и

ныне действующем стандарте ГОСТ 34.10-2018 используется арифметика эллиптических кривых, обеспечивающая существенно более высокую криптостойкость.

**Алгоритмы на базе эллиптических кривых.** Использование алгебраических свойств эллиптических кривых применительно к асимметричным криптографическим системам было предложено американскими учеными Нилом Коблицем и Виктором Миллером в 1985 году, что привело к развитию *эллиптической криптографии* (elliptic-curve cryptography (ECC)). Дальнейшие исследования в этой области подтвердили наличие подходящих свойств у данного математического аппарата, и привели к созданию реальных криптосистем на его основе. С 1998 года использование эллиптических кривых для решения криптографических задач, таких, как электронная подпись, было закреплено в стандартах США ANSI X9.62 и FIPS 186-1, а в 2001 году аналогичный стандарт (ГОСТ Р34.10-2001) был принят и в России. К наиболее известным алгоритмам, основанным на эллиптических кривых, в настоящее время относятся ECDSA, ECDH, ECMQV, ГОСТ 34.10-2018. Большинство криптосистем современной криптографии, основанные на дискретном логарифмировании, естественным образом можно переписать на эллиптические кривые, в результате будут получены те же алгоритмы, но с другими математическими операциями.

Основное достоинство асимметричных криптосистем на эллиптических кривых в сравнении с другими асимметричными криптосистемами состоит в их существенно более высокой криптостойкости при равных затратах на обработку и вычисления [3]. Это объясняется сложностью вычисления обратных функций на эллиптических кривых, значительно превосходящей, например, вычисление дискретных логарифмов (алгоритмы Диффи-Хеллмана и Эль-Гамала) или решение задачи факторизации (алгоритм RSA). В результате уровень стойкости, достижимый, скажем, в RSA при использовании 1024-битовых модулей, в системах на эллиптических кривых реализуется при размере модуля 160 бит, что обеспечивает более простую как программную, так и аппаратную реализацию.

В основе криптографии эллиптических кривых лежит достаточно сложный аппарат высшей алгебры, вследствие чего используемые на практике алгоритмы не будут подробно рассмотрены в рамках данного учебного пособия, а ограничимся лишь основными принципами построения криптосистем на их базе.

В криптографии используются эллиптические кривые на плоскости  $X$ - $Y$ , определяемые уравнениями вида

$$Y^2 = X^3 + aX + b \bmod p,$$

где  $p$  – некоторое большое простое число, а  $a$  и  $b$  – константы.

Принцип использования эллиптических кривых следующий. Для группы абонентов выбирается общая эллиптическая кривая  $E$  и некоторая точка  $G$  на ней. Секретным ключом абонента выступает некоторое целое число  $s$ , а открытым ключом – точка  $D$  на кривой  $E$ , полученная в результате специального преобразования композиции с использованием числа  $s$ . Параметры кривой и список открытых ключей абонентов, как и обычно, передаются всем пользователям сети. Открытые и секретные ключи абонентов используются в зависимости от назначения алгоритма.

Криптографические методы на эллиптических кривых считаются перспективными и, закрепленные в различных стандартах, находят применение в современных системах защиты информации. Особый интерес к криптографии эллиптических кривых обусловлен теми преимуществами, которые дает её применение в беспроводных коммуникациях – высокое быстродействие и небольшая длина ключа.

### **3.3.3 Особенности практического применения асимметричных криптографических систем**

Основным достоинством асимметричных криптографических систем как самостоятельных средств защиты передаваемой и хранимой информации является их потенциально высокая безопасность, возможность решения задач распределения ключей по незащищенному каналу связи, аутентификации сообщений и отправителя и т.д. При этом в больших сетях, в сравнении с симметричными криптосистемами, значительно сокращается число ключей.

Вместе с тем, лежащая в их основе необходимость генерации новых больших чисел, проверка их простоты и последующее возведение в степень многозначного числа приводит к значительному снижению быстродействия шифрования и расшифровывания информации. Криптостойкость же асимметричных криптосистем напрямую зависит от длины применяемого ключа. Примерное соответствие [20] для ключей алгоритма симметричного шифрования и алгоритма RSA при атаке полного перебора ключевого множества приводится в таблице 3.1.

Таблица 3.1 – Длины ключей для симметричных и асимметричных криптосистем при одинаковой криптостойкости

Длина симметричного ключа, бит	Длина ключа RSA, бит
56	384
64	512
80	768
112	1792
128	2304

Требование больших вычислительных ресурсов для асимметричных криптографических систем приводит к тому, что на практике наиболее рациональным является их применение вместе с симметричными алгоритмами.

Комбинированный (гибридный) подход позволяет сочетать преимущества высокой секретности асимметричных криптосистем с преимуществами высокой скорости работы, присущих симметричным криптосистемам. В этом случае асимметричные методы шифрования применяются для безопасной передачи секретного ключа симметричной криптосистемы (сеансового ключа), применяемого в дальнейшем для шифрования и передачи исходного открытого текста, что на практике иногда называется *схемой электронного цифрового конверта*.

Также комбинированный метод допускает возможность выполнения процедуры аутентификации сообщений и отправителя. В этом случае отправитель на основе функции хэширования и своего секретного ключа с помощью известного алгоритма электронной подписи генерирует свою подпись и записывает её, например, в конце передаваемого сообщения, а получатель, используя тот же алгоритм электронной подписи и результат хэширования принятого сообщения, проверяет его подпись.

### 3.4 Применение криптографических систем защиты информации

Для обеспечения безопасности данных, хранящихся в системе, как правило, используются программно-аппаратные СКЗИ, реализующие классические симметричные алгоритмы шифрования. Это разумно, поскольку такого рода информация не предназначена для передачи по открытым каналам связи, что снимает проблему распространения ключей, и при этом обеспечивает большую скорость при меньшей длине ключа. В этом случае каждый пользователь формирует для себя персональный симметричный ключ и сам несет ответственность за его сохранность.

Возможно несколько вариантов шифрования хранимой информации [11].

Шифрование *«по требованию»*. В этом случае сообщения, документы, базы данных и т.д. редактируются в открытом виде. Готовый документ, каталог или подкаталог зашифровывается, например, чтобы обеспечить его безопасное хранение на жестком диске или носителе. Пользователь может поставить под таким зашифрованным документом свою электронную подпись.

Шифрование *«на лету»*. Здесь информация в открытом виде существует только в оперативной памяти (в идеальном случае, в видеопамяти) компьютера. Сохранение документа происходит автоматически, вызывая программу его шифрования. Такой способ также носит название *«прозрачное шифрование»*, поскольку процессы криптографического преобразования не требуют участия пользователя и протекают скрытно (прозрачно) для него.

Прозрачное шифрование с *организацией виртуального диска*. Удачным решением защиты информации является организация виртуального зашифрованного диска, который создается внутри дискового пространства компьютера и «подключается» только при необходимости работы с конфиденциальными данными. О его существовании и процедуре его подключения не знает никто кроме владельца. Виртуальный диск представляет собой специальным образом организованный файл и располагается в любом из каталогов файловой системы. После «подключения» виртуального диска операционная система может работать с ним как с любым другим логическим диском. Вся информация, размещаемая на виртуальном диске, зашифровывается автоматически. Средства защиты информации, работающие с виртуальными дисками называются *менеджерами секретных файлов*. Примерами менеджеров секретных файлов являются: Secret Disk, StrongDisk, Rohos Disk Encryption, VeraCrypt, BestCrypt, CipherShed и пр.

Рассмотрим стандартный механизм такого шифрования данных. Структура файла-образа виртуального диска содержит заголовок, непосредственно сами данные и ключ шифрования, который в свою очередь хранится в зашифрованном виде (рис. 3.4).

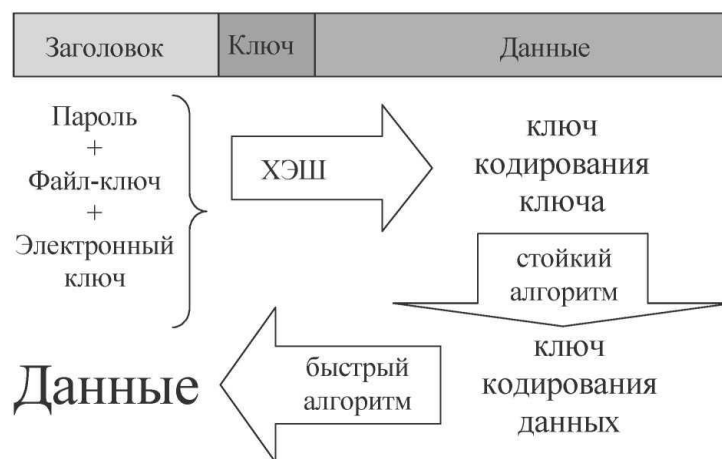


Рис. 3.4 – Структура файла-образа виртуального шифрованного диска.

При подключении диска пользователем вводится «ключевая информация» в виде простого пароля и кодовых последовательностей, разделяющихся в специальном файл-ключе и/или во внешней памяти, которая суммируется по схеме «И». Совокупная ключевая последовательность (комплексный пароль) подвергается операции хэширования, в результате которой формируется «ключ кодирования ключа». С помощью него и стойкого медленного алгоритма шифрования вычисляется «ключ кодирования данных». Данные шифруются на основе быстрого симметричного алгоритма и ключа, который не хранится в открытом виде, а формируется каждый раз при подключении логического диска.

Для хранения стойкого ключа СЗИ программно и/или аппаратно поддерживают большое количество различных внешних носителей ключевой информации, среди которых контактные и бесконтактные смарт-карты, iButton, USB-ключи.

Кроме шифрования непосредственной информации средствами защиты возможно шифрование и таблицы расположения данных. Конечно, существуют специальные программы, которые восстанавливают файловую систему на основании анализа дискового пространства, однако такие процессы потребуют определенных временных затрат и, как правило, оставляют следы в атакуемой системе.

Для обеспечения безопасности данных, передаваемых по сети, используются канальное и сквозное (оконечное) шифрование информации [12].

При *канальном шифровании* каждый канал передачи данных оборудуется на обоих концах устройствами шифрования и в этом случае весь поток передаваемых данных оказывается защищенным. Одним из недостатков такого шифрования является необходимость каждый раз расшифровывать сообщение, когда оно проходит через сетевой коммутатор с целью прочитать адрес (номер виртуального канала) в заголовке пакета для

последующей его передачи по нужному адресу. В этом случае сообщение оказывается уязвимым в каждом коммутаторе, а при использовании общедоступных сетей с коммуникацией пакетов данных оказывается затруднительным контролировать безопасность узлов такой сети.

При реализации канального шифрования каждая пара узлов, находящаяся на концах одного канала, должна применять свой уникальный ключ, и различные для разных каналов ключи. Таким образом, потребуется множество ключей, но каждый из этих ключей должен быть предоставлен только одной соответствующей паре узлов.

При *сквозном шифровании* процесс шифрования исходных данных выполняется только в двух конечных системах – в ведущем узле или терминале источника. Сквозное шифрование реализуется с помощью протокола прикладного уровня или уровня представления модели OSI. В этом случае защищается только содержание передаваемых сообщений, а служебная информация (заголовок пакета) остается открытой. Данные при этом оказываются защищенными от воздействий в канале связи или сетевого коммутатора пакетов, чего нельзя сказать о самом потоке данных, поскольку заголовки пакетов передаются в открытом виде.

Для достижения наилучшей защиты на практике по возможности рекомендуется применение как канального, так и сквозного шифрования по схеме: ведущий узел шифрует порцию пакета данных пользователя, используя ключ сквозного шифрования, после чего весь пакет шифруется с помощью ключа канального шифрования. При передаче пакета по сети каждый коммутатор расшифровывает пакет с применением ключа шифрования соответствующего канала, чтобы прочесть заголовок, после чего снова шифрует весь пакет для его передачи по следующему каналу. Так весь пакет оказывается защищенным в течение всего времени, за исключением, когда находится в памяти коммутатора, где заголовок пакета является открытым.

Важно помнить, что независимо от количества ключей, используемых для шифрования передаваемых по сети данных, существует некий долговременный ключ, на котором построена вся защита. В случае его компрометации защищенный объект оказывается уязвим независимо от количества других используемых при шифровании ключей.

### **3.5 Требования к средствам криптографической защиты информации**

Согласно рекомендациям по стандартизации Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации

шифровальных (криптографических) средств защиты информации» [17] все СКЗИ подразделяются на 5 классов, упорядоченных по старшинству: КС1 (самый младший), КС2, КС3, КВ, КА (самый старший).

К основным особенностям СКЗИ класса КС1 относится их возможность противостоять атакам, проводимым из-за пределов контролируемой зоны. При этом подразумевается, что создание способов атак, их подготовка и проведение осуществляется без участия специалистов в области разработки и анализа СКЗИ. Предполагается, что информация о системе, в которой применяются указанные СЗИ, может быть получена из открытых источников [5].

Если СКЗИ может противостоять атакам, блокируемым средствами класса КС1, а также проводимым в пределах контролируемой зоны, то оно соответствует классу КС2. При этом допускается, например, что при подготовке атаки могла стать доступной информация о физических мерах защиты информационных систем, обеспечении контролируемой зоны и пр.

В случае возможности противостоять атакам при наличии физического доступа к средствам вычислительной техники с установленными СКЗИ говорят о соответствии таких средств классу КС3.

Если СКЗИ противостоит атакам, при создании которых участвовали специалисты в области разработки и анализа указанных средств, в том числе научно-исследовательские центры, была возможность проведения лабораторных исследований средств защиты, то речь идет о соответствии классу КВ.

Если к разработке способов атак привлекались специалисты в области использования НДВ системного программного обеспечения, была доступна соответствующая конструкторская документация и был доступ к любым аппаратным компонентам криптографических СЗИ, то защиту от таких атак могут обеспечивать средства класса КА.

Класс разрабатываемого (модернизируемого) СКЗИ определяется заказчиком СКЗИ путем формирования перечня подлежащих защите объектов информационной системы и совокупности возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак на указанные объекты, с учетом применяемых в системе информационных технологий, среды функционирования и аппаратных средств.

Более подробно с составом и содержанием организационных и технических мер по обеспечению безопасности с использованием СКЗИ можно ознакомиться в Приказе ФСБ России от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

### **3.6 Программно-аппаратные средства криптографической защиты информации**

Как было сказано в начале данного раздела, к СКЗИ относятся аппаратные, программные и программно-аппаратные средства.

Программные СКЗИ реализуют криптографический алгоритм в виде соответствующей программы, вследствие чего такие СКЗИ легко копируются, просты в использовании и модификации в соответствии с конкретными потребностями. Недостатком таких средств является их подверженность атаке методом «холодной перезагрузки», основанной на том, что данные в оперативной памяти могут сохраняться до нескольких минут после выключения компьютера, что создает уязвимость для ключей шифрования.

Программно-аппаратные СКЗИ в большинстве случаев представляют собой энергонезависимую защищенную память, обеспечивающую защиту от модификации алгоритма и ключ шифрования, с программной реализацией вычислений самого алгоритма.

Аппаратные СКЗИ представляют собой блоки шифрования в каналах связи, самодостаточные шифровальные модули, шифровальные платы расширения для установки в персональные компьютеры. К достоинствам таких СКЗИ относятся аппаратная реализация непосредственно криптоалгоритма, что гарантирует его целостность, генератора случайных чисел, позволяющего генерировать действительно случайные числа при формировании ключей, шифрование и хранение ключей в самой плате устройства, а не в оперативной памяти компьютера, прямая загрузка ключей в шифрующее устройство и пр.

Основное различие аппаратных и программно-аппаратных СКЗИ заключается не только в способе реализации криптографических алгоритмов и степени надёжности защиты данных, но и в стоимости, что зачастую становится определяющим фактором при их выборе. Наиболее доступными СКЗИ являются программные и программно-аппаратные средства, следом за которыми идут аппаратные.

Рассмотрим некоторые популярные СКЗИ и их разновидности, применяемые на практике на момент издания данного учебного пособия.

**Secret Disk**<sup>1</sup> – криптографическое программное средство защиты информации, разработанное компанией ЗАО «Аладдин Р.Д.». Secret Disk является менеджером секретных дисков и предназначено для шифрования «на лету» разделов жесткого диска и создания на дисковом пространстве компьютера защищенных виртуальных дисков с многопользовательским доступом.

В продуктовой линейке Secret Disk представлены три следующих решения:

- система защиты информации на персональном компьютере или ноутбуке с возможностью коллективной работы по сети (Secret Disk 5);
- корпоративная система защиты информации с централизованным управлением (Secret Disk Enterprise);
- комплекс защиты информации на сервере от НСД, копирования, повреждения, кражи или неправомерного изъятия (Secret Disk Server NG).

Secret Disk поддерживает криптоалгоритмы AES, RSA, 3DES, ГОСТ 34.12-2018, ГОСТ 34.10-2018, ГОСТ 34.11-2018, имеет сертификат соответствия ФСТЭК России и может применяться для защиты информации в ИСПДн до 1 уровня защищенности, в ГИС до 1 класса защищенности, а также при создании АС до класса защищенности 1Г.

**StrongDisk**<sup>2</sup> – криптографическое программное средство защиты информации, разработанное российской компанией ООО «Физтех-Софт». Включает в себя программные решения:

- криптографической защиты информации на рабочих станциях, сменных носителях, ноутбуках в корпоративной сети (StrongDisk Pro Standard, StrongDisk Pro Corporate);
- криптографической защиты информации при ее обработке и хранении на сервере, защиты корпоративных баз данных, почтовых и бизнес-приложений (StrongDisk Server, StrongDisk Server Standalone).

В функционал StrongDisk входит: возможность многофакторной аутентификация пользователя, шифрование дисковой информации «на лету», одновременное создание, подключение защищенных дисков, изменение параметров аутентификации и механизмов шифрования на нескольких компьютерах, гарантированное удаление данных. StrongDisk поддерживает криптоалгоритмы AES-128, AES-256, Blowfish-128, Blowfish-448, CAST, 3DES, ГОСТ 34.12-2018, а также внешние криптопровайдеры Microsoft, КриптоПро CSP, Signal-COM CSP и др.

---

<sup>1</sup> [www.aladdin-rd.ru](http://www.aladdin-rd.ru)

<sup>2</sup> [www.strongdisk.ru](http://www.strongdisk.ru)

**PGP**<sup>1</sup> (Pretty Good Privacy) – криптографическое программное средство защиты информации, разработанное Филиппом Циммерманном, позволяющее выполнять операции шифрования и электронной подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, в т.ч. на жёстком диске. PGP представляет собой гибридную криптосистему, имеет множество реализаций, совместимых между собой и рядом других программ благодаря стандарту OpenPGP.

Шифрование PGP осуществляется последовательно хешированием, сжатием данных, шифрованием с симметричным ключом, и, наконец, шифрованием с открытым ключом, причём каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов. Симметричное шифрование производится с использованием одного из блочных алгоритмов (AES-128, CAST-128, 3DES, IDEA и др.) на сеансовом ключе. Сеансовый ключ генерируется с использованием криптографически стойкого генератора псевдослучайных чисел. Сеансовый ключ шифруется открытым ключом получателя с использованием алгоритмов RSA или Эль-Гамала (в зависимости от типа ключа получателя). Каждый открытый ключ соответствует имени пользователя или адресу электронной почты.

**BestCrypt**<sup>2</sup> – криптографическое программное средство защиты информации, разработанное компанией Jetico, включающее в себя: BestCrypt Container Encryption для выборочного шифрования файлов и папок, BestCrypt Volume Encryption для шифрования дисков и разделов, и утилиту гарантированного удаления данных BCWipe. BestCrypt реализует прозрачное шифрование с организацией виртуального диска и поддерживает алгоритмы симметричного блочного шифрования: AES, Blowfish, CAST, ГОСТ 28147-89, Twofish, Camellia.

**VeraCrypt**<sup>3</sup> – криптографическое программное средство защиты информации от компании IDRIX, основанное на базе TrueCrypt, применяемое для шифрования «на лету». Помимо шифрования дисков и разделов, VeraCrypt можно использовать для USB-устройств флеш-памяти, шифруя их полностью, либо создавая отдельный контейнер на носителе. VeraCrypt поддерживает симметричные блочные алгоритмы шифрования AES, Serpent, Twofish, Camellia, «Кузнечик», а также комбинации этих алгоритмов.

---

<sup>1</sup> [www.openpgp.org](http://www.openpgp.org)

<sup>2</sup> [www.jetico.com](http://www.jetico.com)

<sup>3</sup> [www.veracrypt.fr](http://www.veracrypt.fr)

***Rohos Disk Encryption***<sup>1</sup> – криптографическое программное средство защиты информации, представленное компанией SafeJKA SRL (Tesline-Service S.R.L до 2016 года), позволяющее организовывать и скрывать защищенные виртуальные диски с применением алгоритма AES-256 и технологии шифрования «на лету», ограничивать доступ к ним с помощью электронных ключей, создавать защищенные области памяти на флеш-накопителях, применять элементы стеганографии для скрытия передаваемой информации в медиа-контейнерах.

***Gilisoft Encryption Tools***<sup>2</sup> – комплекс программ и утилит от компании GiliSoft, предназначенных для шифрования отдельных файлов и запоминающих устройств (жестких дисков, флеш-накопителей), а также защиты файлов от несанкционированного просмотра и копирования. В Gilisoft Encryption преимущественно используется метод шифрования информации «на лету» с применением алгоритма AES-256. Данное средство позволяет создавать защищенные области памяти на портативных запоминающих устройствах, шифровать записи дисков CD/DVD, а также их виртуальные образы, шифровать разделы жесткого диска, включая системный, и многое другое. В состав Gilisoft Encryption входят программы: USB Encryption, Secure Disc Creator, Full Disk Encryption, CD&DVD Encryption, Any Video Encryptor.

***ПСКЗИ ШИПКА***<sup>3</sup> (персональное средство криптографической защиты информации ШИПКА) – аппаратное средство криптографической защиты информации, разработанное компанией ОКБ САПР, представляющее собой USB-устройство с реализованным на нем набором большинства самых необходимых функций и алгоритмов защиты информации, а также набор драйверов и библиотек для использования криптографических функций в различных прикладных программах.

Название ШИПКА означает «Шифрование-Идентификация-Подпись-Коды-Аутентификации», что соответствует функционалу СКЗИ, который включает в себя:

- шифрование и/или подпись файлов на жестком диске или съемных носителях;
- автоматическое заполнение форм авторизации и хранения в защищенной памяти необходимых для этого данных, в том числе паролей и другой персональной информации пользователя (ключей, сертификатов и пр.);
- аппаратную идентификацию и аутентификацию пользователя на автономных компьютерах (в том числе на ноутбуках) или рабочих станциях в составе одноранговой сети;

---

<sup>1</sup> [www.rohos.ru](http://www.rohos.ru)

<sup>2</sup> [www.gilisoft.com](http://www.gilisoft.com)

<sup>3</sup> [www.okbsapr.ru](http://www.okbsapr.ru)

- защищенное хранение ключей шифрования и подписи;
- аппаратный датчик случайных чисел;
- авторизацию пользователя при входе в домены в типовых решениях Microsoft на базе смарт-карт;
- процедуры идентификации/аутентификации, для шифрования/подписи сообщений и т.п.

В ПСКЗИ ШИПКА реализовано большое количество криптографических алгоритмов, среди которых выделяют алгоритмы:

- шифрования ГОСТ 28147-89, RC2, DES, 3DES;
- хэширования ГОСТ Р 34.11-94, MD5, SHA-1;
- электронной подписи ГОСТ Р 34.10-2001, RSA, DSA.

Отличительной особенностью ШИПКА является именно аппаратная реализация вычислений без привлечения ресурсов компьютера, программно здесь задействованы только транспортные процедуры и процедуры согласования форматов данных, не влияющие на защищенность.

**УКЗД КРИПТОН<sup>1</sup>** (устройство криптографической защиты данных КРИПТОН) – аппаратное средство криптографической защиты информации, разработанное российской компанией ООО Фирма «АНКАД», выполненное в виде плат расширения PCI и PCIe и предназначенное для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну со степенью секретности до «совершенно секретно».

УКЗД КРИПТОН позволяет: шифровать компьютерную информацию, осуществлять электронную подпись, создавать прозрачно шифруемые логические диски, формировать криптографически защищённые виртуальные сети, создавать системы защиты информации от НСД и разграничения доступа к компьютеру.

Особенностью данного СКЗИ является применение алгоритма шифрования ГОСТ 28147-89 и наличие аппаратного датчика случайных чисел.

### **3.7 Средства электронной подписи**

Под *средствами электронной подписи* понимают криптографические средства, используемые для реализации таких функций как создание и проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

---

<sup>1</sup> [www.ancud.ru](http://www.ancud.ru)

Средства электронной подписи позволяют установить факт изменения подписанного электронного документа после момента его подписания, а также обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

**Электронная подпись** (digital signature) – это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

На практике, как и в некоторой литературе, можно также встретить термин «электронная цифровая подпись», принятый в 2002 году в рамках Федерального закона от 10 января 2002 года N 1-ФЗ «Об электронной цифровой подписи». Однако, в связи со вступлением в силу Федерального закона от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи», данный термин был заменен на «электронная подпись». Такая замена является логичной, поскольку определение «электронная» уже подразумевает цифровой формат.

Федеральный закон N 63-ФЗ регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

**Назначение электронной подписи.** Электронная подпись предназначена для идентификации лица, подписавшего электронный документ, является полноценным аналогом собственноручной подписи в случаях, предусмотренных законом, вследствие чего обеспечивает доказательное подтверждение авторства документа. Также она обеспечивает проверку целостности электронных документов, поскольку вычисляется на основании исходного состояния документа и соответствует лишь ему.

В общем случае электронная подпись обеспечивает защиту от следующих видов злоумышленных действий.

*Активный перехват* – злоумышленник (условный абонент С), подключившийся к каналу информационного обмена между участниками сеанса связи (условными абонентами А и В), перехватывает документы (файлы) и изменяет их.

*Маскарад* – злоумышленник отправляет документ одному из участников сеанса связи от имени другого участника сеанса связи. Например, абонент С посылает документ абоненту В от имени абонента А.

*Ренегатство* – отказ одной из сторон сеанса связи от ранее переданного сообщения. Например, абонент *А* заявляет, что не отправлял сообщения абоненту *В*, хотя на самом деле его отправлял.

*Подмена* – одна из сторон сеанса связи сама генерирует документ и выдает его за документ, ранее полученный другого абонента. Например, абонент *В* изменяет или формирует новый документ и заявляет, что получил его от абонента *А*.

*Повтор* – третья сторона повторяет ранее переданный документ между участниками сеанса связи. Например, абонент *С* повторяет ранее переданный документ, который абонент *А* посылал абоненту *В*.

Данные злоумышленные действия могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, частным лицам, применяющим в своей деятельности компьютерные информационные технологии.

**Состав электронной подписи.** Электронная подпись включает в себя три составляющие:

- ключ электронной подписи (секретный ключ) – уникальная последовательность символов, предназначенная для создания электронной подписи;
- ключ проверки электронной подписи (открытый ключ) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;
- сертификат ключа проверки электронной подписи (сертификат электронной подписи) – электронный или бумажный документ, подтверждающий принадлежность ключа проверки электронной подписи владельцу данного сертификата.

Ключ электронной подписи наиболее уязвим и должен храниться в надежном месте, например, на электронных ключах, смарт-картах, защищенных носителях памяти. Ключ проверки электронной подписи находится в открытом доступе, в силу чего при управлении им необходимо обеспечить порядок проверки на принадлежность конкретному владельцу, что осуществляется с помощью сертификатов электронной подписи, которые являются своего рода «электронным паспортом» любого участника информационного обмена.

**Сертификат электронной подписи.** Созданием и выдачей сертификатов электронной подписи занимается *удостоверяющий центр* (центр сертификации) – сторона, чья честность неоспорима, а открытый ключ широко известен. Технически такой центр реализуется как компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Удостоверяющий центр вправе выдавать

сертификаты как в форме электронных документов, так и в форме документов на бумажном носителе.

Перечень обязательных и необязательных полей, которые могут присутствовать в сертификате, определяется данным стандартом, а также законодательством. В общем случае сертификат электронной подписи содержит следующую информацию:

- уникальный номер сертификата, даты начала и окончания его срока действия;
- идентификационные данные владельца сертификата – фамилию, имя, отчество (для физических лиц), наименование и место нахождения (для юридических лиц);
- уникальный ключ проверки электронной подписи (открытый ключ);
- наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;
- наименование удостоверяющего центра, выдавшего данный сертификат;
- иную информацию, предусмотренную Федеральным законом N 63-ФЗ.

Возможны несколько способов получения сертификатов, зависящих от целей их дальнейшего использования.

Если сертификат используется для внутреннего, априори безопасного, информационного обмена между несколькими знакомыми между собой людьми (например, сотрудниками небольшой компании), то допускается возможность применения так называемых *самоподписанных сертификатов* – сертификатов, изданных самими пользователями без обращения к удостоверяющему центру. Обменявшись такими сертификатами между собой, они могут пересылать друг другу подписанные и зашифрованные электронные данные, не беспокоясь о перехвате или искажении информации. Сгенерировать такой сертификат возможно с помощью различных утилит или приложений, например, путем применения универсального программного средства, предназначенного для шифрования и электронной подписи файлов ***КрунтоАРМ***<sup>1</sup> (ООО «Цифровые технологии»). Однако здесь важно помнить, что такие сертификаты не являются квалифицированными и их использование не позволяет решать конфликтные ситуации, возникающие при обмене конфиденциальными данными, с помощью суда.

Если сертификат необходим для информационного обмена с незнакомыми людьми в глобальной сети, следует использовать только *квалифицированный сертификат*, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной

---

<sup>1</sup> [www.cryptoar.ru](http://www.cryptoar.ru)

власти, уполномоченным в сфере использования электронной подписи.

Общий механизм функционирования сертификатов заключается в следующем. Пусть имеются две стороны информационного обмена  $A$  и  $B$ , и третья сторона  $Z$  (удостоверяющий центр), которой доверяют  $A$  и  $B$ . Стороне  $A$  принадлежит пара  $\{K_{RA}, K_{UA}\}$ , где  $K_{RA}$  – открытый ключ  $A$ ,  $K_{UA}$  — секретный ключ  $A$ . Аналогично, стороне  $B$  принадлежит пара  $\{K_{RB}, K_{UB}\}$ , а стороне  $Z$  – пара ключей  $\{K_{RZ}, K_{UZ}\}$ .

1. Абонент  $A$  посылает запрос на подпись стороне  $Z$ , указывая данные о себе и свой открытый ключ  $K_{RA}$ .

2. Сторона  $Z$  выдает абоненту  $A$  сертификат  $S$ , устанавливающий соответствие между  $A$  и  $K_{RA}$ . Данный сертификат содержит:

- открытый ключ  $K_{RA}$ ;
- идентификационные данные абонента  $A$ ;
- идентификационные данные удостоверяющей стороны  $Z$  и её электронную подпись  $\text{sign}(S, K_{UZ})$ , представляющую собой результат применения хэш-функции к данным сертификата  $S$ , зашифрованный с использованием своего секретного ключа  $K_{UZ}$ ;

- иную информацию.

3. Абонент  $A$  отправляет абоненту  $B$  свой сертификат  $S$ .

4. Абонент  $B$  проверяет электронную подпись удостоверяющей стороны  $Z$  для чего:

- самостоятельно вычисляет хэш-функцию от данных сертификата  $S$ ;
- расшифровывает электронную подпись  $\text{sign}(S, K_{UZ})$  с помощью всем известного открытого ключа  $K_{RZ}$ , получив тем самым другую хэш-функцию;
- проверяет равенство вычисленной и расшифрованной хэш-функций.

Если полученные хэш-функции равны, значит, подпись удостоверяющего центра  $Z$  достоверна, и что открытый ключ  $K_{RA}$ , содержащийся в сертификате  $S$ , действительно принадлежит абоненту  $A$ .

5. Аналогичным образом абонент  $B$  получает свой сертификат у стороны  $Z$ , после чего отправляет его абоненту  $A$ , где, после проверки его подлинности, возможно последующее информационное взаимодействие между абонентами  $A$  и  $B$ .

Рассмотрим данные процессы более подробно.

**Механизм электронной подписи.** В основе механизма электронной подписи лежат методы асимметричной криптографии, реализующие два основных процессов:

1) формирование электронной подписи;

2) проверка электронной подписи.

В процедуре формирования электронной подписи в качестве исходных данных используется сообщение  $M$ , ключ электронной подписи  $K_U$  и параметры схемы электронной подписи, общие для всех субъектов информационного обмена. Физически электронная подпись представляет собой строку битов, структура которой зависит от конкретного механизма формирования подписи.

Схематическое представление подписанного сообщения представлено на рис. 3.5. Здесь дополняющее поле «Текст» может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.



Рис. 3.5 – Схема подписанного сообщения.

Поскольку подписываемые документы, как правило, переменного и достаточно большого объема, в схемах электронной подписи подпись ставится не на сам документ, а на значение его хэш-функции.

Хэш-функция  $H$  является односторонней функцией, предназначенной для получения дайджеста  $h$  (message digest) исходного подписываемого сообщения  $M$  – относительно короткого числа, состоящего из фиксированного небольшого количества битов. Дайджест  $h = H(M)$  является своего рода «отпечатком пальцев» всего документа и представляет собой сжатое представление документа, сложным образом зависящее от него и не позволяющее восстановить сам исходный документ.

Хэш-функция чувствительна к всевозможным изменениям в тексте сообщения  $M$ , обладает свойством необратимости, вычислительной неразрешимости, а также сопротивляемостью коллизиям (коллизией называют совпадение дайджестов для различных данных). Все эти свойства обеспечивают целостность подписываемого документа.

Хэш-функция не является частью алгоритма электронной подписи, поэтому в схеме может электронной подписи может быть использована любая надежная хэш-функция.

Среди зарубежных алгоритмов хэширования наиболее известными являются MD5 и SHA-1, а также пришедший им на смену SHA-2. В виду алгоритмической схожести SHA-2 с SHA-1 и наличия у последнего потенциальных уязвимостей, в 2012 году был проведен

конкурс Национального института стандартов и технологий (NIST) на новую криптографическую хеш-функцию «SHA-3», где в качестве SHA-3 был утвержден алгоритм хеширования переменной разрядности Кессак (размер хэша может составлять 224, 256, 384, 512 бит). На ряду с ним также известны финалисты данного конкурса, алгоритмы: BLAKE, Grøstl, JH, Skein.

Среди отечественных алгоритмов хеширования широко известен стандарт вычисления хеш-функции ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования», замененный с 1 января 2013 года на ГОСТ Р 34.11-2012, а с 1 июня 2019 года на ГОСТ 34.11-2018. Данный алгоритм также носит название «Стрибог» (Streebog), хотя в тексте стандарта явно это не упоминается, и имеет размер хэша 256 и 512 бит.

Существует большое количество алгоритмов электронной подписи, основанных на асимметричных криптосистемах, о некоторых из которых сообщалось в разделе 3.3. Одни из них опираются на сложность разложения больших чисел на простые множители, другие – на сложность дискретного логарифмирования в одной из конечных групп.

Рассмотрим общий случай схемы формирования и проверки электронной подписи более подробно.

Пусть имеется некоторый отправитель  $A$  сообщения  $M$ . Стороне  $A$  принадлежит пара ключей  $\{K_{RA}, K_{UA}\}$ , где  $K_{RA}$  – открытый ключ  $A$ ,  $K_{UA}$  — секретный ключ  $A$ . Открытый ключ  $K_{RA}$  (в составе сертификата) рассылается остальным участникам информационного обмена или делается доступным, например, на разделяемом ресурсе. Для формирования электронной подписи отправитель  $A$  с помощью хеш-функции вычисляет дайджест  $h = H(M)$  подписываемого сообщения  $M$ , после чего шифрует его своим секретным ключом  $K_{UA}$ . Полученное при этом число  $E_{K_{UA}}(h)$  представляет собой электронную подпись данного сообщения, которая присоединяется к нему и отправляется на адрес получателя (рис. 3.6). Для упрощения описываемой процедуры в данном случае мы опускаем следующий за подписанием процесс шифрования передаваемого сообщения.

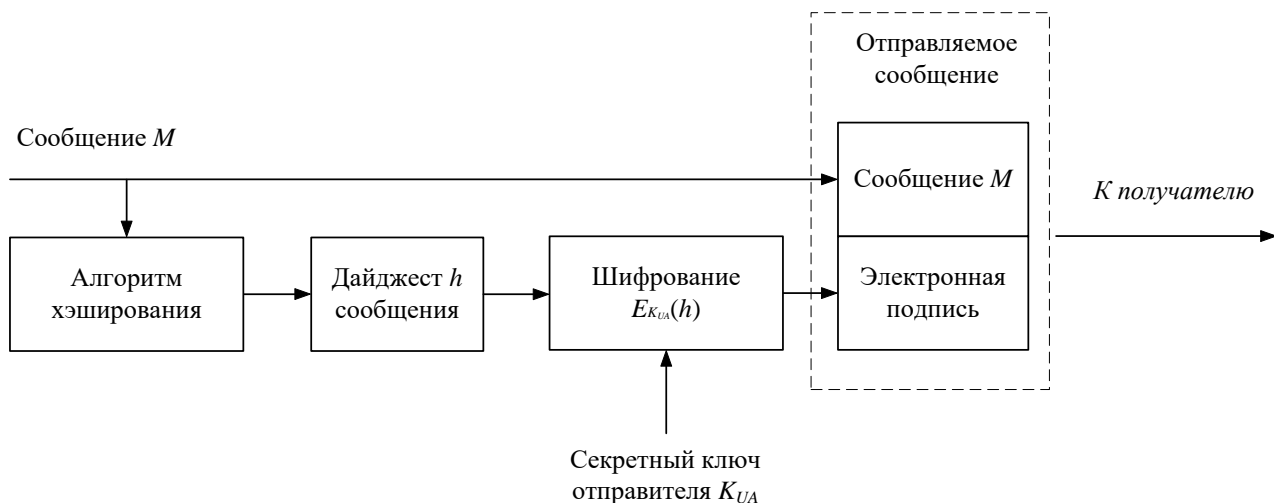


Рис. 3.6 – Схема формирования электронной подписи.

При проверке электронной подписи получатель сообщения расшифровывает принятый дайджест посредством открытого ключа  $K_{RA}$  отправителя в результате чего получается дайджест  $h = D_{K_{RA}}(E_{K_{UA}}(h))$ . Кроме того, получатель сам вычисляет с помощью хэш-функции отправителя дайджест  $h' = H(M)$  принятого сообщения и сравнивает его с расшифрованным дайджестом  $h$  (рис. 3.7). Если эти два дайджеста совпадают, то электронная подпись является подлинной. В противном случае либо подпись подделана, либо нарушена целостность переданного сообщения.

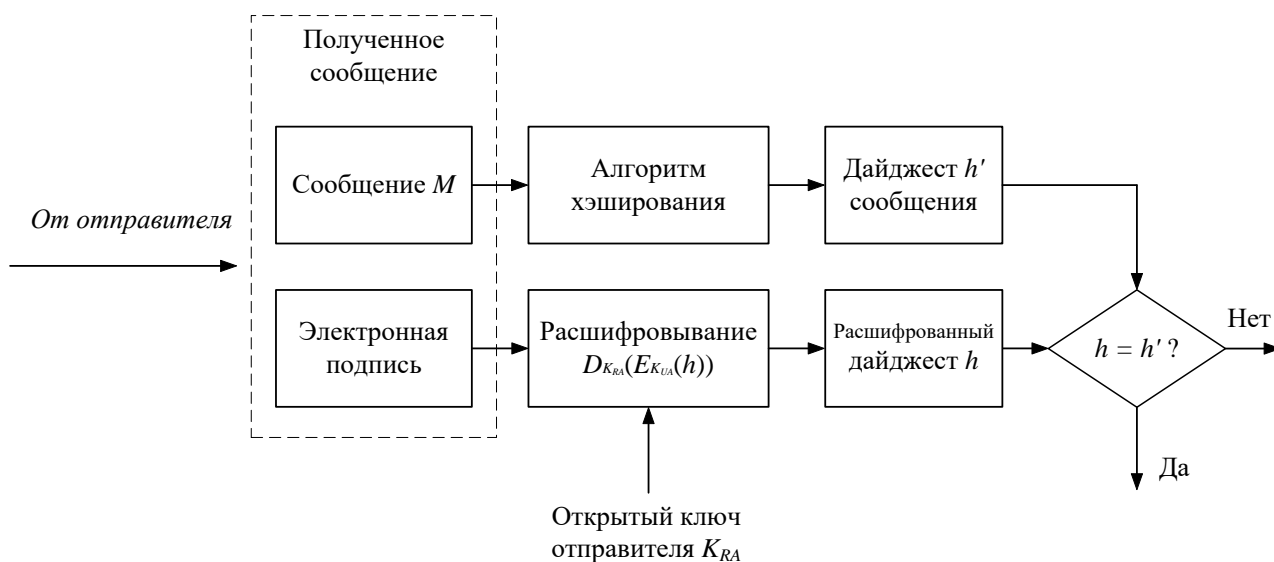


Рис. 3.7 – Схема проверки электронной подписи.

Помещаемая в подписываемый файл (или в отдельный файл электронной подписи) структура электронной подписи обычно содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация добавляется к документу до вычисления электронной подписи, что обеспечивает её целостность. Каждая подпись содержит следующую информацию:

- дату подписи;
- срок окончания действия ключа данной подписи;
- информацию о лице, подписавшем документ;
- имя открытого ключа;
- собственно подпись.

Проверить сформированную подпись может любое лицо, поскольку ключ проверки подписи является открытым. При этом если получателя интересует, не является ли полученное сообщение повторением отправленного или не было ли оно задержано на пути следования, то он должен проверить дату и время его отправки, а при наличии – порядковый номер.

**Виды электронной подписи.** Федеральный закон N 63-ФЗ определяет два вида электронных подписей – простая и усиленная электронная подпись. Усиленная электронная подпись в свою очередь различается как неквалифицированная и квалифицированная.

*Простая электронная подпись* – это электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. Применение такой подписи для подписания документов, содержащих сведения, составляющие государственную тайну, не допускается.

*Неквалифицированная электронная подпись* – это электронная подпись, полученная в результате криптографического преобразования информации с использованием ключа электронной подписи, и позволяющая идентифицировать лицо, подписавшее документ, а также обнаружить факт внесения изменений в документ после момента его подписания.

*Квалифицированная электронная подпись* соответствует всем признакам неквалифицированной подписи с тем отличием, что ключ проверки электронной подписи указывается в квалифицированном сертификате, а для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом.

### 3.8 Криптопровайдеры

*Криптопровайдер* (Cryptography Service Provider, CSP) – это программный или программно-аппаратный комплекс, позволяющий осуществлять криптографические операции (шифрование, электронная подпись и пр.) в операционной системе. Иными словами, это посредник между операционной системой и программным или аппаратным комплексом, взаимодействующим с пользователем. В операционных системах Microsoft управление комплексом происходит с помощью интерфейса CryptoAPI, содержащего набор функций, реализующих базовые криптографические преобразования, работу с сертификатами X.509, криптографическими сообщениями и поддерживающих инфраструктуру открытых ключей (Public Key Infrastructure, PKI).

Все версии операционной системы Windows, начиная с Windows 2000, имеют встроенный криптопровайдер *Microsoft Base Cryptographic Provider*, однако используемые им алгоритмы не сертифицированы и на практике для обеспечения защищенного документооборота в ряде случаев требуется применения специализированных внешних криптопровайдеров.

Приведем краткий перечень некоторых популярных российских криптопровайдеров, применяемые на практике на момент издания данного учебного пособия. С более подробной и актуальной информацией по ним можно ознакомиться на веб-ресурсах разработчиков.

**КриптоПро CSP<sup>1</sup>** – криптопровайдер от одноименной компании ООО «КРИПТО-ПРО», обеспечивающий весь набор криптографических преобразований и поддерживающий, наряду с российскими, также зарубежные криптографические алгоритмы (RSA, ECDSA). В продуктовой линейке «КриптоПро», помимо поддержки классических токенов и других пассивных хранилищ секретных ключей (КриптоПро CSP) также реализована возможность использования ключей, хранящихся на облачном сервисе, через интерфейс CryptoAPI (КриптоПро DSS) и поддержки носителей с неизвлекаемыми ключами (КриптоПро ФКН CSP/Путокен CSP).

**Верба-OW<sup>2</sup>** – криптопровайдер, разработанный ЗАО «Московское отделение Пензенского научно-исследовательского электротехнического института» (МО ПНИЭИ), включающий динамические библиотеки, предназначенные для встраивания в прикладное программное обеспечение, с возможностью шифрования файлов и областей оперативной памяти, формирования и проверки электронной подписи в соответствии с российскими стандартами.

---

<sup>1</sup> [www.cryptopro.ru](http://www.cryptopro.ru)

<sup>2</sup> [www.security.ru](http://www.security.ru)

**ViPNet CSP<sup>1</sup>** – криптопровайдер, разработанный ОАО «ИнфоТеКС» и сертифицированный ФСБ России, обеспечивающий вызов криптографических функций из различных приложений Microsoft и другого программного обеспечения, использующего интерфейс CryptoAPI 2.0. Поддерживает все российские криптографические стандарты, а также работу с электронными ключами на различных внешних устройствах.

**Signal-COM CSP<sup>2</sup>** – криптопровайдер от компании «Сигнал-КОМ», обеспечивающий доступ к различным криптографическим алгоритмам из пользовательских приложений через стандартный криптографический интерфейс CryptoAPI 2.0. Осуществляет поддержку международных стандартов и рекомендаций в области защиты информации (X.509, PKIX, PKCS, CMS), а также всех российских криптографических алгоритмов, обеспечивает поддержку различных типов ключевых носителей и криптографических токенов.

**LISSI-CSP<sup>3</sup>** – криптопровайдер от компании ООО «ЛИССИ-Софт», являющийся надстройкой над СКЗИ «ЛИРССЛ-CSP» и позволяющий использовать российские криптографические алгоритмы в операционных системах Microsoft через стандартные интерфейсы (CryptoAPI, CAPICOM, MSXML, SSPI, Certificate Enrollment Control). Поддерживаемые практически все типы ключевых носителей, включая токены с аппаратной реализацией российской криптографии.

---

<sup>1</sup> [www.infotecs.ru](http://www.infotecs.ru)

<sup>2</sup> [www.signal-com.ru](http://www.signal-com.ru)

<sup>3</sup> [www.soft.lissi.ru](http://www.soft.lissi.ru)

## 4 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА СЕТЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Автоматизированные информационные системы большинства коммерческих и государственных организаций могут быть связаны между собой сетевыми соединениями в пределах одной организации, между различными организациями, между организацией и неограниченным кругом лиц. При этом если локальная сеть организации или персональный компьютер пользователя имеют выход в сеть Интернет, то количество угроз безопасности увеличивается в десятки раз по сравнению с изолированной сетью или компьютером. К перечню наиболее типичных сетевых угроз относятся: сетевые вирусы, попытки внешнего проникновения в систему (используя подобранный или перехваченный пароль, уязвимости программного обеспечения и пр.), перехват и подмена данных, передаваемых в сеть или получаемых из сети. Среди существующих средств и методов сетевой защиты информации выделяют межсетевые экраны, виртуальные частные сети и системы обнаружения вторжений. Их сочетание, обеспечивающее комплексную защиту от сетевых угроз, объединяют в рамках понятия «шлюз безопасности» (security gateway) – точки соединения между сетями, между сегментами сетей или между программными приложениями в различных доменах безопасности, предназначенной для защиты сети в соответствии с существующей политикой безопасности [6].

### 4.1 Технологии межсетевых экранов

#### 4.1.1 Понятие межсетевого экрана

**Межсетевой экран** (firewall) – это специализированный комплекс межсетевой защиты, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. Под *фильтрацией* понимается процесс приема или отклонения потоков данных в сети в соответствии с определенными критериями.

Приведем также определение согласно ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции»:

*Межсетевой экран* – это вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности

нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности.

В общем случае межсетевой экран позволяет разделить общую сеть на две или более частей и реализовать условия прохождения пакетов с данными из одной части общей сети в другую.

Наряду с термином «межсетевой экран» на практике также широко применяются термины, заимствованные из немецкого и английского языков – «брандмауэр» (brandmauer) и «файервол» (firewall), соответственно.

Межсетевые экраны используются в качестве первой линии защиты сетей и размещаются между защищаемой внутренней сетью (например, корпоративной (локальной) сетью предприятия), называемой также интранет (intranet), и потенциально опасной внешней (глобальной) сетью Интернет (рис. 4.1).

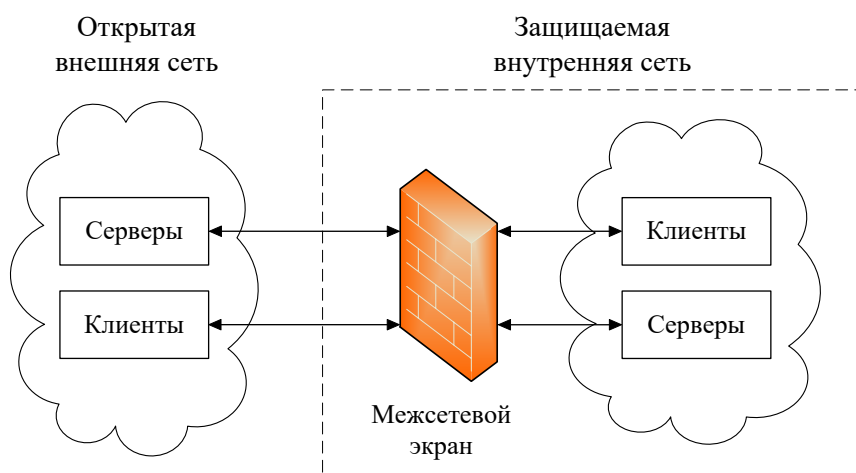


Рис. 4.1 – Схема подключения межсетевого экрана.

К основным задачам межсетевого экрана относятся:

1) ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, злоумышленники, а также сотрудники самой организации, пытающиеся получить доступ к серверам баз данных, защищаемых межсетевым экраном;

2) разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требующимся для выполнения служебных обязанностей.

Организационно межсетевой экран входит в состав защищаемой сети и все взаимодействия между сетями должны осуществляться только через него. При этом по схеме подключения межсетевых экранов выделяют:

- схему единой защиты сети;
- схему с защищаемым закрытым и незащищаемым открытым сегментами сети;
- схему с отдельной защитой закрытого и открытого сегментов сети.

#### 4.1.2 Классификация межсетевых экранов

Единой и общепризнанной классификации межсетевых экранов до сих пор не существует, поэтому возможны различные схемы их классификации, отличающихся типом критерия [32].

*По способу реализации* различают: программные и программно-аппаратные межсетевые экраны.

*По охвату контролируемых потоков данных* выделяют:

- традиционный межсетевой экран (программный или программно-аппаратный), устанавливаемый на шлюзе (сервере передающем трафик между сетями) и контролирующий входящие и исходящие потоки данных между подключенными сетями;
- персональный межсетевой экран (как правило, программный), устанавливаемый на отдельной рабочей станции и предназначенный для защиты от НСД только её.
- распределенный межсетевой экран, представляющий собой централизованно управляемую совокупность сетевых мини-экранов, защищающих отдельные компьютеры сети.

*По используемой технологии* выделяют межсетевые экраны:

- контроля состояния протокола (stateful inspection);
- на основе модулей посредников (proxy).

*По функционированию на уровнях модели OSI* различают:

- пакетный фильтр (экранирующий маршрутизатор);
- межсетевой экран сеансового уровня (экранирующий транспорт);
- межсетевой экран прикладного уровня (экранирующий шлюз);
- межсетевой экран экспертного уровня.

Также к классу межсетевых экранов иногда причисляют *управляемые коммутаторы*, поскольку они осуществляют фильтрацию трафика между сетями или узлами сети. Однако они функционируют на канальном уровне и разделяют трафик в рамках только внутренней сети, вследствие чего не могут быть использованы для обработки трафика из внешних сетей.

Тем не менее, данное решение может быть довольно рентабельно при реализации политики безопасности в рамках корпоративной сети.

#### 4.1.3 Структура и функции межсетевого экрана

Фильтрация потоков данных состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований. Данный процесс осуществляется на основе набора предварительно загруженных в межсетевой экран правил, соответствующих принятой политике безопасности. В связи с этим межсетевой экран удобно представлять как последовательность фильтров, обрабатывающих информационный поток (рис. 4.2).

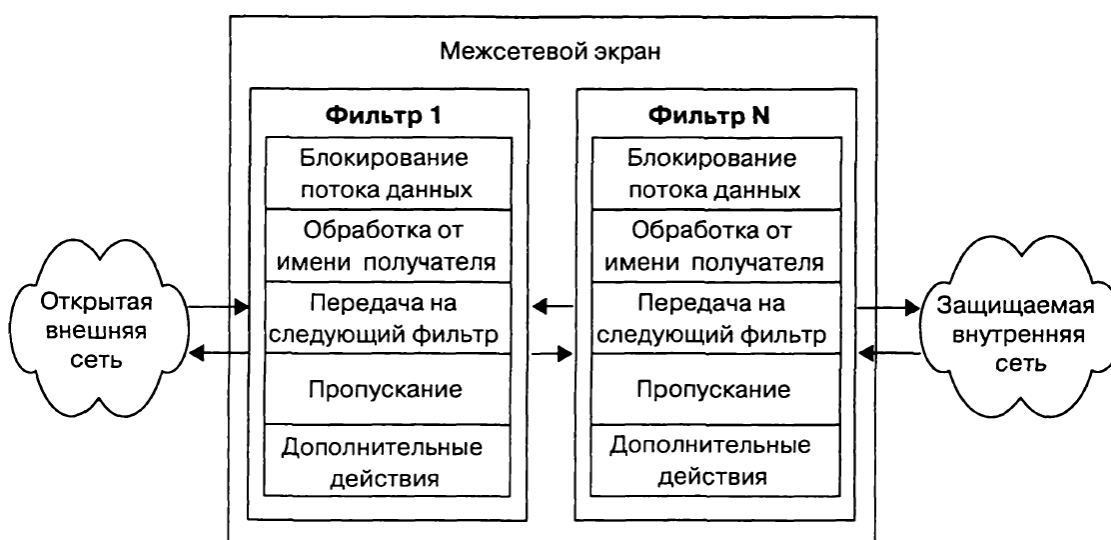


Рис. 4.2 – Структура межсетевого экрана.

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения анализа информации по заданным в интерпретируемых правилах меритериям (например, по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена) и принятие на основе интерпретируемых правил одного решений. К принимаемым решениям относятся:

- блокировка потока данных (не пропустить данные);
- обработка данных от имени получателя и возврат результата отправителю;
- передача данных на следующий фильтр для продолжения анализа;
- пропуск данных, игнорируя следующие фильтры.

Используемые критерии анализа информационного потока зависят от уровней модели OSI, на которых осуществляется фильтрация. В их качестве критериев могут использоваться:

- служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
- непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
- внешние характеристики потока информации (например, временные и/или частотные характеристики, объем данных и т.д.).

Также правила фильтрации могут задавать дополнительные действия, которые относятся к функциям посредничества, например, преобразование данных, регистрация событий и др.

Функции посредничества межсетевой экран реализует с помощью специальных программ, называемых экранирующими агентами или программами-посредниками. Данные программы запрещают непосредственную передачу сообщений между внешней и внутренней сетями. При передаче информации через межсетевой экран первоначально устанавливается логическое соединение с программой-посредником, проверяющей допустимость запрошенного межсетевого взаимодействия, и при его разрешении установлении отдельного соединения с требуемым компьютером. Далее информационный обмен между компьютерами внутренней и внешней сетей осуществляется через программного посредника, выполняющего различные защитные функции. Межсетевой экран с посредниками позволяет также организовывать защитные виртуальные сети VPN.

Помимо функций фильтрации трафика и посредничества современные межсетевые экраны позволяют реализовывать ряд других важных функций обеспечения защиты периметра внутренней сети:

- идентификацию и аутентификацию пользователей;
- трансляцию сетевых адресов;
- регистрацию событий.

*Идентификация и аутентификация пользователей* осуществляются при предъявлении обычного идентификатора (имени) и пароля. При этом для предотвращения НСД путем перехвата сетевых пакетов пароль следует передавать через общедоступные коммуникации только в зашифрованном виде. Более надежным методом аутентификации является использование одноразовых паролей или цифровых сертификатов, выдаваемых доверенными органами, например центром распределения ключей. Большинство программ-посредников разрабатывается таким образом, чтобы пользователь аутентифицировался

только в начале сеанса работы с межсетевым экраном. После этого от него не требуется дополнительная аутентификация в течение времени, определяемого администратором.

*Трансляция внутренних сетевых адресов* применяется для скрытия адресов рабочих станций, а также топологии всей сети. Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю для чего выполняется автоматическое преобразование IP-адресов компьютеров-отправителей в один IP-адрес межсетевого экрана (рис. 4.3).

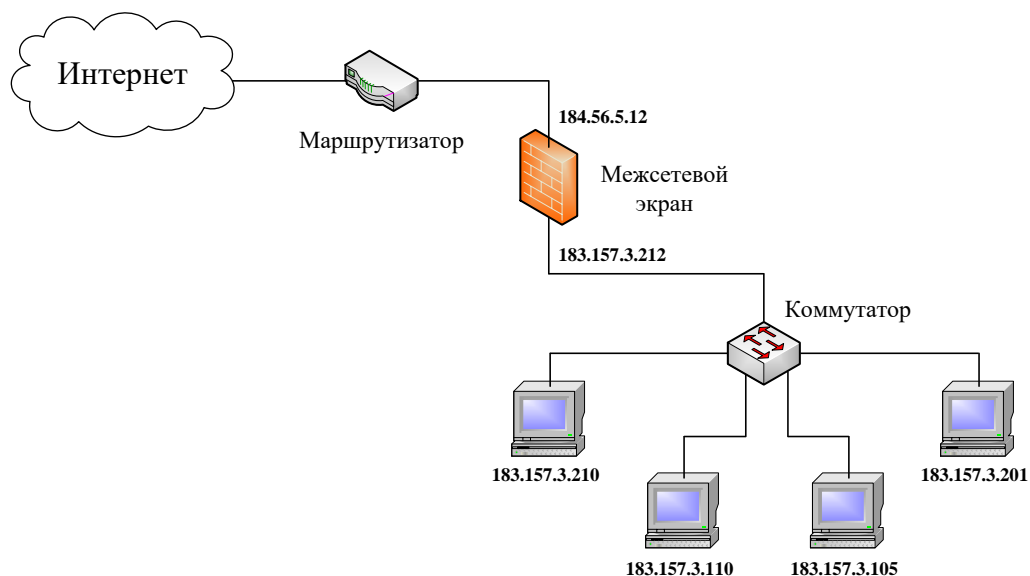


Рис. 4.3 – Трансляция сетевых адресов.

Трансляция внутренних сетевых адресов может осуществлять динамически или статически. В первом случае адрес выделяется узлу в момент обращения к межсетевому экрану, а после завершения соединения адрес освобождается и может быть использован любым другим узлом корпоративной сети. Во втором случае адрес узла всегда привязывается к одному адресу межсетевого экрана, из которого передаются все исходящие пакеты. В результате все исходящие из внутренней сети пакеты оказываются отправленными межсетевым экраном, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью.

Кроме повышения безопасности трансляция адресов также позволяет иметь внутри сети собственную систему адресации и разрешает проблему расширения адресного пространства внутренней сети.

*Регистрация событий* позволяет выполнять аудит безопасности для последующего анализа инцидентов безопасности или сбора доказательств для предоставления их в

судебные инстанции, либо внутреннего расследования. Журнал событий содержит сведения о пропуске или блокировании сетевых пакетов, об ошибках и предупреждениях, изменениях правил разграничения доступа администратором, других событиях, возникающих при работе компонентов межсетевого экрана. При корректно настроенной системе фиксации сигналов о подозрительных событиях межсетевой экран может дать детальную информацию попытках атаки или зондирования сети.

#### **4.1.4 Особенности функционирования межсетевых экранов на различных уровнях модели OSI**

Возможности межсетевых экранов зависят от уровня эталонной модели OSI, на которой они функционируют. Напомним, что модель OSI (Open Systems Interconnection) включает семь уровней сетевой архитектуры: физический, канальный, сетевой, транспортный, сеансовый, уровень представления и прикладной уровень. Для того, чтобы обеспечить фильтрацию трафика, межсетевой экран должен работать как минимум на третьем уровне модели OSI, т.е. сетевом. Чем выше уровень OSI, на которой он построен, тем выше обеспечиваемый им уровень безопасности.

Используемые в сетях протоколы (TCP/IP, SPX/IPX) не полностью соответствуют эталонной модели OSI, поэтому вышеперечисленные межсетевые экраны при выполнении своих функций могут охватывать и соседние уровни эталонной модели.

**Пакетный фильтр** (экранирующий маршрутизатор) функционирует на сетевом уровне модели OSI, но для выполнения своих отдельных функций может также охватывать и транспортный уровень. Он относится к самым простым межсетевым экранам и предназначен для фильтрации пакетов сообщений, обеспечивая прозрачное взаимодействие между внутренней и внешней сетями. Решение о том, пропустить или отвергнуть данные принимается для каждого пакета независимо на основе заданных правил фильтрации. Для принятия решения анализируются заголовки пакетов сетевого и транспортного (например, UDP или TCP) уровней, включая следующие параметры: IP-адреса отправителя и получателя, тип транспортного протокола, поля служебных заголовков протоколов, номера портов источника и получателя.

Пакетные фильтры могут быть реализованы в таких компонентах сетевой инфраструктуры как: пограничные маршрутизаторы, операционные системы, персональные межсетевые экраны. К их преимуществам относится низкая цена, а также высокая скорость, в силу проверки данных только в заголовках сетевого и транспортного уровней. В связи с этим пакетные фильтры в составе пограничных маршрутизаторов являются приемлемым

решением для размещения на границе с сетью с низкой степенью доверия. К их недостаткам относится отсутствие контроля и защиты содержимого пакетов сообщений, и, как следствие, уязвимости к таким распространенным типам сетевых атак как подмена исходных адресов и несанкционированное изменение содержимого пакетов сообщений.

**Межсетевой экран сеансового уровня** (экранирующий транспорт) функционирует на сеансовом уровне модели OSI, охватывая в процессе работы также транспортный и сетевой уровни. Данный экран исключает прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая в качестве посредника, реагирующего на все входящие пакеты и проверяющего их допустимость на основании текущей фазы соединения. Он гарантирует, что ни один сетевой пакет не будет пропущен, если не принадлежит ранее установленному соединению.

Поскольку межсетевой экран данного типа исключает прямое взаимодействие между узлами, то он является единственным связующим элементом между внешней сетью и внутренними ресурсами, что создает видимость того, что на все запросы из внешней сети отвечает шлюз, и делает практически невозможным определение топологии защищаемой сети. Кроме того, он предотвращает возможность реализации DoS-атаки, присущей пакетным фильтрам, т.к. контакт между узлами устанавливается только при условии его допустимости.

Преимуществами межсетевых экранов сеансового уровня являются относительно низкая цена и отсутствие существенного влияния на скорость маршрутизации. Они дополняют пакетный фильтр функциями контроля виртуальных соединений и трансляции внутренних IP-адресов. К их недостаткам относится отсутствие контроля содержимого пакетов сообщений, а также невозможность проверки содержимого поля данных, в результате чего злоумышленнику предоставляется возможность передачи в защищаемую сеть «троянских коней» и других вредоносных программ. На практике большинство межсетевых экранов сеансового уровня не являются самостоятельными продуктами, а поставляются в комплекте с межсетевыми экранами прикладного уровня.

**Межсетевой экран прикладного уровня** (экранирующий шлюз) функционирует на прикладном уровне модели OSI, охватывая также уровень представления. Данные шлюзы также называются прокси-серверами.

Их защитные функции, как и у межсетевого экрана сеансового уровня, относятся к функциям посредничества, однако с существенно большим количеством возможностей. К ним относятся: идентификация и аутентификация пользователей при попытке установления соединений через межсетевой экран, проверка подлинности передаваемой через шлюз

информации, разграничение доступа к ресурсам внутренней и внешней сетей, фильтрация и преобразование потока сообщений, регистрация событий, реагирование на задаваемые события, кэширование данных, запрашиваемых из внешней сети.

Межсетевой экран данного рода исключает прямые соединения между внутренней и внешней сетями за счет соответствующих программных посредников (экранирующих агентов), функционирующих по одному для каждого обслуживаемого прикладного протокола. При этом посредники прикладного шлюза имеют важные отличия от канальных посредников шлюза сеансового уровня, а именно связь с конкретными приложениями (программными серверами) и возможность фильтрации потока сообщений на прикладном уровне OSI.

Такие межсетевые экраны предлагают более надежный способ защиты сетей по сравнению с межсетевыми экранами сеансового уровня и пакетными фильтрами, однако в значительной степени оказывают влияние на уменьшение скорости маршрутизации.

*Межсетевые экраны экспертного уровня* сочетают в себе элементы пакетных фильтров и межсетевых экранов прикладного уровня. Они обеспечивают фильтрацию пакетов по содержимому их заголовков сетевого и транспортного уровней модели OSI, а также выполняют все функции прикладного шлюза по части фильтрации пакетов на прикладном уровне OSI, при этом оценивая содержимое каждого пакета в соответствии с заданной политикой безопасности.

Межсетевые экраны данного рода осуществляют контроль каждого передаваемого пакета на основе имеющейся таблицы правил, каждой сессии на основе таблицы состояний, а также каждого приложения на основе разработанных посредников. Их достоинством является прозрачность для конечного пользователя и более высокая скорость обработки информационных потоков. Однако данные межсетевые экраны допускают прямое соединение между авторизованным клиентом и компьютером внешней сети, вследствие чего обеспечивают менее высокий уровень защиты. Поэтому на практике данная технология используется для повышения эффективности функционирования комплексных межсетевых экранов.

Комплексный межсетевой экран представляется в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI. Чаще всего он функционирует на сетевом, сеансовом и прикладном уровнях.

#### 4.1.5 Политика межсетевого взаимодействия

Конфигурирование системы межсетевого экранирования, выбор схемы подключения и настройка параметров функционирования межсетевого экрана и формирование политики межсетевого взаимодействия являются залогом эффективной защиты корпоративной сети.

Политика межсетевого взаимодействия является составной частью общей политики безопасности в организации, она определяет требования доступа к сетевым сервисам и к работе межсетевого экрана.

В требованиях к доступу к сетевым сервисам задаются все сервисы, предоставляемые через межсетевой экран, допустимые адреса клиентов для каждого сервиса, для пользователей указывается порядок использования сервисов и компьютеров, задаются ограничения на методы доступа, исключающие обращение к запрещенным сервисам Интернета обходными путями. Кроме того, определяются правила аутентификации пользователей и компьютеров.

Политика работы межсетевого экрана может задавать один из двух принципов:

- «запрещено все, что явно не разрешено»;
- «разрешено все, что явно не запрещено».

В зависимости от выбора принципа решение может быть принято как в пользу безопасности, но в ущерб удобству использования сетевых сервисов, так и наоборот.

При выборе принципа *«запрещено все, что явно не разрешено»* межсетевой экран настраивается таким образом, чтобы блокировать любые явно не разрешенные межсетевые взаимодействия. Такой подход позволяет адекватно реализовать принцип минимизации привилегий и с точки зрения безопасности является наилучшим. В данном случае на каждый тип разрешенного взаимодействия задаются правила доступа, при этом остальные сервисы по умолчанию будут запрещены. Данный принцип соответствует классической модели доступа, используемой во всех областях информационной безопасности, но при нем пользователи могут испытывать определенные неудобства.

При выборе принципа *«разрешено все, что явно не запрещено»* межсетевой экран блокирует только явно запрещенные межсетевые взаимодействия. В этом случае повышается удобство использования сетевых сервисов со стороны пользователей, но снижается безопасность межсетевого взаимодействия, поскольку пользователи имеют больше возможностей обойти межсетевой экран, поскольку администратор может учесть не все действия, запрещенные пользователям. При реализации данного принципа внутренняя сеть оказывается менее защищенной, поэтому производители межсетевых экранов обычно отказываются от использования данного принципа.

В обоих случаях межсетевой экран не является симметричным: для него отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю сеть и наоборот. В общем случае межсетевой экран осуществляет фильтрацию проходящих через него информационных потоков и посредничество при реализации межсетевых взаимодействий. В зависимости от типа экрана эти функции могут выполняться с различной полнотой.

#### **4.1.6 Персональные и распределенные межсетевые экраны**

Для индивидуальных пользователей представляет интерес технология персонального сетевого экранирования. В этом случае межсетевой сетевой экран устанавливается на защищаемый персональный компьютер. Такие экраны, называемые *персональными межсетевыми экранами*, являются программными продуктами, которые располагаются внутри компьютера на низшем уровне операционной системы – между сетевыми платами и всеми протокольными стеками.

Персональный межсетевой экран выполняет защиту от внешних атак и защиту от атак со стороны данного компьютера, контролируя весь исходящий и входящий трафик независимо от всех прочих системных средств защиты. В этом случае поддерживается доступность сетевых сервисов, но уменьшается нагрузка, индуцированная внешней активностью, в результате чего снижается уязвимость внутренних сервисов защищаемого компьютера, поскольку первоначально сторонний злоумышленник должен преодолеть межсетевой экран, где защитные средства особенно тщательно и жестко сконфигурированы. Такие межсетевые экраны управляются только с того компьютера на котором они установлены и являются подходящим решением для небольших офисов и домашнего применения.

Для корпоративных пользователей реализация политики безопасности организации требует централизованного управления межсетевыми экранами с единой консоли, установленной в главном офисе организации. Централизованно управляемая совокупность сетевых мини-экранов, защищающих отдельные компьютеры сети, называют *распределенными межсетевыми экранами*. При построении распределенных систем межсетевого экранирования функциональные компоненты сетевого экрана распределяются по узлам сети и могут обладать различной функциональностью. При обнаружении подозрительных на атаку признаков управляющие модули распределенного межсетевого экрана могут адаптивно изменять конфигурацию, состав и расположение компонент.

Общий принцип распределенного межсетевого экранирования рассмотрим на примере одной из схем функционирования распределенного межсетевого экрана (рис. 4.4).

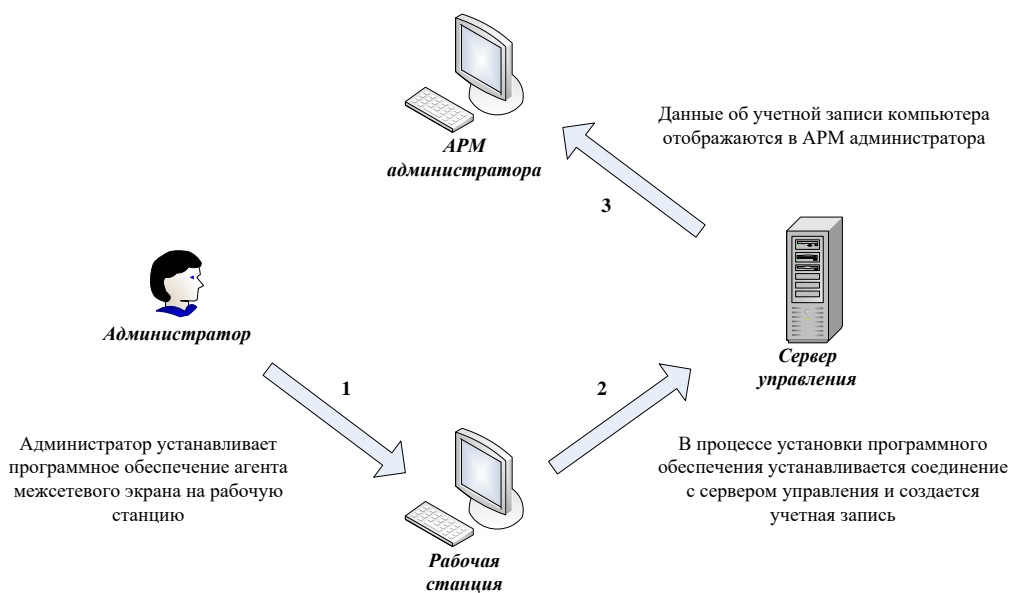


Рис. 4.4 – Схема функционирования межсетевого экрана.

На каждую рабочую станцию администратором устанавливается агент межсетевого экрана, представляющий собой программный компонент, предназначенный для образования доверенного канала передачи данных и обеспечения функции разграничения доступа к защищаемым ресурсам сети. В процессе установки устанавливается соединение с сервером управления (центральной частью межсетевого экрана, обеспечивающей взаимодействие всех его компонентов, обработку и хранение данных), где автоматически создается учетная запись рабочей станции. Данные об учетной записи рабочей станции отображаются в АРМ администратора, обеспечивающем централизованное управление средствами и механизмами защиты, абонентами. Для удобства администрирования учетные записи пользователей группируются.

Все последующее управление субъектами доступа и защищаемыми объектами осуществляется посредством учетных записей, хранящихся в базе данных на сервере управления, в свою очередь управляемых средствами АРМ администратора. Права доступа авторизованных абонентов к защищаемым компьютерам регулируются специальными правилами. Функция предоставления доступа к защищаемым компьютерам обеспечивается агентами межсетевого экрана и работает на основе заданных субъектов доступа (пользователей и компьютеров) и параметров соединения с защищаемыми компьютерами (протоколами, портами и т. п.).

#### 4.1.7 Проблемы безопасности традиционных межсетевых экранов

**Возможности обхода межсетевого экрана.** Поскольку межсетевые экраны являются первым элементом защиты, то на них, как правило, сосредотачиваются основные усилия атакующих при проведении атак на корпоративные сети. При этом выделяют два основных подхода к обходу межсетевого экрана: постепенный подход и туннелирование.

**Постепенный подход** (firewalking) предусматривает сбор информации о защищаемой сети. Способ использует посылку и анализ IP-пакетов подобно утилите *traceroute* (служебной программе, предназначенной для определения маршрутов следования данных в сетях TCP/IP) для определения возможности определенного пакета пройти на хост назначения через устройство фильтрации пакетов. В случае такого зондирования определяются открытые порты данного устройства, возможность прохождения пакетов для различных служб через данный порт и т.д.

Утилита *traceroute* предназначена для перечисления всех хостов на маршруте к цели. Она посылает на хост назначения UDP или ICMP echo (ping) пакеты, в которых постепенно увеличивается значения поля TTL (Time To Live) после каждого удачного шага (по умолчанию шаг состоит из посылки трех пакетов). Если используется пакет UDP, то номер порта назначения увеличивается на единицу с каждой пробой. При получении пакета с TTL = 0 маршрутизатор удаляет пакет и посылает на хост-инициатор ICMP error message (time to live exceeded in transit). Это позволит хосту-инициатору узнать, на каком маршрутизаторе пакет удален.

Чтобы удостовериться, что получен ответ от хоста-назначения (ICMP port unreachable или ICMP echo reply), утилита *traceroute* посылает следующий пакет UDP на порт с большим номером, который вероятнее всего не используется приложениями. На основе утилиты *traceroute* разработаны средства, позволяющие проводить требуемый анализ.

**Туннелирование** (tunnelling) подразумевает передачу протокола через общую сеть с использованием другого протокола посредством инкапсуляции протоколов при межсетевом взаимодействии.

Предположим, что межсетевой экран разрешает пакеты протокола HTTP. Тогда, если за ним во внутренней сети имеется машина, на которой установлен клиент туннелирования, можно организовать скрытый канал обмен данными, которые будут пропускаться межсетевым экраном. Под скрытым каналом принято понимать любой коммуникационный канал, который может быть использован в процессе передачи информации в обход политики безопасности системы.

В процессе туннелирования применяются три типа протоколов: несущий протокол, протокол-пассажир, протокол инкапсуляции. Транспортный протокол объединяемых сетей является протоколом-пассажиром, а протокол транзитной сети – несущим протоколом.

Пакеты протокола-пассажира помещаются в поле данных несущего протокола с помощью протокола инкапсуляции. Пакеты протокола-пассажира не обрабатываются при их транспортировке по транзитной сети. Инкапсуляцию и извлечение пакетов протокола-пассажира выполняют пограничные устройства, располагающиеся на границе между исходной и транзитной сетями, которые указывают в несущих пакетах свои адреса, а не адреса узлов назначения.

В качестве несущего протокола наиболее часто применяется протокол HTTP. Это объясняется широтой его распространения, легкостью скрытия потока данных, простотой реализации, а также сложностью обнаружения аномалий в протоколе. На нижних уровнях также существуют механизмы для построения скрытых каналов (например, можно использовать идентификатор IP-пакета, сообщения, запросы-ответы DNS), но эти механизмы, как правило, требуют от пользователя привилегированных прав и обладают различными ограничениями.

Чтобы пакет с данными пересек периметр безопасности, протокол должен быть разрешен для использования субъекту, инициировавшему передачу. В качестве субъекта может выступать пользователь системы или приложение, работающее от его имени (например, браузер). Таким образом, чтобы организовать передачу данных по туннелю требуется иметь разрешение на отправку данных через периметр безопасности и успешно скрывать тот факт, что авторизованный канал используется не по назначению.

Протокол-пассажир оказывает весьма незначительное влияние на общую структуру туннеля и представляет собой некие данные, которые необходимо передать по туннелю. Это может быть поток данных, создаваемый определенным приложением (например, SSH), или любая другая информация (например, файл), набор управляющих команд и т.д. Вид передаваемой информации существенно влияет на протокол инкапсуляции.

Инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты немаршрутизируемых протоколов. На основании протокола, инкапсулируемого в несущий протокол, скрытые каналы можно подразделить на две группы:

- 1) канал передачи потока данных приложения;
- 2) канал, специально создаваемый злоумышленником.

В первом случае, как правило, создается относительно большой трафик, который демаскирует скрытый канал. Во втором случае обнаружение скрытого канала усложняется, особенно когда канал использует методы стеганографии.

Практическим примером туннелирования являются сетевые черви и макровирусы, заносимые в корпоративную сеть в виде вложений в сообщения электронной почты.

**Ограничения в применении традиционных межсетевых экранов.** При проектировании межсетевых экранов различные технологии не могут предусмотреть всех возможностей проникновения в защищаемую сеть, а на этапе реализации такого сложного программно-аппаратного или программного комплекса возможны технологические ошибки. Любая же программная ошибка, уязвимость программного обеспечения, ошибка конфигурирования межсетевого экрана могут привести к проникновению в защищаемую сеть.

Традиционный межсетевой экран не позволяет решить все проблемы безопасности корпоративной сети. Отметим некоторые наиболее существенные ограничения в применении межсетевых экранов.

*Возможное ограничение пропускной способности.* Традиционные межсетевые экраны являются потенциально узким местом сети, так как все соединения должны проходить через межсетевой экран и в некоторых случаях изучаться межсетевым экраном.

*Отсутствие встроенных механизмов защиты от вредоносного программного обеспечения.* Традиционные межсетевые экраны не могут защитить от пользователей, загружающих зараженные вирусами программ из архивов или при передаче таких программ в качестве приложений к электронным письмам, поскольку эти программы могут быть зашифрованы или сжаты большим числом способов.

*Отсутствие эффективной защиты от получаемого из Интернета опасного содержимого* (апплетов Java, управляющих элементов ActiveX, сценариев JavaScript и т.п.). Специфика мобильного кода такова, что он может быть использован как средство для проведения атак. Мобильный код может быть реализован в виде компьютерного вируса, агента, перехватывающего пароли или номера кредитных карт, программы, копирующей конфиденциальные файлы и пр.

Также следует помнить, что межсетевой экран, как любое другое СЗИ, не может защитить от ошибок и некомпетентности администраторов и пользователей. Администрирование межсетевого экрана является сложной задачей, требующей определенной квалификации и опыта, при этом необходимо учитывать, что атаки могут проводиться и со стороны защищаемой сети, что усложняется тем, что они инициируются

пользователями, которые, имеют доступ к элементам сети и представляют организацию системы защиты. В основном именно эти причины вызвали необходимость ведения подробных журналов регистрации событий (аудита), итогом которых является заключение экспертов о совершившихся проникновениях.

Традиционные межсетевые экраны являются, по существу, средствами, только блокирующими атаки, которые уже находятся в процессе осуществления. Более эффективным было бы не только блокирование, но и устранение предпосылок реализации вторжений. Для организации упреждения вторжений атак необходимо использовать средства обнаружения вторжений и поиска уязвимостей, которые будут своевременно обнаруживать и рекомендовать меры по устранению слабых мест в системе защиты.

Все вышеприведенные ограничения учитываются при разработке и реализации так называемых *межсетевых экранов нового поколения* – Next-Generation Firewall (NGFW). Межсетевые экраны нового поколения представляют собой интегрированные платформы сетевой безопасности, в которых традиционный подход сочетается с другими сетевыми решениями для фильтрации трафика, такими как системы глубокого анализа трафика (Deep Packet Inspection), предотвращения вторжений и проверки трафика на уровне приложений (Web Application Firewall). Некоторые NGFW также включают проверку зашифрованного трафика TLS/SSL, фильтрацию веб-сайтов, управление пропускной способностью, антивирусную проверку и интеграцию со сторонними системами управления идентификацией.

#### **4.1.8 Показатели защищенности межсетевых экранов**

В 1997 году Гостехкомиссия России установила требования и показатели защищенности межсетевых экранов в руководящем документе «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [25]. Документ устанавливает классификацию межсетевых экранов по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации. Требования к межсетевым экранам приведены в таблице 4.1, где знак «+» означает наличие или дополнительные требования, знак «=» – требования из низкого класса.

Таблица 4.1 – Требования к межсетевым экранам

Показатели защищенности	Классы защищенности				
	5	4	3	2	1
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	–	–	+	=	+
Регистрация	–	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	–	–	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	+
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Дифференциация подхода к выбору функций защиты в межсетевом экране определяется АС, для защиты которой применяется межсетевой экран. Установлено 5 классов защищенности межсетевых экранов.

Межсетевые экраны 1 класса (самого высокого) применяются для АС класса 1А. Если в АС классов 3А, 2А обрабатывается информация с грифом «особой важности», то также требуется использовать межсетевой экран не ниже 1 класса.

Межсетевые экраны 2 класса используются для АС класса 1Б. Если в АС классов 3А, 2А обрабатывается информация с грифом «совершенно секретно», также необходимо использовать межсетевые экраны не ниже указанного класса.

Межсетевые экраны 3 класса обеспечивают защиту АС класса 1В. Если в АС классов 3А, 2А происходит обработка информации с грифом «секретно», то также требуется межсетевой экран не ниже 3 класса.

Межсетевые экраны 4 класса требуются в случае защиты АС класса 1Г.

Межсетевые экраны 5 класса (самого низкого) применяются для АС класса 1Д. Также требуется использовать межсетевые экраны их не ниже этого класса для автоматизированных систем класса 3Б и 2Б.

В 2016 году ФСТЭК России были утверждены новые требования к межсетевым экранам и опубликованы методические документы, содержащие профили защиты межсетевых экранов для 5 типов и 6 классов межсетевых экранов.

Согласно данным документам выделяют следующие типы межсетевых экранов:

- межсетевой экран сети (*тип «А»*) – межсетевой экран, применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы;
- межсетевой экран логических границ сети (*тип «Б»*) – межсетевой экран, применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы;
- межсетевой экран узла (*тип «В»*) – межсетевой экран, применяемый на узле (хосте) информационной системы;
- межсетевой экран веб-сервера (*тип «Г»*) – межсетевой экран, применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера);
- межсетевой экран промышленной сети (*тип «Д»*) – межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами.

Межсетевые экраны типа «А» реализуется только в программно-аппаратном исполнении, типа «Б», «Г» и «Д» могут быть как в виде программного продукта, так и в программно-аппаратном исполнении. Исключительно в виде программного продукта реализуется межсетевые экраны типа «В».

По классам защиты соблюдается принцип: чем выше класс (1 класс самый высокий), тем больше к ним требований и тем для более высокого класса систем они могут применяться (рис. 4.5).

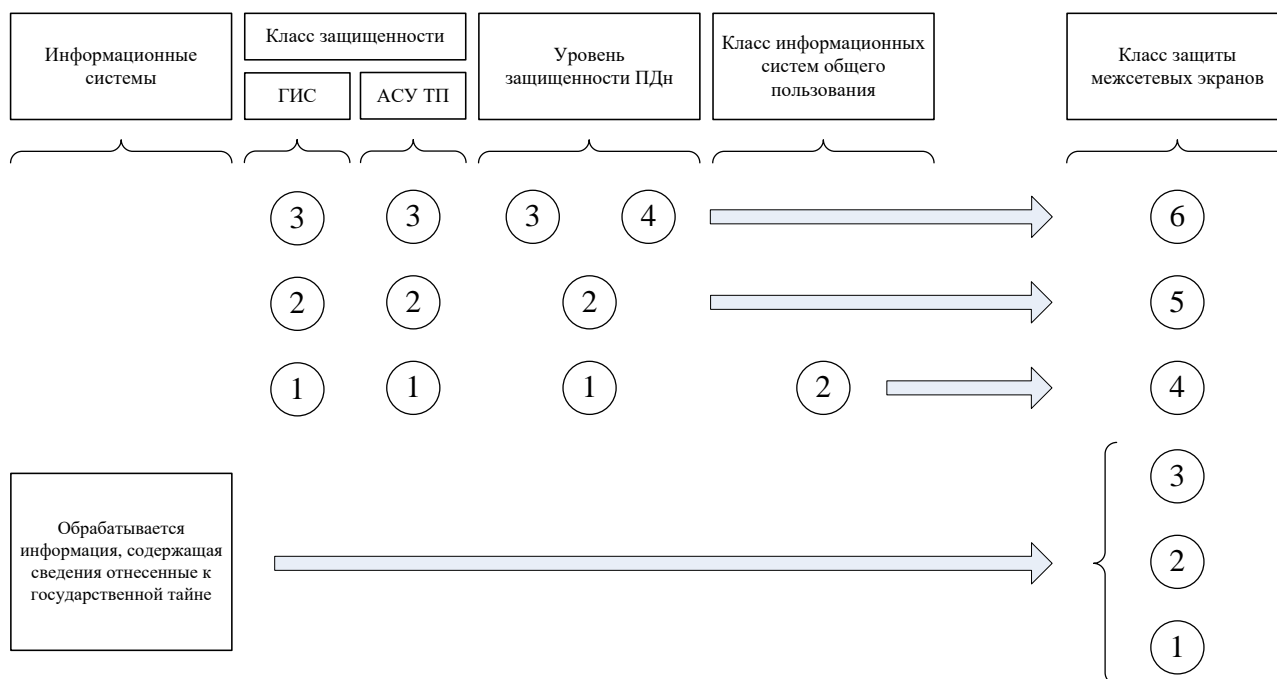


Рис. 4.5 – Классификация межсетевых экранов по классам защиты [5].

Согласно такому подходу, в информационных системах защиты информации, содержащей сведения, отнесенные к государственной тайне, должна обеспечиваться с помощью межсетевых экранов 3, 2 и 1 классов защиты.

В ГИС 1, 2 и 3 классов защиты, а также для АСУ ТП должны использоваться межсетевые экраны 4, 5 и 6 классов соответственно.

Для случая обеспечения 1 и 2 уровней защищенности персональных данных в ИСПДн потребуется устанавливать межсетевые экраны 4 и 5 классов, соответственно. Для 3 и 4 уровня защищенности персональных данных достаточно межсетевого экрана 6 класса защиты.

Для защиты информации в информационных системах общего пользования II класса необходимо использования межсетевые экраны 4 класса.

Идентификаторы профилей защиты представляются формате «ИТ.МЭ.тип/класс.ПЗ», где ИТ – «информационная технология», МЭ – «межсетевой экран», ПЗ – «профиль защиты». Спецификация профилей защиты межсетевых экранов для каждого их типа и класса приведена в таблице 4.2.

Таблица 4.2 – Идентификаторы профилей защиты межсетевых экранов

Тип межсетевого экрана	Класс защиты					
	6	5	4	3	2	1
Межсетевой экран типа «А»	ИТ.МЭ.А6.ПЗ	ИТ.МЭ.А5.ПЗ	ИТ.МЭ.А4.ПЗ	ИТ.МЭ.А3.ПЗ	ИТ.МЭ.А2.ПЗ	ИТ.МЭ.А1.ПЗ
Межсетевой экран типа «Б»	ИТ.МЭ.Б6.ПЗ	ИТ.МЭ.Б5.ПЗ	ИТ.МЭ.Б4.ПЗ	ИТ.МЭ.Б3.ПЗ	ИТ.МЭ.Б2.ПЗ	ИТ.МЭ.Б1.ПЗ
Межсетевой экран типа «В»	ИТ.МЭ.В6.ПЗ	ИТ.МЭ.В5.ПЗ	ИТ.МЭ.В4.ПЗ	ИТ.МЭ.В3.ПЗ	ИТ.МЭ.В2.ПЗ	ИТ.МЭ.В1.ПЗ
Межсетевой экран типа «Г»	ИТ.МЭ.Г6.ПЗ	ИТ.МЭ.Г5.ПЗ	ИТ.МЭ.Г4.ПЗ	—	—	—
Межсетевой экран типа «Д»	ИТ.МЭ.Д6.ПЗ	ИТ.МЭ.Д5.ПЗ	ИТ.МЭ.Д4.ПЗ	—	—	—

#### 4.1.9 Программные и программно-аппаратные межсетевые экраны

Приведем некоторые решения межсетевого экранирования, представляющие собой как отдельные межсетевые экраны, так и межсетевые экраны в составе комплексных систем защиты информации.

*Межсетевой экран Secret Net Studio*<sup>1</sup> – персональный межсетевой экран с централизованным управлением в составе СЗИ «Secret Net Studio» (ООО «Код Безопасности»), выполняющий функции защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования. Межсетевой экран для Secret Net Studio соответствует требованиям ФСТЭК к межсетевым экранам типа В по 4 классу защиты (ИТ.МЭ.В2.ПЗ), межсетевой экран для Secret Net Studio-С соответствует требованиям по 2 классу защиты (ИТ.МЭ.В2.ПЗ). Механизм защиты обеспечивает фильтрацию сетевого трафика на сетевом, транспортном и прикладном уровнях на основе формируемых для приложений правил. При этом наравне с режимом фильтрации сетевого трафика может функционировать в режиме обучения, разрешающем весь сетевой трафик с автоматическим добавлением разрешающих правил для используемых приложений.

*Межсетевой экран Dallas Lock*<sup>2</sup> – сертифицированный модуль СЗИ «Dallas Lock» (ООО «Конфидент»), выполняющий функции персонального межсетевого экрана с централизованным управлением, аудитом событий информационной безопасности.

<sup>1</sup> [www.securitycode.ru](http://www.securitycode.ru)

<sup>2</sup> [www.dallaslock.ru](http://www.dallaslock.ru)

Предназначен для защиты рабочих станций и серверов от НСД по сети. Межсетевой экран Dallas Lock контролирует и фильтрует проходящие через интерфейсы ПК сетевые пакеты в соответствии с заданными правилами, блокирует нежелательную сетевую активность и уведомляет о попытках нарушения заданных правил.

Межсетевой экран для Dallas Lock 8.0-К соответствует требованиям ФСТЭК к межсетевым экранам типа В по 4 классу защиты (ИТ.МЭ.В4.ПЗ), межсетевой экран для Dallas Lock 8.0-С – требованиям по 4 классу защиты (ИТ.МЭ.В2.ПЗ). Может быть использован:

- при создании защищенных АС до класса защищенности 1Г включительно;
- в ИСПДн до 1 уровня защищенности включительно;
- в ГИС 1 класса защищённости;
- при создании защищенных АСУ ТП на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1 класса защищенности включительно;
- при защите значимых объектов критической информационной инфраструктуры, до 1 категории включительно.

**Межсетевой экран Блокхост-сеть 2.0<sup>1</sup>** – персональный межсетевой экран в составе автономного или с удаленным управлением варианта поставки СЗИ «Блокхост-Сеть 2.0» (ООО «Газинформсервис»), реализующий защиту компьютера от НСД к его ресурсам из внешних источников, разграничение доступа пользователя компьютера к ресурсам сети и фильтрацию сетевого трафика. Функции защиты информации от НСД персонального межсетевого экрана соответствуют 4 классу защищенности согласно руководящему документу «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

В межсетевом экране реализованы следующие функциональные возможности:

- фильтрация пакетов на сетевом уровне на основе сетевых адресов отправителя и получателя;
- фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

---

<sup>1</sup> [www.gaz-is.ru](http://www.gaz-is.ru)

- фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрация с учетом любых значимых полей сетевых пакетов;
- регистрация и учет фильтруемых пакетов.

**Межсетевой экран АПКШ «Континент»<sup>1</sup>** – межсетевой экран в составе аппаратно-программного комплекса шифрования «Континент» (ООО «Код Безопасности»), реализующего, наряду с межсетевым экранированием, функции криптографической защиты данных, передаваемых по каналам связи общих сетей передачи данных между составными частями VPN, автоматическую регистрацию событий, связанных с функционированием комплекса, централизованное управление компонентами комплекса. Соответствует требованиям ФСТЭК к межсетевым экранам типа А по 3 классу защиты (ИТ.МЭ.А3.ПЗ) и может применяться для защиты: АС до класса 1В включительно, в информационных системах персональных данных до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно.

Данный межсетевой экран по умолчанию работает в режиме блокировки проходящего через криптографический шлюз трафика, его настройка осуществляется путем определения списков правил фильтрации и трансляции трафика согласно топологии сети и требованиям безопасности. Поддерживает обнаружение различных типов сетевых приложений, в том числе систем удалённого администрирования, мессенджеров, торрентов и систем туннелирования трафика.

**Межсетевые экраны Cisco<sup>2</sup>** – программно-аппаратные межсетевые экраны в составе многофункциональных устройств обеспечения сетевой безопасности от американской компании Cisco. Среди них наиболее популярны продукты Cisco ASA и Cisco Firepower, обеспечивающие межсетевое экранирование с контролем состояния соединения, мониторинг и контроль работы приложений, предотвращение вторжений, защиту от вредоносного ПО, фильтрацию трафика, блокировку DDoS-атак. Некоторые модели Cisco ASA соответствуют требованиям ФСТЭК к межсетевым экранам типа А и типа Б по 6 классу защиты (ИТ.МЭ.А6.ПЗ, ИТ.МЭ.Б6.ПЗ). Cisco Firepower соответствует требованиям ФСТЭК России к системам обнаружения вторжений по 5 классу защиты (ИТ.СОВ.С5.ПЗ).

В NGFW от Cisco следует отметить сервис Talos, обеспечиваемый большой командой исследователей, ежедневно анализирующих многочисленные потоки угроз и создающих инструменты, применяемые для защиты от следующей масштабной атаки. Cisco NGFW

---

<sup>1</sup> [www.securitycode.ru](http://www.securitycode.ru)

<sup>2</sup> [www.cisco.com](http://www.cisco.com)

используют встроенные расширенные функции безопасности, такие как системы предотвращения вторжений следующего поколения, расширенная защита от вредоносных программ и «песочница», позволяющая видеть пользователей, хосты, сети и инфраструктуру.

**CheckPoint**<sup>1</sup> – линейка межсетевых экранов нового поколения от Check Point Software Technologies Ltd. Шлюз безопасности Check Point Security Gateway соответствует требованиям ФСТЭК к межсетевым экранам типа А и типа Б по 4 классу защиты (ИТ.МЭ.А4.ПЗ, ИТ.МЭ.Б4.ПЗ), а также требованиям ФСТЭК к системам обнаружения вторжений по 4 классу защиты (ИТ.СОВ.С4.ПЗ). Функциональность преимущественного большинства продуктов Check Point основана на технологии программных блейдов – виртуальных комплексах программного обеспечения, устанавливаемых на аппаратные решения Check Point. Например, межсетевой экран содержит программный блейд Check Point IPS, защищающий корпоративную сеть путем проверки пакетов, проходящих через шлюз. Это полнофункциональная система, обеспечивающая надежную защиту от вторжений и частые автоматические обновления базы определений угроз. Технологии программных блейдов позволяют гибко изменять и масштабировать защищенность сети, на лету добавлять или убирать защитные механизмы и распределять защитные функции по разным устройствам.

**Межсетевые экраны ZyWALL**<sup>2</sup> – серия программно-аппаратных межсетевых экранов от международной компании Zyxel. Помимо функций межсетевого экранирования Zyxel ZyWALL также включает в себя функции потокового антивируса, механизмы обнаружения и предотвращения вторжений, защиты от спама, контроля полосы пропускания для разнообразных объектов сети, VPN-доступа для удаленных подключений. В продуктовую линейку входят ZyWALL USG, ZyWALL VPN, ZyWALL ATP, а также Zyxel Nebula – шлюзы безопасности с управлением из облака Nebula.

**Barracuda CloudGen Firewall**<sup>3</sup> – семейство физических, виртуальных и облачных устройств от американской компании Barracuda Networks, которые нацелены на защиту инфраструктуры распределенной сети предприятия. Такие устройства обеспечивают повышенную безопасность, поскольку содержат полный набор технологий NGFW, включая профилирование приложений уровня 7, предотвращение вторжений, веб-фильтрацию, защиту от вредоносных программ и угроз, защиту от спама и контроль доступа к сети. Кроме того, межсетевые экраны Barracuda CloudGen сочетают в себе продвинутую

---

<sup>1</sup> [www.checkpoint.com](http://www.checkpoint.com)

<sup>2</sup> [www.zyxel.com](http://www.zyxel.com)

<sup>3</sup> [www.barracuda.com](http://www.barracuda.com)

отказоустойчивую технологию VPN с интеллектуальным управлением трафика и возможностями оптимизации глобальной сети. Облачные межсетевые экраны Barracuda оптимально подходят для предприятий с множеством филиалов, поставщиков управляемых услуг и других организаций со сложной распределенной сетевой инфраструктурой.

**Palo Alto Networks**<sup>1</sup> – межсетевые экраны нового поколения от одноименной американской компании, поставляемые в виде виртуальных и аппаратных устройств, обнаруживающие как известные, так и неизвестные угрозы (в том числе в зашифрованном трафике) за счет использования данных, полученных с множества установленных устройств. С помощью NGFW от Palo Alto Networks предприятия могут быстро создавать правила безопасности, соответствующие политике безопасности, просты в обслуживании и адаптируются к динамической среде предприятия. Они сокращают время отклика благодаря автоматическим ответным действиям на основе политик, при этом ИТ-департамент получает возможность быстро автоматизировать рабочие процессы за счет интеграции с инструментами администрирования.

Данные межсетевые экраны поставляются в виде виртуальных и аппаратных устройств. Например, серия VM защищает частные и общедоступные облачные среды, обеспечивая доступ к приложениям и предотвращая угрозы. Трафик классифицируется на основе приложений, а не портов, что дает детальное представление об угрозах.

**SonicWall**<sup>2</sup> – виртуализированные версии межсетевых экранов нового поколения от одноименной американской компании, позволяющие упростить администрирование благодаря общей системе управления виртуальной и физической инфраструктурой. Серия устройств SonicWall Network Security (NSA) предоставляет компаниям среднего и крупного размера набор функций для расширенного предотвращения угроз. За счет инновационных технологий глубокого обучения в облачной платформе SonicWall Capture, серия NSA обеспечивает автоматизированное детектирование и блокирование атак в режиме реального времени.

Другими примерами популярных программных персональных межсетевых экранов могут служить: **Kaspersky Internet Security**, **Comodo Firewall**, **Avast Premium Security**, **AVG Internet Security**, **TinyWall** и пр.

---

<sup>1</sup> [www.paloaltonetworks.com](http://www.paloaltonetworks.com)

<sup>2</sup> [www.sonicwall.com](http://www.sonicwall.com)

## 4.2 Системы обнаружения вторжений

### 4.2.1 Понятие системы обнаружения вторжений

Традиционные межсетевые экраны являются механизмами создания барьера, преграждающего вход одним типам сетевого трафика и разрешающего другим, построенного на основе политики безопасности межсетевого экрана. Вместе с тем, эффективность сетевой безопасности обеспечивается посредством ведения контрольных журналов и постоянного мониторинга с быстрым обнаружением, исследованием событий безопасности и оповещением и реагированием на них, а затем – на инциденты. С целью мониторинга, наблюдения активности и принятия решений о том, являются ли наблюдаемые события подозрительными, применяются системы обнаружения вторжений, обеспечивающие дополнительный уровень защиты компьютерных систем.

**Система обнаружения вторжений (COB/IDS<sup>1</sup>)** – программный или программно-аппаратный комплекс, который по результатам анализа контролируемых и собираемых данных принимает решение о наличии атаки или вторжения.

Под *вторжением* понимают несанкционированный (преднамеренный или случайный) доступ к сети или подсоединенной к сети системе, включая злонамеренную деятельность против информационной системы или несанкционированное использование ресурсов в информационной системе [6].

Процесс обнаружения вторжений характеризуется сбором сведений об аномальном характере использования, а также о том, какая уязвимость была использована и каким образом, включая то, когда и как это произошло.

Приведем также определение согласно ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции»:

*Система обнаружения вторжений* – специализированная система, используемая для идентификации того факта, что была предпринята попытка вторжения, вторжение происходит или произошло, а также для возможного реагирования на вторжение в информационные системы и сети.

Применение COB позволяет:

– реализовать активную или пассивную реакцию на атаку;

---

<sup>1</sup> Intrusion detection system.

- распознать некоторую активность как атаку и выполнить действие по блокированию её источника;
- определить предпосылку атаки, имеющей вид сетевого зондирования или некоторого другого тестирования для обнаружения уязвимостей, и предотвратить её дальнейшее развитие;
- выполнить документирование существующих угроз для сети и систем;
- обеспечить контроль качества разработки и администрирования безопасности;
- получить полезную информацию о проникновениях, которые имели место, с предоставлением улучшенной диагностики для восстановления и корректирования вызвавших проникновение факторов;
- определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов сети.

#### 4.2.2 Структура системы обнаружения вторжений

В общем случае в структуре СОВ выделяют: подсистему сбора информации, подсистему анализа, модуль управления и модуль реагирования (рис. 4.6).

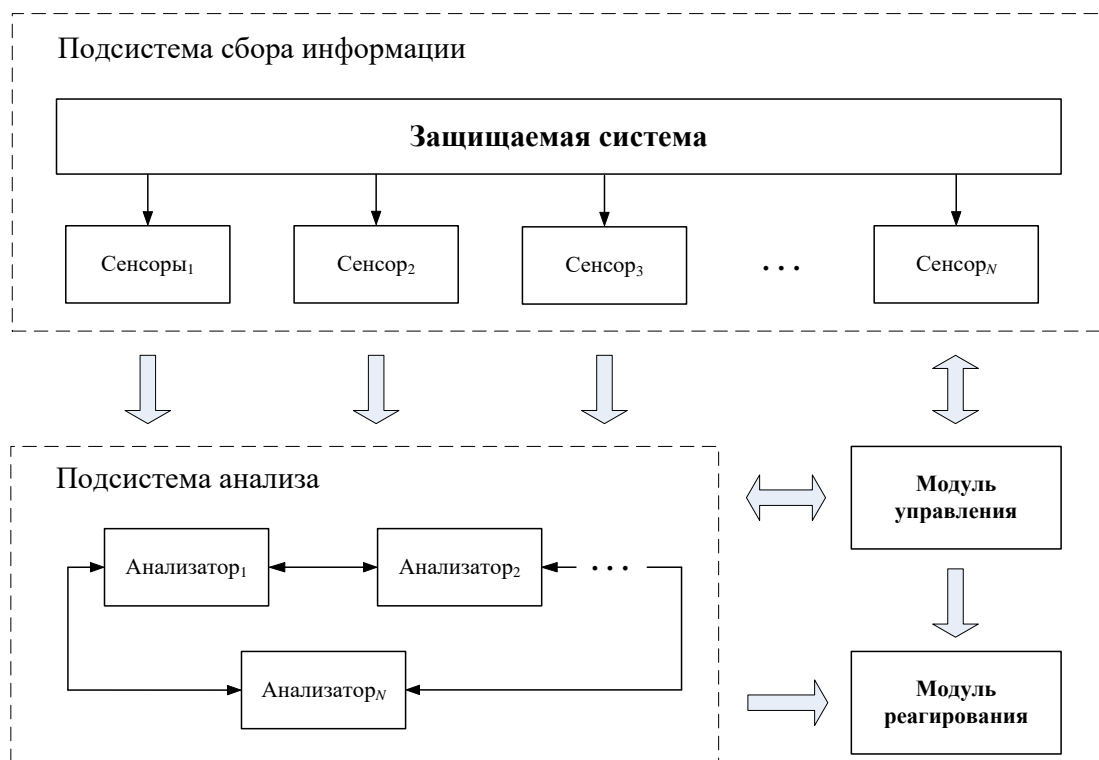


Рис. 4.6 – Общая структура СОВ.

Подсистема сбора информации используется для сбора первичной информации о работе защищаемой системы. Сбор информации осуществляется с применением автономных модулей – сенсоров (датчиков, детекторов) СОВ, количество  $N$  которых зависит от специфики защищаемой системы.

Подсистема анализа выделяет подозрительный трафик и атаки, основываясь на данных от сенсоров. При этом она структурно состоит из одного или более анализаторов – каждый анализатор выполняет поиск атак или вторжений определенного типа. Входными данными для анализатора может быть информация от сенсоров или другого анализатора, а результат их работы – индикация о состоянии защищаемой системы.

Модуль управления (консоль управления) позволяет управлять компонентами СОВ, выполнять её конфигурирование, а также следить за состоянием защищаемой системы. Модуль реагирования предназначен для выполнения predetermined действий в случае установления факта атаки, информирования заинтересованных лиц о состоянии защищаемой системы.

#### **4.2.3 Классификация систем обнаружения вторжений**

Существует несколько способов классификации СОВ, каждый из которых основан на их различных характеристиках (рис. 4.7). Рассмотрим подход, в котором в качестве таких характеристик выбраны типичные функции и особенности реализации СОВ:

- по способу обнаружения вторжения;
- по виду источников данных;
- по способу сбора информации об атаке;
- по структуре системы;
- по характеру реакции;
- по времени анализа данных.

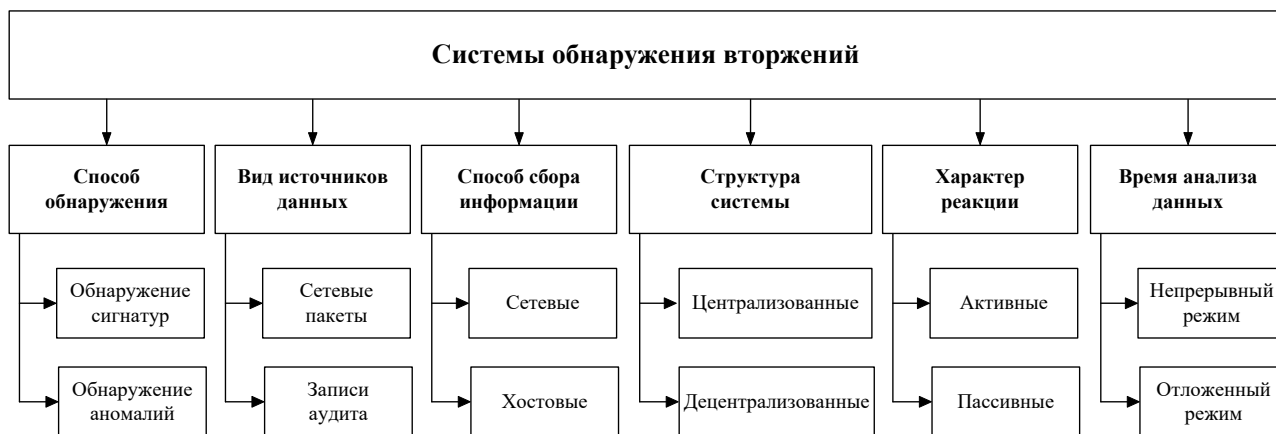


Рис. 4.7 – Классификация СОВ.

*По способу обнаружения вторжения* СОВ принято разделять на две категории:

- обнаружение сигнатур (signature detection) или злоупотреблений (misuse detection);
- обнаружение аномалий (anomaly detection).

Обнаружение сигнатур предполагает выявление вторжений на основе накопленных знаний об известных типах атак, характерные признаки которых описаны в виде сигнатуры (образца, шаблона), и поиск данной сигнатуры в контролируемом пространстве (сетевом трафике или журнале регистрации). Процесс обнаружения сигнатур производится посредством наблюдения за появлением точно описанных последовательностей событий в системе, для реализации которых применяется широкий спектр математических методов (сигнатурный метод, экспертные системы, методы анализа состояний).

Обнаружение аномалий основывается на выявлении отклонений значений параметров системы, последовательности событий от значений и последовательностей, хранимых в профиле нормального поведения системы, сформированном в условиях отсутствия атак. К таким отклонениям может быть отнесено большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора и т.п. Данный способ ориентирован на выявление новых типов атак, в связи с чем возникает необходимость постоянного обучения системы. Для реализации данного подхода применяются методы математической статистики и искусственного интеллекта.

В независимости от используемого в СОВ способа обнаружения вторжения процесс анализа предполагает наличие базы знаний о признаках атак или определенных правилах и

характеристиках нормального поведения системы. В процессе анализа оценивается возможность трактовки того или иного события в системе как попытки вторжения.

***По виду источников данных*** (для последующего принятия решения) выделяют:

- COB, анализирующие сетевые пакеты, захватываемые из сети;
- COB, анализирующие данные аудита.

К записям аудита относятся как специально организованные записи собственно аудита, так и системные журналы, которые могут вестись операционной системой. Такие системные журналы могут включать в себя конфигурационные файлы системы, данные для авторизации пользователей и т.д. Эта информация создает основу для последующего принятия решения. Способ сбора информации определяется политикой генерации событий, которая определяет режимы фильтрации просматриваемых событий.

***По способу сбора информации об атаке*** выделяют:

- сетевые COB (network-based);
- хостовые COB (host-based).

Сетевые COB осуществляют сбор и анализ сетевых пакетов, на основании которых проводится обнаружение, т.е. «прослушивают» трафик в сети, определяя возможные действия злоумышленников. Сенсоры таких систем располагаются в различных точках сети. Поиск атаки происходит по принципу «от хоста до хоста», анализируя сетевой трафик, используя сигнатуры атак, механизм поиска в трафике определенных строк, которые могут характеризовать несанкционированную деятельность. Сетевые COB могут обнаруживать сигнатуры и аномалии, однако методы обнаружения аномалий для них используются редко из-за необходимости большого периода времени для построения модели «нормального» поведения системы и большого числа ложных срабатываний.

Хостовые COB осуществляют анализ активности отдельного компьютера – мониторинг, детектирование и реагирование на действия злоумышленников осуществляется на защищаемом хосте. Для хостовых COB обычно используется комбинация обнаружения сигнатур и обнаружения аномалий. Такие системы интерпретируют результаты анализа журналов регистрации, создаваемых операционной системой, прикладным программным обеспечением, маршрутизаторами и т.д. Среди хостовых COB также выделяют подмножество систем обнаружения атак на уровне приложений (application-based), которые анализируют события, поступившие в ПО приложения, где наиболее общими источниками информации являются лог-файлы транзакций приложения.

Хостовые СОВ, использующие, помимо анализа журналов регистрации, и анализ сетевых пакетов, приходящих на данный хост, являются гибридными.

***По структуре*** СОВ подразделяют на:

- централизованные;
- децентрализованные.

При централизованном развертывании многие из существующих СОВ, как хостовые так и сетевые, имеют архитектуру, в которой реализуются все операции системы: сбор данных, их анализ и принятие решения, включая генерацию сигнала тревоги. Преимущество централизованного подхода в том, что одно устройство позволяет видеть весь трафик сети. Однако при этом имеется единая точка отказа. Кроме того, чтобы весь трафик направить через перехватчик, необходима перестройка сети, которая обычно связана с большими затратами.

Постоянное совершенствование атак, затрагивающих различные стороны безопасности сети организации, ее сетевых устройств и хостов, а также относительная дороговизна отдельных СОВ привели к необходимости их децентрализации.

При децентрализованном подходе по сети размещается множество перехватчиков, начиная от входа в сеть и спускаясь на более глубокие её сегменты. Преимущества децентрализации СОВ заключаются в отсутствии необходимости перепланировки сети, простоте развертывания, наличии множества точек наблюдения для расследований инцидентов, невысокой стоимости. Кроме того, при сбое одного перехватчика имеется возможность воспользоваться остальными, а при совмещении с электронной невидимостью практически устраняется опасность неавторизованного доступа в систему, а перехватчики, размещенные перед рабочими группами, покажут пересылку данных во внутренней корпоративной сети. Как недостаток отмечается рост затрат для обслуживания множества перехватчиков.

***По характеру реакции*** СОВ различают:

- активные;
- пассивные.

Реакция на вторжение – последовательность действий, осуществляемых СОВ в случае обнаружения вторжения. Процесс принятия решения по выбору реакции на вторжение должен быть защищен от внешнего влияния, чтобы исключить возможность предотвращения реагирования СОВ на это вторжение.

Активные действия СОВ предполагают изменения в ответ на атаку значений системных параметров, обеспечивают проведение комплекса мероприятий, направленных на снижение возможного ущерба от атаки. Набор мероприятий может быть достаточно разнообразным: блокировка учетной записи атакующего пользователя, автоматическое завершение сессии с атакующим узлом, реконфигурация межсетевых экранов и маршрутизаторов и т.д.

Пассивные действия СОВ не модифицируют поведение системы, а лишь извещающие администратора о факте вторжения. Данный тип реакции не предусматривает никаких действий по снижению возможного ущерба от атаки, а просто фиксирует факт атаки, записывая данные в файл журнала и выдает предупреждения, предполагая, что человек сам выполнит дальнейшие действия на основе данной информации.

***По времени анализа данных*** рассматривают СОВ, функционирующие в непрерывном и отложенном режиме.

Как правило, сетевые СОВ работают непрерывно (в масштабе реального времени), а системы, функционирующие на уровне хоста, обеспечивают автономный анализ регистрационных журналов операционной системы или приложений после совершения события. Применение того или иного метода зависит от многих факторов. В случае высококритичных систем обнаружение атак в реальном времени является обязательным.

Необходимо отметить, что лишь некоторые СОВ могут быть однозначно отнесены к одному из названных классов. Гибридные СОВ, представляющие собой комбинацию различных типов систем, как правило, включают в себя возможности нескольких категорий.

#### **4.2.4 Методы обнаружения сигнатур**

В настоящее время нет точного толкования понятия «сигнатура». В общем случае под сигнатурой понимается набор битовых критериев, используемых в качестве шаблона для обнаружения атак в трафике. Исходя из этого, в контексте дальнейшего изложения материала, под *сигнатурой* будем понимать множество условий, при удовлетворении которых наступает событие, определяемое как атака или вторжение.

Для обнаружения сигнатур могут применяться следующие методы:

- по совпадению с шаблоном;
- по совпадению с шаблоном состояния;
- анализа на основе шаблона используемого протокола;
- эвристический.

**Совпадение с шаблоном** базируется на поиске фиксированной последовательности байтов в рассматриваемом элементе данных (например, в единичном пакете). Как правило, шаблон сопоставляется только в том случае, если подозреваемый пакет ассоциирован с определенной службой (предназначен определенному порту). Существуют протоколы, которые не имеют определенных портов.

К достоинствам метода относятся: простота задания правил обнаружения, прямая связь с используемой данной атакой уязвимостью, высокая надежность, применимость для всех протоколов. К недостаткам: вероятность ложного срабатывания, если шаблон не уникален, необходимость множества шаблонов для одной уязвимости, ограниченность подхода, связанная с анализом только одного пакета, наличие различных вариантов обхода данного метода.

**Совпадение с шаблоном состояния** заключается в установлении состояния потока данных по одному пакету. При этом появление другого пакета (или пакетов), который соответствует данным состояния, считается атакой.

К достоинствам метода относятся: большая эффективность по сравнению с совпадением с шаблоном, прямая связь с используемой данной атакой уязвимостью, высокая надежность, применимость к множеству протоколов, затруднительный обход системы анализа. К недостаткам: вероятность ложного срабатывания, если шаблон не уникален, пропуск обнаружения в случае модификации атаки, необходимость множества шаблонов для одной уязвимости.

**Анализ на основе шаблона используемого протокола** подразумевает для формирования состояния декодирование различных элементов протокола. При декодировании протокола COB применяет правила, определенные RFC для нарушений. В некоторых случаях эти нарушения могут находиться в определенных полях протокола, что требует более детального анализа.

К достоинствам метода относятся: минимизация числа пропусков вторжений в случае хорошо определенного протокола, прямая связь с используемой данной атакой уязвимостью, возможность обнаружения вариантов атаки, надежность при определенных правилах протокола. К недостаткам: большое число пропусков, если RFC позволяет различные интерпретации, сложность формирования сигнатур.

**Эвристический подход** основывается на использовании логических правил, полученных эвристически. Например, для обнаружения сканирования портов можно использовать порог затронутых портов целевой системы. Кроме того, сигнатура может быть ограничена заданием только определенных типов пакетов.

К достоинствам метода относятся: возможность сигнатур отражать сложные взаимосвязи, возможность обнаружения атак, не обнаруживаемых предыдущими методами. К недостаткам: трудоемкость разработки эвристик и требование для этого высокой квалификации, требовательность эвристических алгоритмов приспособления к соответствующему трафику.

Возможны различные варианты разработки сигнатур, которые и определяют соответствующие технологии обнаружения.

#### 4.2.5 Методы обнаружения аномалий

Основой для обнаружения аномалий является понятие «нормального» поведения – любые отклонения от нормальности система будет рассматривать как аномалию. В связи с этим методы обнаружения аномалий могут различаться как по способу определения нормальности, так и по способу определения отклонений от нормальности.

Обнаружение аномалий обычно включает в себя процесс установления профилей нормального поведения пользователей, сравнение действительного поведения с этими профилями, сигнализацию об отклонениях от нормального поведения. Основой обнаружения аномалий является то, что образцы ненормального поведения идентифицируются как злоупотребление системы. Профили определяются как множества метрик, которыми являются измерения различных случаев поведения системы или пользователя. Для каждой метрики предусматривается или порог, или диапазон разрешенных значений.

При обнаружении аномалий исходят из того, что пользователи выполняют предсказуемые последовательные действия. Такой подход допускает адаптацию к изменениям поведения пользователей во времени. Полноту метода обнаружения аномалий необходимо постоянно контролировать в целях определения достаточности данного множества метрик для представления всего множества возможного аномального поведения.

Схема принятия решения при использовании технологий обнаружения аномалий и сигнатур приведена на рис. 4.8.

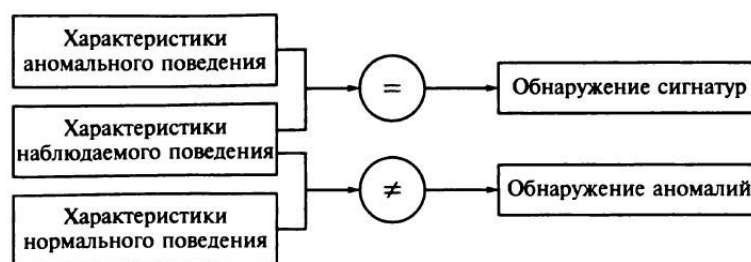


Рис. 4.8 – Принцип принятия решений при обнаружении сигнатур и аномалий.

Некоторые современные СОВ нельзя отнести ни к системам обнаружения сигнатур, ни к системам обнаружения аномалий. Они опираются на альтернативные методы обнаружения, к числу которых относят: методы Data Mining, технологии мобильных агентов, построение иммунных систем, применение генетических алгоритмов, нейросетевые технологии [16].

#### **4.2.6 Проблемы безопасности систем обнаружения вторжений**

Системы обнаружения вторжений имеют свои слабые стороны и уязвимости, что может быть использовано нарушителем с целью их обхода. Основной слабостью сетевых СОВ является то, что они принимают решение на основе анализа сетевого трафика, поэтому не могут предсказать как поведет себя целевая система при получении этого трафика. Обход СОВ существенно зависит от того, достаточно ли сильна сама СОВ, чтобы СОВ и целевая система рассматривали разные потоки данных одинаковым образом.

Если СОВ слабее целевой системы, на которую направлена атака, то при принятии решения СОВ может рассматривать пакет, который целевая система рассматривать не будет. В этом случае атакующий может использовать эту возможность вставкой дополнительных специально сформированных пакетов, которые замаскируют атаку для СОВ. Поскольку данные пакеты будут отброшены целевой системой, то атака обнаружена не будет.

Если СОВ сильнее целевой системы, то целевая система будет принимать пакеты, которые СОВ не будет рассматривать, что может быть достигнуто использованием метода вставки – атакующий может вставлять элементы атаки типа phf в пакеты для СОВ с дополнительной информацией. В этом случае СОВ отбросит эти пакеты, но они будут рассмотрены целевой системой, в результате чего такой подход может замаскировать атаку для СОВ.

Рассмотрим некоторые из базовых методов обхода СОВ [16], преимущественно основанные на принципе ошибкоустойчивости.

*Сбивание с толку.* Представляет собой процесс манипулирования данными таким образом, чтобы сигнатура СОВ не соответствовал проходящему пакету, который бы интерпретировался приемной стороной. Такой подход работает и против сетевых, и против хостовых СОВ.

*Фрагментация.* Данный метод характерен для обхода сетевых СОВ и основан на разбивке пакета данных на фрагменты, которые можно послать в различном порядке и с различными временными интервалами между ними, что может обмануть СОВ, которая не

производит реассемблирования. Отсылая фрагментированные пакеты, атакующий способен обойти сигнатурные COB, так как в этом случае COB не сможет обнаружить сигнатуру атаки, а следовательно и принять какие-то меры по ее предотвращению. Если COB проводит реассемблирование, то атакующий может превысить физический объем памяти COB, отведенный для реассемблирования, путем отправки большого числа фрагментов, содержащих «мусор», или превысить временной промежуток, в течение которого пакет должен быть реассемблирован.

*Шифрование.* Метод также характерен для обхода сетевых COB, которые должны иметь возможность исследовать полезную нагрузку пакета, чему может противодействовать атакующий, зашифровав трафик. Для этого используются шифрованные SSL, SSH и IPSec туннели, что позволяет атакующему использовать средства безопасности целевого хоста против него же самого. Это может быть опасно в случае, когда система имеет одну и ту же корневую директорию для нешифрованных (HTTP) и зашифрованных (HTTPS) веб-страниц – нарушитель может использовать любую атаку против веб-сайта с HTTPS, такую как SQL-вставка, переполнение буфера или обход директории. Поскольку HTTPS использует SSL, трафик шифруется, что позволяет ему проходить COB. Данная проблема также усугубляется широким применением SSL VPN.

*Отказ в обслуживании.* Метод переполнения сетевой COB, при котором с применением основной атаки производится «затопление» другими атаками с фиктивными адресами источников, что приводит к генерации большого количества сигналов тревоги и мешает определить истинного нарушителя.

*Контроль расположения и целостности файлов.* Один из методов обхода хостовых COB. Большинство COB, использующих контроль файлов, используют алгоритм хеширования. База данных хэш-значений обычно защищена паролем или зашифрована отдельным ключом. В этом случае атакующий может использовать слабости в методе контроля файлов. Для большинства систем контроля указываются директории, файлы в которых не проверяются, вследствие чего такие директории могут использоваться для обхода COB. Когда нарушитель скомпрометирует систему, находясь в такой временной директории, он может удалить систему контроля файлов или пересчитать значения хэш-функции для измененных файлов в других директориях. Атакующий может заменить программы, которые загружаются при старте системы, т.к. большинство хостовых COB контролируют файлы и скрипты загрузки.

*Перехват приложения.* Метод основан на той особенности COB, что многие из их сеансовых разновидностей не рассматривают прикладной уровень, чтобы увидеть, что сеанс

продолжен другим источником, а некоторые из хостовых не просматривают стек, чтобы убедиться, что сеанс продолжен тем же источником. При этом пользователь начинает законный сеанс, а атакующий, определив это, делает невозможным продолжение работы машины законного пользователя и присваивает его атрибуты аутентификации. При использовании протокола без состояний (как HTTP) атакующему не нужно ограничивать законного пользователя, ему необходимо только иметь перехваченную метку сеанса, что может быть достигнуто применением программ перехода на другой сайт или атакой машины, содержащей метки сеанса (при условии, если машина пользователя недостаточно защищена). Другим вариантом является метод «человек посередине», при котором атакующий претендует предстать законным пользователем для сервера и сервером для законного пользователя, после чего может модифицировать сеанс, чтобы не быть обнаруженным.

#### **4.2.7 Развертывание систем обнаружения вторжений**

Дополнение инфраструктуры сетевой безопасности в организации СОВ требует её тщательного планирования, подготовки, прототипирования и тестирования. Стратегия развертывания СОВ должна быть совместима с сетевой инфраструктурой предприятия, политикой его безопасности и имеющимися ресурсами.

Для защиты сети предприятия рекомендуется рассмотреть комбинацию сетевых и хостовых СОВ: сначала определить стадии развертывания сетевых СОВ, поскольку они являются более простыми для установки и сопровождения, а затем защитить критичные серверы с помощью хостовых СОВ. Далее, используя инструментальные средства анализа уязвимостей, следует протестировать СОВ и другие механизмы сетевой безопасности относительно их правильности конфигурирования и функционирования.

При развертывании сетевых СОВ основным вопросом является расположение системных сенсоров. Существуют различные варианты их расположения [13], приведенные на рис. 4.9 и обозначенные цифрами 1, 2, 3 и 4. Каждый из приведенных вариантов обладает своими преимуществами.

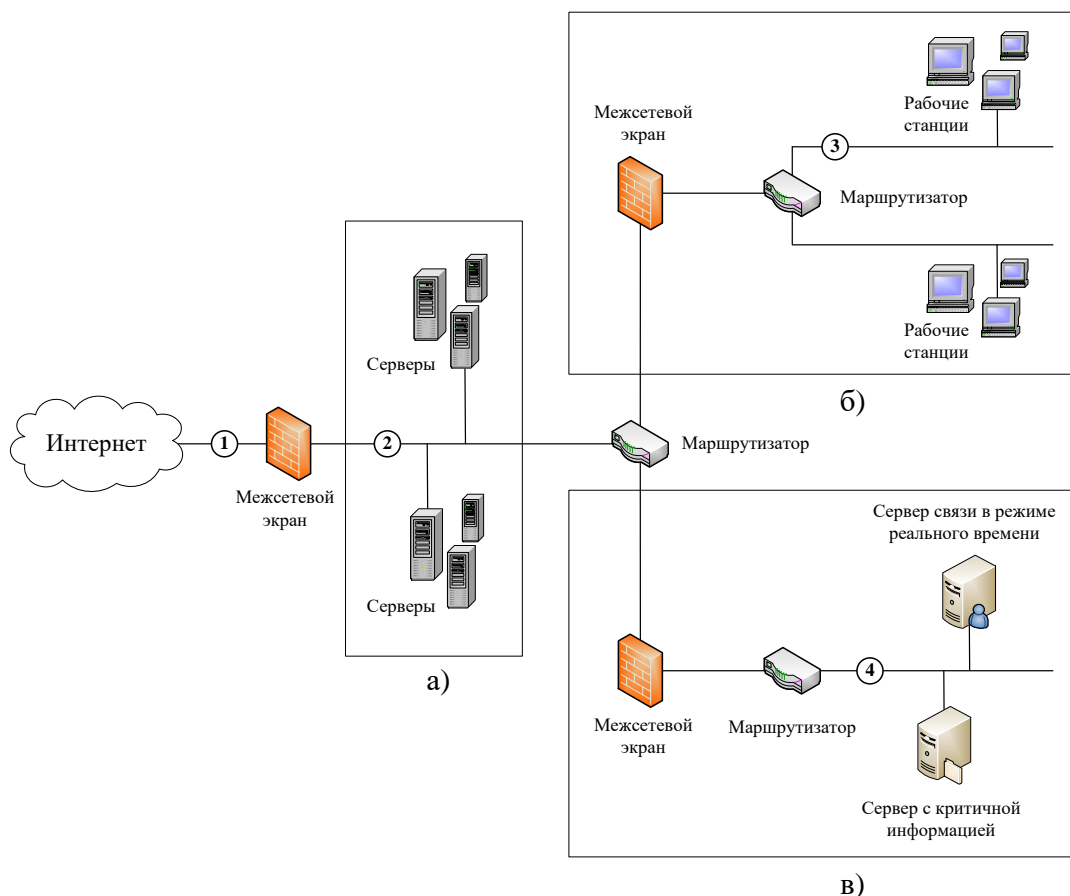


Рис. 4.9 – Возможные варианты расположения сенсоров сетевых СОВ:

а) DMZ-сеть; б) основная подсеть; в) подсеть с критичными ресурсами и дополнительными точками доступа.

1. *Перед внешним межсетевым экраном.* При таком расположении СОВ документирует количество и типы атак, исходящих из Интернета, целью которых является сеть.

2. *Позади межсетевого экрана в демилитаризованной зоне<sup>1</sup> (DMZ-сети).* В этом случае СОВ замечает внешние атаки, преодолевшие первую линию обороны сетевого периметра, обеспечиваемую межсетевым экраном, может анализировать проблемы, связанные с политикой межсетевого экрана, видит атаки, целями которых являются прикладные серверы, расположенные в DMZ. При этом если входящая атака не распознана, СОВ может распознать исходящий трафик, возникающий в результате компрометации сервера.

<sup>1</sup> Демилитаризованная зона (Demilitarized Zone) – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных.

3. *На основной магистральной сети.* СОВ просматривает основной трафик, увеличивая тем самым вероятность распознавания атак, а также определяет неавторизованную деятельность авторизованных пользователей внутри периметра безопасности организации.

4. *В критичных подсетях.* Преимуществом такого расположения СОВ является определение ими атак, целью которых являются критические системы и ресурсы, а также возможность фокусироваться на ограниченных ресурсах наиболее значимых информационных ценностей, расположенных в сети.

Установка хостовых СОВ, после размещения сетевых, может потребовать существенных временных затрат, в связи с чем рекомендуется в первую очередь устанавливать их на критичных серверах. Такая стратегия позволяет уменьшить общую стоимость развертывания и уделить внимание реагированию на тревоги, касающиеся наиболее важных хостов. После их установка организациями с повышенными требованиями к безопасности могут быть рассмотрены возможности установки СОВ и на другие хосты. В этом случае следует использовать хостовые СОВ с централизованным управлением и функциями создания отчетов, существенно снижающим сложность управления сообщениями о тревогах от большого числа хостов.

После развертывания СОВ рекомендуется рассмотреть возможность повышения квалификации администраторов с целью различия ложных и верных тревог, генерируемых СОВ, а также установить график проверки результатов СОВ.

#### **4.2.8 Требования к системам обнаружения вторжений**

С 2011 года ФСТЭК России утверждены требования к СОВ, включающие общие требования к ним и требования к их функциям безопасности.

Для дифференциации требований к функциям безопасности СОВ установлено 6 классов защиты СОВ: самый низкий класс – шестой, самый высокий – первый (рис. 4.10).

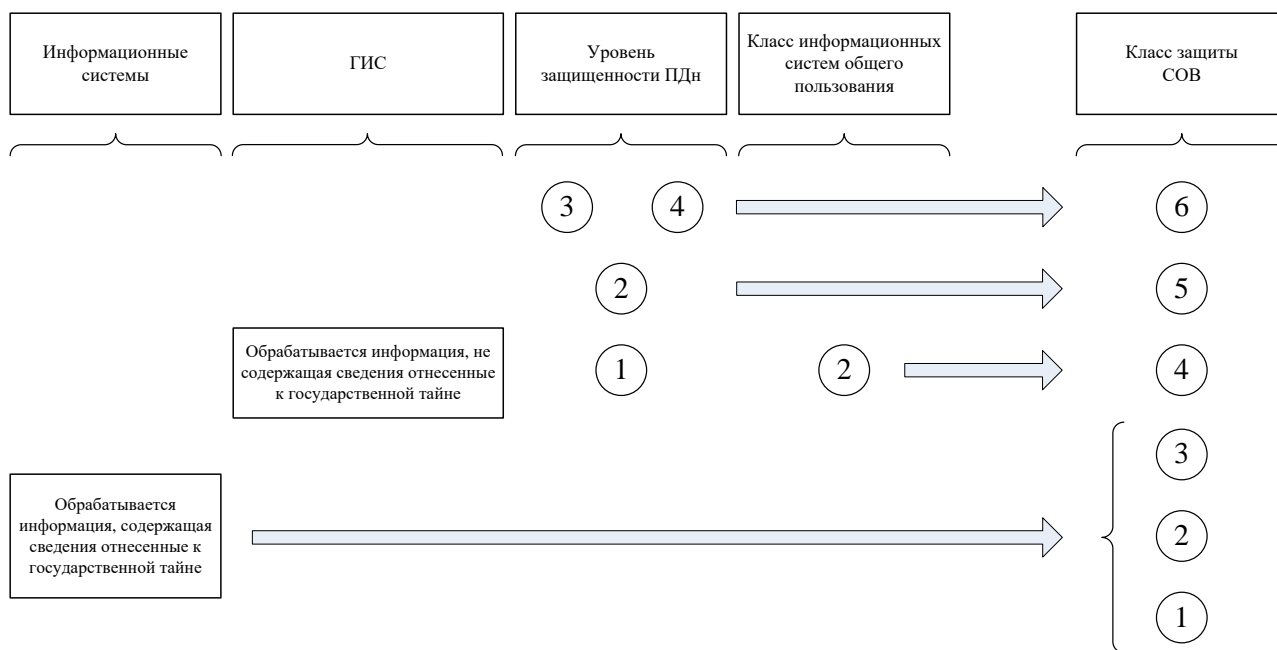


Рис. 4.10 – Классы защиты СОВ [5].

Системы обнаружения вторжений, соответствующие 6 классу защиты, применяются в ИСПДн 3 и 4 классов.

Системы обнаружения вторжений, соответствующие 5 классу защиты, применяются в ИСПДн 2 класса.

Системы обнаружения вторжений, соответствующие 4 классу защиты, применяются в ГИС, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в ИСПДн 1 класса, а также в информационных системах общего пользования II класса.

Системы обнаружения вторжений, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Детализация требований к функциям безопасности СОВ, а также взаимосвязи этих требований отражены в профилях защиты, утвержденных ФСТЭК России в качестве методических документов.

Согласно спецификации профилей защиты выделяют СОВ уровней следующих типов:

- *система уровня сети* – подключается к коммуникационному оборудованию (например, коммутатору) и контролирует сетевой трафик, наблюдая за несколькими сетевыми узлами. Сенсоры системы могут быть реализованы в виде программного обеспечения, устанавливаемого на стандартные программно-технические платформы,

а также в виде программно-аппаратных устройств, подключаемых к информационной системе;

- *система уровня узла* – устанавливается на узел и проводит анализ системных вызовов, журналов работы приложений и прочих источников узла. Сенсоры системы представляют собой программные модули, устанавливаемые на защищаемые узлы информационной системы.

Идентификаторы профилей защиты представляются формате «ИТ.СОВ.тип/класс.ПЗ», где ИТ – «информационная технология», СОВ – «система обнаружения вторжений», ПЗ – «профиль защиты». Спецификация профилей защиты СОВ для каждого их типа и класса защиты приведена в таблице 4.3.

Таблица 4.3 – Идентификаторы профилей защиты систем обнаружения вторжений

Тип системы обнаружения вторжений	Класс защиты					
	6	5	4	3	2	1
Система обнаружения вторжений уровня сети	ИТ.СОВ.С6.ПЗ	ИТ.СОВ.С5.ПЗ	ИТ.СОВ.С4.ПЗ	ИТ.СОВ.С3.ПЗ	ИТ.СОВ.С2.ПЗ	ИТ.СОВ.С1.ПЗ
Система обнаружения вторжений уровня узла	ИТ.СОВ.У6.ПЗ	ИТ.СОВ.У5.ПЗ	ИТ.СОВ.У4.ПЗ	ИТ.СОВ.У3.ПЗ	ИТ.СОВ.У2.ПЗ	ИТ.СОВ.У1.ПЗ

#### 4.2.9 Программные и программно-аппаратные системы обнаружения вторжений

Каждое сетевое СЗИ ориентировано для конкретной угрозы безопасности в системе и имеет слабые и сильные стороны. Обеспечение максимальной защиты от различных атак достижимо только в случае их комбинирования, что в контексте информационной безопасности носит название «обороны в глубину». Как было сказано ранее, современные межсетевые экраны представляют собой интегрированные платформы сетевой безопасности, в которых традиционный подход сочетается с другими сетевыми решениями, в том числе СОВ. Тем не менее, приведем некоторые СОВ, функционирующих как автономно, так и представляющих собой модуль комплексной системы защиты информации.

**СОВ Dallas Lock** – сертифицированный модуль СЗИ «Dallas Lock» (ООО «Конфидент»), соответствующий требованиям к СОВ по 4 классу защиты (ИТ.СОВ.У4.ПЗ). Интеграцией защитных механизмов СОВ в «Dallas Lock» создается инструмент с высокой эффективностью защиты от компьютерных атак и единой управляющей оболочкой. СОВ Dallas Lock обеспечивает обнаружение и блокирование основных угроз безопасности,

выполняя одновременно функции как сетевой, так и хостовой СОВ. При это обладает функциями сигнатурного и эвристического анализа сетевого трафика, журналов операционных систем и приложений на предмет нештатных ситуаций и попыток проведения вторжений, а также аномалий в поведении системы и пользователей, возможностью перехвата вызова функций операционной системы сторонними приложениями с возможностью гибкой настройки ограничения доступа к системным функциям для недоверенных приложений.

**COB Secret Net Studio** – сертифицированный модуль СЗИ «Secret Net Studio» (ООО «Код Безопасности»), соответствующий требованиям к СОВ по 4 классу защиты (ИТ.СОВ.У4.ПЗ). Управление работой механизма СОВ осуществляется централизованно в программе управления и может выполняться на разных уровнях структуры объектов управления. Обладает функциями обнаружения атак сигнатурными и эвристическими методами, автоматической блокировки атакующих хостов при обнаружении аномальных пакетов, сканировании портов, DoS-атаках и др., автоматической загрузки актуальной базы разрешающих правил через Сервер Обновлений, проверки по базе вредоносных IP-адресов и фишинговых URL-адресов.

**COB Континент** – система обнаружения и предотвращения вторжений с иерархическим управлением и контролем сетевых приложений от компании ООО «Код Безопасности», соответствующая требованиям к СОВ по 3 классу защиты (ИТ.СОВ.СЗ.ПЗ). Включает в себя двухуровневую система анализа трафика (сигнатурный и эвристический анализ сетевых приложений), систему мониторинга состояния сети и отдельных узлов в режиме реального времени с возможностью создания отчетов о событиях безопасности. Обеспечивает централизованное иерархическое управление системой защиты в территориально распределенных организациях с большим количеством филиалов, дистанционное обновление системного программного обеспечения и сигнатур (базы решающих правил).

**ViPNet IDS**<sup>1</sup> – программно-аппаратный комплекс для обнаружения вторжений в информационные системы от компании ОАО «ИнфоТеКС», функционирующий на основе динамического анализа сетевого и прикладного трафика стека протоколов TCP/IP. Соответствует требованиям к СОВ по 4 классу защиты (ИТ.СОВ.С4.ПЗ). Обеспечивает обнаружение сетевых атак в режиме близком к реальному масштабу времени на основе сигнатурного и эвристического методов выявления аномалий в сетевом трафике,

---

<sup>1</sup> [www.infotecs.ru](http://www.infotecs.ru)

поддерживает сетевые интерфейсы 1 Гбит/с и 10 Гбит/с (в зависимости от модификации), обновление в автоматизированном режиме баз сигнатур атак, поставщиком которой является российская компания «Перспективный мониторинг».

**Рубикон**<sup>1</sup> – сертифицированный программно-аппаратный комплекс сетевой защиты информации, разработанный российской компанией АО «НПО «Эшелон», выполняющий функции маршрутизатора, межсетевого экрана и COB. Соответствует требованиям к межсетевым экранам по 2 классу защиты (ИТ.МЭ.А2.ПЗ и ИТ.МЭ.Б2.ПЗ) и к COB по 2 классу защиты (ИТ.СОВ.С2.ПЗ). Предназначен для организации эффективной защиты периметра сетей предприятий различного масштаба в соответствии с нормативными требованиями регуляторов, используется в АС военного назначения, в которых обрабатывается информация (некриптографическими методами), составляющая государственную тайну. Функции контроля и фильтрации сетевого трафика реализуются в соответствии с заданными правилами проходящих через него информационных потоков.

**UserGate UTM**<sup>2</sup> – универсальное шлюзовое решение от российской компании UserGate (ООО «еСЛ Девелопмент», ООО "Юзергейт", Entensys), объединяющее межсетевой экран, COB, защиту от вредоносных программ и вирусов, систему контент-фильтрации, серверный антиспам, VPN-сервер и другие функции. Соответствует требованиям к межсетевым экранам по 4 классу защиты (ИТ.МЭ.А4.ПЗ и ИТ.МЭ.Б4.ПЗ) и к COB по 4 классу защиты (ИТ.СОВ.С4.ПЗ). COB позволяет обеспечить безопасность корпоративной сети от внешних интернет-угроз. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз, а также предоставление отчетов. Выявление проблем безопасности осуществляется с помощью использования эвристических правил и анализа сигнатур известных атак. База данных правил и сигнатур предоставляется и обновляется разработчиками UserGate при наличии соответствующей лицензии.

**Snort**<sup>3</sup> – свободная сетевая COB с открытым исходным кодом, созданная Мартином Рёшем и в дальнейшем развиваемая и поддерживаемая основанной им компанией «Sourcefire», позже поглощенной Cisco. Система Snort может работать в трех режимах: анализатор пакетов (режим «сниффера» – перехвата и прослушивания сетевого трафика), регистратор пакетов и режим обнаружения вторжений. В первом случае система просматривает пакеты на сетевом уровне и выводит информацию о них на консоль, во втором – записывает файлы журнала на диск, в третьем – анализирует сетевой трафик на

---

<sup>1</sup> [www.npo-echelon.ru](http://www.npo-echelon.ru)

<sup>2</sup> [www.usergate.com](http://www.usergate.com)

<sup>3</sup> [www.snort.org](http://www.snort.org)

предмет совпадения сигнатур атак и сигнализирует о них. COB является переносимой системой на многие операционные системы. Также одной из сильных сторон Snort является возможность для пользователя разрабатывать и использовать свои собственные правила для поиска атак в трафике, для чего используется язык описаний. Правила Snort отбирают пакеты, основываясь на IP-адресах, портах, заголовках, флагах, и на содержании пакета. Snort используется для активного блокирования или пассивного обнаружения целого ряда нападений и зондирований, таких как попытки атак на переполнение буфера, скрытое сканирование портов, атаки на веб-приложения, SMB-зондирование и попытки определения операционной системы.

*Suricata*<sup>1</sup> – COB с открытым исходным кодом, разработанная организацией «Open Information Security Foundation» в качестве многопоточной альтернативы Snort. Аналогично Snort, Suricata состоит из нескольких модулей (захвата, сбора, декодирования, обнаружения и вывода), по умолчанию до декодирования захваченный трафик идет одним потоком, что оптимально с точки зрения детектирования, но больше нагружает систему. В отличие от Snort настройками можно переопределять такое поведение и разделять потоки сразу после захвата, а также указывать как будут распределяться потоки по процессорам, что дает широкие возможности для оптимизации обработки трафика на конкретном оборудовании в конкретной сети. Изначально поддерживается декодирование IPv6, в том числе и туннели IPv4-in-IPv6, IPv6-in-IPv6, Teredo и др. Одним из преимуществ COB Suricata является обработка прикладного уровня OSI, что повышает её способность обнаруживать вредоносные программы для приложений.

Другими примерами систем обнаружения вторжений могут служить: **«Фортност»** (АО «РНТ»), **АПК «Аргус»** (ООО «Центр Специальной Системотехники»), **ПК «Ребус-COB»** (ЗАО «Научно-исследовательский институт “Центрпрограммсистем”»), **COB «Креchet»** (ФГУП «НПП «Гамма»), **PT Network Attack Discovery** (Positive Technologies) и др.

---

<sup>1</sup> [www.suricata-ids.org](http://www.suricata-ids.org)

## 5 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

### 5.1 Понятие вредоносного программного обеспечения

К угрозам безопасности информации относятся воздействия на вычислительную систему при помощи вредоносных программ, прямо или косвенно дезорганизующих процесс обработки информации или способствующих её утечке или искажению.

**Вредоносная программа** – компьютерная программа или переносимый код, предназначенные для повреждения информации, хранимой в компьютерной сети, скрытого использования компьютерных ресурсов или другого воздействия, нарушающего нормальные операции компьютерной системы [16].

Создание вредоносных программ может преследовать цель хищения кодов доступа к банковским счетам, рекламирования услуг или продуктов средствами компьютера жертвы, нелегального использования ресурсов зараженного компьютера для разработки и осуществления сетевых атак (DDoS-атак), шантажа и пр.

Приведем также определение из ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»:

*Вредоносная программа* – программа, используемая для осуществления НСД к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

В общем случае для вредоносных программы можно выделить ряд характерных функций, а именно:

- способность к самодублированию, ассоциированию себя с другими программами и/или перенос своих фрагментов в иные области оперативной или внешней памяти;
- искажение кода программ в оперативной памяти;
- выполнение без инициирования со стороны пользователя или пользовательской программы деструктивных функций (копирование, уничтожение, блокирование и т.д.);
- сохранение фрагментов информации из оперативной памяти в некоторых областях внешней памяти прямого доступа;
- искажение, блокирование или подмена выводимого во внешнюю память или в канал связи массива информации, образовавшегося в результате работы

прикладных программ, или уже находящиеся во внешней памяти массивы данных;

- скрытие признаков своего присутствия в программной среде компьютера.

Часто на практике понятие «вредоносная программа» отождествляется с понятием «компьютерный вирус», что обусловлено широким распространением последнего на заре популяризации компьютерной техники, однако компьютерный вирус относится лишь к одному из характерных видов вредоносных программ. В настоящее время вредоносные программы большей частью именно не вирусы, хотя такие термины как «вирус» и «заражение вирусом» применяются по отношению ко всем вредоносным программам.

## 5.2 Классификация вредоносного программного обеспечения

Существует большое число различных классификаций вредоносных программ. Приведем один из вариантов общей классификации (рис. 5.1).

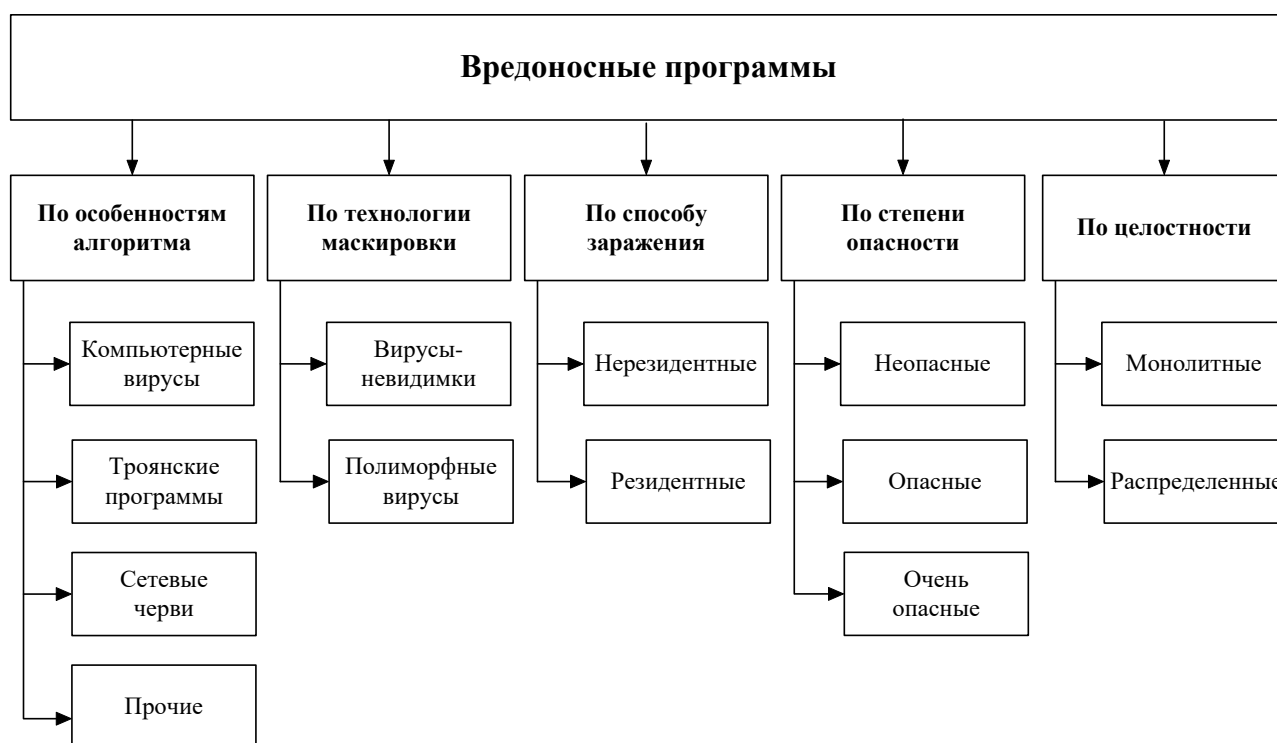


Рис. 5.1 – Общая классификация вредоносных программ.

Наиболее распространенными видами вредоносных программ, отличающимися *особенностями своего алгоритма*, поведением и назначением, являются:

- компьютерные вирусы;

- троянские программы;
- сетевые черви.

Приведем определения данных вредоносных программ согласно ГОСТ Р 57429-2017 «Судебная компьютерно-техническая экспертиза. Термины и определения» [9].

*Компьютерный вирус* – программа, обладающая способностью к самораспространению по локальным ресурсам средства вычислительной техники, не использующая сетевых сервисов.

*Троянская программа* – программа, не обладающая возможностью самораспространения, маскирующаяся под легитимный файл.

*Сетевой червь* – программа, обладающая способностью к самораспространению в компьютерных сетях через сетевые ресурсы.

При этом строгое разделение вредоносных программ практически невозможно, поскольку отдельные их виды часто выполняют и функции другого вида, а также потому, что вредоносные программы используют вспомогательные средства для скрывания своего присутствия и выполнения действий на инфицированной машине. Более подробно о них будет рассмотрено в следующем подразделе.

К числу *прочих вредоносных программ* относят разнообразные программы, не входящие в основные классы, но дающие возможность проникновения в удаленные компьютеры с целью дальнейшего управления ими (устанавливая на инфицированном компьютере потайной ход) или установки других вредоносных программ. Приведем некоторые примеры таких вредоносных программ.

*Потайной ход* или бэкдор (backdoor) – средство удаленного администрирования, позволяющее злоумышленнику обходить нормальный контроль безопасности входа и предоставляя доступ к компьютеру-жертве. Данное вредоносное программное обеспечение может быть также отнесено к троянским программам в силу особенности её установки. Установка потайного хода на машину-жертву может быть осуществлена в результате получения доступа к этой машине, путем автоматической установки сетевым червем или троянской программой или обусловлена заинтересованностью пользователя (методами социальной инженерии) в запуске программы, содержащей потайной ход. В зависимости от функциональных особенностей конкретного потайного хода злоумышленник может установить и запустить на компьютере жертвы любое программное обеспечение, сохранять все нажатия клавиш, загружать и сохранять любые файлы, включать микрофон или камеру и

пр. Часто используются для объединения группы компьютеров-жертв в ботнет или зомби-сеть для использования в криминальных целях.

*Руткит* (rootkit) – набор утилит (или специальный модуль ядра), скрытно действующих в зараженной системе и обладающих специальными средствами, затрудняющими их обнаружение системами безопасности. Этот набор, как правило, злоумышленник устанавливает на взломанной им компьютерной системе сразу после получения прав суперпользователя. Различают два их основных вида: руткиты уровня пользователя и руткиты уровня ядра. Первые обладают теми же правами, что и большинство приложений, вторые – полными правами доступа ко всем компонентам операционной системы. Руткиты могут использоваться для кражи персональных и банковских данных, быть элементом ботнета, а также применяться в качестве потайного хода для удаленного управления устройством.

*Шпионские программы* (spyware) – семейство программ, предназначенных для хищения персональных и конфиденциальных данных пользователя. Типичным представителем таких программ является клавиатурный шпион или кейлогер (keylogger), регистрирующий каждое нажатие клавиш на клавиатуре компьютера и пересылающий собранные данные своему хозяину.

*Рекламные программы* (adware) – программы, предназначенные для демонстрации рекламных сообщений, перенаправления запросов поиска на рекламные веб-сайты и сбора маркетинговой информации о владельце компьютера (например, на основании информации о посещенных пользователем сайтах, чтобы реклама соответствовала его интересам). Среди разновидностей рекламных программ – всплывающие рекламные объявления на веб-страницах и реклама, входящая в состав «бесплатного» программного обеспечения. Некоторые рекламные программы относительно безвредны, в других используются инструменты отслеживания для сбора информации о местонахождении пользователя или истории его посещения сайтов. Рекламные программы осуществляют сбор данных с согласия пользователя, в отличие от шпионских, собирающих информацию без его ведома.

*Программы-вымогатели* (ransomware) – программы, блокирующие доступ к компьютерной системе или предотвращающие считывание записанных в ней данных (с использованием методов шифрования) и последующим требованием от жертвы выкупа для восстановления исходного состояния. Технически такие программы представляют собой компьютерный вирус или сетевой червь с характерным для них способом заражения – из массовой рассылки при запуске исполняемого файла, либо при атаке через уязвимость в сетевой службе.

*Логическая бомба* (logic bomb) – программа, которая запускается при определённых временных или информационных условиях для осуществления вредоносных действий (как правило, искажения или удаления информации). Такие программы приводят к несообщённым заранее последствиям для пользователей. Многие вредоносные программы, например, вирусы или черви, часто содержат логические бомбы, которые срабатывают в заранее заданное время.

**По технологии маскировки** выделяют:

- вирусы-невидимки;
- полиморфные вирусы.

*Вирусы-невидимки* (stealth viruses) используют набор средств для маскировки своего присутствия путем перехвата обращения операционной системы к пораженным файлам или секторам и подставляют неинфицированный код. Например, файловый вирус может перехватывать функции чтения/записи в файл, чтение каталога и т.д., чтобы скрыть увеличение размера зараженных программ, перехватывает функции чтения/записи файла в память, чтобы скрыть факт изменения файла.

*Полиморфные вирусы* (polymorphic viruses) модифицируют свой код в зараженных программах таким образом, чтобы два экземпляра одного и того же вируса не могли совпадать ни в одном бите, что затрудняет анализ и обнаружение их антивирусом. Полиморфизм реализуется методами различного шифрования основного тела вируса и модификациями программы-расшифровщика. Такие вирусы также называют «полиморфики», вирусы-призраки, вирусы-мутанты.

**По способу заражения** выделяют: резидентное и нерезидентное вредоносное программное обеспечение.

Резидентное вредоносное программное обеспечение логически состоит из установщика (инсталлятора) и резидентного модуля. При запуске инфицированной программы управление получает установщик, который размещает резидентный модуль вредоносной программы в оперативной памяти и выполняет операции, необходимые для того, чтобы последний функционировал в ней постоянно. Он также подменяет некоторые обработчики прерываний, чтобы резидентный модуль мог получать управление при возникновении определенных событий.

Нерезидентное вредоносное программное обеспечение не заражает оперативную память и проявляет свою активность лишь однократно при запуске инфицированной программы.

**По степени опасности** вредоносные программы подразделяется на:

- неопасные, не влияющие на работу компьютера, кроме уменьшения памяти на диске в результате заражения файлов;
- опасные, приводящие к модификации инфицированных файлов или сбоям в работе компьютера;
- очень опасные, содержащие функции нанесения вреда (например, удаления файлов).

**По целостности** среди вредоносных программ можно выделить:

- монолитные, представляющие единый блок;
- распределенные, разделенные на части и содержащие инструкции с указанием как собрать их воедино для воссоздания вредоносной программы.

### **5.2.1 Компьютерные вирусы**

**Компьютерный вирус** (computer virus) – вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, и распространять среди них свои копии (необязательно совпадающие с оригиналом).

В зависимости от среды обитания компьютерные вирусы подразделяются:

- файловые;
- макровирусы;
- загрузочные.

**Файловые вирусы** (file infectors) относятся к вирусам-невидимкам и при своем размножении используют файловую систему операционной системы. Они внедряются в исполняемые файлы на компьютере (заражают их), дописывая самих себя в начало, середину или в конце файла. Дальнейшее их распространение осуществляется через зараженные файлы. Среди них по способу заражения выделяют: перезаписывающие вирусы, паразитические вирусы, компаньон-вирусы,

Перезаписывающие вирусы записывают свой код вместо кода заражаемого файла, уничтожая его содержимое. При этом файл перестает работать и не восстанавливается. Паразитические вирусы изменяют содержимое файлов, оставляя при этом сами файлы полностью или частично работоспособными. Компаньон-вирусы не изменяют зараженные файлы, а создают для него файл-двойник, которому при запуске зараженного файла

передается управление, или переименовывают заражаемый файл и запоминают его, а свой код записывают под его именем.

Файловые вирусы обнаруживаются, как правило, за счет увеличения размера исполняемых файлов, а также путем проверки целостности программ в момент их запуска, что применимо только для нерезидентных вирусов.

**Макровирусы** (macro viruses) также относятся к вирусам-невидимкам и являются программами на языках (макроязыках) встроенных в некоторые прикладные пакеты обработки данных (текстовые/графические/табличные редакторы, СУБД и пр.). Макросы – это процедуры, написанные на встроенном для таких прикладных пакетов языке программирования и выполняемые в ответ на определенные события (нажатие кнопки или открытие документа). Для своего размножения макровирусы используют возможности макроязыков и с их помощью переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макровирусы для прикладных пакетов Microsoft Office, содержащих в себе макроязыки Word Basic, Visual Basic for Applications.

Внедренный в документ соответствующего формата макровирус, запускающийся автоматически при его открытии, ищет другие доступные документы этого формата, внедряется в них и выполняет заложенные в него функции (возможностей современных макроязыков вполне хватает, чтобы содержать серьезные деструктивные функции).

Различные версии прикладных программ, поддерживающих макроязыки, как правило, предупреждают пользователя о наличии в документе макросов. Характерными признаками проявления макровирусов, например в Microsoft Word, являются: невозможность конвертирования зараженного документа Word в другой формат, появление файлов в формате Template (шаблон), невозможность записи документа в другой каталог или на другой диск по команде «Сохранить как» и т.п.

**Загрузочные вирусы** (boot viruses) тоже относятся к вирусам-невидимкам и предназначены для заражения носителей данных. Загрузочный вирус записывается в первый (нулевой) сектор гибкого или жёсткого диска, где обычно находится системный загрузчик. При загрузке операционной системы системный загрузчик считывает содержимое первого сектора диска, с которого производится загрузка, помещает считанную информацию в память и передает на неё (т.е. на вирус) управление. В дальнейшем загрузочный вирус ведет себя подобно файловому: перехватывает обращения операционной системы к дискам и инфицирует их, в зависимости от установленных условий совершает специальные действия (иногда деструктивные), может выполнять звуковые и видеоэффекты. Загрузочные вирусы

внедряются в память компьютера при загрузке с инфицированного диска, поэтому всегда являются резидентными. Размножается загрузочный вирус записью в загрузочную область других накопителей компьютера.

Классические загрузочные вирусы в настоящее время устарели, однако актуальна их вариация, распространяющаяся через флэш-накопители. Такой вирус представляет собой исполняемый файл с атрибутом «скрытый», который записывается в корневой каталог флэш-накопителя либо в скрытую папку, эмулирующую корзину Windows, либо другую системную папку. В корневом каталоге размещается файл autorun.inf со ссылкой на вирус. Вирус активируется, если у флэш-накопителя срабатывает автозапуск при условии, что настройки Windows установлены по умолчанию. Вирус оставляет свои копии (вместе с autorun.inf) на всех разделах жесткого диска и, таким образом, получает управление во время каждого сеанса работы пользователя, когда тот случайно активирует автозапуск на одном из этих разделов. Далее вирус постоянно находится в оперативной памяти, выполняет свои функции, а также отслеживает подключение к компьютеру новых переносных носителей и заражает их.

Другой разновидностью вредоносных программ, использующих те же технологии заражения дисков, что и загрузочные вирусы, являются так называемые буткиты. *Буткит* (bootkit) представляет собой разновидность руткита, который загружается из главной загрузочной записи (Master Boot Record, MBR) или загрузочного сектора перед загрузкой операционной системы. В связи с этим их также называют MBR-руткиты. Они предназначены для срабатывания в начале загрузки компьютера с целью управления всеми этапами запуска операционной системы, изменения системного кода и драйверов до загрузки антивирусных программ и других компонентов безопасности.

### 5.2.2 Троянские программы

**Троянская программа** (trojan) – вредоносная программа, не имеющая способности к самовоспроизведению, которая маскируется под полезную программу и вместе с тем содержит скрытую вредоносную функцию. Троянская программа также наиболее известна под названием «троянский конь», «троян» или просто «троянец».

В отличие от компьютерных вирусов и сетевых червей, которые распространяются самопроизвольно, распространение троянских программ происходит посредством самих пользователей. Они могут быть непосредственно загружены в компьютерную систему злоумышленниками внутренними сотрудниками организации, так и побуждать пользователей загружать и/или запускать их в своих системах. Как правило, данные

программы маскируются под другие типы файлов – от пакетов установщиков до мультимедийных данных. Троянская программа может имитировать имя и иконку существующей, несуществующей, или просто привлекательной программы, компонента, или файла данных, как для запуска пользователем, так и для маскировки в системе своего присутствия. Троянская программа может в той или иной мере имитировать или даже полноценно выполнять задачу, под которую она маскируется (в последнем случае вредоносный код встраивается злоумышленником в существующую программу).

После своего запуска троянская программа удаляет себя из файла-носителя и принимает меры к обеспечению своей выживаемости при перезагрузке и к постоянному функционированию на компьютере, применяя различные методы маскировки от обнаружения. Таким образом, троянский конь существует на инфицированном компьютере в одном экземпляре и является постоянно выполняющимся процессом.

Действия троянского коня могут включать: удаление, блокирование, изменение, копирование данных, замедление работы компьютеров и компьютерных сетей.

Троянские программы классифицируются в соответствии с типом действий, выполняемых ими на компьютере. Приведем их классификацию согласно «Лаборатории Касперского» [28].

***Trojan-Banker.*** Предназначены для кражи учетных данных систем интернет-банкинга, систем электронных платежей и кредитных или дебетовых карт.

***Trojan-DDoS.*** Служат для проведения удаленных атак типа «отказ в обслуживании» с инфицированной машины по целевым веб-адресам. При такой атаке с зараженных компьютеров системе с определенным адресом отправляется большое количество запросов, что может вызвать ее перегрузку и привести к отказу в обслуживании.

***Trojan-Downloader.*** Программы для загрузки и установки на инфицированный компьютер новых версий вредоносных программ, включая троянские и рекламные программы.

***Trojan-Dropper.*** Предназначены для установки троянских программ и/или вирусов или предотвращения обнаружения вредоносных программ.

***Trojan-FakeAV.*** Имитируют работу антивирусного программного обеспечения. Предназначены для вымогания у пользователя денежных средств в обмен на обещание обнаружения и удаления угроз, в действительности не существующих.

***Trojan-Game Thief.*** Программы для кражи информации об учетных записях участников сетевых игр.

**Trojan-IM.** Служат для хищения логинов и паролей к программам мгновенного обмена сообщениями, таких как Skype, ICQ, Агент Mail.ru и др.

**Trojan-Ransom.** Предназначены для модификации (обычно с применением шифрования) данных на инфицированной машине, например блокировки, и требованием выкупа за возврат операционной системы к рабочему состоянию.

**Trojan-SMS.** Служат для несанкционированной с пользователем рассылки SMS-сообщений с инфицированных мобильных устройств на платные номера, записанные в теле вредоносной программы.

**Trojan-Spy** (шпионские программы). Предназначены для скрытого наблюдения за использованием компьютера, например, отслеживая вводимые с клавиатуры данные, делая снимки экрана и получая список работающих приложений.

**Trojan-Mailfinder.** Программы, собирающие адреса из почтовой службы пользователя и пересылающие их злоумышленнику с целью, например, последующей рассылки спама.

**Trojan-ArcBomb** – архивы, специально сформированные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные – зависание или существенное замедление работы компьютера или заполнение диска большим количеством «пустых» данных.

**Trojan-Clicker.** Предназначены для обращения к целевым интернет-ресурсам, что достигается либо передачей соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса сайтов.

**Trojan-Notifier.** Отправляют злоумышленнику сигнал (электронным письмом, обращением к веб-странице злоумышленника, сообщением в мессенджере), что зараженное устройство подключено к сети. При этом в сообщении содержится информация о компьютере или мобильных устройств и его владельце. Подобные троянские программы используют в многокомпонентных троянских наборах для извещения злоумышленника о закреплении вредоносных программ в атакуемой системе.

**Trojan-Proxy.** Предназначены для осуществления злоумышленником несанкционированного пользователем анонимного доступа к различным интернет-ресурсам через компьютер-жертву.

**Trojan-PSW.** Служат для хищения пользовательских аккаунтов (логин и пароль) с зараженных компьютеров.

Также к отдельным видам троянских программ можно отнести потайные ходы, эксплойты и руткиты.

**Backdoors** (потайные ходы). Предоставляет злоумышленникам возможность удаленного управления зараженными компьютерами: позволяют автору выполнять на зараженном компьютере любые действия, включая отправку, получение, открытие и удаление файлов, отображение данных и перезагрузку компьютера.

**Exploits** (эксплойты). Содержат данные или исполняемый код, способный воспользоваться одной или несколькими уязвимостями в программном обеспечении на локальном или удаленном компьютере.

**Rootkits** (руткиты). Предназначены для сокрытия в системе определенных объектов или действий. Часто основная их цель – предотвратить обнаружение вредоносных программ, чтобы увеличить время работы этих программ на зараженном компьютере.

### 5.2.3 Сетевые черви

**Сетевые черви** (computer worms) – вредоносные программы, самостоятельно распространяющиеся через локальные и глобальные компьютерные сети, для НСД к системе. Наряду с наименованием «сетевые черви» их также называют просто «черви» или «сетевые вирусы».

В отличие от компьютерных вирусов они не могут заражать существующие файлы, однако могут кооперироваться с вирусами в результате чего самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса).

Большинство сетевых червей являются резидентными. Как правило, они содержат «инфекционную часть» – эксплойт (шелл-код) и тело червя («полезная нагрузка»), полностью находящегося в оперативной памяти, поэтому могут заражать только ранее загруженные другими программами динамические библиотеки.

Основным принципом работы таких программ является уникальная возможность самостоятельно передать свой код на рабочую станцию или удаленный сервер. Они имеют два основных механизма проникновения на компьютер:

- 1) через стандартные коммуникационные сервисы;
- 2) через уязвимости в популярных сетевых приложениях, в том числе самой операционной системе.

В роли стандартного коммуникационного сервиса чаще всего выступает электронная почта, где вирус распространяется в виде прикрепленного к электронному письму файлового вложения, которое пользователи могут запустить, например, спровоцированные средствами социальной инженерии.

Второй механизм заражения – ошибки в сетевых программах, позволяющие вредоносной программе проникать на компьютер пользователя и получать на нем управление без каких-либо действий со стороны самого пользователя. В этом случае единственный способ противостоять подобным вирусам – своевременная разработка и установка обновлений.

Кратко рассмотрим основные механизмы сетевого червя.

1. Выбор цели. Осуществляется по заранее подготовленным спискам сетевых адресов, почтовых адресов из адресной книги, сетевых соседей, доверенных систем, либо по случайному выбору адреса, запросам DNS.

2. Поиск уязвимости. Проводится сканирование цели, идентификация операционной системы и прикладного программного обеспечения, посылка пакетов, использующих уязвимость.

3. Проникновение. Код использует известную злоумышленнику уязвимость (переполнение буфера, совместное использование файлов, посылка электронной почты с приложением, использование ошибок конфигурирования и т.д.).

4. Распространение. После получения доступа к машине необходимо получить основное тело червя, для чего используются протоколы HTTP, SMB и др.

5. «Полезная нагрузка» (набор кодов, разработанных для выполнения определенных действий в интересах злоумышленника на целевой машине). Среди некоторых видов «полезной нагрузки» сетевого червя: установка потайного хода, установка бота, программы выполнения сложных математических операций, установка троянского коня и т.п.

Приведем классификацию сетевых червей представляемую «Лабораторией Касперского» [29].

**Email-Worm** – сетевые черви, использующие для распространения почтовые системы. В процессе распространения червь отправляет либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе.

**IM-Worm** – черви способные к саморазмножению в системах мгновенного обмена сообщениями, таких как Facebook Messenger, Skype или WhatsApp. Для этих целей черви, как правило, рассылают контактам жертвы сообщения, содержащие URL-ссылку на файл с телом червя, что практически полностью повторяет способ рассылки, использующий Email-Worm.

**IRC-Worm** – черви, обладающие способностью к несанкционированному пользователем саморазмножению через IRC (Internet Relay Chats) – протокол прикладного уровня для обмена сообщениями в режиме реального времени. Способы распространения по

IRC-каналам аналогичны Email-Worm и IM-Worm – либо через отсылку URL-ссылки на копию червя, либо через отсылку зараженного файла какому-либо пользователю IRC-канала.

**Net-Worm** – сетевые черви, использующие для распространения стек протоколов TCP/IP. Отличительной особенностью данного типа червей является отсутствие необходимости в пользователе как в звене в цепочке распространения для активации вредоносной программы. Принцип его распространения посредством критических уязвимостей программного обеспечения описан ранее.

**P2P-Worm** – сетевые черви, обладающая способностью к несанкционированному пользователем саморазмножению по каналам файлообменных одноранговых (пиринговых) сетей. Механизм внедрения в P2P-сеть большинства подобных червей состоит в их самокопировании в каталог обмена файлами, который обычно расположен на локальной машине. Всю последующую работу по распространению вируса одноранговая сеть берет на себя – при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера. Более сложные P2P-черви имитируют сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечают положительно – при этом червь предлагает для скачивания свою копию.

**Worm** – сетевые черви, не попавшие в предыдущие категории, поскольку по тем или иным причинам не обладают ни одним из других поведений. В отличие от Net-Worm для активации Worm пользователю необходимо его запустить.

В развитии современных сетевых червей можно выделить некоторые тенденции:

- кроссплатформенность;
- использование множества уязвимостей, в том числе «уязвимостей нулевого дня» (т.е. ещё неизвестных и неустранённых уязвимостей);
- принятие специальных мер для увеличения начальной скорости распространения (заранее подготовленных списков адресов, сразу несколько эксплойтов для своего распространения и т.п.);
- наличие модулей обхода или блокировки средств защиты;
- изощренные методы маскировки присутствия и выполнения.

### 5.3 Наименование вредоносного программного обеспечения

Исторически сложилось так, что практически все вредоносные программы имеют свои имена. Общепринятым является подход, когда имя вредоносной программы строится по следующему правилу:

#### *Префикс.Имя.Суффикс*

Поле «Префикс» обозначает платформу распространения вредоносной программы или её тип. Поле «Имя» извлекается из тела вредоносной программы. Поле «Суффикс» предназначено для различения вариантов вредоносных программ одного семейства.

В настоящее время компания «Лаборатория Касперского» установила следующую систему наименования вредоносных программ, структура которой выглядит как:

#### *Поведение. Платформа. Имя. [Вариант]*

Поле «Поведение» устанавливает вид детектируемого объекта по его поведению. Для вирусов и червей поведение определяется по способу распространения, троянских программ и вредоносных утилит – по совершаемым ими действиям, потенциально опасных программ – по функциональному назначению детектируемого объекта. Для отдельных видов поведения может указываться тип поведения, который записывается через дефис, например: P2P-Worm, Net-Worm, Trojan-Downloader.

Поле «Платформа» определяет среду выполнения программного кода. Платформа может быть как программной, так и аппаратной. Если детектируемый объект использует множество платформ, то реализуется платформа с наименованием Multi. Примеры платформ: Win32, BAT, IRC и т.п.

Поле «Имя» используется для названия детектируемого объекта или его семейства. Если объект не подпадает под известные семейства, то ему приписывается обобщенное имя, например Trojan.Win32.Dialer. Имя обычно дается, исходя из текстовых строк, присутствующих в детектируемом объекте.

Поле «Вариант» может отсутствовать, если это единственный экземпляр (первый образец объекта). Обычно данное поле содержит буквы, начиная с *a* до *z*, далее с *aa* до *zz* и т.д.

Поскольку имя дает антивирусная компания, получившая экземпляр инфицированного файла, то часто одно и тот же вредоносное программное обеспечение имеет разные наименования.

## **5.4 Методы и средства защиты от вредоносных программ**

### **5.4.1 Признаки возможного заражения**

Большинство современных вредоносных программ не оставляет явных следов своего присутствия. Тем не менее можно выделить некоторые признаки возможного заражения компьютера:

- снижение производительности – процессы происходят медленнее, загрузка окон занимает больше времени, в фоновом режиме работают посторонние программы;
- изменение домашних интернет-страниц в браузере или более частое, чем обычно, появление всплывающих объявлений;
- компьютер перестает реагировать на клавиатуру или периодически блокирует ее работу;
- отображение в искаженном виде меню и диалоговых окон;
- невозможность запуска антивирусной программы или получения для нее обновлений;
- появление на рабочем столе новых ярлыков или исчезновение некоторых программ и приложений.

В некоторых случаях вредоносные программы могут влиять на базовые функции компьютера: не запускается операционная система, нет подключения к Интернету или доступа к более высокоуровневым функциям управления системой.

Настораживающим признаком может считаться самопроизвольные перезагрузки компьютера и необычные сообщения об ошибках, в том числе появление критической ошибки синего экрана смерти. Однако такое поведение компьютера также может быть вызвано ошибками аппаратного или программного обеспечения.

Приведенные признаки при функционирующем антивирусном программном обеспечении свидетельствуют о том, что компьютер инфицирован ещё неизвестным вирусом. Интервал возможного заражения компьютера пользователя новым видом вредоносной программы может составлять до нескольких дней и даже недель. Антивирусные средства обеспечивают защиту от уже известных вредоносных программ и их вариантов, а в некоторых случаях и от новых вирусов.

### 5.4.2 Методы обнаружения вредоносных программ

Для обнаружения и защиты от вредоносных программ применяют специальные средства антивирусной защиты, также называемые антивирусами или антивирусным программным обеспечением.

**Антивирусное программное обеспечение** (anti-virus software) – специализированное программное обеспечение для обнаружения нежелательных программ, восстановления измененных такими программами файлов, а также для предотвращения изменения такими программами файлов или операционной системы [9].

В современных антивирусных продуктах выделяют два основных подхода к обнаружению вредоносных программ:

- реактивная защита (сигнатурный метод);
- проактивная защита.

**Реактивная защита** подразумевает обнаружение вредоносных программ на основе *сигнатурного анализа* – сравнения файла с известными образцами вирусов. Сигнатурой вируса считается совокупность черт (фрагментов кода), позволяющих однозначно идентифицировать наличие вирусов в файле.

Основной принцип, по которому выделяются сигнатуры – она должна содержать только уникальные строки из этого файла, настолько характерные, чтобы гарантировать минимальную возможность ложного срабатывания. Все вместе сигнатуры известных вредоносных программ составляют *антивирусную базу*. Эта технология предполагает непрерывное отслеживание новых экземпляров вредителей, их описание и включение в базу сигнатур. Задача выделения сигнатур, как правило, решается экспертами в области компьютерной вирусологии, способными выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска.

Каждое антивирусное программное обеспечение имеет обширную базу сигнатур, которая регулярно обновляется. Антивирусные базы в разных антивирусах отличаются, однако между антивирусными компаниями существует договоренность об обмене образцами вирусов, в связи с чем сигнатура нового вируса рано или поздно попадает в антивирусные базы практически всех антивирусов. Из этого с высокой долей уверенности можно считать, что антивирусные базы наиболее известных антивирусов эквивалентны.

Достоинством сигнатурного метода является точное и гарантированное определение типа вируса, что позволяет занести в базу не только сами сигнатуры, но и способы «лечения» вируса. Среди недостатков выделяют их беззащитность перед шифрующимися или

полиморфными вирусами, способными полностью изменять свой код при заражении новой программы или загрузочного сектора. В связи с этим появляется задержка при реакции на новые угрозы, связанная со временем, необходимым на получение сигнатуры, что в свою очередь возможно только после получения образца нового вируса. При этом создание сигнатуры и её доставка пользователям может занимать от нескольких часов до нескольких дней, что несоизмеримо со скоростью распространения нового вируса по глобальной сети. Таким образом, способы реактивной защиты обеспечивают безопасность преимущественно только от уже известных вредоносных программ и их вариантов.

**Проактивная защита** основана на выявлении неуникальных особенностей кода и поведения, характерных для вредоносных программ, с целью предотвращения заражения системы. Методы проактивной защиты интегрируются практически во все современные антивирусные программы, на их основе создаются новые антивирусные системы, комбинирующие несколько методов проактивной защиты и позволяющие обнаруживать новые вредоносные программы.

Проактивные методы защиты относятся к приблизительным методам обнаружения вредоносных программ, позволяющим с определенной вероятностью предположить заражение файла.

Наиболее применимы следующие методы проактивной защиты:

- эвристический анализ;
- эмуляция;
- песочница;
- поведенческий анализ;
- метод обнаружения изменений.

**Эвристический анализ** – метод анализа программного кода выполняемого приложения, скрипта или макроса на основе эвристик с целью обнаружения участков кода, отвечающих за вредоносную активность.

Эвристика – тип аналитического компонента защиты, использующий знания, полученные от экспертов при решении заданных проблем. Суть эвристических методов состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок. Если сигнатурный анализ основан на выделении характерных признаков вредоносной программы и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на предположении, что новые вирусы часто оказываются похожи на какие-либо из уже

известных. Такое предположение оправдывается наличием в антивирусных базах сигнатур для определения не одного, а сразу нескольких вирусов.

Эвристический анализ, совместно с сигнатурным, позволяет в ряде случаев распознавать модифицированные версии вируса, когда его сигнатура не совпадает с телом неизвестной программы, но присутствуют более общие признаки вируса, например, в виде подозрительных команд. Такая разновидность эвристического анализа называется *статическим эвристическим анализом* (поиском вирусов, похожих на известные).

Особенностью статического эвристического анализатора является простота его реализации и высокая скорость работы, а также возможность обнаружения полиморфных вирусов. При этом уровень обнаружения новых вредоносных кодов остается довольно низким, а вероятность ложных срабатываний достаточно высокой.

**Эмуляция** – метод выявления неизвестных угроз, при котором подозрительное приложение запускается в виртуальной копии компьютера, имитирующей поведение операционной системы и центрального процессора. Такой подход позволяет средству защиты наблюдать за поведением программы «на лету», не ставя под угрозу операционную систему и данные пользователя, а при обнаружении опасных действий блокировать его для проведения дополнительных исследований.

Несмотря на кажущуюся эффективность данного подхода, он также не лишен недостатков – эмуляция требует временных затрат и вычислительных ресурсов, что негативно сказывается на быстродействии при выполнении повседневных операций. За счет этого современные вредоносные программы способны обнаруживать свое присутствие в эмулированной среде и прекращать выполнение вредоносных функций.

Технология эмуляции является промежуточной ступенью между обработкой программы как набора байт и обработкой программы как определенной последовательности действий.

**Песочница** (Sandbox) – это система для выявления вредоносных программ, при использовании которой подозрительный объект запускается в виртуальной машине с полнофункциональной операционной системой, а для обнаружения зловредности объекта применяется анализ его поведения. Данная технология также иногда называется *динамическим эвристическим анализом*.

В отличие от технологии эмуляции, которая предоставляет среду для исполнения программы и в процессе работы «содержит» программу и полностью управляет ею, в песочнице в качестве среды уже выступает сама операционная система, а её технология лишь контролирует взаимодействие между операционной системой и программой, находясь

с ней на равных. Таким образом, песочница представляет собой логическое продолжение эмуляции, поскольку уже работает с исполняющейся в реальной среде программой, но все еще ее контролирует, ограничивая в правах доступа к критическим системным файлам, веткам реестра и другой важной информации. При этом если исследуемый объект выполняет вредоносные действия, песочница признает его вредоносной программой и блокирует.

Анализ поведения объекта в процессе его выполнения в песочнице позволяет эффективно бороться с теми вредоносными программами, которые способны обмануть статический анализ, но при этом также как и эмулятор, является ресурсоемкой технологией.

**Поведенческий анализ** – метод контроля активности программного обеспечения, основанный на мониторинге выполняемых им операций и блокировке выполнения потенциально опасных действий, осуществляемых без ведома пользователя.

К основным видам потенциально опасных действий относятся: удаление файла, запись в файл, запись в определенные области системного реестра, открытие порта на прослушивание, перехват вводимых с клавиатуры данных, рассылка писем и т.п. Технология поведенческого анализа позволяет оценивать не только единичное действие, но и цепочку действий, что многократно повышает эффективность противодействия вирусным угрозам. Также, поведенческий анализ является технологической основой для целого класса программ – поведенческих блокираторов.

В отличие от динамических эвристических анализаторов, где подозрительные действия отслеживаются в режиме виртуализации, поведенческие блокираторы работают в реальных условиях. Современные поведенческие блокираторы способны контролировать широкий спектр событий, происходящих в системе – анализ поведения всех запущенных процессов, сохранение изменений, производимых в файловой системе и реестре и пр. Таким образом, поведенческий блокиратор может предотвратить распространение как известного, так и неизвестного вируса, что является его достоинством. Вместе с тем его недостатком остается срабатывание на действия ряда легитимных программ. При этом принятие окончательного результата о вредоносности приложения требует участия пользователя, что предполагает наличие у него достаточной квалификации.

**Метод обнаружения изменений** (контроль целостности) осуществляет постоянный мониторинг ядра операционной системы на предмет выявления изменений, которые могло произвести вредоносное программное обеспечение.

Метод предполагает запись в специальных файлах образа главной загрузочной записи, загрузочных секторов логических дисков, параметров всех контролируемых файлов, а также информации о структуре каталогов и номера плохих кластеров дисков. В случае

обнаружения изменений внесенных вредоносной программой об этом оповещается пользователь и по возможности производится откат действий, произведенных вредоносным программным обеспечением.

Преимуществом метода является кроссплатформенность, малое количество обращений к пользователю, а также отсутствие со стороны последнего специальных знаний и навыков. Недостатком – необходимость контроля большого количества различных параметров, что может негативно сказаться на производительности компьютера, а также невозможность противодействия стадии активного заражения.

В настоящее время проактивные технологии являются важным и неотъемлемым компонентом антивирусного программного обеспечения. Более того, как правило, в антивирусных продуктах используется сочетание сразу нескольких технологий проактивной защиты, например эвристический анализ и эмуляция успешно сочетаются с поведенческим анализом, что позволяет многократно повысить эффективность современных антивирусных комплексов против новых, все более изощренных вредоносных программ.

Наряду с рассмотренными методами антивирусной защиты информации существует также так называемый метод «белого списка».

**Метод «белого списка»** (whitelist) представляет собой общую технологию по борьбе с вредоносными программами, основанную на предотвращении выполнения всех компьютерных кодов за исключением тех, которые были ранее обозначены системным администратором как безопасные, т.е. были добавлены в список доверенных (белый список).

Такой способ составления белых списков подходит крупным компаниям с централизованной ИТ-инфраструктурой, поскольку в них всегда есть лицо, принимающее решение, а список используемых приложений, как правило, хорошо известен, сравнительно короток и редко меняется.

Для индивидуальных пользователей невозможно точно предсказать, какое приложение и в какой момент может потребоваться. В этом случае некоторые средства антивирусной защиты информации предлагают динамически обновляемый белый список пользовательских приложений на базе облачной технологии, представляющий собой постоянно обновляемую базу знаний существующих приложений, в том числе популярных программ, офисных пакетов, браузеров, программ просмотра изображений и т.п. В связи с этим метод «белого списка» в ряде случаев также называется *методом проверки репутации* приложений до их запуска.

Например, «Лаборатория Касперского» предоставляет технологию «Доверенные приложения» (Whitelist Security Approach), включающую динамически обновляемый белый

список разнообразных программ, отобранных по результатам тестирования данных, полученных через сеть Kaspersky Security Network – облачную инфраструктуру, предназначенную для интеллектуальной обработки потоков данных, связанных с киберугрозами, добровольно предоставляемых многочисленными пользователями.

#### 5.4.3 Виды антивирусных программ

Среди антивирусных программ по выполняемым ими функциям различают следующие виды:

- программы-сканеры;
- программы-доктора (фаги);
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины.

**Программы-сканеры** (детекторы) осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Некоторые программы-сканеры снабжаются блоками эвристического анализа.

**Программы-доктора** или фаги помимо нахождения зараженных файлов, также «лечат» их, удаляя из файла вредоносный код, возвращая их в исходное состояние. Среди фагов выделяют также полифаги – программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Для эффективного использования и программ-сканеров, и программ-докторов необходимо регулярно обновлять базы данных сигнатур.

**Программы-ревизоры** предназначены для поиска обнаружения изменений. Они анализируют текущее состояние файлов и системных областей диска и периодически сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние загрузочного сектора, FAT-таблицы, а также длина файлов, их время создания, атрибуты, контрольные суммы. Программы-ревизоры потенциально могут обнаружить любые компьютерные вирусы, даже те, которые ранее были неизвестны. Дополнительной их возможностью является способность восстановления инфицированных файлов и загрузочных секторов путем использования ранее запомненной информации.

**Программы-фильтры** (блокировщики) представляют собой небольшие резидентные программы, предназначенные для мониторинга подозрительных действий при работе компьютера, характерных для размножения вредоносных программ: обновление

программных файлов и системной области диска, форматирование диска, резидентное размещение программ в оперативной памяти и т.п. При попытке какой-либо программы произвести указанные действия фильтр посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. К достоинствам программ-фильтров относится их способность обнаруживать и останавливать распространение вредоносных программ на самой ранней стадии их размножения, что полезно в случаях появления известного вируса. Однако такие программы не «лечат» файлы и диски, для чего требуется применение программ-докторов.

**Программы-вакцины** или иммунизаторы – резидентные программы, предотвращающие заражение файлов. Вакцины делятся на два типа: сообщающие о заражении и блокирующие заражение определенным типом известного вируса. Вакцинация первого типа состоит в записи в конец файла специального модуля контроля, следящего за его целостностью. Вакцинация второго типа состоит в модификации программы или диска таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. Такой тип вакцинации не может быть универсальным, поскольку нельзя вакцинировать все файлы от известных вирусов. Программы-вакцины применяют, если отсутствуют программы-доктора, «лечащие» от вируса.

Современные антивирусы представляют собой многофункциональные программные комплексы, которые способны обнаруживать, «лечить» (удалять) вирусы, а также препятствовать их проникновению на компьютер. При этом они могут работать в двух режимах: в режиме монитора и в режиме сканера.

В *режиме монитора* антивирус функционирует непрерывно, отслеживая все обращения системы к файлам и проверяя эти файлы на предмет заражения. Таким образом, при первой попытке вируса активироваться антивирус блокирует эту попытку и выдает предупреждение. Поскольку часть вычислительных ресурсов тратится на работу антивируса, а любое обращение к файлам и некоторым другим объектам сопровождается процедурой сканирования, то при использовании этого режима работа компьютера замедляется. Особенностью данного режима также является то, что если на компьютере присутствуют зараженные файлы, которые не проявляют активности и обращения к ним не происходит, они остаются незамеченными.

В *режиме сканера* антивирус проверяет все файлы в заданной области (определенный каталог, раздел жесткого диска или все устройства хранения информации) и «лечит» (удаляет) зараженные, либо оповещает о них. Проверка всех данных при этом может занять значительное время.

Для повышения безопасности рекомендуется применение обоих режимов: постоянная работа антивируса в режиме монитора и периодическая проверка всех данных с помощью сканирования.

В корпоративных сетях защита от вредоносных программ не ограничивается лишь традиционной установкой средств антивирусной защиты на рабочие станции пользователей, а требует комплексного подхода, а именно рассмотрение подсистемы защиты корпоративной информации как многоуровневой системы. Первый уровень включает в себя средства защиты от вредоносных программ, совместимые с межсетевым экраном, устанавливаемом на стыке с глобальными сетями. Второй уровень – средства защиты, устанавливаемые на внутренних корпоративных серверах и серверах рабочих групп (файловых хранилищах, серверах приложений и т.д.). Третий уровень – средства антивирусной защиты информации, устанавливаемые на рабочих станциях пользователей, в том числе удаленных и мобильных.

### **5.5 Классификация защищенности средств антивирусной защиты информации**

С 2012 года ФСТЭК России утверждены требования к средствам антивирусной защиты информации, включающие общие требования к средствам антивирусной защиты и требования к функциям безопасности средств антивирусной защиты. Данные требования применяются к программным средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом.

Для дифференциации требований к функциям безопасности средств антивирусной защиты установлено 6 классов защиты антивирусных средств. Самый низкий класс – шестой, самый высокий – первый. Данная система классификации аналогична системам обнаружения вторжений и приведена на рис. 5.2.

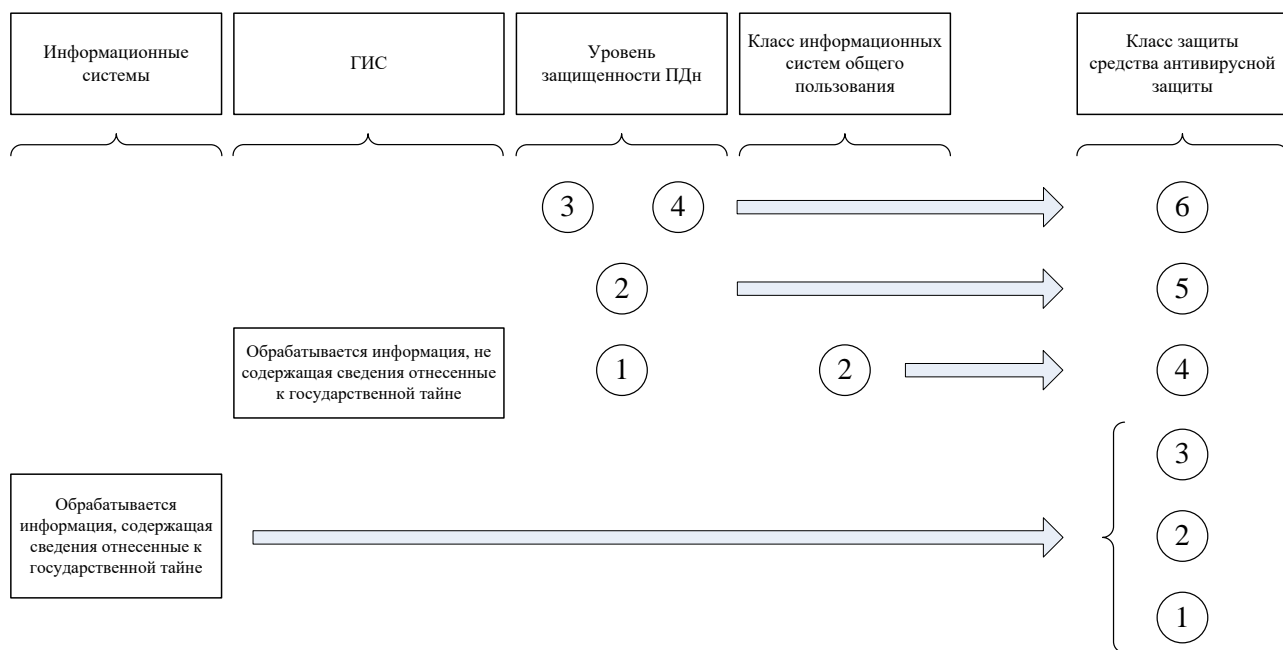


Рис. 5.2 – Классы защиты средств антивирусной защиты информации.

Средства антивирусной защиты, соответствующие 6 классу защиты, применяются в ИСПДн 3 и 4 классов.

Средства антивирусной защиты, соответствующие 5 классу защиты, применяются в ИСПДн 2 класса.

Средства антивирусной защиты, соответствующие 4 классу защиты, применяются в ГИС, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в ИСПДн 1 класса, а также в информационных системах общего пользования II класса.

Средства антивирусной защиты, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Детализация требований к функциям безопасности средств антивирусной защиты, а также взаимосвязи этих требований приведены для каждого класса и типа средств антивирусной защиты в профилях защиты, утвержденных ФСТЭК России в качестве методических документов.

Согласно спецификации профилей защиты выделяют средства антивирусной защиты (компоненты средств антивирусной защиты) следующих типов:

- *тип А* – средства антивирусной защиты, предназначенные для централизованного администрирования средствами антивирусной защиты,

установленными на компонентах информационных систем (серверах, автоматизированных рабочих местах);

- *тип Б* – средства антивирусной защиты, предназначенные для применения на серверах информационных систем;
- *тип В* – средства антивирусной защиты, предназначенные для применения на автоматизированных рабочих местах информационных систем;
- *тип Г* – средства антивирусной защиты, предназначенные для применения на автономных автоматизированных рабочих местах.

Средства антивирусной защиты типа А не применяются в информационных системах самостоятельно и предназначены для использования только совместно со средствами антивирусной защиты типов Б и/или В.

Идентификаторы профилей защиты представляются формате «ИТ.САВЗ.тип/класс.ПЗ», где ИТ – «информационная технология», САВЗ – «средство антивирусной защиты», ПЗ – «профиль защиты». Спецификация профилей защиты систем обнаружения вторжений для каждого их типа и класса защиты приведена в таблице 5.1.

Таблица 5.1 – Идентификаторы профилей защиты средств антивирусной защиты

Тип средства антивирусной защиты	Класс защиты					
	6	5	4	3	2	1
тип «А»	ИТ.САВЗ.А6.ПЗ	ИТ.САВЗ.А5.ПЗ	ИТ.САВЗ.А4.ПЗ	ИТ.САВЗ.А3.ПЗ	ИТ.САВЗ.А2.ПЗ	ИТ.САВЗ.А1.ПЗ
тип «Б»	ИТ.САВЗ.Б6.ПЗ	ИТ.САВЗ.Б5.ПЗ	ИТ.САВЗ.Б4.ПЗ	ИТ.САВЗ.Б3.ПЗ	ИТ.САВЗ.Б2.ПЗ	ИТ.САВЗ.Б1.ПЗ
тип «В»	ИТ.САВЗ.В6.ПЗ	ИТ.САВЗ.В5.ПЗ	ИТ.САВЗ.В4.ПЗ	ИТ.САВЗ.В3.ПЗ	ИТ.САВЗ.В2.ПЗ	ИТ.САВЗ.В1.ПЗ
тип «Г»	ИТ.САВЗ.Г6.ПЗ	ИТ.САВЗ.Г5.ПЗ	ИТ.САВЗ.Г4.ПЗ	ИТ.САВЗ.Г3.ПЗ	ИТ.САВЗ.Г2.ПЗ	ИТ.САВЗ.Г1.ПЗ

## 5.6 Антивирусные программы и комплексы

Приведем примеры некоторых популярных средств антивирусной защиты.

**Kaspersky**<sup>1</sup> – комплексное программное средство антивирусной защиты информации, разработанное международной компанией АО «Лаборатория Касперского», включающее в себя многочисленные решения для защиты как отдельных пользователей, так и корпоративных сетей любого масштаба, в том числе защиты конечных устройств (Endpoint Protection) – **Kaspersky Endpoint Security**. Kaspersky Endpoint Security для Windows

<sup>1</sup> [www.kaspersky.ru](http://www.kaspersky.ru)

соответствует требованиям ФСТЭК к средствам антивирусной защиты типа Б, В, Г второго класса защиты (ИТ.САВЗ.Б2.ПЗ, ИТ.САВЗ.В2.ПЗ, ИТ.САВЗ.Г2.ПЗ).

Обеспечивает многоуровневую защиту компьютеров и ноутбуков под управлением Windows в локальной сети организации посредством:

- проактивной борьбы с угрозами, включающей обнаружение и блокирование вредоносного программного обеспечения, анализа поведения программ, контроля приложений и сетевой активности на основе персонального межсетевого экрана и системы предотвращения вторжений;
- контроля программ с помощью динамических белых списков и ограничения прав доступа программ к выбранным файлам и ресурсам;
- веб-контроля доступа к ресурсам сети Интернет;
- контроля внешних устройств.

Инструмент централизованного управления защитой в локальной сети организации позволяет удаленно устанавливать антивирусное решение на рабочие станции, выполнять настройку параметров защиты для компьютеров сети, управлять обновлениями программного обеспечения и антивирусных баз, контролировать статус защиты.

Расширенные пакеты Kaspersky Endpoint Security также обладают технологией полного шифрования диска (FDE) и шифрования файлов (FLE) для безопасной передачи данных, и обеспечивают функции управления и контроля для всех типов конечных точек – как виртуальных, так и физических.

В многочисленную линейку продуктов от «Лаборатории Касперского» также входит множество средств защиты для отдельных пользователей, например, Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security и т.д.

**Dr.Web**<sup>1</sup> – семейство средств антивирусной защиты информации, разрабатываемое российской компанией ООО «Доктор Веб», включающее программные и программно-аппаратные решения, а также решение для обеспечения безопасности всех узлов корпоративной сети – **Dr.Web Enterprise Security Suite**. Dr.Web Enterprise Security Suite соответствует требованиям ФСТЭК к средствам антивирусной защиты типа А, Б, В, Г второго класса защиты (ИТ.САВЗ.А2.ПЗ, ИТ.САВЗ.Б2.ПЗ, ИТ.САВЗ.В2.ПЗ, ИТ.САВЗ.Г2.ПЗ).

Dr.Web Enterprise Security Suite представляет собой комплекс корпоративной централизованной защиты. В состав комплекса входит: центр управления, веб-консоль для

---

<sup>1</sup> [www.drweb.ru](http://www.drweb.ru)

контроля работы всех сервисов с любого компьютера, мобильный центр управления для контроля состояния безопасности сети с помощью мобильного устройства, антивирусный сервер, обеспечивающий централизованное управление защитой сети, антивирусные агенты, устанавливаемые на защищаемые компьютеры, серверы и мобильные устройства.

Также к средствам корпоративной защиты относится программно-аппаратное средство Dr.Web Office Shield, представляющее собой шлюз доступа в Интернет, позволяющий организовать централизованную антивирусную защиту рабочих станций и файловых серверов Windows, почтового и интернет-трафика.

В линейку Dr.Web также входит ряд средств защиты для отдельных пользователей (Dr.Web Security Space, Антивирус Dr.Web, Dr.Web Katana). Средства антивирусной защиты включают в себя технологии сигнатурной и проактивной защиты от вредоносных программ. Dr.Web Security Space помимо антивируса межсетевого экрана имеет в своем составе ряд других компонентов, в том числе «Криптограф Atlansys Bastion», обладающий технологией шифрования с применением известных алгоритмов (ГОСТ 28147-89, AES, Blowfish и т.д.) и гарантированного удаления устаревших данных.

**ESET NOD32<sup>1</sup>** – комплексное антивирусное решение, разрабатываемое международной компанией ESET. Имеет в составе линейки продуктов сертифицированный ФСТЭК России программный комплекс **ESET NOD32 Secure Enterprise Pack**, соответствующий требованиям к средствам антивирусной защиты типа А, Б, В, Г четвертого класса защиты (ИТ.САВЗ.А4.ПЗ, ИТ.САВЗ.Б4.ПЗ, ИТ.САВЗ.В4.ПЗ, ИТ.САВЗ.Г4.ПЗ).

Комплексное решение ESET NOD32 Secure Enterprise Pack включает в себя компоненты: ESET Endpoint Antivirus для защиты рабочих станций, ESET File Security для Microsoft Windows Server для защиты файловых серверов, ESET Mail Security для Microsoft Exchange Server для защиты почтовых серверов, ESET Remote Administrator, обеспечивающее централизованное управление.

Антивирусная защита обеспечивается методами проверки репутации приложений до их запуска на базе облачной технологии, оценки и контроле всех приложений и процессов с помощью поведенческого анализа и репутационной эвристики, контроле целостности прошивки и обнаружения попыток модификации, песочницы на основе технологий машинного обучения.

---

<sup>1</sup> [www.esetnod32.ru](http://www.esetnod32.ru)

***Symantec Endpoint Protection***<sup>1</sup> – комплексное средство защиты информации для серверов, переносных и настольных компьютеров, разработанное американской компанией Broadcom Inc., обеспечивающее помимо защиты от вредоносных программ (Symantec AntiVirus), также функции межсетевого экранирования, обнаружения и предотвращения вторжений. Соответствует требованиям ФСТЭК к системам антивирусной защиты типа А, Б, В, Г шестого класса защиты (ИТ.САВЗ.А6.ПЗ, ИТ.САВЗ.Б6.ПЗ, ИТ.САВЗ.В6.ПЗ, ИТ.САВЗ.Г6.ПЗ).

Symantec Endpoint Protection использует Insight, реализующую проверку сигнатур и проактивные методы защиты со снижением затрат ресурсов на сканирование, благодаря предварительной сортировке файлов. Обеспечивает централизованное управление безопасностью в физических и виртуальных конечных системах.

***McAfee***<sup>2</sup> – антивирусное программное обеспечение, изначально разработанное подразделением американской компании «Intel Security», включающее ряд решений для защиты разнообразных вредоносных программ для компьютеров и мобильных устройств. В составе линейки многочисленной программных продуктов McAfee имеются ранее сертифицированные ФСТЭК России программные продукты: ***McAfee Web Gateway***, соответствующий требованиям к средствам антивирусной защиты типа Б и Г шестого класса защиты (ИТ.САВЗ.Б6.ПЗ, ИТ.САВЗ.Г6.ПЗ), и ***McAfee Advanced Threat Defence***, соответствующий требованиям к средствам антивирусной защиты типа Б пятого класса защиты (ИТ.САВЗ.Б5.ПЗ).

McAfee Web Gateway представляет собой безопасный веб-шлюз, обеспечивающий защиту от интернет-угроз посредством локального анализа намерений и облачной защиты на основе технологий McAfee Labs. Предлагается в виде разных моделей аппаратных устройств и в виде виртуальной машины с поддержкой VMware и Microsoft Hyper-V.

McAfee Advanced Threat Defence совмещает в себе автоматические аналитические модули, такие как средства анализа антивирусных сигнатур, репутации и эмуляции в режиме реального времени с функциями динамического анализа посредством песочницы. Конечная проверка на наличие вредоносных признаков проводится с помощью методов машинного обучения на базе глубокой нейронной сети.

---

<sup>1</sup> [www.broadcom.com](http://www.broadcom.com)

<sup>2</sup> [www.mcafee.com](http://www.mcafee.com)

**Comodo**<sup>1</sup> – комплексное антивирусное программное обеспечение, разрабатываемое американской компанией «Comodo Group, Inc.», имеющее широкую продуктовую линейку как для домашнего, так и корпоративного использования.

Антивирус Comodo включает в себя антивирусный монитор и сканер, работающий по нескольким сценариям. В его функционал входят сигнатурные и проактивные интеллектуальные механизмы защиты – поведенческий анализ, песочница, облачные технологии, позволяющие проверять репутацию файлов. В комплексе Comodo Internet Security наряду с антивирусом для защиты от сетевых атак предлагается межсетевой экран. Для корпоративной защиты – Comodo Endpoint Security Manager, имеющий единую централизованную консоль для управления как локальными, так и удаленными конечными точками.

Другими примерами популярных антивирусных комплексов могут служить: *Avast, AVG AntiVirus, Avira, Norton AntiVirus, BitDefender, Microsoft Security Essentials, Panda, 360 Total Security* и пр.

---

<sup>1</sup> [www.comodo.com](http://www.comodo.com)

## ЗАКЛЮЧЕНИЕ

Защита информации представляет собой принятие правовых, организационных и программно-технических мер, обеспечивающих её сохранность от несанкционированного доступа, уничтожения, модифицирования, блокирования, копирования и других неправомерных действий.

Основой системы защиты компьютерной информации являются программные, аппаратные или программно-аппаратные средства, которые в большинстве случаев обеспечивают безопасность информации, доступ к которой ограничен на основании требований закона, например, составляющей государственную или коммерческую тайну, персональные данные и др. Правила их использования полностью или частично регламентируются на уровне государства. Статус охраняемой информации определяется законами (например, Федеральным законом «О персональных данных»), а правила выбора программно-аппаратных средств – нормативными актами и рекомендациями ФСТЭК Российской Федерации.

В настоящее время на рынке систем информационной безопасности представлен широкий спектр средств разграничения доступа, идентификации и аутентификации, криптографической и сетевой защиты информации. Разработчики СЗИ постоянно совершенствуют свои продукты, расширяя их номенклатуру и придавая им все больше функциональных возможностей.

Поскольку потенциальные угрозы безопасности информации весьма многообразны, цели защиты информации могут быть достигнуты только путем создания комплексной системы защиты информации, под которой понимается совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в автоматизированной информационной системе. При этом для обеспечения максимально достижимого уровня безопасности, необходимо осуществлять постоянный контроль функционирования механизма защиты.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Авезова Я.Э. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах / Я.Э. Авезова, А.А. Фадин // Вопросы кибербезопасности. – 2016. – №1(14). – С. 24-30.
2. Астайкин А.И. Методы и средства обеспечения программно-аппаратной защиты информации: научно-техническое издание / А.И. Астайкин, А.П. Мартынов, Д.Б. Николаев, В.Н. Фомченко. – Саратов: Российский федеральный ядерный центр – ВНИИЭФ, 2015. – 224 с.
3. Басалова Г.В. Основы криптографии. – М.: НОУ «Интуит», 2016. – 282 с.
4. Варлатая С.К. Программно-аппаратная защита информации: учеб. пособие / С.К. Варлатая, М.В. Шаханова. – Владивосток: Изд-во ДВГТУ, 2007. – 318 с.
5. Веретенников А. Классификация средств защиты информации от ФСТЭК и ФСБ России. – URL: [https://www.anti-malware.ru/analytics/Market\\_Analysis/infosecurity-systems-classification-fsb-fstek](https://www.anti-malware.ru/analytics/Market_Analysis/infosecurity-systems-classification-fsb-fstek) (дата обращения: 11.05.2020).
6. ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 683-ст).
7. ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. № 514-ст).
8. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст).
9. ГОСТ Р 57429-2017 «Судебная компьютерно-техническая экспертиза. Термины и определения» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2017 г. № 198-ст).
10. Громов Ю.Ю. Программно-аппаратные средства защиты информационных систем: учебное пособие / Ю.Ю. Громов, Иванова О.Г., К.В. Стародубов, А.А. Кадыков. – Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2017. – 193 с.
11. Духан Е.И. Программно-аппаратные средства защиты компьютерной информации.

- Практический курс: учебное пособие / Е.И. Духан, Н.И. Синадский, Д.А. Хорьков. – Екатеринбург: УрГУ, 2008. – 240 с.
12. Криптографическая защита информации: учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. – М.: РИОР : ИНФРА-М, 2018. – 321 с.
  13. Лапониная О.Р. Межсетевое экранирование: учебное пособие / О.Р. Лапониная. – Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. – 344 с.
  14. Масюк М.И. НСД: теория и практика : научное издание / М.И. Масюк // Спец. техн. – 2003. – №3. – С. 60-63.
  15. Нестеров С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров – СПб: Санкт-Петербургский политехнический университет Петра Великого, 2014. – 322 с.
  16. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования / В.В. Платонов. – М.: Издательский центр «Академия», 2013. – 336 с.
  17. Рекомендации по стандартизации Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации» (утверждены и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2017 г. № 2068-ст).
  18. Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» (утверждены и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст).
  19. Рекомендации по стандартизации Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» (утверждены и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст).
  20. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; под ред. В.Ф. Шаньгина. – М.: Радио и связь, 2001. – 376 с.
  21. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных

- систем и требования по защите информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
22. Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.
  23. Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114.
  24. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
  25. Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.
  26. Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации. Классификация автоматизированной системы. – URL: <https://www.intuit.ru/studies/courses/3648/890/lecture/32381> (дата обращения: 29.05.2020).
  27. Федеральная служба по техническому и экспортному контролю. Информационное сообщение «Об утверждении Требований к средствам доверенной загрузки» от 6 февраля 2014 г. № 240/24/405.
  28. Что такое троянская программа? – URL: <https://www.kaspersky.ru/resource-center/threats/trojans> (дата обращения: 15.05.2020).
  29. Что такое компьютерный вирус и компьютерный червь? – URL: <https://www.kaspersky.ru/resource-center/threats/viruses-worms> (дата обращения: 15.05.2020).

30. Шабанов И. Обзор сертифицированных средств защиты информации от несанкционированного доступа (СЗИ от НСД). – URL: [https://www.anti-malware.ru/analytics/Market\\_Analysis/certified-unauthorized-access-security](https://www.anti-malware.ru/analytics/Market_Analysis/certified-unauthorized-access-security) (дата обращения: 02.06.2020)
31. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.
32. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК Пресс, 2010. – 544 с.
33. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2010. – 592 с.
34. Шевченко А. Технологии обнаружения вредоносного кода. Эволюция. – URL: <https://securelist.ru/tehnologii-obnaruzheniya-vredonosnogo/1073/> (дата обращения: 26.05.2020).